A Multi-faceted Model to Support Authentication and Authorization for Online Services

by

Luzuko Tekeni

A Multi-faceted Model to Support Authentication and Authorization for Online Services

by

Luzuko Tekeni

Dissertation

submitted in fulfillment
of the requirements
for the

Masters Degree

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Reinhardt A Botha

Co-Supervisor: Prof. Kerry-Lynn Thomson

April 2017

Declaration

I, Luzuko Tekeni, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognized.
- This dissertation has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognized educational institute.

Luzuko Tekeni

Abstract

As the number of users accessing the Internet is growing, many organizations today offer online services to their customers. The Internet makes these services searchable, readily available and easily accessible. However, these organizations face challenges to restrict access to only authenticated and authorized users. Ensuring adequate access control in an IT ecosystem requires cooperation and on-going communication among stakeholders.

This research study postulates that access control requires a holistic view, as opposed to the traditional technical perspective. Thus, this research study develops a model to support authentication and authorization for online services in a holistic manner.

A literature study illuminates the problem space, while argumentation is used to construct a multi-faceted model that supports authentication and authorization for online services. The three facets of the model correspond to the three layers commonly found when discussing management in organizations: strategic, tactical and operational. Guidance from existing policies and standards comprises the strategic level. The tactical level covers planning for influencing the behaviour of users through awareness, provisioning, and support. The operational layer deals with technology considerations.

The utility of the proposed multi-faceted model is demonstrated through a use case: the eduroam facility currently offered by SANReN (South African National Research Network).

Acknowledgements

A dissertation is the results of the collaborative efforts of different individuals. Support, motivation and encouragement originate from different individuals in various ways. My dissertation has been influenced and supported by many individuals within and outside of where it was written. Without this kind of support, motivation and encouragement, the completion of it would have not been possible. Hence I take this wonderful opportunity to express my sincerest gratitude to:

The Lord, for providing me with the opportunity, strength, courage and perseverance to achieve more than I ever imagined.

My **Supervisor**, **Prof. Reinhardt A. Botha** and my **Co-Supervisor**, **Prof. Kerry-Lynn Thomson**, for acting the roles of a father and a mother more than supervisors. Their caring attitudes, patience, guidance, motivation, and support during the course of this study was very important to me.

Prof Rossouw Von Solms, for encouraging me to do my masters degree, without his encouragement I would have not taken this journey.

My **Family**, for their love and patience.

Nelson Mandela Metropolitan University and SANReN, for their financial support that made this study possible and some other individuals who contributed financially.

My **friends and colleagues**, doing research can be a lonely journey sometimes but their presence and the atmosphere they provided made it an enjoyable ride.

Many thanks to you all!

Contents

List of Tables

List of Figures

Part I

Background

Chapter 1

Introduction

It has become commonplace for organizations to run their businesses online. This is influenced by many factors. Among these factors are the rapid speed at which networks are growing and the number of Internet users accessing the Internet daily. Of course, making services available online provides many benefits to Internet users and customers such as convenience, security, ease of use, speed, and flexibility.

User registration is a simple, quick process and needs to be performed only once whenever the user want. This also allows the users to enroll in multiple services at any time. Online services are designed to be secure to protect the users' personal information when doing transactions. A user has the option of using a single login to access all of his or her online services. This removes the difficulties of remembering multiple usernames and passwords. Further, users want to have quick access to the needed services. Using the Internet to access online services removes the need to physically go to the sellers' premises and que in long lines. This also allows the sellers to respond quickly. Users are able to make purchases and orders even after hours as the systems take care of the process. Most online services will be available at any time.

These benefits complement the ever growing desire of users for services to be searchable, readily available and easily accessible on the Internet. However, achieving this could be challenging to organizations, because, at times, some of these services are sourced from other stakeholders. Moreover, these stakeholders protect their online service content by licensing it. Therefore, organizations need to provide administrative control to ensure that only authorized users can access such online services. Furthermore, they also have to limit users' permissions to licensed service content while accessing the Internet. However, ensuring adequate access control in the IT ecosystem, where stakeholders need to trust each other, require cooperation between multiple organizations.

To provide consistency in this dissertation the phrase "IT ecosystem" will be used to refer to multiple organizations that are interconnected to share a common goal of making services available online for their users and customers. For example, a library in the context of a university provides online databases to their users (service provider 1). However, the online databases are sourced from different publishers or vendors (service provider 2). Therefore, this dissertation argues that access control should encompass the whole IT ecosystem i.e. to extend across organizations in the quest of protecting online services.

1.1 Motivation for this Study

The research study was motivated by the following realizations.

The realization that access control spans across the organizational boundaries

With the growth of the Internet, online services are being provided across multiple organizations. However, these online services require cooperation and inter-networking between multiple organizations, systems and entities (Bhoj, Singhal, & Chutani, 2001). Therefore, managing access to online services is essential.

In a world of IT ecosystems, where organizational systems are linked to other systems outside their boundaries, it could be challenging to implement adequate access control. Furthermore, foreign stakeholders associated with these outside systems need to come on board and play a role towards ensuring adequate and effective access control.

For example, from a library perspective, libraries form alliances with hundreds and thousands of publishers or vendors. These alliances are formed with the goal of making academic content available and easily accessible to users online. Initially, when this alliance is formed, the online content is licensed. Therefore, libraries are required to obey any access restrictions specified by the publisher or vendor of this online service.

The realization that there could be inconsistencies between legal specifications and technical access control measures

Authorizing access to online services requires legal specifications. These legal specifications are widely known as policies. Policies are sets of rules that govern how access to online services is provided and controlled. When implementing access control policies inconsistencies could exist, especially when new online services, that come with their own legal specifications, are provided. As noted by Bauer, Cranor, Reeder, Reiter, and Vaniea (2009), this is due to the fact that the people who make policies are different from the people who implement those policies. Therefore, coming up with a mutual understanding of a policy between different stakeholders could be challenging (Jaferian, Rashtian, & Beznosov, 2014).

Think of a library policy that says "*Users may not be given means to access licensed online services when they are not within the library premises.*" This becomes a problem when a user accesses the licensed online services using wireless networks because wireless coverage could extend outside the library premises. Some libraries use IP addresses as their line of defence to protect licensed online services. In this situation there is a mismatch between the legal specification and technical access control measures concerning how the network operates.

This was the case when the author visited CSIR (Council for Scientific and Industrial Research). The author could access their library online database content (the ACM Digital Library which was unavailable at home) because the library online database authorizes a user by means of IP address. This means that anyone whose device is associated with their IP address will have full access to the ACM online database content. This primarily motivated the research study.

The realization that users just want to do their job without worrying about who should have access to online services

Organizations cannot rely on users to do the right thing and follow the implemented legal specifications. Users are more concerned with doing their work regardless of whether access is provided legally or illegally. Although legal specifications often specify who can do what on which object, it is just not enough. Unfortunately users cannot be fully trusted to act accordingly when accessing online services, although it is a requirement for them.

Organizations need to look further than trusting their users and explore some available techniques that can change or influence their behaviors. Such techniques could include education, awareness and training if needed.

1.2 Problem Statement

Access control is seen from a technical perspective. However, knowledge on its holistic perspective is limited. A model that would support both authentication and authorization for online services is yet to be proposed. Therefore the problem statement for this research study is stated as follows: **Currently, a model to support authentication and authorization for online services is lacking.**

1.3 Research Objectives

This section defines the primary objective of this research study together with the secondary objectives.

The primary objective of this research study is to **develop a multi-faceted model to support authentication and authorization for online services.**

In order to achieve the primary objective, three secondary objectives are stated:

1. To investigate the governance of IT ecosystems through access control policies.

2. To investigate and identify available ways of influencing users' behaviors towards access control in IT ecosystems.

3. To investigate and identify possible technology solutions within the environment of IT ecosystems.

In order to achieve these research objectives it is necessary to follow a systematic structured research methodology. Such research methodology is discussed in the following section.

1.4 Research Methodology

Good scientific research requires a systematic structured research approach. In the case of this research study, a mixed methods approach is used.

The first part of the research study provides an understanding of the problem space. This is achieved by using a literature study in response to the stated research objectives. Literature regarding access control and various technologies currently in use for controlling and preventing unauthorized access in IT ecosystems is studied in chapter 2, which is in line with sub-objective three. Furthermore, the literature study continues to investigate the management of IT ecosystems in chapter 3. This addresses sub-objective one.

In the second part of the research study, the problem space is conceptually divided into three layers using existing theories found in the results of the literature study, together with argumentation to build the model components. This is in line with sub-objective two.

Thereafter, a model entitled "A multi-faceted model to support authentication and authorization for online services" is proposed and developed. This addresses the primary objective of the research study. The model is based on the existing literature study.

Finally, the effectiveness and utility of the proposed model is shown by making use of a use case method at an eduroam facility.

Additionally four papers were written during the course of the research study and the results of these papers were published. One of these papers was published in an accredited journal, two of them were presented at conferences

(Nationally and Internationally) and published in the conference proceedings, and the last was presented as a poster at a conference (Locally).

1.5 Research Methods

A brief overview of the used mixed methods and how each of them is utilized in the entire research study is given in the following section.

1.5.1 Literature Study

In scientific research it is important to have a well-founded literature study. A literature study provides the foundation of the research. According to Gregor and Hevner (2013), a literature study should include knowledge that is relevant to the initial problem. This knowledge could come from existing artefacts (models, frameworks and theories). For example, if the problem area involves access control, existing access control theories, models, and frameworks should be reviewed and studied.

Therefore, this research study uses a literature study in the following ways:

1. Literature is accessed regarding access control in IT ecosystems. The aim is to identify and support the existence of the problem, specifically the lack of holistic support for access control in IT ecosystems.

2. Literature is accessed to investigate how IT ecosystems are managed and controlled. Further, the components that make up the solution in the form of a model are discussed through the literature study.

The results of the literature study are used to build the model components through argumentation which is discussed in the following subsection.

1.5.2 Argumentation

Argumentation is a core principle in developing a research solution. Several authors have identified different approaches of reasoning (Spens & Kovács, 2006; Hyde, 2000). There are two general approaches of reasoning used across different research disciplines to acquire new knowledge (Hyde, 2000), the inductive research approach and the deductive research approach. The inductive research approach seeks to develop a theory by firstly observing a specific instance and then"establishing generalizations about the phenomenon under investigation" (Spens & Kovács, 2006). The deductive research approach begins with establishing a theory, and seeks to observe if the theory fits to a specific instance (Hyde, 2000).

In the context of this research study an inductive research approach is employed. It uses a theory building to argue towards the development of the proposed multi-faceted model to holistically support access control through an IT ecosystem.

Argumentation together with a use case method which is discussed in the following subsection shows the effectiveness and utility of the proposed model.

1.5.3 A Use Case

Use cases can be considered a formal method within systems, analysis, and design. To provide an in-depth understanding of the problem area, pointing out the causes and stating the current status in the area in real-world context, a use case is utilized. This dissertation argues that the eduroam facility architecturally represents a complete IT ecosystem and is a suitable environment that collaborate with multiple providers. Therefore, the research study uses the eduroam facility as a use case scenario.

1.6 Research Scope and Delineation

This research study focuses on developing a multi-faceted model to support authentication and authorization for online services. A use case method is utilized to provide an in-depth understanding of the problem, pointing out the causes and stating the current status in the environment.

The use of the Internet Protocol (IP) address to authorize roaming users to use online services at home or in remote institutions (this is discussed in more detail in chapter 8) by eduroam, is of particular interest. There are many online services that authenticate and authorize users via an IP address on the Internet and it is impossible to analyze all of them. Therefore, when performing a use case in chapter 8, the attention will be focused primarily on online digital library databases found in eduroam-enabled institutions and libraries within the South African context.

1.7 Chapter Layout Of the Dissertation

This dissertation consists of three parts, each of which consists of a number of chapters. Four appendices are also attached to this dissertation. Figure 1.1 provides a graphical depiction of the dissertation layout. The contents of these three parts and subsequent chapters are briefly summarized below.

Part I introduces the problem domain. It does so by considering the three realizations that motivated this research study. This sets the scene for the problem statement, research objectives and subsequently the research methodology used in this dissertation. Further, the research scope and delineation is also discussed in chapter 1. **Chapter 2** introduces the reader to access control. The general concepts of access control, in particular a subject requesting access to an object through a decision maker, are discussed. **Chapter 3** discusses the management of IT ecosystem environments.

Part II is dedicated to introducing the proposed model to the reader by positioning it in **Chapter 4**. Thereafter, **Chapter 5, 6 and 7** will discuss each part of the proposed model in detail.

Part III is dedicated to showing the utility of the proposed model by using eduroam as a use case in **Chapter 8**. This simply means that the proposed model in **Part II** will now be utilized by the eduroam facility. Finally, **Chapter 9** concludes the dissertation by reflecting on the research, determining whether the objectives have been achieved and suggesting future directions.

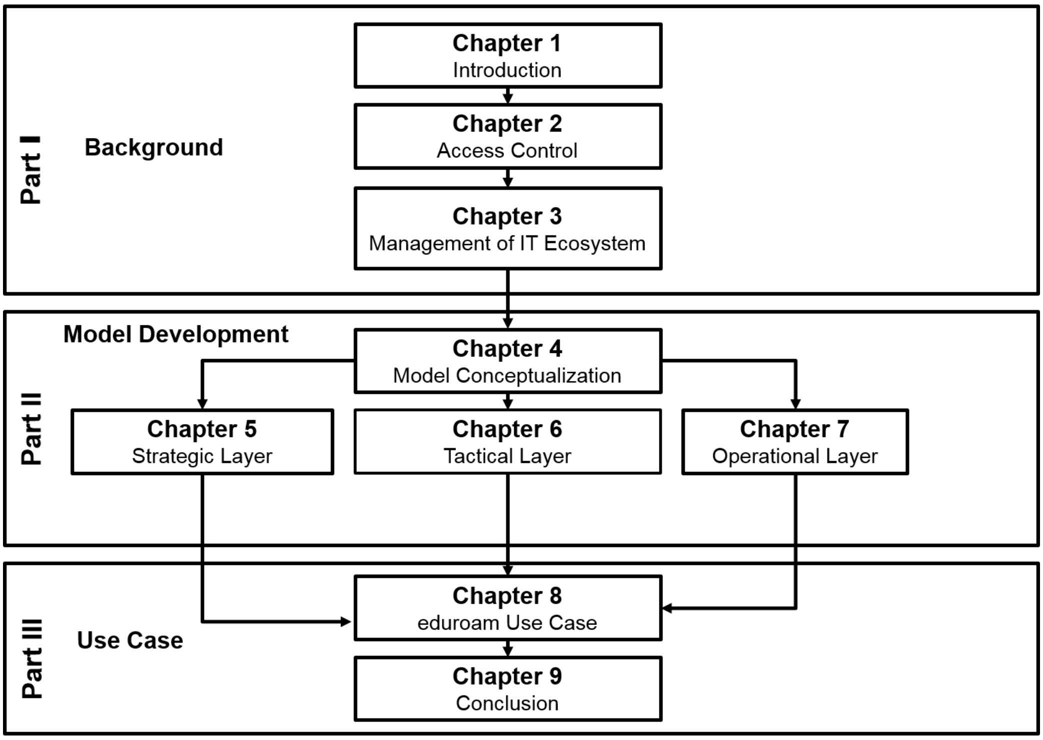


Figure 1.1: Lay-out of the Dissertation

1.8 Conclusion

This first chapter discussed the three realizations that motivated this research study. Furthermore, the focus area of the research study together with the problem statement was defined. Consequently, this research study sets to develop a multi-faceted model to support authentication and authorization for online services. Therefore, the research objectives defined in order to achieve the primary objective were stated. Thereafter, the research methods used to achieve the stated objectives were also discussed. Finally, the research scope and delineation together with the layout of this dissertation were discussed and illustrated.

Chapter 2

Access Control

Information resources are just as important as any other valuable organizational asset (ISO/IEC27002, 2013). Therefore, these information resources must be protected at all times (Saint-Germain, 2005). Information security implementers must ensure that their approaches or methods are effective and adequate to the extent specified by the policies of the organization. Access control is one of the oldest aspects associated with the protection of an organization's information resources (Tekeni, Botha, & Thomson, 2016). Access control can be either physical or logical in nature. However, a combination of physical and logical protection can be utilized. Depending on the nature of the asset that must be protected.

Access control in this dissertation is defined as a set of controls defined to restrict or limit access to organizational resources. In other words, who can have access to which resource? Security guards that control access to the organization's buildings, employee access cards, biometric scanners and tokens are all examples that view access control from both a physical and logical protection perspective. However, this dissertation addresses access control to information resources in IT ecosystems. Access control must be enforced across federated IT ecosystems.

Chapter 1 introduced the three realization that motivated this dissertation to set the scene for the problem statement and research objectives of the dissertation. This chapter presents an access control overview in a federated IT ecosystem environment. The primary question answered in this chapter is: Who can access what on which object(s)? This sets the scene for the next chapter which answers the question of how IT ecosystems are managed?. The current chapter begins by conceptually positioning access control in terms of the focus of this dissertation.

2.1 Access Control Conceptualization

Access control should ensure that access is only given to authorized users. Its main purpose is to manage the provision of user access rights to ensure that resources can be appropriately shared between properly authenticated users (Tekeni et al., 2016). It includes a *Reference Monitor* who permits or denies a *Subject* to do an *Operation* on a particular *Object* according to *Access Rules* predefined (Hulsebosch et al., 2005). The subject is the access requester, i.e. it identifies a specific user who wants to do an operation on an object. An operation is responsible for collection and delivery of user credentials from the subject to the reference monitor in order to make an informed decision. According to Hulsebosch et al. (2005), the access rules specify the usage of access rights associated with the subject for the purpose of verifying that the subject has the authority to perform a task on an object.

The reference monitor is the "brain" of the access control process. Its role is extremely important as it is responsible for subject authentication by means of biometrics or tokens. Furthermore, it is also responsible for authorization, i.e. determining the degree of access rights of the subject to do a particular task on an object. Finally, it permits or denies the subject to have access to an object. Access is denied if the subject is neither authenticated nor authorized. Subsequently, access is permitted if the subject is properly authenticated and authorised. Figure 2.1 illustrates this process in a graphical manner.

In Figure 2.1, the *Subject* requests access from the *Reference Monitor* to do a specific *Operation* on a particular *Object*. In order to make an informed decision, the *Reference Monitor* needs to know the source of the request to determine the identity of the user ("Who is accessing?"). This is called **authentication**. Furthermore, the *Reference Monitor* must also verify the access rules associated with the resource required by the *Subject* ("What can be accessed?"). This is called **authorization** (Lampson, Abadi, Burrows, & Wobber, 1992). Therefore, once the *Reference Monitor* obtains the results, the decision is made to either 'Permit' or 'Deny' access to the *Subject* and

Contol Process.png

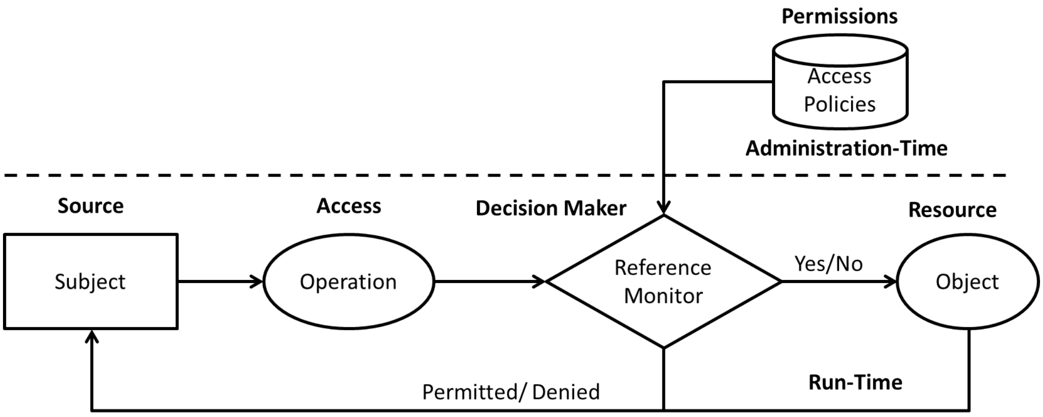


Figure 2.1: Access Control Process, based on Hulsebosch et al. (2005)

the *Subject* is notified of the outcome.

However this happens when the subject attempts to access a particular object: thus it is a *run-time* decision. Furthermore, this decision is based on a set of access rules which must be created first. Therefore, there is also the *administration-time* activity of setting up those access rules to consider. Considering administration of access control separately from the operational access control to ensure that the policies and objectives are not compromised, is not a new idea (Sandhu, Bhamidipati, & Munawer, 1999; Botha, 2008). Access control must be considered from both *administration-time* and *run-time* perspectives. These access control perspectives are discussed next in 2.2 and 2.3.

2.2 Access Control Administration Mindsets

During the *run-time* of access control, decisions to allow or deny access to a particular information resource are enforced. These decisions are based on a set of access rules specifying “what can be accessed and by whom?”. However, these access rules must be created first. Therefore, the author refers to the *administration-time* used to set up those access rules.

Access control rules are created as either **discretionary** (Wang & Osborn, 2007), or **mandatory** (Fen, Zhen, Liu, et al., 2009). Furthermore, it has become commonplace to create access rules and map those created access rules into roles. This is called **role-based** access control (Bao, Song, Wang, Shen, & Yu, 2008). Each of these mindsets when creating access rules are discussed in the following subsections.

2.2.1 Discretionary Administration

Discretionary Access Control (DAC) has been discussed by many (Wang & Osborn, 2007; Osborn, Sandhu, & Munawer, 2000) and is widely used in many systems and networks. The idea behind discretionary access control is that the user creates a resource and controls access to the created resource through ownership. The resource owner can then pass the access rights associated with the created resource to other users based on his/her discretion. Access Control Lists (ACLs) are good examples of DAC. For example, in networks the administrator (who acts as the owner) can create an ACL that allows or denies access to a server from a group of users.

This kind of ownership may not be appropriate in many organizations as the organization is the owner of the server but, at the same time, the server could have been configured by a specific user. It then becomes confusing to answer the question of "Who the owner is?". However, an organization could give access to a specific user to permit access to other users according to his/her discretion.

2.2.2 Mandatory Administration

Mandatory Access Control (MAC) disallows the users privileges of deciding who can access their resources. The system is a decision maker. MAC is a way of restricting access to resources based on security labels assigned to users and resources (Fen et al., 2009). A label on a user is called a security classification, whereas a label on a resource is commonly referred to as a security clearance (Yuan & Tong, 2005).

MAC divides access rights to resources unequally. However, the fact that access rights are unequal poses a challenge on its own. For example, a user with security classification of X and a resource with a security clearance of Y can access the resources with security clearance Y and below even if he/she has no intentions of doing so.

It must be noted that both discretionary and mandatory access control are based on the resource, i.e. not on the user's job requirements. Role-based access control (RBAC) addresses access rights from the user's perspective rather than from the resource's perspective. This is discussed in the next subsection.

2.2.3 Role-Based Administration

Role-based access control is popular across organizations today. Most organization are implementing the concepts of roles (Bao et al., 2008). Instead of giving individuals access rights, rather map them to specific roles according to their jobs. Roles, in turn, are assigned specific access rights based on the job requirements of that role. This simplifies administration of access rights. Consider a situation where a single user holds multiple access rights for different tasks. These multiple access rights could conflict with one another. For example, a user needs to log the total number of hours worked per day for the purpose of calculating the salary earned (Task 1). However, Task 2 requires the same user to approve the number of hours logged. This could be seen as a potential conflict or conflict of interest. Hence, such conflict can be avoided by carefully creating roles.

Furthermore, as the number of users and the information resources increases in an organization, it becomes challenging to administer the user's access rights on an individual level. RBAC first map roles to access rights and users to their roles as can bee seen in Figure 2.2 (Zhou, Varadharajan, & Hitchens, 2012).

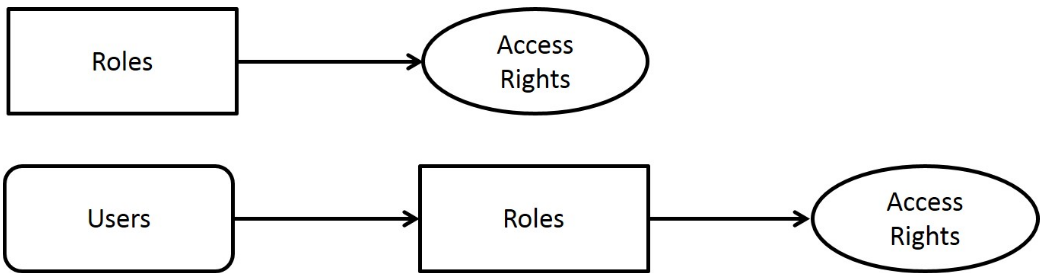


Figure 2.2: Role-Based Access Control Mappings

Moreover, if a user gets a promotion within an organization, the roles can be easily reassigned from one user to another user. Furthermore, during user resignation, roles can be easily revoked as necessary. Roles make the provision of access rights much simpler than providing each user access rights that are not mapped to a particular role. However, this does not mean the user cannot hold two or more roles. If it is the case, proper care should be taken when assigning users to their roles.

2.3 Access Control Enforcement

At *run-time* access control rules that were created during the *administration-time* are enforced. To access a particular service the decision maker (as discussed in figure 2.1) needs the user to be authenticated using any of the authentication methods specified by the organization.

The decision to enforce access control conceptually allows or disallows access based on the question: "Should the subject have access to this object?". However, this question relies on the subject being who he or she claims to be. This requires a trustworthy authentication mechanism. Three of the most common authentication mechanisms used in organizations are shared secret passwords, biometrics and tokens.

Each of these authentication mechanisms are discussed in the following subsections.

2.3.1 Shared Secret Passwords

This is the easiest method of authenticating and authorizing users, whether they are inside the organization's boundaries or outside. A login username to identify the user and the password for approving the user need to be provided to the user by the organization. This method works in the following way: 1) The *Organization* requests a subscription from the *Resource Owner* 2) The *Organization* together with the *Resource Owner* creates login details (a username and a password) 3) These login details are distributed to authorized *Users* by the *Organization* 4) Thereafter, the *User* can login to any computer or device that has Internet access and access the electronic resource content offered by the *Resource Owner* via their affiliated *Organization* 5) Finally, the *Resource Owner* decides whether to permit or deny access and the response is sent to the *User* (see Figure 2.3).

There is flexibility with shared secret passwords as the user can use it anywhere regardless of the Internet Service Provider the user connects to.

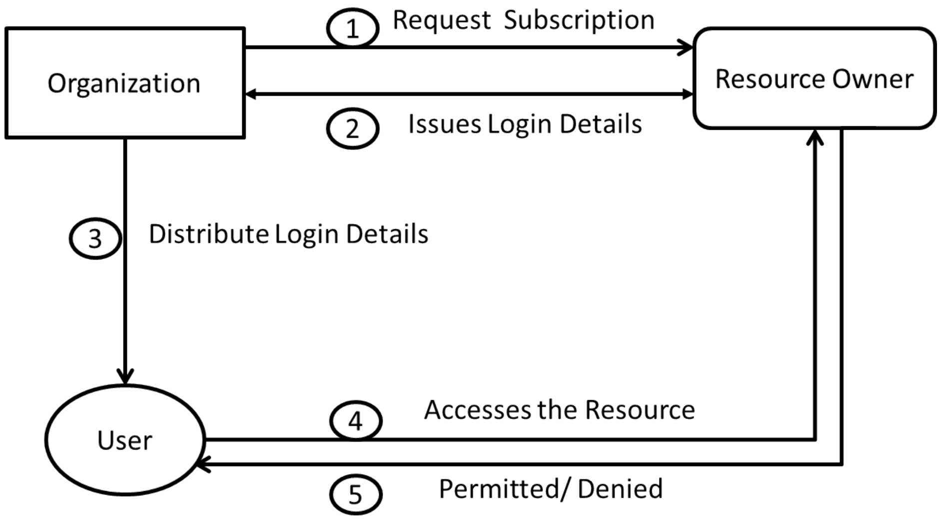


Figure 2.3: Secret Password Login Process

However, some disadvantages can be noted with this method. Firstly, the password created by the organization and the resource owner could already exist elsewhere. If this is the case, the possibility of electronic resource content misuse could occur. Secondly, organizations subscribe to many resource owners and each of them is different. That means that a long list of passwords needs to be maintained and updated often. Lastly, some users could share the password to unauthorized users. This could breach the SLA agreed on by the organization and the resource owner.

2.3.2 Biometrics

Shared secrets passwords require the users to always remember a username and a password. This could prove to be a nuisance to users as the passwords can be easily forgotten. Moreover, if an unauthorized user could get hold of the shared secret password, the protected resource could be accessed.

One way to avoid entering credentials such as usernames and passwords is to utilize a user-based behavior's characteristics as an authentication method. Biometrics allow users to be authenticated through measurable behavior's characteristics that can be automatically checked (Bolle et al., 2004). This includes scanning fingers or eyes on a biometric system.

A biometric system captures the user's characteristics and creates a profile for the user. When the user has been authenticated, the supplied characteristics are compared against the created profile and the user is either authenticated or denied access.

2.4 Access Control Techniques: Status Quo

Access control in federated IT ecosystems has been a problem for many decades. Organizations have been coping with imperfect solutions to address access control for their organization's valuable assets in federated ecosystems. Most of these solutions lack scalability, privacy and federation of administration. With federated administration, the resource owner only performs authorization after the user has been successfully authenticated by their own home organization using their own preferred method of authentication. This not only protects the user's privacy but also provides scalability as the authentication of the user remains at the user's home organization, while authorization to access a particular resource is carried out by the resource owner.

Firstly, before this section provides a summary of the existing approaches used to restrict access to resources, it is worth highlighting that these approaches may commonly fall under one or a combination of the three forms of access control discussed in subsections 2.2.1, 2.2.2 and 2.2.3: discretionary, mandatory or role-based access control.

2.4.1 IP Address Restriction

IP addresses are widely adopted by organizations as their preferred authorization method, especially in academic and research institutions (Blansit, 2007). Furthermore, IP addresses are commonly used in large organizations, because the setup is relatively straightforward for a large number of users. The organization releases a block of IP addresses to their associated resource providers to be registered, making it easy to allow thousands of authorized users to have access to the electronic resources hosted by their organization (Mikesell, 2004). This, however, increases administrative workload of organizational administrators. An organization needs to register IP addresses with each resource provider (Blansit, 2007). At times, when the organization changes the block of IP addresses, an update is required and must be communicated to the resource provider. This becomes a burden to organization's administrators. The IP based method operates this way (see Figure 2.4).

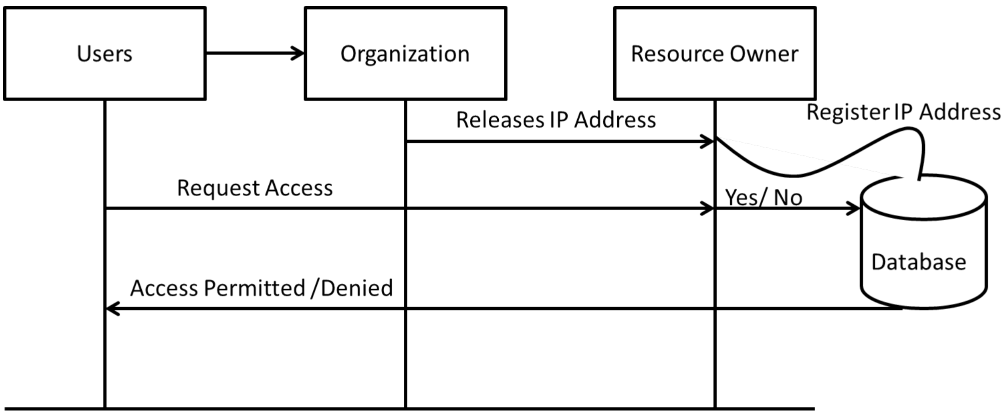


Figure 2.4: IP-based Process

Each organization is assigned a pool or pools of IP address by their Service Provider (an assigned IP address uniquely identifies a device to other devices locally or to the Internet at large (Mikesell, 2004)). The organization then releases the assigned pool of IP addresses to its resource providers. The resource providers' accept the released pool of IP addresses from the organization, add them to their lists of allowed addresses on the server and add a tag that specifies where the IP addresses come from. Thereafter, when the user uses a computer or any type of device that can access the Internet on the organization's premises, the resource provider's server looks at the arriving IP address and compares it to the list of registered IP addresses. Finally, if a match is found, the user is given access to the protected electronic resources. If not, no access is given.

IP addresses undoubtedly provide a convenient way of authorizing users to access electronic resources. However, the disadvantages cannot be overlooked, especially when access is required by users working at home.

2.4.2 Web Proxy Servers

A Web proxy server is a computer located within the organization's premises that authorized users can connect to over the Internet. Web proxy servers are necessary for users who want access to their organization's internal resources while they are at home. Web proxy servers are normally placed outside the firewall of the organization. Their main job is to play the role of intermediary device between the home user and the organization holding the resource (Mikesell, 2004). This server simply transmits data. For example, *User_W* affiliated with *Organization_X* wants access to *Database_Y*, which is outsourced by *Organization_X*. In order to access *Database_Y*, *Organization_X* uses an IP address. This IP address is only assigned to users while on-campus. Then *User_W* request access to *Database_Y* while working at home. However, this is not possible because the IP address of *User_W* while working at home is different from the IP address usually assigned to *User_W* while working on-campus (see Figure 2.5).

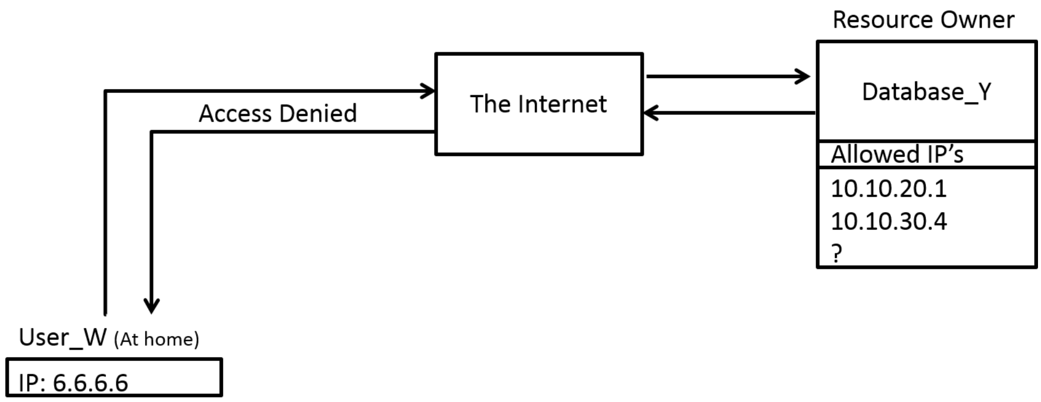


Figure 2.5: User Accesses at Home without a Proxy Server

In order for *User_W* to access *Database_Y*, *Organization_X* will have to place a web proxy server outside their firewall. This server will have the ability to communicate with another inside server that has the valid IP address of *Organization_X*. When the user accesses *Database_Y*, the request will have a valid IP address of *Organization_X* because of the communication between the Web proxy server and the user working at home (see Figure 2.6).

The web proxy server process is shown in Figure 2.7. The remote user tries to access licensed material using a proxy-enabled browser. The request is directed to a proxy server located on campus. When the proxy server receives the request and forwards it to the organization, the organization validates that the IP address came from the proxy and authenticates the request. Thereafter, an inside system returns the data to the proxy server which, in turn, sends the retrieved data back to the remote user.

Although web proxy servers work well to provide access regardless of the Internet Service Provider (ISP) the user is connected to, noticeable disadvan-

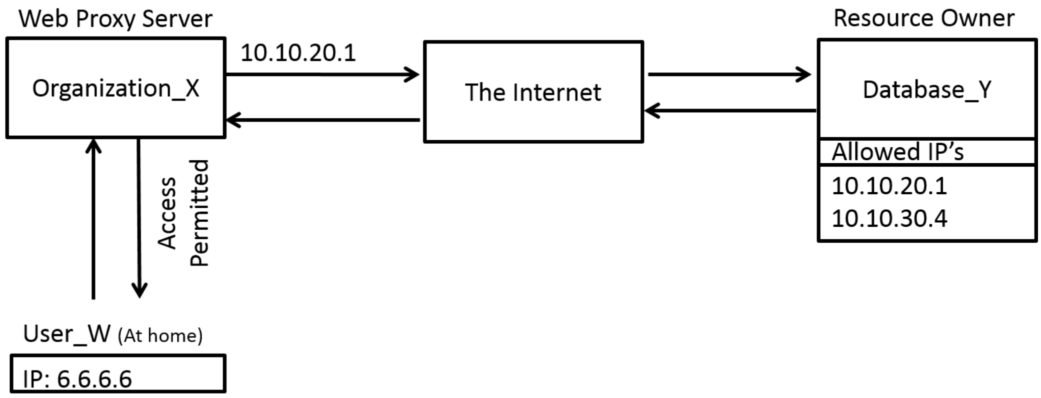


Figure 2.6: User Accesses at Home with a Proxy Server

tages cannot be overlooked. With the wide spread of the Internet, free open proxy softwares could be used by hackers in the process of gaining access to protected resources of an organization. According to Cain (2003), this was the case at JSTOR when their articles got downloaded by a hacker. A valid authorized IP address "succeeded in downloading 50,000 journal articles" from their database. This was because a computer was configured as a valid Web proxy server located from a valid organization. A more secure approach to access control in distributed IT ecosystem could be the use of a Virtual Private Network. The next section will discuss what the VPN concept entails.

2.4.3 VPN

A VPN provides complete data privacy and integrity to users who access the network from outside their intranet in a secure manner (Rangarajan, Takkallapalli, Mukherjee, Paul, & Miller, 2004). A VPN creates a tunnel between the user sitting outside the organization's premises and their affiliated organization. This technique provides flexibility in communication and complements the experience of a roaming user. The same resource the user accesses at the home organization will be readily available wherever he or she roams provided that the VPN tunnel is established. A VPN tunnel is triggered by the user who wants access to his or her affiliated organization's resources while roaming to remote networks. A VPN makes use of the Internet to transmit data from point A to point B (Mikesell, 2004). As this data

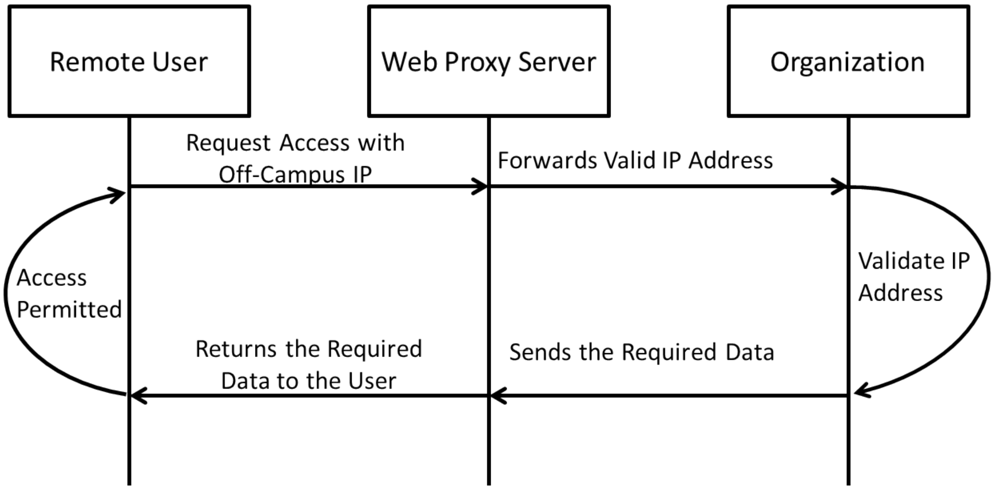


Figure 2.7: Web Proxy Server Process

traverses over the Internet it should be encrypted and a VPN addresses such requirements. A VPN is similar to a Web proxy server because the roaming user is assigned an IP address associated with the user's affiliated organization. Then the users can access any resource available on-campus while roaming to remote networks. However, the security of a VPN is what separates it from Web proxy servers. An example of a VPN tunnel is abstracted in Figure 2.8.

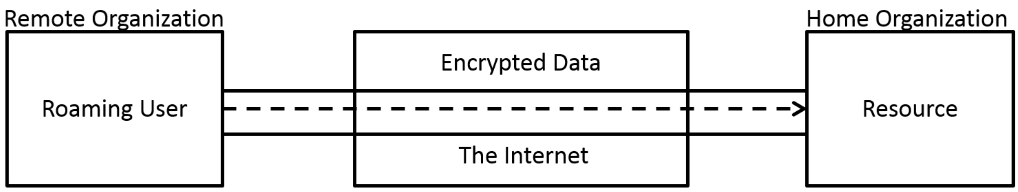


Figure 2.8: A VPN Tunnel between the User and the Home Organization

In Figure 2.8, the user wants access to a particular resource hosted by the home organization while at a remote location. The user is authenticated as a VPN client on his or her personal device. If the user is properly authenticated, the VPN tunnel is established and the data that traverses through this tunnel is encrypted by the tunnel. The IP address assigned to the user belongs to the home organization which allows the user to have direct access to the resource hosted by the home organization.

VPNs provide flexibility to users accessing resources outside the organization's boundaries. However, they require installation of software on the user's personal device, a heavier workload for the home organization's IT support personnel and data encryption that can slow down the speed of the network connection (Cain, 2003).

2.4.4 Shibboleth

Shibboleth is an initiative based on an open source software package developed by Internet2/MACE. It emphasizes user privacy protection (Erdos & Cantor, 2002) and has the ability to request user attributes between federations using SAML. Internet2 involves federated identity management organizations and research and higher education communities, with the goal of ensuring that members belonging to such communities and organizations "have access to the right services, at the right time, with the right protections and privacy considerations, while supporting easy collaboration globally" (Internet2, n.d.).

Shibboleth is a system for authentication (carried out at the user's home organization) and authorization (performed by the resource owner) to support collaboration and sharing of resources that are subject to access control in research and higher education institutions (Needleman, 2004; Erdos & Cantor, 2002). Shibboleth provides scalability and flexibility because the actual identification that the user is who he/she claims to be happens at the user's home institution, while all the rights associated to the user are verified at the resource owner's site. Of course, the trust relationship is essential between the resource owner and the user's home institution to ensure that the user really belong to that institution, has been properly authenticated and has the authority to access the resource.

Shibboleth is built on a number of software components. Apart from the end-users and their web browser, Shibboleth relies on three main players during the exchange of information between federated institutions, namely (Paschoud, 2004) the resource provider (ReP), the identity provider (IdP), and the where-are-you-from service (WAYF).

The ReP is the owner of the resource that the user wants to access. Authorization decisions are made by the ReP about whether access to the resource is granted or denied. The access decisions are based upon the reply form the end-user's IdP. To establish communication between the ReP and IdP, the ReP operates two Shibboleth software components, the SHIRE (SHibboleth Indexical Reference Establisher), and the SHAR (SHibboleth Attribute Requester).

The IdP is the end-user's home institution which has a trust relationship with the ReP for resource access. IdP authenticates its own users using their preferred authentication method. Furthermore, the IdP maintains the local database of registered users. The IdP operates two Shibboleth software components, the HS (Handle Server), and the AA (Attribute Authority).

The WAYF is a service that is placed between the ReP and IdP to discover the user's home institution. The WAYF service contains a list of all the Shibboleth participating institutions. The user is presented with a web form to choose his/her home institution from a list of participating institutions provided that his/her home institution is also part of the Shibboleth federation. Therefore, the main task of the WAYF service is to discover the user's home institution so that the assertions between the ReP and IdP can take place.

Figure 2.9 illustrate the operation of Shibboleth.

When the user tries to access the required resource, the following steps take place:

1. The user tries to access a Shibboleth protected resource hosted by a ReP.

2. The ReP at the destination will redirect the user into a WAYF service by using SHIRE.

3. The user is provided with a web form to choose his/her home institution by the WAYF service.

4. Then the WAYF service returns the user's home institution to the ReP which in turn creates the Handle that contains the URL the user wants to access and passes it to the user's home institution for authentication.

5. The IdP ask the user to enter his/her institutional credentials.

6. Then the user's credentials are sent back to the IdP to be verified using the local database hosted by the IdP.

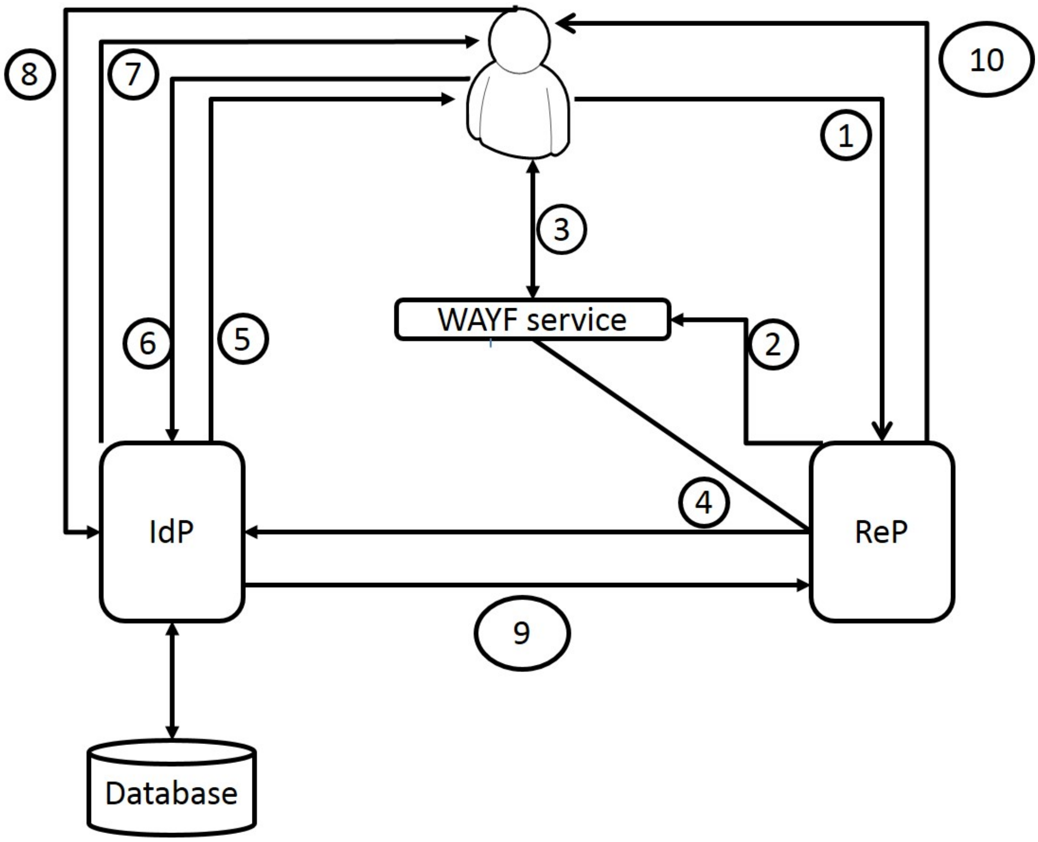


Figure 2.9: Shibboleth Operation based on Paschoud (2004)

7. For privacy purposes, the IdP ask the user to specify which attributes should be sent to the ReP.

8. The user returns the attributes that he/she want to be sent to the Rep.

9. Thereafter, the IdP will send the user's attributes to the ReP and the ReP will make the decision whether to grant or deny access to the user.

10. Finally, the user is notified of the outcome by the ReP.

The advantages Shibboleth provides within the access control environment cannot be overlooked. Furthermore, Shibboleth is based on open source software which means it can be implemented easily without any cost.

2.5 Conclusion

Access control must be enforced across federated IT ecosystems to ensure adequate access to information resources, especially to those resources accessible via the Internet. This chapter positioned access control in terms of this dissertation by arguing that access control has an *administration-time* to set up the access control rules and a *run-time* to enforce the created access control rules. Furthermore, current access control prevention techniques were reviewed and discussed. This showed that several potential solutions to access control in federated IT ecosystem exist, each with its own advantages and disadvantages.

Access control is not a once-off activity, but requires administration to be done from time to time, and the actual access control decision is made every time there is an attempt to access a particular resource. The resource could be hosted by another organization, i.e. not localized. Therefore, access control must be enforced across IT ecosystems.

Chapter 3

Management of IT Ecosystem

Management of IT ecosystems in this dissertation refers to ensuring that all of the information technology resources of an organization are managed properly. These resources may include logical resources such as data, information that is stored physically such as computer hardware, device facilities as well as the people who look after them.

Managing these resources within an organization requires basic management functions such as organizing, controlling, staffing and budgeting. These functions may also include network design, planning, and technical support to customers.

The previous chapter examined the access control authentication and authorization components. Three access control administration mindsets were explored before access control enforcement and the status quo of the access control technologies were discussed.

This chapter will investigate the management of IT ecosystems and the important role that senior management should be playing. Moreover, the crucial role played by each layer present within an IT ecosystem will be discussed. The roles of policies, processes, products and people together with technologies and associated external partners will be explored. The current chapter commences by discussing the importance of IT in organizations.

3.1 The Value of Information Technology in Organizations

Most organizations need an Information Technology (IT) department in order to function and achieve their business goals. Organizations have become increasingly reliant on IT to carry out their day-to-day work activities. In fact, IT has become the weapon organizations use to survive.

Securing information resources has been perceived as an IT responsibility in many organizations (Clinch, 2009). However, such perception could be argued against. Implementing anti-viruses on computers and setting up firewalls in networked devices cannot prevent the ignorance of internal or external users from sharing sensitive information outside of the organization.

The protection and management of information resources in any organization is everyone's responsibility (Clinch, 2009; Von Solms & von Solms, 2006). The responsibility of protecting information starts at the top and circulates down to the lower layers.

3.2 Organizational Layers

Within an IT ecosystem, decisions are often categorized according to three management layers. These are: strategic, tactical, and operational. These layers influence each other, as can be seen in Figure 3.1.

A decision at the strategic layer will impact the decisions at the tactical layer, and decisions at the tactical layer will impact decisions at the operational layer. The following subsections briefly highlights the role of these layers.

3.2.1 Strategic Layer

The strategic layer is there to guide the direction an organization takes. Certain decisions need to be made. These decision are often embodied through policies (Von Solms, Thomson, & Maninjwa, 2011a) and agreements with suppliers and partners.

At this layer, the IT managers are responsible and accountable for all

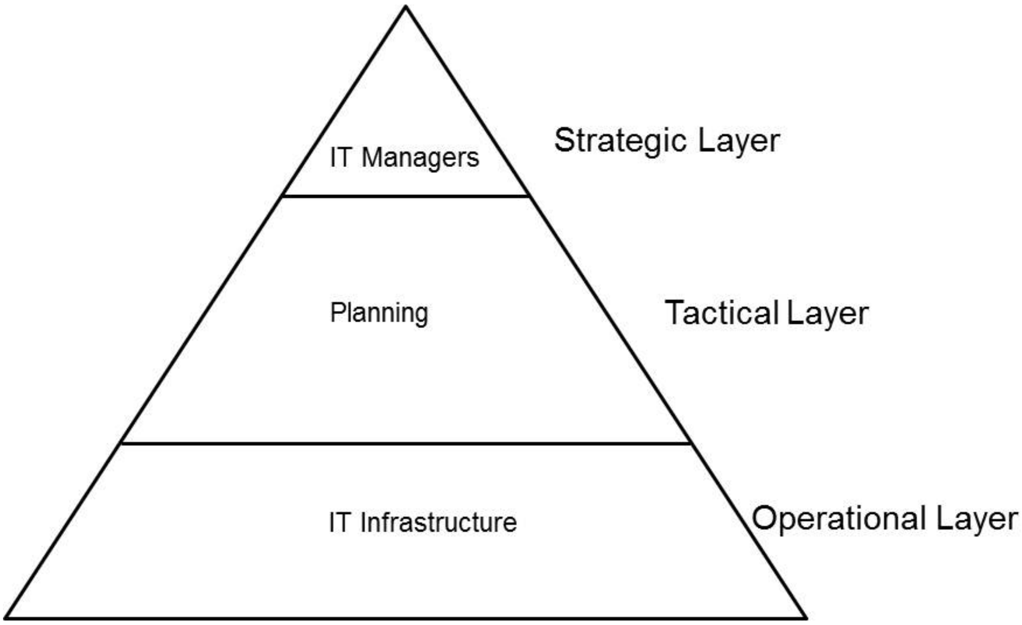


Figure 3.1: IT Management Layers

ongoing IT services within the organization. They work towards achieving organizational goals by directing the activities of employees. IT Managers must provide clear direction concerning what exactly they expect from their employees in order to achieve these organizational goals. Employees' behaviours and actions need to be controlled. Developing policies can address these issues. Thus, ensuring that the policies are properly enforced is the responsibility of IT managers.

In the case of this research study, policies must define how access to online services will be provided. An IT ecosystem is controlled by a policy that defines the behaviours of the internal employees and online users of the service, access to online services and the degree to which access is provided to external partners.

3.2.2 Tactical Layer

At this layer, tactical planning is done in accordance with the strategic directives. After the strategic directives have been created, plans must be put in place to ensure that the strategic choices can actually be implemented feasibly. This may involve project planning activities including raising awareness of the strategic direction and training in the use of technologies.

After the policies are created at the strategic layer, the tactical component needs to execute them and perform action plans such as procedures (Harrington & Ottenbacher, 2009). Training sessions need to be performed at this level.

3.2.3 Operational Layer

The operational layer represents an organization's underlying infrastructure and is concerned with operational implementations.

The output from the tactical layer acts as an input to the operational layer. Decisions related to the functionality of the underlying infrastructure should be made. The operational managers will need to communicate the impact that a particular decision set forth by the tactical managers and possibly by the strategic managers will have on the underlying infrastructure.

von Solms (2005) states that activities in the operational layer within an organization are always executed well . Activities in this layer include logical access control management, identification and authentication management and several others (von Solms, 2005).

It can be argued that these three layers work hand-in-hand. Decision made at any layer has the potential to influence the other layers. These layers are distinctively discussed in chapters 5, 6 and 7.

3.3 An Integration of ITIL's Four P's in Managing IT Ecosystems

As stated earlier, the responsibility of protecting of information starts at the top of the organization's hierarchy and extends through it to the bottom and possibly beyond the organization to their associated partners. At the top, the importance of ensuring adequate access control in federated IT ecosystems should be emphasized through the development of policies. These policies should extend into lower levels of the hierarchy (Von Solms et al., 2011a).

Therefore, the management of IT ecosystems should encompass the broader aspects of the organization, i.e. understand the reporting structure, culture and value proposition of the organization. Figure 3.2 conceptually positions such a reporting structure.

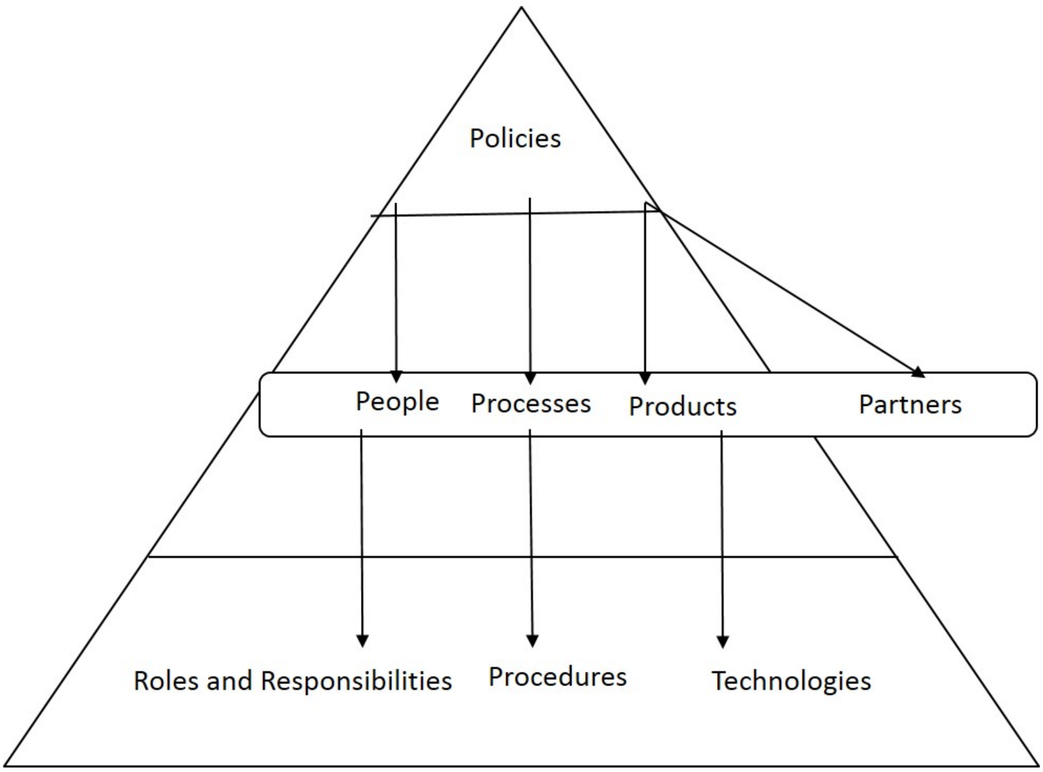


Figure 3.2: ITIL's Four P's Utilization

At the top of the pyramid, policies that direct and control organizational assets are developed. They are then distributed to each layer of the pyramid to be enforced. A way to achieve effective management of federated IT ecosystem environments might be the utilization of ITIL's Four P's of the Service Design (shown in the middle of the pyramid in Figure 3.2) (Hunnebeck, 2011). The four P's in this research study are described as follows:

1. **People:** All the employees of the organization including the management staff members.

2. **Processes:** This includes procedures.

3. **Products:** Organizational services, tools and technologies.

4. **Partners:** External vendors and suppliers.

Each of ITIL's Four P's and their functions are discussed in the following subsections.

3.3.1 People assigned Roles and Responsibilities

Ensuring access control in IT ecosystems starts with people. They are a valuable asset just like any other organizational asset. Without them it is challenging for an organization to perform its day-to-day operations. They are the core of the organization's success and the drivers for organizational resources and capabilities to produce value (Hunnebeck, 2011). It is imperative that effective communication throughout the organization is maintained. Proper communication will lead to the success of the organization while poor communication will result in the failure of the organization. People should be able to carry out their assigned job requirements and ensure that they know their roles and responsibilities.

Effective communication can be achieved through the development of policies. Policies are developed and revised from time to time by the top-level managers (Mooi, 2014). These policies should be circulated through all levels of management as previously highlighted. They should not only be circulated but also communicated and understood by people from all levels. Moreover,they should be properly enforced and measured from time to time in the process of determining their effectiveness.

It is through these policies that people will behave accordingly. Policies set common ground and boundaries for people in an organization. They define the associated roles and responsibilities of people. If people fail to follow these policies it could potentially damage an organization. As highlighted by Von Solms et al. (2011a), "information has the potential to damage an organization if it falls in the wrong hands". According to Whitman and Mattord (2013, p.58), some people fail to follow policies, whether through ignorance or intentionally. The fact that they fail to read and understands policies could damage an organization.

In summary, policies are created at the top level of management to direct and control access to the organization's valuable assets such as people. The roles and associated responsibilities of the people are communicated through policies. Therefore, it is imperative that people read and understand the policies communicated to them.

These policies also apply to other assets of the organization such as processes. Therefore, the following section discusses the relationship between policies and processes.

3.3.2 Processes and Procedures executed according to Policies

Policies and processes provide directions to people towards completion of a particular task (Mooi, 2014). Policies set boundaries and define the roles and responsibilities of each member of the organization while processes and procedures specify how the actions within those roles and responsibilities are performed (Von Solms et al., 2011a). Policies and processes should define procedures for both internal and external partners. Such procedures should include service level agreements, sharing of information resources and the degree to which internal and external partners can access the organization's information resources, i.e. access organizational systems, services and premises.

The level at which an organization may want to secure its valuable assets could inconvenience the important role that partners play in the organization's success. Hence, when policies and processes are developed they should provide an acceptable level of security that will also satisfy the associated partners. The relationship between policies and processes plays an important role in directing and controlling access to organization's valuable assets beyond its boundaries, i.e. to its associated partners (both internal and external parties).

3.3.3 Products and Services created with Tools and Technologies

The role performed by people in an organization cannot be overemphasized; they bring enormous value to the organization (Duffy, 2001). It is people that make the organization run with the guidance of policies set forth. But without necessary tools and technologies, it could be challenging to provide services and create products. Products are developed using tools and technologies. Tools and technologies are necessary to provide services. In federated IT ecosystems, new tools and technologies continue to advance at an increasing rate. To manage access control in federated IT ecosystems, necessary tools and technologies are of most the utmost importance.

As noted by Duffy (2001), "the business world is increasingly competitive, and the demand for innovative products and services has yet to be satisfied."

An important phrase that can be highlighted in this statement is "innovative products and services". Such innovative products and services might not be satisfied without the necessary tools and technologies and, of course, the right people in place. These tools and technologies are managed through policies. A typical policy intended for the use and management of tools and technologies would include statements that specify who can use them, how they can be used and when they can be used.

The answer to the first question might also include the use of tools by external partners and suppliers. The relationship of external partners and suppliers to the organization is discussed in the following section.

3.3.4 Partner and Supplier relations governed by Policy

To survive in today's competitive marketplace organizations are increasingly forming alliances with other organizations. This kind of partnership is becoming more important and its success depends on common agreements and trust between the two organizations (Gallivan & Depledge, 2003). Some everyday operations of the organization may be performed by external partners. For example, when a bank has a problem with network infrastructure they might want to partner with a networking organization that can take full responsibility of their network infrastructure. Whenever they have a network related problem, their partner will identify and troubleshoot the problem.

Therefore, it is imperative that the policies of the organization clearly specify the degree to which external partners can have access to the organization's valuable assets.

3.4 Conclusion

In this chapter the relationships between policies that direct and control people, processes, products and partners were discussed. The main argument provided in this chapter was that these policies should be developed and communicated to all levels of management. Such communication should extend from the top (were policies are defined) to the middle (were action plans starts to take place) through to the bottom (were action plans are executed). Failure to communicate, could lead to the misuse, damage and loss of the organization's valuable assets. The chapter was structured according to ITIL's four P's, these four P's were utilised as they cover a complete IT ecosystem. Subsequently, they were further discussed in detail.

This chapter along with the previous two chapters conducted a literature study and mark the end of the background chapters (Part I). The literature study was necessary to provide the foundation of this research study. Furthermore, the results of the literature study together with argumentation will play an important role in the development of the proposed model. The next chapter marks the beginning of Part II which discusses the model development.

Part II

The Proposed Multi-faceted Model

Chapter 4

The Conceptual Model

The previous chapter marked the end of the background chapters by arguing the various relationships that should exist in order to effectively manage IT ecosystems. Together with the two chapters before it, the chapter provided a foundation for the development of the proposed multi-faceted model to support authentication and authorization for online services.

This chapter motivates the conceptual model and its components. Chapters 5, 6, and 7 discuss each component in more detail. The chapter starts off by conceptually positioning the proposed model.

4.1 Conceptual Positioning

As highlighted in Chapter 3, decisions in organizations are often categorized according to three management layers: strategic, tactical, and operational. In order to have a common understanding within an organization, it is important that the decisions at each of the layers align with one another in order to realize the vision and mission of organization.

Chapter 3 highlighted two important aspects. Firstly, the layers influence one another. A decision at the strategic layer will impact the decisions at the tactical layer, and decisions at the tactical layer will impact decisions at the operational layer. Secondly, what is considered part of each layer is dictated by the vantage point taken. What might be considered a decision at the tactical layer when arguing from the perspective of the top management of an organization might be considered a decision at the strategic layer when viewed from the perspective of the manager of a business unit.

In this dissertation our premise is that the organization wants to achieve a strategic goal, for example, provide relevant and cost-effective information to its employees and customers. From an organizational perspective this strategic decision must be tactically implemented through providing, for example, access to online libraries. Decisions at the operational layer, to implement specific technologies to access these libraries, must follow.

The proposed model is not aimed at the complete organization. Instead, it aims to help the information technology department that must ensure access to certain online services in support of a decision made at the strategic layer. The focus of the model is illustrated by the shaded triangle in Figure 4.1. The shaded triangle in Figure 4.1 thus represents the proposed model within the larger organizational context. From an organizational perspective the proposed model is thus primarily a tactical model.

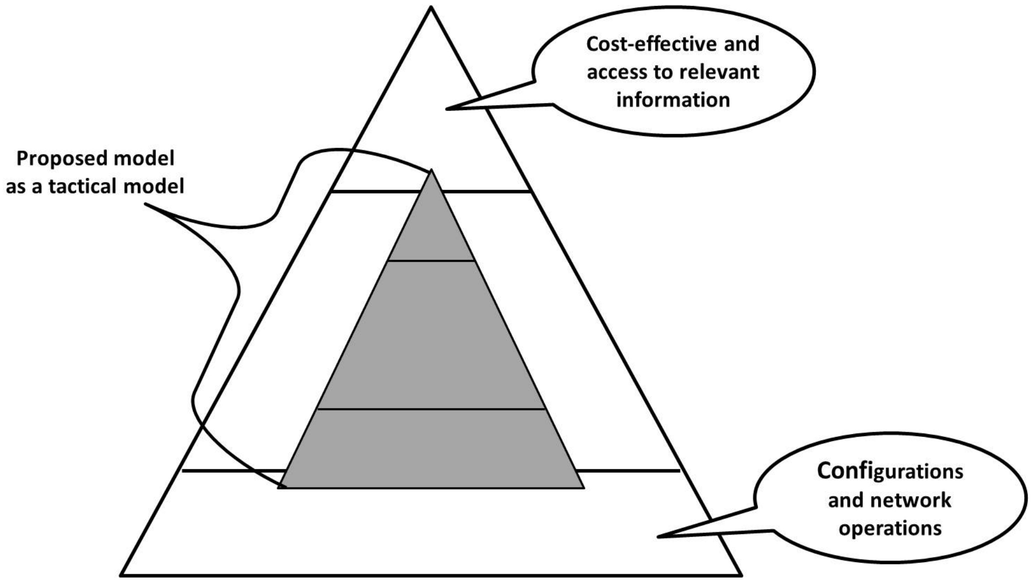


Figure 4.1: Conceptual Positioning of the Model

In Figure 4.1 the unshaded triangle represents the organizational perspective in terms of the three management layers as pointed out in Chapter 3. The shaded triangle emphasizes where the proposed model is positioned. Further, the shaded triangle slightly overlaps with the strategic and operational layers of the organization. This highlights the fact that the proposed model will be influenced by some decisions at the strategic layer and, in turn, will influence decisions at the operational layer.

Therefore, it can be argued that to achieve a strategic goal, for example, providing relevant and cost-effective information to organizational employees and associated customers, decisions at each layer must support and acknowledge the decisions made at the other layers.

The following section introduces the model layers in more detail.

4.2 The Model Layers

As highlighted in Chapter 1, this research study was primarily motivated by three realizations. Firstly, that access control spans across the organizational boundaries. Secondly, that there could be inconsistencies between legal specification and tactical access control measures, as access control needs to be maintained across organizations. And thirdly, that an organization's employees and its customers might breach these legal requirements unknowingly.

Based on these three realizations, the research sub-objectives in Chapter 1 were formulated and are also repeated in Table 4.1. Therefore, each of the proposed model layers is in line with these research sub-objectives stated in Chapter 1 and Table 4.1.

Table 4.1: Reach objectives mapped to chapters

Sub-Objective	Chapter
SO1 investigates the governance of policies	5
SO2 investigates and identifies ways of influencing users behaviours	6
SO3 Investigates and identifies possible access control technologies	7

The proposed model consists of three layers: the strategic layer (guidance), the tactical layer (planning), and the operational layer (technology considerations) as illustrated in Figure 4.2 and Figure 4.3.

A brief overview of each of the three layers of the proposed model will be outlined in the following subsections.

4.2.1 Strategic Layer: Guidance

This layer represents strategic guidance to ensure that strategic goals set out by the organization can be achieved accordingly. The primary question that

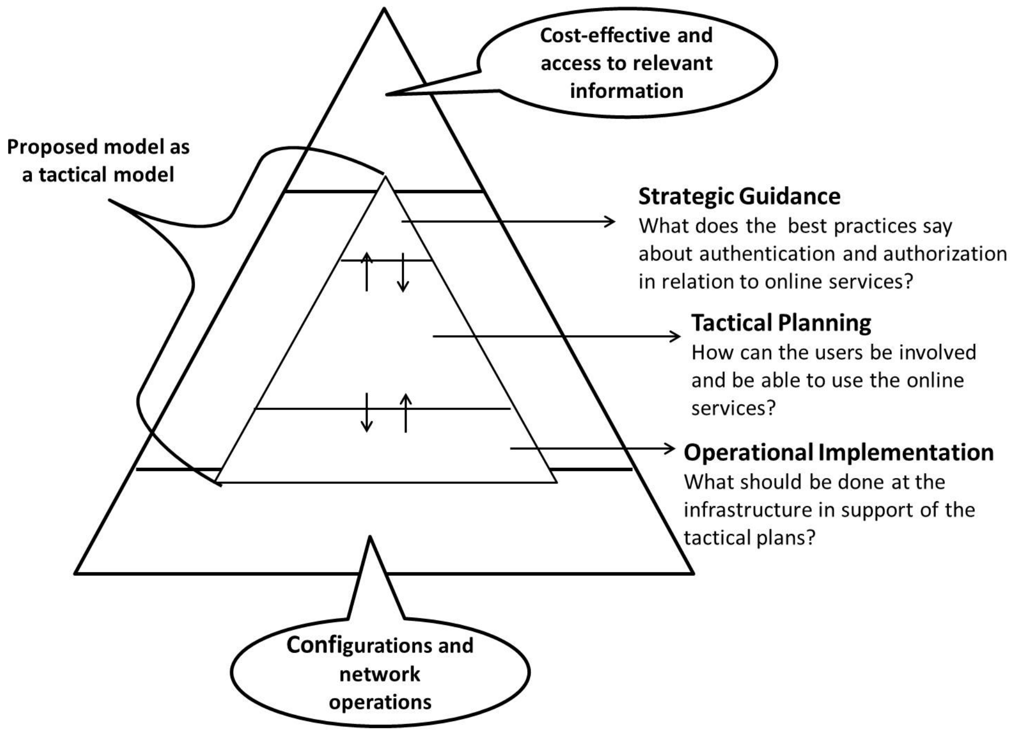


Figure 4.2: Positioning of the Proposed Model Layers

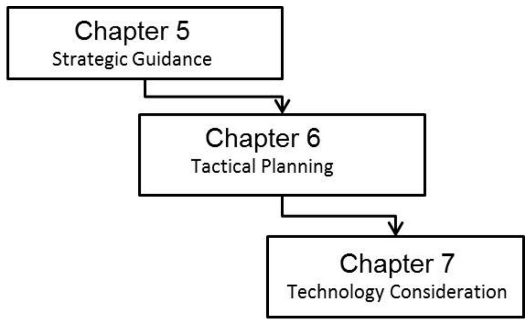


Figure 4.3: Model Layers Indicating their Chapters

should be addressed in this layer is: "What guidance does IT best practices, management frameworks and IT standards provide about authentication and authorization in an IT ecosystem?" Answering this question will address SO1.

4.2.2 Tactical Layer: Planning

At this layer, tactical planning is done in accordance with the strategic directives. Thus, the question that should be answered in this layer is: "How can the users and customers be attracted to the online service offered by the organization?" Answering this question will address SO2.

4.2.3 Operational Layer: Technology Considerations

The operational layer represents an organization's underlying infrastructure and is concerned with operational implementations. The primary question that should be addressed in this layer is: "What should be changed or implemented with regard to the infrastructure in order to support the decisions at the tactical layer which, in turn, support the decisions made at the strategic layer?" A series of questions should be asked such as, should we consider joining existing federations that support both authentication and authorization for online services and, if so, how will that impact the existing networking configurations?

Therefore, there are many considerations that the operational layer is responsible for beyond simply taking the decisions made at the tactical layer and implementing them. A decision made at each layer could have a positive or negative impact. For example, consider a decision to join an existing federated identity management system. There could be some costs involved which might not be in line with what the strategic managers would want.

The answer to the primary question stated in this paragraph will also address SO3.

4.3 Conclusion

This chapter presented a conceptual view of the model. The three layers, namely the strategic, tactical and operational layers, constitute the proposed model. A brief overview of these layers introduces the next three chapters which are dedicated to providing details of the model layers.

The following chapter starts off by looking at the strategic layer in more detail.

Chapter 5

Strategic Decisions

The previous chapter conceptually positioned the proposed multi-faceted model in the bigger picture. This was followed by an introduction to the proposed multi-faceted model and its layers. In addition, the chapter further provided an overview of each of the layers to create a foundation. This chapter continues to discuss the first (strategic decisions) layer of the proposed multi-faceted model and the next two chapters will discuss the other two layers.

The current chapter commences by firstly providing a brief overview of the purpose of the strategic layer in general.

5.1 An Overview

The general structure of the organization is in the form of a pyramid. Managers of the organizations are the drivers for other parts of the pyramid. Their role is to direct and control (Von Solms, Thomson, & Maninjwa, 2011b). They provide direction on what needs to be done in order to realize the organization's business goals. Furthermore, they also check whether the directives given are being executed to their satisfaction.

IT best practices, management frameworks, IT standards and other related documents that might provide guidance are important to their role as managers. This dissertation as a whole is concerned with the provision of authentication and authorization to online services. Therefore, IT managers should provide direction to other parts of the pyramids by making use of these documents.

The following sections discuss these IT best practices, management frameworks and IT standards from the perspective of an IT business unity.

5.2 An Overview of ITIL, COBIT 5 and ISO/IEC 27002

As can be expected, access control to information systems has been discussed by many, including in IT best practices, management frameworks and IT standards. Among these, the most commonly used are ITIL (OGC, 2007), COBIT 5 (ISACA, 2013)and ISO/IEC 27002 (ISO/IEC27002, 2013). Although ITIL is considered as a best practice guideline, COBIT 5 as a management framework, and IS0/IEC 27002 as a standard, in this research study they are collectively referred to as frameworks.

Many organizations are under pressure to control access to their business systems and services. Organizations should use IT best practices, guidelines, frameworks and standards for guidance when implementing access control. ITIL, COBIT 5 and ISO/IEC 27002 all discuss the concept of access control. However, access control views are scattered through the frameworks. This could make it challenging to use them during access control implementation.

Much research has been done in an attempt to integrate them (Sahibudin, Sharifi, & Ayat, 2008). Furthermore, the access control issues are not discussed at the same level of detail. To understand the differences, think of these three in this way: COBIT 5 discusses what to monitor and control, ITIL clarifies how to go about implementing the processes for performing those services, while ISO/IEC 27002 discusses the process for securing those services (Greenfield, 2007). As the focus of this section is the analysis of access control views within ITIL, COBIT5, and ISO/IEC 27002, the following subsections focus not only on an overview of these frameworks, but also provide directions with which the information concerning access control views can be located within them.

5.2.1 ITIL

Information Technology Infrastructure Library (ITIL) is a best practice guideline introduced by the Office of Government Commerce (OGC), situated in the United Kingdom (UK), to provide best practices for IT service management in an organization (Năstase, Năstase, & Ionescu, 2009). This framework discusses issues related to different entities such as people, processes, and infrastructure technology, to provide cost effective and high-quality IT services (OGC, 2007). ITIL is comprised of five publications, namely (Verma, 2014) Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

Service Strategy discusses the concept of identifying market opportunities for new services, while Service Design is concerned with developing a strategy into a designed document (Greenfield, 2007). Service Transition deals with the implementation of the activities laid down by Service Design and Service Operation focuses on the operational side to ensure that services are delivered. Furthermore, Continual Service Improvement provides consistency between the other four publications. It focuses on how the service can be improved over time (Verma, 2014).

In ITIL, the access management process is described in the Service Operation publication. Views are clearly defined in the access management section (4.5) as lifecycle activities.

5.2.2 COBIT 5

COBIT 5 is a management framework developed by ISACA (Information Systems Audit and Control Association) for IT governance and IT management (Sahibudin et al., 2008). This framework defines 34 control objectives in a hierarchy of processes and domains (Ridley, Young, & Carroll, 2004). The processes are subdivided into four domains: Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Evaluate, Direct and Monitor (EDM) (Greenfield, 2007). Under each domain, the process objectives, key activities, input, output, performance measures, Work Product (WP) and Best Practice (BP) are discussed.

There is no specific section that discusses access control views in this management framework. However, access control views could be found in any of the four domains mentioned above. During the integration of access control views in COBIT 5, the Deliver and Support domain discuss more access control views than the other domains.

5.2.3 IS0/IEC 27002

This is an information security standard introduced by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) for information security management (Sahibudin et al., 2008). The main purpose of this standard is to provide guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization (ISO/IEC27002, 2013). The three areas of information security, namely Confidentiality, Integrity and Availability, are covered in this standard. Furthermore, the standard contains 14 security control clauses in which access control is included (ISO/IEC27002, 2013). Each of these 14 clauses defines a number of main security categories within them.

Although access control views are primarily found in section 9 under the access control clause, other sections also make references to access control related views.

The next section considers how the mapping of these frameworks will be performed.

5.3 Mapping Approach of the Frameworks

As pointed out earlier in Chapter 2, access control must be considered from both an *administration-time* and a *run-time* perspective. Clearly access control is not a once-off activity, but requires administration to be done from time to time, and the actual access control decision is made every time an attempt to access a resource is made. This nature of access control is best acknowledged by ITIL which views access management activities as part of a lifecycle. Therefore, this research structures the mappings between the frameworks according to the ITIL access management activities to ensure a holistic view.

Figure 5.1 conceptually positions the access management activities identified by ITIL in terms of *administration-time* and *run-time* perspectives.

The first three activities, namely Requesting Access, Verification, and Providing Rights, ensure that users will receive the access rights they require. The Monitoring Identity Status and Logging and Tracking Access activities take place continually to ensure that access rights reflect the busi-

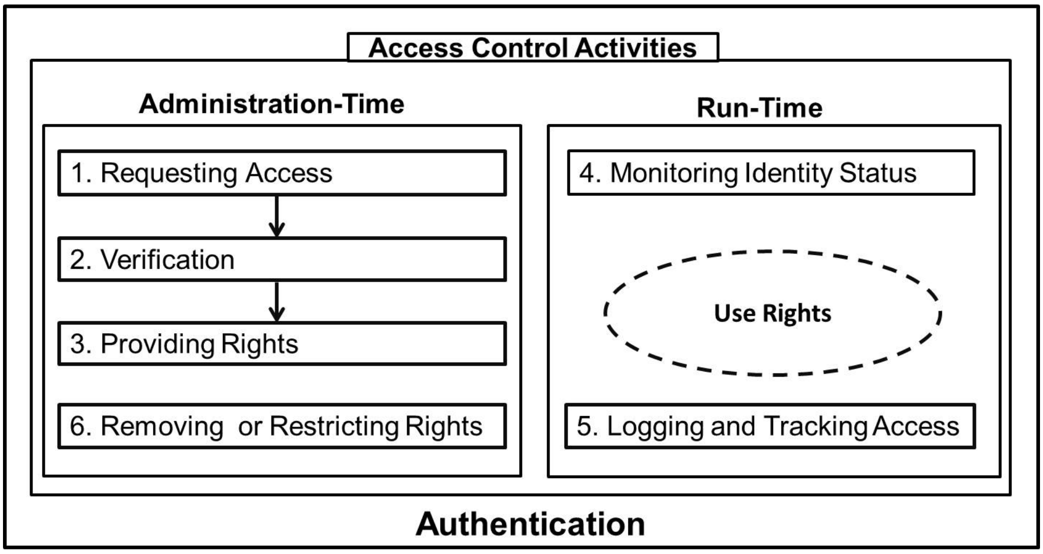


Figure 5.1: Activities for Access Control Mappings

ness requirements and are not misused. Anomalies and changes to business requirements may in turn trigger some of the administration-time activities. Finally, the Removing or Restricting Rights activity ends the lifecycle of the access rights.

5.4 Access Control Activities

The provision of access to a particular service or resource has been discussed by IT frameworks. This section looks at what guidance is available regarding access control views by using ITIL lifecycle access management activities as a framework. The discussion integrates material from the three frameworks discussed in section 5.2. In order to facilitate easier integration of the views, the following cross-referencing mechanisms are used:

- For ITIL specific concepts, the reference would indicate the ITIL lifecycle and the relevant section in the lifecycle documentation. For example (SOP, 11.4) refers to Service Operation Processes section 11.4.

- For COBIT 5 specific concepts, the reference would indicate the framework and the process number. For example (COBIT 5, BAI06-BP1).

The referencing will use the acronyms introduced in section 5.2.2.

- For ISO/IEC 27002 specific concepts, the reference would indicate the standard and relevant section in the documentation. For example (ISO/IEC 27002, 8.1).

- Where a statement relates to more than one document the references would be combined and separated by a semi-colon.

The following sections perform the mapping of the access control views.

5.4.1 Activity 1: Requesting access

The first step towards gaining access to resources is requesting access. Users (Employees, Contractors and Visitors) could request access to a specific service or a set of services. These requests may originate from different sources. ITIL (SOP, 4.5) identifies four sources, namely HR (Human Resource) Management, a Service Request by the user, RFC (Request for Change), and a request from the Manager. Whenever someone is hired HR is required to initiate a request. The request is based on the user's job requirements and access policies of the organization (IS0/IEC 27002, 9.2.2). The HR department must verify the user's identity and should ensure that his/her job requires the services being requested. To accomplish such a goal the request should be automated. In other words, HR systems for allowing access to information systems and services should be in place prior to employment (ISO/IEC 27002, 9.2.1).

This applies to the current services, but when there is a new service being deployed in the organization the RFC will initiate the request. Such requests could happen when there are large upgrades to the system that affect a large number of user access rights within a particular group of users (SOP, 4.5.6). It is thus imperative that the change management processes consider the impact of user access.

General service requests, which may also include requests to access a service/system, are handled by the IT service desk. Such service requests should be classified and prioritized in order to assess the risks they might pose to the organizational processes and services (COBIT 5, DSS02-BP1). These requests must be recorded as they could help in future investigations (ISO/IEC 27002, 12.4). Some requests may not come from the user, but could originate from the manager of a particular department. This could happen when the manager assigns an internal user to perform a task that requires more access rights than currently available to that user. The request will then be channelled via the service desk.

Once a request is received, the next step is to verify that the user is who he/she claims to be and that he/she really needs the access. The next activity will discuss the verification process.

5.4.2 Activity 2: Verification

Verification according to ITIL is an administration-time activity that follows requests for access. It involves two actions. Firstly, the requester must be authenticated to ensure that he/she is who he/she claims to be (SOP, 4.5.5.2). Secondly, it must be ensured that he/she really needs the service (COBIT 5, DSS05-WP6). The process is illustrated in Figure 5.2.

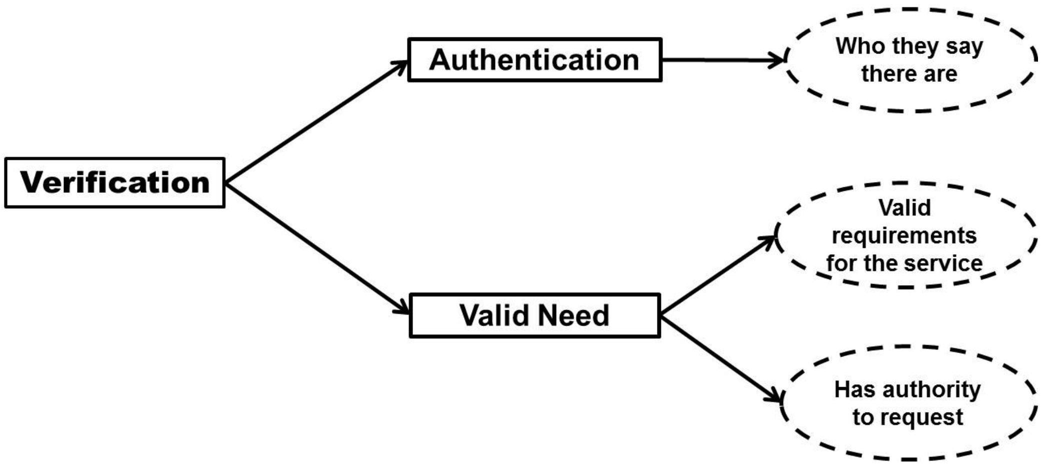


Figure 5.2: The Verification Process Activity

Sometimes the need might be validated by the fact that the requester is not the grantee and that the requester has the authority to request this. Other times, if the requester is the grantee, logical mechanism such as usernames and passwords might not be sufficient. In that case physical mechanisms such as a user visiting the Service Desk with a suitable identification document may be required. However, for an indirect request, where a manager might request access for his/her users, a username and a password might still be acceptable as this is really just an execution of the manager's right to request access.

Where the access request deals with sensitive services, other verification mechanisms such as hardware tokens (e.g. smart cards) and biometrics (e.g. fingerprints or signatures) (SOP, 4.5.5.2), may be required.

Once the request has been verified the user may be provided with the access rights required. This is further discussed in the next activity.

5.4.3 Activity 3: Providing rights

As soon as the verification process is complete the user is eligible to be given access rights in order to perform his/her day-to-day activities (ISO/IEC 27002, 9.2.2). Access rights are provided according to the user's job requirements and should be used for business purposes (COBIT 5, DSS06-02). One of the challenges of providing access rights arises when the user holds multiple access rights for different tasks. These multiple access rights could conflict with one another (SOP, 4.5.5.3). For example, a user needs to log the total number of hours worked per day for the purpose of calculating the salary earned (Task 1). However, Task 2 requires the user to approve the number of hours logged. This could be seen as a potential conflict or conflict of interest. However, such conflict can be avoided by carefully designing roles (SOP, 4.5.5.3).

At present most organizations are implementing the concept of role-based access control when providing access rights to users (Bao et al., 2008). Role-based access control has two steps. Firstly, mapping roles to access rights and secondly, mapping users to their roles (Zhou et al., 2012) as depicted in Figure 5.3.

This makes the provision of access rights much simpler than providing each user access rights that are not mapped to a particular role. Since the user might have two or more roles assigned to him/her, each of the roles assigned should be recorded and documented (COBIT 5, DSS05; ISO/IEC, 9.2.2).

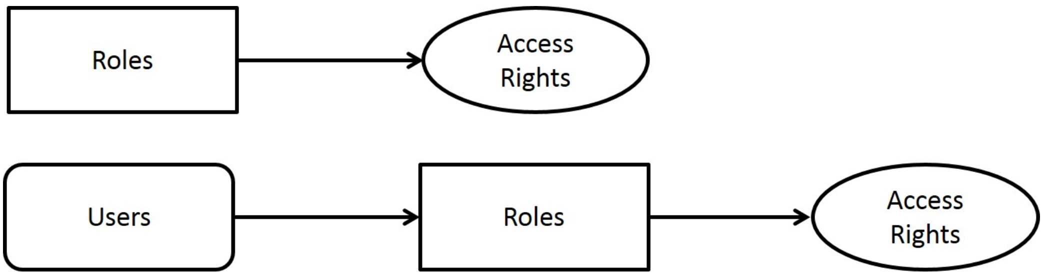


Figure 5.3: Role-Based Access Control Mappings

5.4.4 Activity 4: Monitoring identity status

In the previous activity users were mapped to their roles according to their business needs and requirements. As users continue in these roles, changes to the roles may be required and changes to access rights might arise (SOP, 4.5.5.4). It then becomes challenging to monitor the user's identity status or changes. Access control should cater for the prevention of redundant user IDs and accounts (ISO/IEC 27002, 9.2.1)and keep track of the date and time of changes, the type of change, the type of file accessed and the program used to execute the change (COBIT 5,EDM03) when doing monitoring. The changes should be explicitly authorized by the appropriate authority prior being approved (ISO/IEC 27002, 12.1.1, 12.1.2).

A change could be triggered by a user changing his/her password. In this case automated tools could be useful to monitor such a change and automatically update the involved database or systems. Of course, these changes could be legitimate or illegitimate. If the change is legitimate the records on the database will show that the user is actually active on the system. Whereas if the change is illegitimate, the database probably needs to integrate with intrusion detection tools which will lookout for passwords changing at the same time or odd patterns in passwords.

Today most organizations use tools, such as intrusion detection tools (COBIT 5, DSS05-BP7), to monitor their systems. Although changing the password of the user could be seen as minor, "big" changes such as job changes, promotions or demotions, transfers, resignation or death, dismissals, disciplinary action, and retirement (SOP, 4.5.5.4) can be challenging to monitor if automated tools are not in place.

It is of interest to discuss disciplinary action and dismissals. These might bring harm to the organization's valuable assets due to user's behaviour during the disciplinary action or dismissal period. In serious cases of misconduct, the user's access rights, duties and privileges should be temporarily suspended (ITIL: SOP, 4.5.5.4; ISO/IEC 27002, 7.2.3) and if necessary, he/she can be escorted off the organizational premises. Similarly, during suspension all access should be restricted until the employee is ready to resume his/her duties. Again, automated tools should be in place to re-activate the access rights revoked when appropriate.

5.4.5 Activity 5: Logging and tracking access

Threats originate not only from the outside world, but internal users can initiate threats unintentionally if policies are not followed. Users could breach the policies or misuse the organization's resources (SOP, 4.5.5.5). However, these threats can be minimized by implementing intrusion detection tools for tracking and logging user activities (ISO/IEC 27002, 12.4.1; COBIT 5, DSS05-BP7; ITIL: SOP, 4.5.5.5). When a user is suspected of resource misuse the logged files could help to speed up the investigation process (IS0/IEC 27002, 12.4.1; COBIT 5, DSS05-WP9). Even when there is a change in a user's identity or role, the change needs to be logged and kept for the minimum duration period specified by the organization's security policies (ISO/IEC 27002, 9.2.5).

Access control should track not only unauthorized user access activities, but also authorized user activities (ISO/IEC 27002, 19.2.5). A user can be given access rights to execute a task but never use them. This could bring harm to the organization. For example, if a user has legitimate access rights and chooses not use them, the access rights are compromised by the third party. This introduces vulnerability to other organizational systems unnecessarily. This activity is also accountable for making sure that the user access rights that were provided in Activity 3 are properly used for their purpose. Clearly this activity should also be utilized when there is a change within the organization and such changes must be logged at all times.

5.4.6 Activity 6: Removing or restricting rights

Activity 3 discussed the concept of providing access rights to users. This activity is responsible for revoking those rights whenever the need arises. The process of removing or revoking access rights can take place when the user is dismissed, dies or resigns (ISO/IEC 27002, 7.2.3; SOP, 4.5.5.6). The task of removing rights needs to be performed in a timely manner to prevent unauthorized access by the dismissed user. Having the user de-registration procedures in place (ISO/IEC 27002, 9.2.1), which should be developed by information security management, could speed up the process.

The removal of the access rights process does not mean the user access rights should be completely erased as these could be needed again. Rather, the access rights should be deactivated. The same goes for restricting access rights to the user. the need to restrict access rights could be triggered when the user has changed roles, is under the disciplinary process or is on temporary leave for a short period of time (COBIT 5, APO07; ITIL: SOP, 4.5.5.6; ISO/IEC 27002, 7.2.3). However, a record of access rights should still be kept until the user is ready to resume his/her duties (COBIT 5, EDM03).

5.5 The Discussion of Access Control Themes

The previous section identified six ITIL lifecycle access management activities and used them as a framework for integrating access control views found in ITIL, COBIT 5 and ISO/IEC 27002. This section serves to uncover the main access control themes found in the frameworks discussed in 5.4. Each of the six ITIL lifecycle access management activities are illustrated in Table 5.1 to highlight these main access control themes.

In Table 5.1, if minimal information is provided in a framework regarding a chosen theme, the (✓) will be shown. Furthermore, the (✓✓) will indicate that the framework has detailed information regarding the chosen theme. If the table entry is empty, there is no information contained in a framework for the chosen theme.

As can be seen in Table 5.1, many similarities exist between ITIL and ISO/IEC 27002. Where ITIL provides detailed information regarding a theme, similar detailed information is often provided by ISO/IEC 27002. For example, as can be seen in Table 5.1, both ITIL and ISO/IEC 27002 discuss

ITIL Activities	Access Control Themes	COBIT 5	ITIL	ISO/IEC 27002
Requesting Access	Automate access requests		✓✓	✓✓
	Classifying and prioritizing requests	✓✓		
	Record and document access requests	✓	✓✓	✓✓
	Originating sources of requesting access		✓✓	✓
Verification	Authentication	✓	✓✓	✓✓
	Verifying business needs		✓✓	✓✓
Providing Rights	Designing roles		✓✓	✓✓
	Record and document roles		✓✓	✓✓
Monitoring Identity Status	Changes to access rights		✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓
	Prevention of redundant user IDs			✓✓
Logging and Tracking Access	Log files	✓	✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓✓
	Proper use of access rights	✓✓	✓✓	✓
Removing and Restricting Access	Resignations		✓✓	✓✓
	Suspensions	✓	✓✓	✓✓
	Dismissals	✓	✓✓	✓✓

Table 5.1: A Summary of access control themes from COBIT 5, ITIL and ISO/IEC 27002

the theme of automated access requests and agree that these requests should be recorded and documented at all times. The same applies to Verification and Providing Rights activities where authentication and designing of roles are also discussed. Similarly, when no information is provided for a theme in ITIL, no information is provided in ISO/IEC 27002 most of the time. For example, classifying and prioritizing requests is not detailed in either ITIL or ISO/IEC 27002. However, it is not always the case that information provided by ITIL is also provided by ISO/IEC 27002. For example, as shown in Table 5.1, ISO/IEC 27002 discusses the theme of prevention of redundant user IDs while ITIL does not.

Conversely, COBIT 5 addresses some of the themes which are not discussed in either ITIL or ISO/IEC 27002. For example, as shown in Table 5.1, the theme of ‘classifying and prioritizing requests, under the Requesting access activity, is discussed by COBIT 5 but not by ITIL or ISO/IEC 27002. Where ITIL and ISO/IEC 27002 discuss a theme, COBIT 5 does not always provide information for that theme as can be seen in Table 5.1. For example, Table 5.1 highlights that information is not provided by COBIT 5 for certain themes such as designing of roles and record and document roles under the theme of Providing Rights. Therefore, it can be determined that COBIT 5 is not as detailed as ITIL and ISO/IEC 27002 in terms of access control.

Based on this discussion, it can be argued that a combination of ITIL, COBIT 5 and ISO/IEC 27002 gives a more comprehensive view of access control, as themes that are not covered in one framework or standard are covered by another framework or standard.

5.6 Strategic Guidance for Access Control for Online Services

As was discussed earlier in this chapter, access control should be managed from the time the user is registering to an online service until the user de-registers from the online service. Table 5.2 illustrate a useful input that strategic managers should keep in mind when preparing to offer an online service.

The questions showed in Table 5.2 should be kept in mind when thinking strategically. Depending on the type of online service being offered, some of the questions in Table 5.2 may not be applicable to some extent. However, if a question does apply, it should be addressed accordingly by also noting the potential impact it might have on other layers below the strategic layer.

Take as an example, the question of how do we differentiate the level of access rights (as illustrated in Table 5.2) in the context of an online digital library. The individuals accessing these digital libraries might not require different levels of access as they access the same content in an article.

With a multi-faceted model, any decision made in one layer will have a potential impact on the other layers below it. To better understand and clarify this, consider the question of who is allowed to request access, as can be seen in Table 5.2. The answer to this question might require that the tactical layer formulate some policies that need to be signed before access to

Table 5.2: Questions to consider throughout the six ITIL lifecycle activities

Strategic Guidance	
Channels	Questions to be asked
Requesting Access	Who is allowed to request access? When is he or she allowed to request access? How do we provide means of requesting access? How do we prioritise requests?
Verification	How do we authenticate the requests? How do we limit access to only authorised users?
Providing Rights	How do we plan on allocating access rights? How do we differentiate levels of access rights?
Monitoring Identity Status	What could trigger an access control change to an online service?
Logging and Tracking Access	How do we identify unused allocated access rights?
Removing and Restricting Access	When should the access rights to an online service be revoked?

an online service is requested. At the operational layer, different channels for requesting access might need to be developed and implemented, for example, an online form that will capture the details of the requester.

Answering the questions in Table 5.2 assists us in thinking about the complete access control lifecycle. The answers to these questions will aid us in various ways, from dictating the need for certain policies to influencing the technological decisions. Furthermore, the answers produce an output that the tactical layer needs to look at when planning. These outputs are depicted in Figure 5.4.

Figure 5.4 shows that the strategic layer is concerned with delivering business goals and in order to realize this goal, certain outputs must be produced and communicated to lower layers. These outputs could be in the form of an access control policy and guidance statements drawn from IT best practices, management frameworks or standards when, for example, offering an online service.

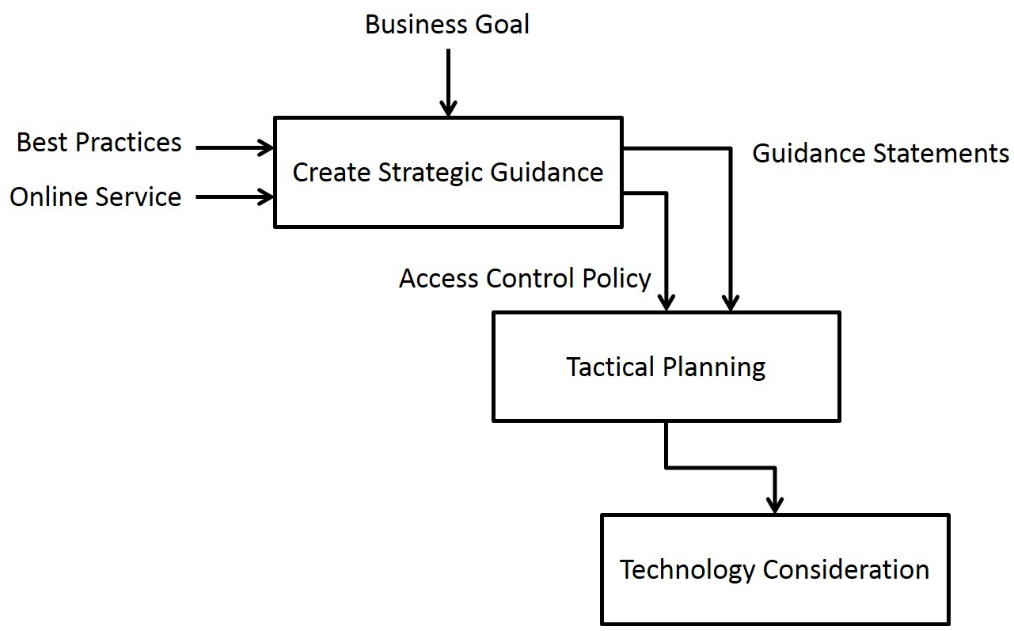


Figure 5.4: Strategic guidance Outputs

5.7 Conclusion

This chapter discussed the top layer of our model. The discussion involved an overview of access control frameworks commonly used in organizations for access control, before analyzing the access control views found from the frameworks. The six ITIL access management activities were utilized to structure the discussion as they provide a lifecycle of access control. Thereafter, the discussion of the access control themes found during the integration of the access control views was provided. Lastly, the strategic guidance for access control for online services was highlighted, which acts as an input in the next chapter.

The next chapter discusses the middle level of the proposed model where tactical issues will be discussed.

Chapter 6

Tactical Layer: Planning

The previous chapter discussed the decisions that must be made at the strategic layer. The discussion involved policy implications in IT ecosystems and also mapped access control views as discussed by major IT best practices, management frameworks and standards. The current chapter introduces the tactical layer. The primary question to be answered in this chapter is: "How can the users and customers be attracted to the online service offered by the organization?" With this query, the current chapter utilizes Osterwalder's Customer Buying Cycle (CBC) and is structured in such a manner as to discuss CBC.

When deploying a new service, the goal is to reach the intended environment and its users. To achieve such a goal, the provider of the new service needs to establish a common means of channelling the service to the intended environment. This is needed from introducing the user to the new service, helping them to make an informed decision on using it, to the transaction process, through to the use of the new service by the user. Of course, there are contacts points that the provider of the service needs to consider. Such contact points are outlined by Osterwalder et al. (2004) in the Customer Buying Cycle (CBC) and are defined as channels. Thus, this chapter commences by looking at the first channel, i.e awareness.

6.1 Awareness

Awareness involves knowing what is happening in a particular environment, system or service, what events are occurring within that environment, system or service, and who is doing what. "Awareness is not training"(Wilson & Hash, 2003). People often confuse awareness with training. The user in an awareness program is the recipient of information, while the user in a training environment is the active role player (Wilson & Hash, 2003).

In the context of information security for example, an uninformed person belonging to a particular organization cannot be held accountable of his or her actions such as exposing the organization's information assets by making naive mistakes, opening harmful websites, responding to phishing emails, using weak passwords, storing their login information in unsecure locations, giving passwords to others or giving out sensitive information over the phone when exposed to social engineering techniques, if they are not made aware of these kinds of threats in advanced (Gundu & Flowerday, 2012). His/her mistakes and vulnerabilities can never be completely eliminated, but through a structured awareness program the risk posed could be reduced to an acceptable level.

Based on the above example, it is unlikely that organizations in today's highly networked IT ecosystem could protect the confidentiality, integrity, and availability of information without ensuring that all people involved in managing and using such information understand their roles and responsibilities, the policies, processes and procedures, and their associated practices (Wilson & Hash, 2003). They should have adequate knowledge and awareness of the various management, operational and technical measures or controls made available to them to secure the IT assets for which they are responsible.

People are one of the "weakest links" in protecting IT assets. On the other hand, they are the key that drives other organizational assets and ensures adequate security to those assets (Wilson & Hash, 2003). If people are the key, but are also the weakest link, it is imperative that an awareness program is developed to ensure that they understand their roles and responsibilities and are aware of the services around them.

Therefore, the following subsections provide a brief discussion on what should constitute a good and comprehensive awareness program. It firstly discusses the concept of identifying the target audience, the information and issues related to them, and the techniques used to deliver such awareness to the intended users.

6.1.1 Existence

The users and customers are likely to have a few questions in mind before joining or subscribing to any online service available to them, especially since there are many illegitimate services on the Internet today. Such questions include: Who are you? Why you do what you do? How did you come to offer an online service? These questions should not be seen as negative towards the service provider but rather as interest being shown in the service. Users and customers want to trust the service provider before they buy or subscribe to what the service provider is promoting.

Like with any other business, an objective comes first, followed by a strategic plan for how the strategy will be implemented. A strategy should not be too broad because it will be too difficult to measure the effectiveness of a broad strategy.

6.1.2 Target Audience

The target audience in an awareness program can be determined by the type of awareness program that one is conducting, i.e. whether it is about a new facility, service or protection of personal identities such as passwords protection. No matter what type of awareness program is being conducted, the technique(s) of delivering such awareness need to be investigated, identified, carefully selected and implemented properly. Such delivery techniques are enumerated in the following subsection.

6.1.3 Delivery Techniques

There are various delivery techniques that can be incorporated into an awareness program. A single technique or a combination of these techniques can be used depending on the type of awareness program being conducted and the type of message that needs to be delivered. The techniques may include the following, as outlined in the PCI (2014):

1. E-mails and circulators

2. Memos

3. Notice boards

4. Bulletins

5. Posters

The awareness program may also include other delivery techniques not present on the above list, such as using the organizational websites. According to Wilson and Hash (2003), regardless of the delivery technique or approach taken, the volume of information should not be overwhelming to the audience. In other words, each point made should be brief, straightforward to the point.

6.1.4 Benefits

Any awareness program should explain the benefits of using or not using a particular service to the intended users. A benefit in the context of this dissertation refers to the real value a user or a customer experiences through using or interacting with an online service.

As highlighted in Chapter 1, online services offer benefits to Internet users, such as convenience, security, ease of use, speed, and flexibility. These benefits are expanded on below:

Convenience

User registration is a simple, quick process and needs to be performed only once whenever the user wants. This also allows the user to enrol to multiple services at any time.

Security

Online services are designed to be secure to protect the users' personal information when doing transactions.

Ease of Use

A user has the option of using a single login to access all of his or her online services. This removes the difficulties of remembering multiple usernames and passwords.

Speed

Users want to have quick access to the needed services. Using the Internet to access online services removes the need to physically go to the sellers premises and queue in long lines. This also allows the sellers to respond quickly.

Flexibility

Users are able to make purchases and orders even after hours as the systems take care of the process. Most online services will be available at any time.

6.1.5 Subscription

Most online services have either a minimum joining fee depending on the usage of the service or aonce-off fee, while other services are free of charge. Hence, it is important that the users are made aware of any fees involved prior to considering subscribing to any online service.

An expensive service will probably have fewer participants, while an inexpensive service is likely to have more participants. Therefore, when considering offering an online service it is important to keep the service subscription as low as possible. However, there are some services that cannot be offered at a low rate due to their deployment and maintenance costs.

6.2 Evaluation

Once customers are aware of the new online service and have identified that it could impact them positively, they will want to know more about it, and the benefits and advantages it offers. According to Osterwalder et al. (2004), in this channel, it is imperative to provide all the necessary information that could help the customer make a precise decision about whether or not it is worthwhile to use the new online service. This information may include factors such as design, accessibility, usability, reliability, trust relationships and how much it costs to obtain the service.

Each of these factors is briefly discussed in the following subsections.

6.2.1 Design

An eye-catching graphic and great colours for an online service could mean the difference between a customer reading about the service offerings or sending them straight to the bin. Producing a good design is easy only if creativity is present. Something as simple and cost effective as online shopping websites like bid or buy (or Buy, 1999) or Olx in South Africa attract hundreds of customers to buy and sell products online. According to Osterwalder and Pigneur (2010), design is important but could prove to be a difficult element to measure. They further argue that a product may stand out because of superior design, i.e. a well-designed service or product is likely to attract and capture a customer's attention.

Therefore, among other things design should be given attention like any other customer evaluation factors. Of course, what design mean to an online service may differ to the design of a tangible system. However, an online service with good design but difficult to access may prove of no use or influence a customer's decisions negatively. The following subsection discusses the concept of service accessibility.

6.2.2 Accessibility

Rapidly, more and more organizations (educational institutions, companies, and government agencies) provide users and their customers with online services using a number of methods (Fang, Sheng, & Chau, 2007). For example, many institutions are implementing or have implemented web portals to provide their users and customers with online services such as an online prospectus, online admission procedures and online registration. In the case of banks, web portals provide online services such as managing personal accounts, while government web portals provide online services such as paying traffic fines (Fang et al., 2007).

With thousands of online services available today, accessing and finding a desired service is not an easy task for some users. Hence, an online service should be designed in such a way that it can be easly accessed by its associated users and customers at the time when it is needed.

6.2.3 Usefulness and Usability

Usefulness is of the utmost importance when evaluating a service, because it influences people's decision to accept or reject it. Thus, amongst the evaluation factors mentioned in this chapter, usefulness should be the determining factor. Davis (1989) provides the best argument that usefulness should go hand-in-hand with ease of use because, if customers believe that the new service is very useful but it is too hard to use their decision can be influenced negatively. He further defines usefulness as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989).

If the service is easy to use, customers will evaluate the service as a quality service because it eliminates difficulties and complexities and saves them time and effort (Shamdasani, Mukherjee, & Malhotra, 2008). For example, two new online services are developed. One requires less effort and the other requires more effort. It is obvious that the customers will accept the former over the latter. Thus, ease of use can be defined here as the least amount of effort that the customer needs to put in while increasing his or her job performance when using a newly developed service as highlighted by Davis (1989).

A service that is convenient or easier to use can create substantial value for the customer (Osterwalder & Pigneur, 2010). Dropbox, a free online service that lets customers or users bring videos, photos and documents anywhere at any time and share them easily with others with less effort, is now attracting hundreds and thousands of customers or users while also allowing them to have more space at their disposal (Dropbox, n.d).

6.2.4 Reliability

As discussed by Kim and Lee (2002) and also noticed by Lee and Lin (2005), reliability represents the ability of an online service, for example, a website, to completes orders correctly and also make sure that the user's or customer's personal information is secured at all times. In this dissertation reliability is the degree to which a service is free from errors and returns expected consistent desired output.

According to Zhu, Wymer, and Chen (2002) reliability has a direct positive effect on customer satisfaction and evaluation of an online service, especially to electronic banking systems. Hence, this factor should be well achieved when delivering a new online service to the users or customers.

6.2.5 Trust

Trust in an online service is a difficult relationship to achieve because it commonly takes place between the user or customer and the service provider who have never met before, and in an environment where the user or customer often has little or no information about the service provider or even about the service itself. According to Jøsang, Ismail, and Boyd (2007), this kind of trust forces the users or customers to pay for a service before even trying the service to see if it works for them. They further note that the service provider knows exactly "what he gets, as long as he is paid in money".

Therefore, trust in an online service could possibly be achieved by having all the service provider's details such as his website, phone number, email address, physical address and possibly social media profiles. These details allow the users or customers to connect with the service provider in the way they prefer. Some users or customers may prefer to speak with a real person over the phone, while others might research the service provider through a website before they can trust him.

6.2.6 Cost

Users or customers would want an online service that is less expensive. However, a service that is less expensive might prove to have too low quality for some users or customers. For example, if an online service is free of charge, some users or customers might not even consider subscribing to it while others may be even more interested. Maybe this behavior is also influenced by the type of environment in which the service is offered. For example, if a university offers free Wi-Fi to their academic staff members and requires a subscription before obtaining access, more users may subscribe. However, this might not be the case when an online cell phone company offers low prices for their cell phone purchases.

It is important that when any online service is deployed it should balance its cost according to two types of users or customers: those who can easily afford it and those who might have a difficulty affording it. Such a balance can positively attract both types of users or customers.

6.3 Purchase

This is the phase that provides common means of payment or making a purchase. Service negotiations, signing of contracts, and decision-making are done in this phase (Osterwalder et al., 2004). If customers find it difficult to make a payment for a service, there is the possibility of moving to other providers of the service. Hence it is important to make the transaction methods more convenient and simpler for customers.

6.4 After Sales

This channel is the most important one to users or customers, because it has the ability to create customer loyalty (Osterwalder et al., 2004). Customer satisfaction is determined in this phase as this is where problems from a new online service are likely to arise. It is imperative to have a clearly defined reporting structure in place in case of problems. The reporting structure should be easily accessible to users or customers and also provide frequently asked questions (FAQs) to help those customers who can assist themselves. However, not all the users or customers can assist themselves, hence other methods should be implemented such as a help desk, automated services and/or personal assistance.

6.5 Output from Tactical Planning

The rest of the chapter discusses Osterwalders Customer Buying Cycle in detail. Table 6.1 provides a summary of the phases that form part of the customer buying cycle. In addition, it summaries some of the factors associated with the phases in the customer buying cycle and provides a brief description of what the factors entail.

Each of the channels produces an output that the online Service Provider needs to think about when dealing with the tactical planning. These outputs are depicted in Figure 6.1.

Table 6.1: Factors to consider throughout Osterwalder's Customer Buying Cycle

Channels	Factors	Description
Awareness	Intended Auidience	A specific group of customers who might buy or use the online service
	Benefits	The real value that a customer experiences through using an online service
Evaluation	Design	The creativity that include features such as functionality and looks of an online service
	Accessibility	An extent to which a customer can obtain an online service at the time it is neede
	Usability	The simplicity of an online service that a customer can interact without putting too much effort.
	Reliability	The degree to which an online service is free from errors and returns expected consistent results.
	Trust	A belief that an online service is legitimate, good and will not harm the customer when giving out personal information
Purchase	Application Process	These are the process and procedures needed to be followed in order to obtain a particular service.
	Delivery Methods	Means of making an online service available to customers whether using the Internet or face-to-face interaction.
	Fee (Cost)	An amount that a customer needs to pay in order to obtain an online service.
After Sales	Help desk	A point of contact when a customer fails to use an online service.
	FAQ	These are common questions that customers frequently asked about an online service written on a website.
	Personal Assistance	A dedicated person assigned to assist a customer.

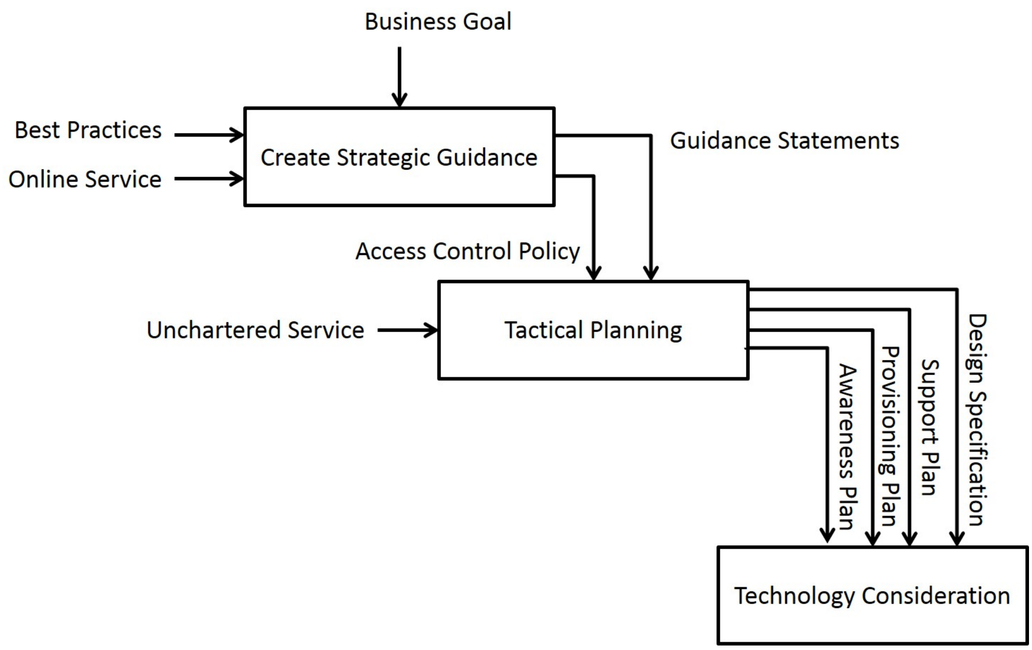


Figure 6.1: Tactical Planning Summary Outputs

Figure 6.1 shows that tactical planning is controlled and directed by the access control policy created by the strategic layer. When chartering an online service, tactical planning is in good position to:

1. Provide a strategy for making customers aware of the online service by means of an awareness plan.
2. Influence the customers' decision by creating a design specification.
3. Specify the way that an online service is provisioned through a provisioning plan.
4. Influence the way that after sales take place through a support plan.

The following subsections discuss the output produced from the phases in more detail.

6.5.1 Awareness Plan

Online Service Providers want their online services to be utilised effectively. Table 6.1 shows two factors to consider when creating an awareness plan. Firstly, the intended audience is considered which helps address the awareness plan to the right audience. Secondly, a value proposition that explains how the online service offered solves the customer's problem, i.e. how it delivers specific benefits to the customer is created.

However, telling customers that an online service exists and explaining the benefits attached to the online service might not be enough. Other phases of the customer buying cycle must be incorporated as part of the awareness plan to give more information about the online service offered. Such information can provide additional understanding about the offered online service to the customer.

Information about how easy to use the service is and how it could improve or solve the customer's problem must be included in the awareness plan when for the customer is evaluating the online service.

Once a customer has a better understanding of the online service, he or she would like to "purchase" the service. All the purchasing processes must be communicated to the customer, whether there is an amount required to purchase an online service or not. Therefore, in the awareness plan, purchasing processes and procedures can be included.

Since it is the first time that the customers will be using an online service, problems after purchasing an online service are likely to exist. It is important to explain all the after sales support strategies during the awareness campaign and therefore they must be part of the awareness plan.

Once all the details needed in the awareness plan are outlined, the online Service Provider needs to define the design specifications. This is further discussed in the following subsection.

6.5.2 Design Specification

The design specifications can help to clarify the kinds of questions that the potential customer would ask when evaluating the value of an online service. Obviously, the online Service Providers would want the customer to make a favorable decision regarding their online service. Table 6.1 identifies five factors to consider during the customers' evaluation of an online service and these factors should be in the design specification document.

The design factor plays an important role when a customer evaluates a service. Consider a situation where a service is designed creatively but fails to produce usability and utility. Such outcomes might impact the customers' decision negatively as they will find it difficult to use. On the other hand, a poorly designed service may show usefulness and utility. In that case, the customer may choose to use the online service as long as it produces the desired output. Therefore, a good design must consider all five factors highlighted in Table 6.1. An online service should be easy and simple to use without requiring the customer to put in too much effort and must return the desired consistent results to the customer.

Thus, a good design specification plan should cover all the important points that helps the customer make a favorable decision.

6.5.3 Provisioning Plan

As can be seen in Table 6.1, the purchase phase identifies three factors, namely the application processes to acquire the service, the delivery methods of channeling the service to a customer, and the fee that might need to be payed before a customer can utilize an online service.

Within the provisioning plan, contract negotiations such as license agreement methods of payment are defined. Customers must be given different options of ways to make transactions. Some customers (if it is a service that requires money) may prefer to pay via debit order while other customers may want to pay in cash. No matter what the customer chooses, they must first agree to terms and conditions which might require that they fill in an electronic form or a printed hard copy. It is therefore, important that all the information needed in the provisioning plan is defined and included.

6.5.4 Support Plan

Customers would like to have their problem solved as soon as it occurs. Table 6.1 shows three factors to consider when creating a support plan, namely the help desk, frequently asked questions, and personal assistance. Depending on the level of agreement with the customer, some customers might want a dedicated person assigned to them to whom they can refer their problem.

Therefore, it is important that the support plan explains all the communication channels available to the customer.

6.6 Conclusion

This chapter utilized four channels as outlined by Osterwalder et al. (2004) in structuring the discussion. Users of the online services should be made aware of the service, allowed to evaluate its value, provided with convenient methods of payment, and also provided with after sales support when problems exist. This was the main focus of this chapter.

The next chapter discusses the operational layer of the model.

Chapter 7

Operational Layer

The previous chapter looked at the tactical layer of the model. Of particular interest were decisions made that might have a significant influence at the operational layer. The dissertation now moves on to discuss the last layer of the model, i.e. operational layer. The primary question to be answered in this chapter is: "What are the technological requirements needed in order to support the decisions at the tactical layer which, in turn, support the decisions made at the strategic layer?"

With this question, the current chapter investigates and considers some of the technological requirements that need to be looked at when a new service such as an online service, is offered.

7.1 Overview

The introduction of new technologies into the Information Technology (IT) ecosystem is generally both interesting and concerning to IT managers, staff members, as well as external partners. With the advancement within the Information and Communication Technology (ICT) ecosystem, new technologies are being introduced and in some cases implemented with the aim of improving the customer's day-to-day activities or solving problems. The functions of these technologies range from capturing and storing information required to run the IT ecosystem such as forms, spreadsheets and databases, to more sophisticated functions such as handling user authentication details and executing tasks.

Most of these technologies have been around for some time and their strengths and weaknesses are known. However, every year, newer technologies which may come with unknown strength and weaknesses are introduced (Tan & Wang, 2010). For example, we now have seamless access to online services in seconds which was not the case before.

While these new technologies offer new possibilities, they may come with unforeseen weaknesses that may compromise the IT ecosystem security and contravene with IT policies. Therefore, careful consideration is necessary before choosing to implement these new technologies, especially if they the potential to impact the IT functions negatively. These considerations could be to take a holistic view of the new technology and to investigate the impact of introducing the new technology, security issues, costs involved and the time needed to market the new technology.

The next sections briefly consider the nature of each consideration in more detail.

7.2 Look at a holistic view of the new Technology

"Techology is just a tool" (ACE, n.d). Any kind of a tool needs a driver (end user). When a technology is about to be deployed to its intended environment, it is important to consider the whole view of the environment. For example, if the technology is offering online services, people (both the provider and the customer) involved should have the necessary skills to use it.

The technology may come with policies or be deployed in an environment where there are policies that need to be acknowledged before the new technology can be offered. Such polices should not be overlooked as there may be penalties once they are breached. Therefore, a holistic view is important not only for the functionality of a new technology but also for the selection of a new technology.

7.3 Consider the impact of introducing the new Technology

When a new technology is being considered, either to be implemented or to replace an old one, it must be assessed to evaluate the potential impact on all people involved.

Once the system or technology is implemented, it must be managed to ensure that problems do not occur and all functions can continue effectively. Furthermore, some strategies to minimize the impact on a new technology are as follows:

- Allow more time for implementation.
- Keep in mind that implementation of a new technology often takes longer than expected.
- Schedule enough time to thoroughly test the new technology.
- Provide training for staff and users as needed.

These strategies discussed by ACE (n.d), ensure that the potential negative impact the new technology may have is minimised to an acceptable level.

7.4 Consider the security issues

Security has become a problem in the IT ecosystem and is increasingly concerning to both Service Providers and their associated Customers. As new concepts such as the Internet of Things (Tan & Wang, 2010) come into life, more and more security issues are manifesting.

Service Providers need to ensure that unauthorized people cannot gain access to their services. The most common mechanisms existing today to protect against unauthorized people include passwords, biometrics, and other verification methods (these where discussed in Chapter 2). An unsecured technology is unlikely to be used by customers.

7.5 Consider the technology costs

Cost is a factor for most profit organizations. Introducing a new technology can increase or decrease cost depending on the nature of the service provided. The new technology might need to be maintained over time. One needs to do a proper comparison, i.e. look at the expenses to maintain the existing technology or acquire a new technology.

Cost is one factor to consider when aiming to make a profit. However, there are many other factors to consider. It could be worthwhile to consider a new technology if it improves service delivery and it might be better to spend money on it than on maintaining the old technology.

The early stages of acquiring the new technology could prove to be expensive. however it may bring more profit later, if the online service is offered successful. Therefore, when considering new technology, one needs to look further than cost and making a profit now, and plan for the future.

7.6 Infrastructure

Infrastructure when offering a new technology needs to be considered to ensure that the technological solution is operating as expected. The infrastructure may include a physical environment, software and hardware packages, and the necessary skills required to operate the technology. These are expanded on in the following subsections.

7.6.1 Environment

The environment in which the technology will be operating should be in accordance with the requirements of the technology offered. Some of the requirements include temperature levels and humidity levels.

7.6.2 Hardware Components and Software Packages

These are computing devices that lay the foundation before any technological solution is offered. These may include severs, personal computers, printing devices, and communication equipment, just to name a few. The use of hardware in any technology offering plays an important role. However, in many cases, hardware might not operate on its own without installing the right software package. Therefore, hardware needs to be coupled with the proper software packages.

7.6.3 Technical Skills

Technology is no use without human intervention. It needs the availability of skilled personnel to operate the technology. Therefore, people are the driving factor for the technology. However, having people without the necessary skills to operate the technology also becomes a problem.

Therefore, training might be required or new staff members may be hired. Of course, this comes with costs and may also be time consuming, especially in a demanding environment such as, for example, a bank.

7.7 Output from the Operational Layer

The rest of the chapter discussed technology considerations. Table 7.1 provides usefull questions that the operational managers need to ask when considering implementing a new technology in the existing network infrastructure.

Table 7.1: Questions to ask at the Operational Layer

Technology Consideration	
Considerations	**Questions to ask**
Hardware Components	What type of hardware components do we require?
Software Packages	What software packages do we need?
Security Configurations	What impact will the configuration of the new security protocols have on our existing network infrastructure?
Consortia	Can we possible join existing consortia who provide solutions to online services?
Technical Training	What training needs to be in place on a technical level?

Each of the questions in Table 7.1 provides an output that the operational managers need to think about when dealing with technology implementation. These outputs are shown in Figure 7.1.

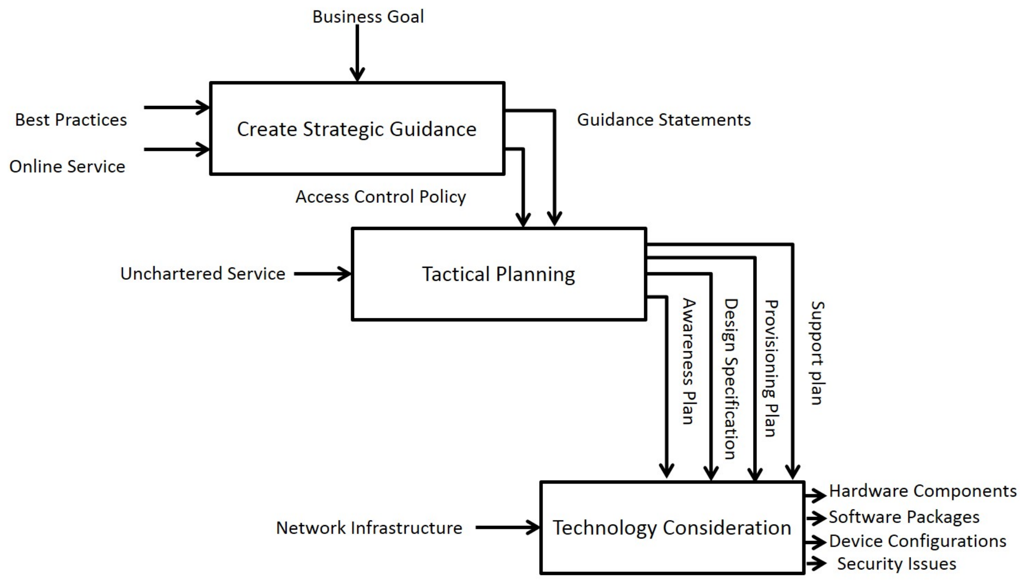


Figure 7.1: Operational Layer Summary Outputs

Figure 7.1 shows that the operational layer is controlled by the outputs provided by the tactical layer. When considering implementing a specific technology, certain hardware components, software packages, and configuration tasks need to be investigated, identified, and executed. The existing network infrastructure and the impact the change will have on it must be kept in mind.

7.8 Conclusion

This chapter discussed the technological considerations at the operational layer of our model. It emphasized the importance of looking at the whole picture when a new technology is offered. This chapter also marks the end of the proposed multi-faceted model.

The next chapter demonstrates the effectiveness and utility of this model in the South African National Research and education Network (SANReN) which offers the eduroam service.

Part III

Model Demonstration: A Use Case

Chapter 8

eduroam Use Case

Part II of this dissertation is dedicated to developing a multi-faceted model to support authentication and authorization for online services. The model is labelled as multi-faceted in nature as it looks at three layers when addressing authentication and authorization for online services. These layers were conceptually positioned in Chapter 4 and later discussed in detail in Chapters 5, 6 and 7.

This chapter uses outputs from the model layers discussed in Chapters 5, 6 and 7 to verify that the proposed multi-faceted model has the potential for practical use in real-world circumstances. The chapter commences by discussing the purpose of the Use Case and indicating the service in which the proposed multi-faceted model will be applied.

8.1 The Purpose of the Use Case

The purpose of the Use Case is to ensure that the proposed multi-faceted model has utility and is beneficial to online services. In order to show such utility, this dissertation argues that the eduroam facility represents a complete IT ecosystem architecturally and is a suitable environment that collaborates with multiple service providers online. Therefore, the research study uses the eduroam facility as a Use Case scenario.

The following sections will discuss the eduroam service in detail before the multi-faceted model is applied.

8.2 What is eduroam?

eduroam stands for **EDUcation ROAMing**. It is an inter-institutional roaming facility for users (academic staff members, researchers and students) from participating institutions. The users have Internet access at all other participating visited institutions and at their home institution when using the credentials provided by their home institution (López, Cánovas, Gómez-Skarmeta, & Sánchez, 2008).

8.3 The Origin of eduroam

The eduroam facility started in 2002 as an idea from Klass Wierenga during his employment at SURFnet, the Dutch National Research and Education Network (NREN) organization (TERENA, 2012). The idea was to combine a RADIUS-based infrastructure with IEEE 802.1x technology for roaming Internet access across institutions in Europe (Wierenga & Florio, 2005).

What triggered his idea was "*the fact that whenever I visited a university I had to register my wireless card or borrow one from the local IT department to get online*". Based on this, he then realized that "*there was no reason why visitors from SURFnet-connected institutions should not get access to the campus and SURFnet network*" (TERENA, 2012). On 30 May 2002 he emailed the idea to a group of experts within the European NREN community who were part of the TERENA Task Force on Mobility which is now called Mobility and Network Middleware (TF-MNM) (Wierenga, 2002). According to Klass "*it was the perfect place to get feedback and improve on a half-baked idea*" (TERENA, 2012).

The actual eduroam implementations started in 2003 within the TERENA Task Force on Mobility (now TF-MNM) (eduroam, 2015a). Initially, many institutions showed an interest in eduroam by joining. Those institutions were from the European continent. They included the Netherlands, Finland, Croatia, the United Kingdom, Portugal and Germany (de Groot, 2004). Later, other NRENs in Europe began joining what was then named eduroam (**EDU**cation **ROAM**ing) (eduroam, n.db). It was not long before eduroam went global, in December 2004, that Australia became involved and was the first non-European country to join eduroam (TERENA, 2004).

8.4 The eduroam Infrastructure

The eduroam facility is based on hierarchically organized RADIUS proxy servers (Willens, Rubens, Rigney, & Simpson, 2000) and the IEEE 802.1x technology as the authentication method (Milinović, Winter, & Florio, 2008). An abstracted overview of RADIUS authentication servers and the IEEE 802.1x technology is discussed in the following subsections:

8.4.1 Hierarchy of RADIUS Servers

RADIUS servers are the brains of the eduroam facility. Their role is extremely important as they are responsible for proxying authentication requests from one server to another, whether locally, nationally or globally. The eduroam facility makes use of three levels of RADIUS proxy servers, namely the top-level server called Confederation, the national-level servers called Federation, and the institutional-level servers called Edge (Wierenga et al., 2006), as shown in Figure 8.1.

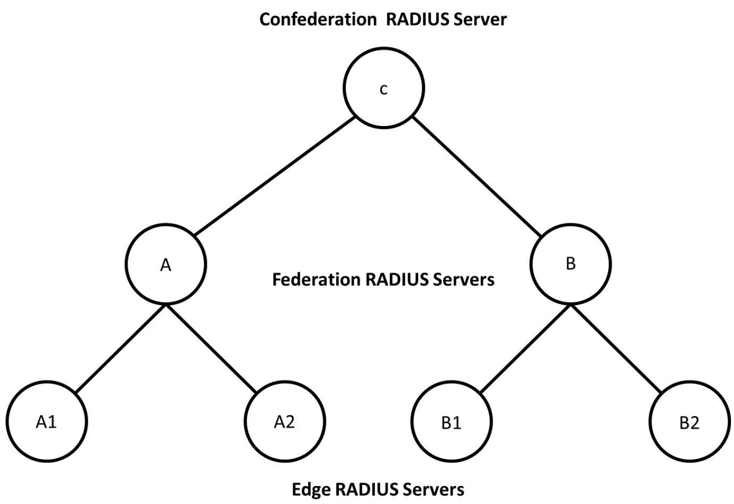


Figure 8.1: Three Levels of RADIUS Proxy Servers

The *Confederation Server* acts as the bridge between *Federation Servers* for global communication. The *Confederation Server* in one region has a view of all other eduroam participating *Confederation Servers*. Each continent should have a *Confederation Server*, also known as a regional server. This *Confederation Server* may in turn connect to other regional servers to allow global communication. In the absence of an African *Confederation Server*, South Africa is presently connected to the European eduroam *Confederation Server* (TENET Board, 2012).

As seen in Figure8.1 the *Confederation Server* follows the *Federation Servers* which connect to the *Confederation Server*. These *Federation Servers* have the complete list of all the eduroam participating institutions within a country and they are responsible for providing authentication to its local users in that country (Wierenga et al., 2006).

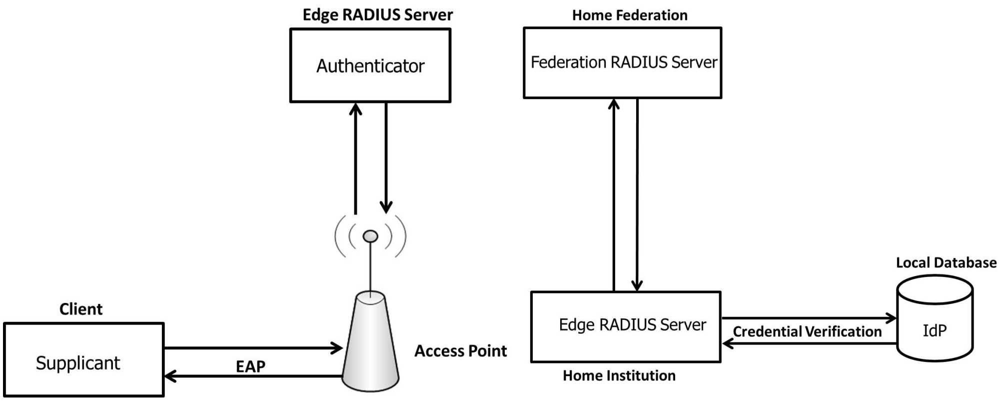
At the bottom of the hierarchy are the *Edge Servers*. Every institution wanting to join eduroam connects to its *Federation Server* and deploys a dedicated *Edge Server* for eduroam.

Since these RADIUS servers are proxying the requests to other servers, they need to know the destination of each request. This is achieved by looking at the realm part of the user's username without interfering with the message itself. The realm is the suffix within the username delimited by '@' and originates from the users home domain name (DNS) (Wierenga et al., 2006). For example, a user coming from institution 'A' will have a realm part of @A.ac.za. This is used to determine that the request is routed to institution 'A'. It is the responsibility of the home institution to determine the prefix of the username. Using the example above, a complete username would be 123456789@A.ac.za.

In summary, this hierarchy of RADIUS servers proxies the user's requests from any eduroam-participating institution to their home institution and back for authentication, this will be discussed in section 8.5.

8.4.2 IEEE 802.1x Technology

As previously mentioned in subsection 8.4.1, eduroam uses the IEEE 802.1x technology as a method for authenticating the user when at home or visiting other eduroam participating institutions. The IEEE 802.1x technology authentication in eduroam requires three components (Winter et al., 2008): a supplicant, access point and authentication RADIUS server. This is illustrated in Figure 8.2. A supplicant is software that uses the 802.1x protocol to automatically send users authentication requests to the access point (AP) using the Extensible Authentication Protocol (EAP) (Winter et al., 2008). The EAP provides integrity and confidentiality to protect the transportation of user credentials throughout the hierarchy of RADIUS servers (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004). The access point provides wireless access to eduroam user's and forwards the users authentication request to the institutional RADIUS server which in turn proxies the request according to the realm part of the username.



(a) supplicant Software Authenticate (b) Verification of User credentials

Figure 8.2: The IEEE 802.1x Authentication Process based on (Winter et al., 2008)

The user's authentication request travels through the hierarchy of RADIUS servers to the home institution for authentication. Once the request reaches the home institution, it is forwarded to the *Local Database* which is under the supervision of the *Identity Provider (IdP)* as shown in Figure 8.2b. The request is then authenticated and the user's credentials are verified.

8.5 How eduroam Works

As previously discussed, eduroam provides a secure facility that allows academic staff members, researchers and students from any eduroam-enabled institution to have Internet access at other eduroam-enabled institutions world-wide. The basic concept of eduroam is that the authentication credentials of users are verified by the home institution using their own preferred method of authentication, while authorization required to obtain Internet access is done by the visited institution (Cánovas, Gómez-Skarmeta, López, & Sánchez, 2007). This not only achieve the security but also allows for the flexibility of roaming users. In other words, roaming users will have their familiar environment when logging in to the eduroam facility while visiting anathor institution. Typically, a hierarchy of RADIUS servers is used to route the authentication request of the user from the visited institution to their home institution for validation of credentials and the response is sent back using the same route in reverse order (Milinović et al., 2008).

Currently, each institution provides a RADIUS server connected to the home local user database which and is linked to the national-level RADIUS server. This is enough to provide national eduroam service. However, if the user is visiting an international institution, the national-level RADIUS server connects to a top-level RADIUS server.

Consider an illustration of how eduroam works in Figure 8.3. A user, whose home institution is `institution_B` (home institution). wants to connect to eduroam at `institution_A` (visited institution). In this case, the supplicant software of the user contacts the Access Point (AP) using 802.1x with the EAP (Extensible Authentication Protocol).

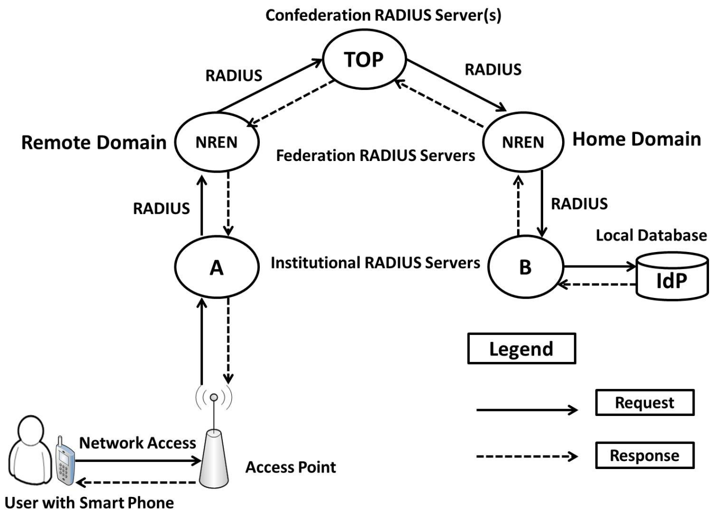


Figure 8.3: How eduroam Works

The AP contacts its local RADIUS server for authentication. The RADIUS server examines the realm part of the username and, as it is not a local realm in this example, proxies the request through the hierarchy of RADIUS servers until `institution_B` is reached. The RADIUS server of `Institution_B` decapsulates the EAP message and sends the credentials to the local user database for verification. Then, the local user database can either accept or deny the request by proxying the results in reverse using the same path. The AP at `institution_A` informs the user of the outcome ('accept' or 'deny') and the connection is established (if the response is 'accept'). Now the user can have Internet access at `institution_A`.

8.6 eduroam Deployment

This section discusses eduroam deployment in world-wide and South Africa.

8.6.1 World Wide

The eduroam facility started in Europe, and has now spread throughout academic and research institutions world-wide and, at the time of writing, is available in 74 countries (eduroam, 2015b). However, it is only accessible at certain locations within those countries, provided that their Roaming Operator (RO) or NREN has agreed and signed the eduroam Compliance Statement (TERENA, 2011).

It is important to note that there may be other countries that are still in the process of getting involved (pilot deployments) all over the world.

8.6.2 In South Africa

In South Africa, eduroam is currently accessible in 8 out of 9 province. Within each province, eduroam is available at universities and research institutions as illustrated in Table 8.1

The following section discuss the eduroam day-to-day operation.

8.7 eduroam Day-To-Day Operation

The eduroam service can be provided at three levels, namely local, national and global level. The local level is provided for by the eduroam enabled institutions (universities). At the national level, the National Research and Education Networks (NRENs) take care of the service. At the global level, the service is under the umbrella of TERENA (Yamaguchi, Suzuki, Goto, & Sone, 2010). National Research and Education Networks (NRENs) focus

Table 8.1: eduroam in South African universities and research institutions

eduroam Participating Institutions		
Province	City/ Town	Institution
Eastern Cape	Alice	University of Fort Hare
	Grahamstown	National Research Foundation
	Port Elizabeth	Nelson Mandela Metropolitan University
Free State	Bloemfontein	University of Free State
	Welkom	Central University of Technology
Gauteng	Johannesburg	University of Johannesburg
	Pretoria	Council for Scientific and Industrial Research
	Roodepoort	Monash South Africa
KwaZulu-Natal	Khandisa	University of Zululand
	Westville	University of KwaZulu-Natal
Limpopo	Polokwane	Tshwane University of Technology
Mpumalanga	Emalahleni	Tshwane University of Technology
	Nelspruit	Tshwane University of Technology
North West	Potchefstroom	North West University
Western Cape	Cape Town	Cape Peninsula University of Technology

on providing Internet connectivity to the research and educational networks within a country (TERENA, 2010) while acting as service providers to the research and educational communities.

Most of these NRENs around the world are under the direct control of government (Pinxteren, 2013), i.e eduroam in each country is managed and monitored by the NREN of that country. In South Africa, the NREN that is responsible for providing eduroam services to its beneficiary institutions is called SANReN (South African Research Network). SANReN is a Pretoria-based initiative of the CSIR (Council for Scientific and Industrial Research) under the Meraka Institute. Their main goal is to provide clients with high-speed network connectivity and to connect them to research and education communities all over the world (SANReN, n.d.).

8.8 eduroam Problem Identification

In eduroam, after the user has been successfully authenticated by the home institution and the response has been received by the visited institution allowing network access, authorization needs to take place (Tekeni, Thomson, & Botha, 2014). Authorization is an agreement between two entities which approves all rights received to use or access a specific service or a set of services (Thomas & Sandhu, 1997). The user is authorized using an IP address of the visited institution to access an online service. Thus, this kind of authorization can be referred to as an IP-based authorization process. This section discusses the effects that IP address authorization could have on the eduroam users. This is achieved by providing an illustration of when the user is accessing the Internet at his/her home institution and an of when visiting a remote institution.

8.8.1 Users at Home Institution

Figure 8.4 below shows a situation when a user is at his/her home institution using eduroam.

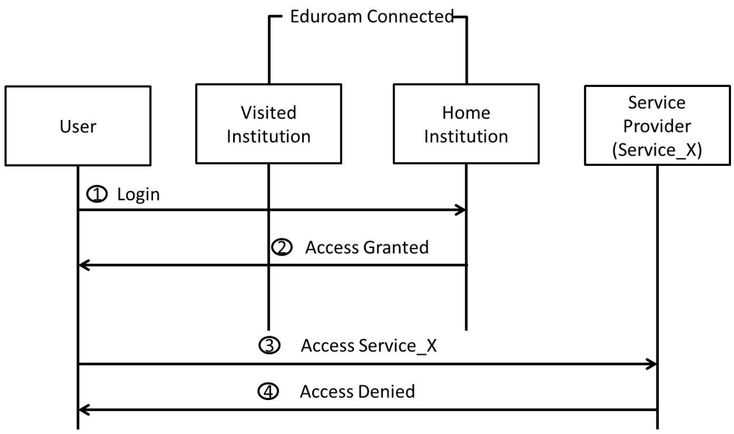


Figure 8.4: eduroam Access at Home Institution

When the user accesses eduroam at the home institution and tries to access a service which the institution does not have access to, the following happens:

1. The user tries to login at the home institution using his or her credentials and the EAP message is carried to the home server.

2. The home institutional server decapsulates the message and verifies the user's credentials. It sees that the user is the home user, assigns an IP address and grants Internet access.

3. The user accesses the service provider's resource (`service_x`) using the assigned IP address.

4. The service provider verifies the validity of the IP address, discovers that the received IP address has no subscription to access the service and denies access to the user.

Therefore, the user does not have access to `service_x` at home (home institution). However, when visiting another institution that does have a subscription to the same `service_x`, the user will be able to access that service without requesting authorization to it, as will be discussed in the following subsection

8.8.2 Users at Visited Institution

Once the user reaches the visited institution, the IP-based process starts for authentication and authorization. Figure 8.5 shows home and visited institutions and their service provider.

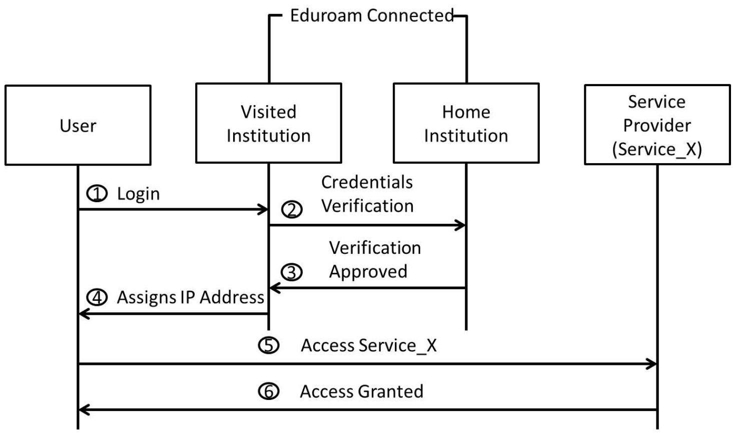


Figure 8.5: eduroam Access at Visited Institution

When the user reaches the visited institution and connects to eduroam, the following happens:

1. The user tries to login at the visited institution using his or her home credentials.

2. The visited institution examines the realm part of the username and sees that the user belongs to the home institution. It then sends the user's credentials to the home institution through the hierarchy of RADIUS servers for authentication (verification) to the home institution.

3. The home institution decapsulates the message and verifies the users credentials. It can either accept or deny the request by sending back the response to the visited institution.

4. The visited institution receives the response, grants Internet access if the results are positive (accepted), and assigns an IP address of the visited institution to the user.

5. The user accesses the service provider's resource (`service_x`) using the assigned visited institutional IP address.

6. The service provider verifies the validity of the IP address and gives permission to the user based on the provided IP address (visited institutional IP address).

Therefore, it can be argued that when a user who does not have the necessary accesses `Service_x`, it present a potential risk to the visited institution. This is for the reason that the visited institution might be held responsible for not ensuring that access to `service_x` is only given to those users covered by the SLA.

The next section states the problem found in the eduroam facility and also provides a definition statement of the problem.

8.9 Problem Statement

Some services such as digital libraries at Institutions use an IP address to authorize users. This presents a potential problem when using eduroam because the eduroam user receives an IP address in the range of the visited institution and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize users via an IP address of the visited institution could result in an unauthorized user gaining access to certain services of the visited institution.

Therefore, the problem introduced by the eduroam facility can be stated as follows: **The current deployed eduroam infrastructure is lacking adequate access control to services that authorize users via an IP address.**

To address this problem, SLAs should be looked at to investigate what they stipulate concerning IP address authorization. This is discussed in the next section.

8.10 What Do SLA's Stipulate?

As stated in subsections 8.8.1 and 8.8.2, when a user accesses an Internet resource while connected via eduroam he/she may not have access to some Internet protected resources while at home. The lack of access to those resources could be due to the fact that his or her institution has no subscription to that particular resource. However, eduroam allows users to have Internet access at any other eduroam participating institution. If the visited institution has a subscription to all Internet resources, which are unavailable at a the user's home institution, this may impact the visited institution negatively. Hence, this section aims to look at what the typical Service Level Agreement (SLA) between an institution and Service Providers states. After that, an example is considered where the authorization may breach the SLA set forth by the Service Providers.

The growth of the Internet and the increase of services available online have forced organizations to outsource some of those services (Huai, 2010) to accommodate their users' needs. When an organization outsources a particular online service, a contract between the organization and the Service Provider is signed. This contract is called a Service Level Agreement (SLA) (Schutz et al., 2013). A "SLA is a contract between a user and a provider of a service specifying the conditions under which a service may be used" (Sandholm, 2005).

Expectations between the organization and Service Providers are stipulated through SLAs. In this research study the "Digital Library Database access" is used as an example between institutions and their Service Providers. This is because most of these Online Digital Library Databases use IP addresses to authorize users. In the quest of uncovering what the stipulation addresses, three of the SLAs were reviewed. The main message of each of these SLAs were all the same."Walk-In Users may not be given means to access the Licenced Material when they are not within the Library Premises". One of the SLAs extracted from the South African Library Consortium Site License

Agreement with Emerald is shown below:

"Authorised Users" means individuals who are authorised by the Licensee to access the Licensee's information services whether from a computer or terminal on the Licensee's Secure Network, or off site via a model link to a valid IP address on the Licensee's Secure Network and who are affiliated to the Licensee as a current student, faculty member or employee of the Licensee. Persons who are not a current student, faculty member or an employee of the Licensee, but who are permitted to access the Secure Network from computer terminals within the Library Premises ["Walk-In Users"] are deemed to be Authorized Users, only for the time they are within the Library Premises. Walk-In Users may not be given means to access the Licensed Material when they are not within the Library Premises.

This SLA clearly states that "Walk-In Users" should only be given access to Licensed Material from computer terminals within the physical Library Premises. However, with the existence of wireless Internet and eduroam, the stated SLA can be considered old-fashioned. eduroam users coming from other participating eduroam institutions would not be categorized as "Walk-In Users" if they connect via eduroam and access the Licensed Material. They may breach the SLA. Of course, this is assuming that the eduroam users access the Service Provider's resources using an IP address registered on the Service Provider's database. The flexibility offered by eduroam comes at the expense of security. Thus there is tension between security and flexibility. The following section discuss the risks of IP-based authorization.

8.11 The Risks of IP-based Authorization

The previous section looked at what the typical legal agreements between the institutions and their associated Service Providers stipulate regarding authorization using IP addresses. It further revealed who can have access to the protected Licensed Material and from where. This section looks at the risks associated with IP-based access from the Digital Library services perspective. This research study explores the risks from different stakeholder perspectives in order to better understand them. Such perspectives include the Users, the Service Providers and Libraries at Institutions.

8.11.1 The Users

eduroam was introduced with the goal of enhancing the flexibility of the roaming user's experience, by ensuring Internet connectivity wherever the user roams, provided that the visited institution also participates in eduroam. This, with IP-based authorization services, the introduction of eduroam creates a tension between flexibility and security. When Users visit any eduroam participating institution, they could have access to Internet services such as Digital Library services that they normally do not have at their home institution. Therefore, the users are happy because they can have access to services which they have not paid for. On the other hand, unhappy Service Providers are unhappy as their service is being misused. The opposite could also be true- Users may have access to certain services at their home institution, but the service becomes unavailable when using another institution.

To better understand and clarify this, Table 8.2 illustrate a comparison of Online Digital Library Databases found at a few selected South African institutions that are eduroam enabled. As this is merely illustrative the institution names are not used.

Table 8.2: Online Library Databases at SA Institutions

Digital Library Databases	**Institution A**	**Institution B**	**Institution C**
Access Engineering	✓	✓	✓
Access Pharmacy	✗	✗	✓
AccessScience	✗	✓	✓
ACM	✓	✓	✗
African Journals	✓	✗	✗
Emerald	✗	✓	✓
IEEE Xplore	✓	✓	✓
ISI Web of Knowledge	✗	✗	✓
SAGE	✓	✓	✓
ScienceDirect	✓	✓	✓

Based on Table 8.2, it could be argued that the risks vary depending on the user's visited institution. For example, if the visited institution is "**Institution A**" and the user is coming from "**Institution C**", that user will have access to the "**ACM**" digital library database. However, at "**Institution C**" he or she is restricted and cannot access the same ACM database. The opposite could also be true. If a user from "**Institution A**" visits "**Institution**

C”, that user will be denied access to the “**ACM**” digital library database. However, if both the home institution and the visited institutions have access to a particular digital library database, this may not be categorized as a risk because the users have access either way.

8.11.2 The Service Providers

The Service Providers have the responsibility of ensuring that the service reaches the intended group of Users. If these Service Providers do not properly ensure that the service is only accessible to properly authenticated and authorized Users, they might find themselves losing a portion of their income when the users access the service unlawfully. For example, as discussed in the previous section, the User might visit a particular institution that has a digital library database which is unavailable at home with the intention of accessing it. Such a visit may present a potential risk to the visited institution as well as the Service Provider. To some extent Service Providers depend on the honesty of the Clients to whom they provide the service . If the Clients fail to enforce the SLAs set forth by the Service Providers, such failure could result in service misuse and have some potential risks. Therefore, ensuring adequate access control to such services is everyone’s responsibility.

8.11.3 Libraries at Institutions

It is common that many Libraries at universities and research institution use an IP address to provide authentication and authorization for Online Digital Library database access to Users. This is so because Libraries at universities and research institutions register hundreds and thousands of Users each year. Therefore, managing single password identities could be a challenge on its own, hence IP addresses are popular. Moreover, the setup of IP addresses is fairly easy and straightforward as highlighted in Chapter 2. However, this may present a potential risk when Users access services through the eduroam facility. eduroam Users are commonly assigned an IP address when visiting an eduroam enabled institution which allows him or her to access online services that might be unavailable at the home institution. There is no doubt that this will result in an unauthorized user gaining access to certain services of the visited institution.

Furthermore, the visited institution could breach the SLA stipulations if the Users access the Licensed Material using their own personal devices and not the Library computers located on the Library Premises as Highlighted in section 8.10 of this chapter. Libraries, therefore, are at the risk of being held legally liable. Libraries also do not want to subscribe to unused (and therefore unnecessary) services.

This section showed that there are indeed risks among the involved stakeholders participating in eduroam. The question now is how to address these risks. This is answered by the proposed multi-faceted model. Therefore, the next section considers the interactions among stakeholders and utilizes the proposed multifaceted model to address the risks identified in this section.

8.12 Model Application

To illustrate the applicability and utility of the model, the three layers that constitute the model were discussed in Chapters 5, 6 and 7 respectively and are repeated in Figure 8.6 here. This section utilises each layer in the eduroam service in order to suggest a possible solution to the problem stated in section 8.9.

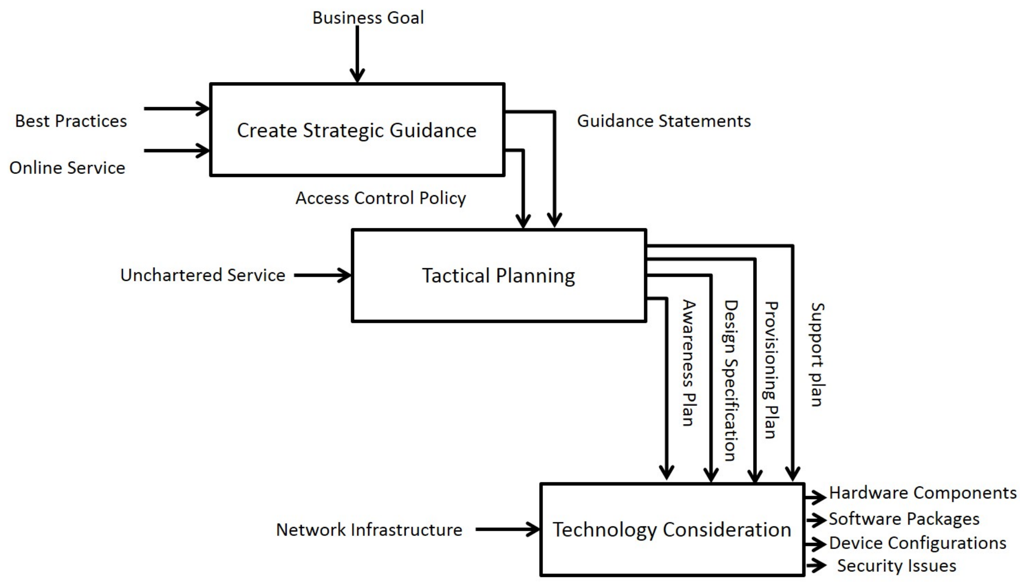


Figure 8.6: The Multi-faceted Model Layers

8.13 Strategic Guidance

In Chapter 5, the first level of the proposed multi-faceted model provided a holistic view of access control. The ITIL lifecycle access management activities were used as a framework. Furthermore, the access control views from COBIT5 and ISO/IEC 27002 were integrated in this framework.

These access control views are now applied to the eduroam facility. The eduroam facility has different role players at different levels. Hence, some of these access control views may not be applicable in eduroam. However, they might be applicable to other similar facilities, for example Cloud Computing.

The eduroam role players include NREN, Institutions, and Users. In the South African context, SANReN currently oversees the eduroam operation throughout the country. Next, consider these ITIL lifestyle activities (as discussed in Chapter 5) applied to eduroam.

8.13.1 Verifying Business Needs

The eduroam service has different role players at different levels that need to interact with one another in order to verify business needs. These eduroam role players include SANReN, Institutions and Users, within the South African context. The various eduroam role players have different relationships between them. Each relationship is briefly discussed below.

Institutions and Users

Institution establish business needs through the relationship they have with their users (academic staff members, researchers and students). As users roam between Institutions throughout the country or beyond its borders, there is no doubts that they would want to connect to the eduroam service and be able to do their work while on the move. The Institutions need to provide access to their users, whether to allow all users or a group of users to have access to the eduroam service. Currently, all users belonging to eduroam participating institutions are eligible to connect to eduroam.

SANReN and Institutions

The relationship between SANReN and Institution is crucial. In order to establish business needs, certain terms and conditions need to be acknowledged. SANReN must discuss with participating Institutions terms and conditions of eduroam use. Institutions then need to acknowledge these terms and conditions set forth by SANReN. Such terms and conditions may specify the laws and responsibilities that need to be upheld by Institutions and roaming users. For example, if the user is from a South African organization and is visiting another country, the laws of that country may be different to the laws in South Africa. In that case, it becomes the responsibility of the visiting user to become familiar with the laws of the visited country or Institution and comply with them. It is only after the signing of contracts that SANReN can deploy the eduroam service to the interested Institution.

8.13.2 Authentication

In order for users to obtain access, they must first provide a username and a password to prove their identity. This process ensures that they are valid users before permitting them to the service access. When the user visits another Institution, his or her credentials are forwarded back to his or her home Institution to be authenticated. The Institution will properly authenticate the user using a local database of registered users before sending the response back to the visited institution. Failure to properly authenticate the user may result in being denied access.

It is the responsibility of the home institution as to how users obtain their eduroam user credentials. Institutions should provide each user with eduroam credentials before they roam between institutions. As Institutions register hundreds and thousands of users each year, it is imperative that the process of obtaining the credentials is automated to ease the administrative workload.

During the authentication process, SANReN receives the user credentials from the visited institution and forwards them to the home Institution for verification and vice versa.

8.13.3 Monitoring Identity Status

The process of monitoring a user's identity status could prove to be a challenge. Each time a user changes his/her user ID or leaves the Institution, such changes need to be tracked and respond to accordingly. It is these changes that require the implementation of intrusion detection tools that will be triggered when such changes occur.

The following subsections discuss the monitoring of a user's identity status in the context of the eduroam role players.

Changes to access rights

As explained by IT best practices and major standards in Chapter 5 Activity 5.4.4, changes should be tracked by recording the date and time of the change, the type of change, and the file accessed when doing monitoring. Institutions need to be alerted when a user changes his or her password. Such a change needs to be recorded and updated to the main server storing the user credentials. In the case of SANReN, this kind of change may not be applicable, because SANReN is only responsible for forwarding the users credentials from the visited Institution to the home Institution and vice versa.

Intrusion detection tools

Anomalies and changes to the system may trigger intrusion detection tools to send an alert to the administrators of the system when a breach occurs. Intrusion detection tools are useful to network facilities such as eduroam. They can detect a breach when it happens. In eduroam, intrusion detection tools could be implemented between SANReN and all eduroam enabled institutions in South Africa. These tools could also be useful when a single user authenticates with redundant user IDs.

Prevention of redundant user IDs

As previously mentioned, eduroam uses a hierarchy of RADIUS proxy servers to forward the users' IDs to the home institution for authentication while logging in at visited institutions. Providing user IDs to the eduroam users is the responsibility of the users' home institution. This is reasonable, because the authentication of the eduroam user happens at the home institution while authorization is carried out at the visited institution.

In Chapter 5 Section 5.4.4, it is stated that access control should cater for the prevention of redundant user IDs and accounts and that the use's identity status should be monitored at all times. In the context of eduroam, institutions must ensure that the users have a single user ID to authenticate for the eduroam facility. Doing so could help simplify the complexities of identifying the user's current login status such as a lecturer, student or contractor, as such information may be needed when a breach occurs.

8.13.4 Removing and Restricting Access

In Chapter 5 Section 5.4.6 discussed the concept of giving users access rights. This activity revokes the given rights of the user whenever the need arises. This can take place when the user resigns, is suspended, or is dismissed. The removal of such rights must be done in a timely manner, especially when the user is under going the disciplinary process.

In the context of eduroam, SANReN is responsible for removing or restricting access from any institution that may be found breaching the eduroam policy. On the other hand, institutions need to keep track of the staff members who are leaving the institution due to resignation, suspension or dismissal. These users' IDs should be immediately removed from the active database. Similarly, when a particular student leaves the institution after completing his/her degree, his/her eduroam user ID must be deactivated. This may require some automatic deactivation tools.

8.14 Tactical Planning

Chapter 6 tabled factors to consider when chartering an online service. The factors were aligned with four channels as discussed by Osterwalder. This section aims to use these factors in the eduroam facility.

8.14.1 Awareness

SANReN: SANReN became aware of eduroam through TERENA's (Trans European Research and Education Network Association) Task Force on Mobility, which is now called Mobility and Network Middleware(TF-MNM) (Wierenga, 2002). As previously mentioned in chapter 1, eduroam in each country is provided by its NREN. In the case of South Africa, SANReN is responsible for it. Their job is to deploy eduroam to all the interested institutions who want to participate in eduroam. Therefore, it is their duty to make all the South African institutions aware of the eduroam facility. This is currently achieved through various methods such as contacting the institutions directly and advertising eduroam to their website(s) (SANReN, n.db).

It can be argued that SANReN has successfully spread the message to its beneficial institutions, as there are currently (at the time of writing) 8 provinces who are participating in eduroam out of the 9 South African provinces. Within those provinces there are 26 Institutions, including research institutions and foundations (SANReN, n.db).

Institutions: Once the institution becomes aware of the eduroam facility through SANReN, it remains their responsibility to make their users aware of the eduroam facility as well. Most (if not all) academic institution in South Africa that participate in eduroam have advertised eduroam through their institutional website(s), for example at Nelson Mandela Metropolitan University (NMMU, n.d). This method of getting end users' attention may be effective since academic institutions have hundreds of students including staff members. To spread a message in this environment could be challenging, especially because it is very common for an academic institution to have two or more campuses. Other methods of getting the message across to end users could include advertising through posters in different campuses of the institution, e-mails to the institutional community, or promotions such as printing T-shirts with the name "eduroam" written on them.

End users: When accessing today's technology or the Internet, usernames and passwords are often required. In the case of an academic staff member, a researcher or a student visiting a remote institution, guest accounts are often provided in order to gain Internet access to the remote institution's network. However, the creation of guest accounts is time consuming and the difficulties of connecting to remote networks and dealing with unfamiliar systems are frustrating. Visitors need to remember extra passwords, which may hinder one of the goals of academics: "to do what they do best research and educate" (GEANT, n.d). The creation of guest accounts undoubtedly frustrates users when they travel to another institution.

Hence, when end users hear about the eduroam facility, there is no doubt that they would like to try it. They use it to avoid frustrations as it allows academic staff members, researchers and students from participating institutions to have Internet access at any other participating visited institution using the credentials provided by their home institution (López et al., 2008).

8.14.2 Evaluation

Once the NREN of a country, institutions, and end users are aware of eduroam and have identified that eduroam could impact them positively, they will want to know more about the eduroam facility such as what benefits and advantages it offers. According to Osterwalder et al. (2004), in this phase, it is imperative to provide all the necessary information that could help the customer make the correct decision regarding whether or not it is worthwhile to use the facility. Hence, the following discussion will help these role players to decide whether it is worthwhile to use eduroam.

What SANReN Offers to Institutions

When a normal end user (non-eduroam user) visit another institution, the visited institution's network administrators are faced with the challenge of performing management duties such as creating end user guest accounts from a centralized interface. They have to provide administrative control to ensure that only authorized end users are connected to their network and also provide end users with permissions to limit the resources that the they can access while connected to their network. The creation of guest accounts provides security control on the visited institution's network. However, it can be argued that this increases the workload of the network administrators as they also have to deal with their internal end users.

However, if an institution is participating in eduroam, half of the workload and implementation cost is reduced. This is because the implementation cost and maintenance of eduroam is very low. The facility results in noteworthy cost savings through the reduced network administrators' workload (eduroam, n.da). Benefits and advantages include, but are not limited to the following:

1. End users login using their home credentials. This removes the need to supply guest accounts and reduces the administrative and support burden enforced by the movement of academic staff members, students, and researchers between institutions.

2. Flexibility is provided to academic staff members, students and researchers.

3. Visited institutions' network administrators only worry about their own end users.

4. Scalabilitity is provided. Authentication is done at the home institution, while authorization is performed at the visited institution.

"*With eduroam, your campus becomes a more attractive venue for meetings and conferences, as it allows participants to access the network without assistance, and without tying up your facilities*" (eduroam, n.da).

What Institutions Offer to their End users

eduroam complements the end users' desire to have their familiar environment and some services and rights available to them whenever they travel from one institution to another (Florio & Wierenga, 2005). This facility automatically authenticates the end user's device whenever he/she enters the eduroam coverage area across campuses provided that the end user chose *Connect automatically* during the setup process. This means that you can "just open your laptop or smartphone and be online" (GEANT, n.d) without the need for user intervention. Connecting to eduroam only grants visitors Internet access. Depending on the policies of the visited institution, the visitor may have some additional resources available to him/her. After being successfully authenticated and authorised to access the Internet, the user will be able to access e-mails, share resources and catch-up on studies while traveling.

In eduroam, whenever the user roams, he/she uses only one password which helps access hundreds of locations in seventy-four countries worldwide (eduroam, 2015b). This kind of access to eduroam is provided at no cost to end users. This means eduroam is free of charge. As long as your home institution participates in eduroam you will be able to experience the advantages and benefits of eduroam.

8.14.3 Purchase

SANReN: SANReN is a national eduroam roaming operator for the South African academic and research institutions. In order for these institutions to add the eduroam facility to their campuses, SANReN needs to sign an eduroam Compliance Statement (TERENA, 2011). The eduroam Compliance Statement provides a brief outline of what is required from the roaming operator of a particular country including the minimum technical and organizational standards for roaming operators such as SANReN. This statement was written by the creators of eduroam, TERENA (Trans European Research and Education Network Association) (TERENA, 2003).

Institutions: Once SANReN signs the eduroam Compliance Statement, they are eligible to offer the eduroam facility to all the interested academic and research institutions throughout South Africa. Eligible institutions who want to join and provide the eduroam facility in South Africa should approach SANReN (TENET, 2012). SANReN will require that an authorized representative personnel of the interested institution signs the South African national eduroam policy (TENET, 2012), before proceeding to configure and deploy the RADIUS server(s) for forwarding end users requests and replies. Thereafter, the representative personnel member from each institution should subscribe to the South African eduroam administrators and operations list for approval (SANReN, n.da).

End Users: For end users to connect to eduroam, usernames and passwords are required. It is the responsibility of the home institution to create and provide user accounts for their local end users. However, eduroam recommends that the username should have two parts: the prefix and the suffix (always referred to as the realm part of the username) (Milinović et al., 2008). The prefix is determined by the home institution using their preferred method and the suffix is derived from the institution's Domain Name Server (DNS). For example, an eduroam username of s123456789@nmmu.ac.za, where s123456789 is the prefix of the username and the @nmmu.ac.za is the suffix of the username. It is this suffix that enable the eduroam RADIUS proxy servers to forward an end user's request from the visited institution to the home institution. In other words, the suffix locates the end user's home institution, where the request is forwarded for authenticity.

Since institutions have hundreds or even thousands of end users, the provision of eduroam usernames and passwords could be a challenge. Hence, some institutions allow their end users to login with their original passwords that were given to them during their registration to the institution. Their institutional e-mail address is used as a username, since it has the DNS of the institution (NMMU, n.d).

8.14.4 After Sales

In this section, the end users problem escalation from the end users themselves, to the institution, through to the NREN of a country and possibly the visited institution and their NREN, is discussed, as shown in Figure 8.7.

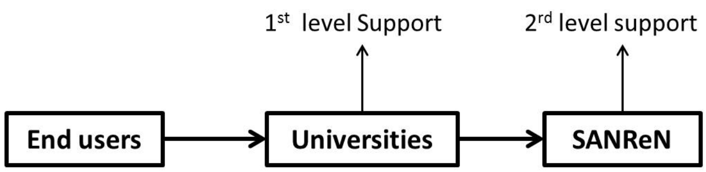


Figure 8.7: eduroam National Problem Escalation

This only applies when the problem is within the same domain (Country). In other words, two institutions linked by the same NREN. However, when the problem goes beyond the NREN of a country, other NRENs could get involved, for example, the visited institution and their NREN as can be seen in Figure 8.8.

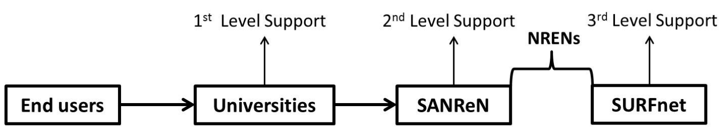


Figure 8.8: eduroam International Problem Escalation

It is important to note that the reporting process might not be as sequential as it is in the above cases. Currently, the eduroam policy states that end users must report problems to their internal IT service/ help desk (TENET, 2012). However, this can be argued against because when end users travel internationally, this kind of reporting might not be accessible to them. A more flexible solution could be to report to any available IT service/help desk. That IT service/help desk wwould become the one to contact the home Institution of the visiting end users.

Consider the two scenarios below that involve End Users, Institutions (Home and Visited), and their NRENs. These Scenarios are based on (Milinović et al., 2008) and provide an overview of the end user support delivery structure. Depending on the problem reported by the end user, other role players could be used as an escalation point to help solve the problem.

Firstly, consider the problem escalation which involves the end user and the institution in Figure 8.9.

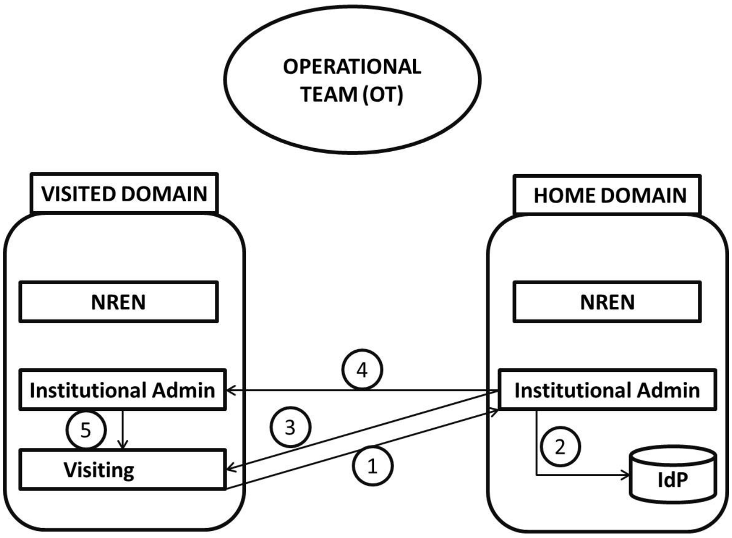


Figure 8.9: Problem escalation between the End User and the Institution

In this scenario, an end user reports difficulty accessing the network while using eduroam from the remote institution. The end user might perform the following steps in reporting the problem:

1. The end user communicates with the home institution and ask for assistance from the institutional administrator.

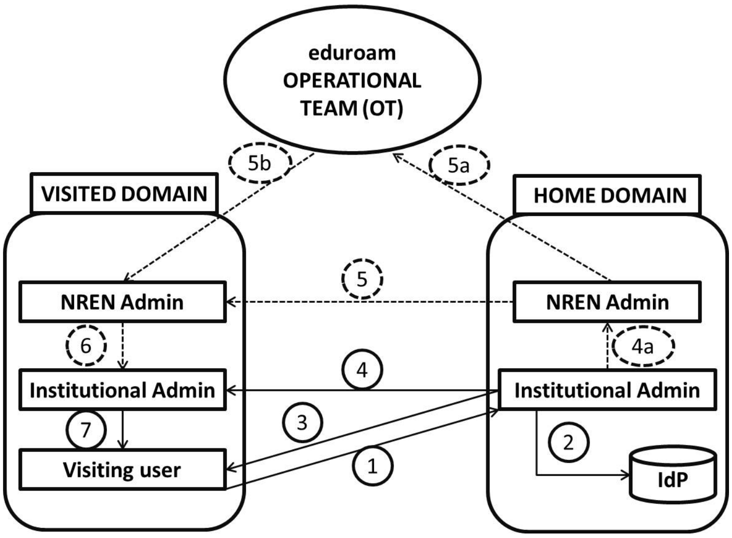


Figure 8.10: Problem escalation between the End User, Institution, NREN(s) and OT

2. The institutional administrator at the end user's home institution will check the legitimacy of the end user's credentials.

3. If there is a problem with the validation of the end user's credentials, the institutional administrator will communicate with the end user and help to set up the end user's device.

4. However, if the institutional administrator discovers that the problem has to do with the visited institution's network, for example, no proper authentication requests were received, the visited institution is consulted to provide the necessary help.

5. If necessary, the institutional administrator at the visited institution will communicate with the visiting end user to solve the problem.

Secondly, consider the problem escalation which involves the end user, Institution, NREN(s) and possibly the eduroam Operating Team (OT) in Figure 8.10.

In this scenario, an end user reports difficulty accessing the network while using eduroam from the remote institution, but the problem requires a next level support. The end user might perform the following steps in reporting the problem:

1. The end user calls the home institution and asks for assistance from the institutional administrator.

2. The institutional administrator at the end user's home institution will check the legitimacy of the end user's credentials.

3. If there is a problem in the validation of the end user's credentials, the institutional administrator will communicate with the end user and help to set up the end user's device.

4. However, the institutional administrator from the end user's home institution may discover that the problem has to do with the visited institution not receiving proper authentication requests from them. If is beyond his/her power to solve it, the home institution administrator will escalate the problem to their NREN (Figure 8.10, 4a).

5. The end user's home institution NREN should continue investigating the problem and must also contact the NREN administrator of the visited institution. If necessary, the eduroam Operational Team (OT) should get involved as presented in Figure 8.10 by 5a and 5b.

6. Thereafter, the visited NREN administrator should communicate with their connected institution.

7. Finally, the institutional administrator at the visited institution should assist the visiting end user in solving the problem if necessary.

In all these scenarios, it is important to note that the problem may be solved by the first level of support without the need to go all the way to the eduroam OT. These scenarios just assume the problem goes beyond the home institutional administrators.

8.15 Technology Considerations

This layer of the proposed multi-faceted model has various operational decisions to be made. Of course, the decisions are guided by the strategic and tactical outputs. Since the network infrastructure may already be in place, decisions related to the operational implementation of the underlying infrastructure should also be made. For example, does the institution allow VPN access to its resources? The use of technologies such as web proxy servers, VPN solutions and Shibboleth, as discussed in Chapter 2, are all operational implementation decisions that must be made. Before deciding to implement any of the mentioned technologies, the operational managers will have to consider the hardware components, the software packages, the impact of new security configurations on the existing network infrastructure and also the necessary skills required.

From the multi-faceted perspective of the model, none of these operational implementation options represent a panacea. Instead, the interplay between the three layers in this essentially tactical model ensures a balanced view that will enhance future decision-making. The next section discusses how this multi-faceted model can be used to aid in decision-making in eduroam when one decides to implement a specific technology.

8.15.1 Deciding to Implement Shibboleth

Firstly, consider a decision to deal with IP-based authorization issues through the use of Shibboleth. Clearly this is a decision aimed at the operational implementation of a technology. When deciding to go that route, one will have to consider the tactical planning required. This would include project planning, but also deciding what training needs to be put in place on a technical level. Furthermore, awareness of the advantages to the user-base must be raised. Finally, the impact on strategy must be considered. Will we, or should we, join specific federated identity management consortia? What kind of cooperation agreements must be put in place with Service Providers? In the case of digital libraries, will the provider support Shibboleth authorization? Clearly, it is not just a case of implementing Shibboleth.

8.15.2 Deciding to use Web Proxy Servers

The risk to the institution is reduced by ensuring that visitors cannot access online libraries illegally. Operational implementation may be by means of managing different IP pools for visitors and not using the same web proxy to exit to the Internet. For home users who may encounter similar measures at other institutions, secure access to their home network through a VPN could be an option. The VPN concept is discussed in the following section.

8.15.3 Deciding to Implement VPN Solutions

The previous section highlighted a VPN as a solution when visitors are restricted by means of a web proxy. Institutions may decide to go that route. However, a such decision would require tactical planning in terms of raising awareness regarding eduroam and the possible issues that users may have while traveling. It further requires tactical planning regarding implementing training programs to help end users understand the concept of a VPN and to teach them how to use it while traveling. Again, thinking about the decision from multiple facets uncovers the fact that it is necessary to look at the bigger picture before applying technical measures.

These three decision cases demonstrated that the multi-faceted model can be used to ensure that the various facets impacted by (or that impact) the decision are all considered. Of course, many more options can be considered, but will be thought of in the same manner as the three illustrated cases.

8.16 Conclusion

This chapter used a use case method to verify that the proposed multi-faceted model has the potential for practical use in real-world circumstances. eduroam was used as a use case scenario for this verification. Firstly background information about eduroam was given. Secondly, the problem that currently exists was stated. Finally, the model was applied to the problem.

The following chapter concludes the research study.

Chapter 9

Conclusion

The previous chapter concluded the demonstration part of this research study by applying the proposed multi-faceted model to support authentication and authorization for online services to the eduroam facility. The aim of this application was to show the effectiveness of the model and its utility, as the eduroam facility presents a suitable demonstration environment which potentially covers all the layers discussed during the model development. The model is described as a multi-faceted model, i.e. it has three layers interdependent on one another. These layers were first conceptualized together before they were discussed in separate chapters. The topics discussed in those separate chapters ranged from strategic decisions (policies), to the tactical planning (awareness), to operational implementations (technology considerations) in today's IT ecosystem. The discussion of each layer addressed the sub-objectives stated in Chapter 1 Section 1.3. Thereafter, the proposed model was demonstrated to show the effectiveness and its utility.

Finally, this chapter concludes the research study by revising the research problem and objectives and arguing that they were met. It also argues that the model was developed and demonstrated to solve the problem stated in Chapter 1 Section 1.2. This is followed by a discussion about the research methodology used and a summary of the chapters before stating the research contribution. Thereafter, the limitations of the research and future directions are discussed. In closing, this chapter is concluded as well.

9.1 Revising the Problem and Objectives

This section firstly discusses what motivated this research study which led to the research problem and subsequent objectives. An overview of the research study is provided by revising the problem statement and research objectives and also discussing how the research objectives were met.

This research study was primarily motivated by the three realizations. These realizations were stated as follows:

1. *The realization that access control spans across organizational boundaries.*

2. *The realization that there could be inconsistencies between legal specifications and technical access control measures.*

3. *The realization that users just want to do their job without worrying about who should have access to online services.*

Each of these realizations was in-line with each of the three layers that form part of the proposed model discussed in Chapters 5, 6 and 7. These realizations provided a foundation to the initial problem statement. *Currently, a model to support authentication and authorization for online services is lacking.* This led to the formulation of the primary research objective.

To develop a multi-faceted model to support authentication and authorization for online services.

In order to meet the primary research objective, the following secondary research objectives were necessary:

1. *To investigate the governance of IT ecosystem level through access control policies.*

2. *To investigate and identify available ways of influencing users behaviors toward access control in IT ecosystems.*

3. *To investigate and identify possible technology solutions within the environment of IT ecosystems.*

How these secondary research objectives were met are discussed in the following subsections.

Sub-objective 1: To investigate the governance of IT ecosystem levels through access control policies.

To address Sub-objective 1, **Part I** of this research study performed a literature study on existing knowledge. In particular, the answer was provided in **Chapter 2** and also in **Part II Chapter 5**.

Chapter 2 discussed the administration and enforcement of access control by arguing that there are various decisions that need to be made by the `Reference Monitor` when the `Subject` attempts to access a particular `Object`. Those decisions are made every time the `Subject` attempts to access a particular `Object`. Thus, they are *run-time* decisions. However, these decisions are based on a set of access rules which must be created first. Therefore, there is also an *administration-time* activity of setting up those access rules (see Chapter 2, Section 2.1). When creating access control policies or rules they should be considered for both their administration and their enforcement.

The answer to this research Sub-objective also came from **Part B Chapter 5** of the research study. The major standards, best practices and management frameworks, specifically **ITIL**, **COBIT5** and **ISO/IEC 27002** were looked at.

Sub-objective 2: To investigate and identify available ways of influencing users' behaviors toward access control in IT ecosystems.

This objective was successfully addressed in **Part II Chapter 6** of this research study. The Customer Buying Cycle (CBC), outlined by Osterwalder and others as four channels, was utilized in order to influence the behaviors of customers when deploying a new service. Of particular interest was the structuring of these channels from introducing the users to the new facility (Awareness), to helping them make an informed decision about using it (Evaluation), to the transaction process (Purchase), through to the use of a new facility (After Sales). These were defined in this research study as contact points. How they were utilized in the proposed multi-faceted model was demonstrated in **Chapter 8** during the model demonstration using eduroam.

Sub-objective 3: To investigate and identify possible technology solutions within the environment of IT ecosystems.

To meet this objective, **Part I Chapter 2** firstly investigated possible technologies commonly available and used in IT ecosystems for access control and highlighted the advantages and operation of each technology in use. **Part II Chapter 7** discussed technology considerations when implementing the identified technologies.

Furthermore, **Part III Chapter 8** utilised some of the previously identified possible technologies based on the conditions presented by the eduroam facility.

Therefore, these secondary research objectives are mapped to the chapters where they were achieved, as summarized in the above sections, in Table 9.1.

Table 9.1: Reach objectives mapped to chapters

Sub-Objective	Chapter(s)
Investigate the governance of policies	2-5
Investigate and identify ways of influencing users' behaviours	6-8
Investigate and identify possible access control technologies	2, 7-8

Of course, these research objectives were achieved in the subsequent chapters (see Table 9.1) using different research methods. The next section discusses the contribution made by this research study.

9.2 Research Contribution

A well conducted scientific research study should contribute to the body of knowledge as was the case with this research study. This section discusses the research contributions made during the course of this research study.

There were two contribution made throughout this research study. The first contribution was the development of the model which satisfies the main aim of the research. The main aim was to develop a multi-faceted model to support authentication and authorization for online services. To achieve this, a multi-faceted model needed to be developed, as shown in Figure 9.1 and Figure 9.2

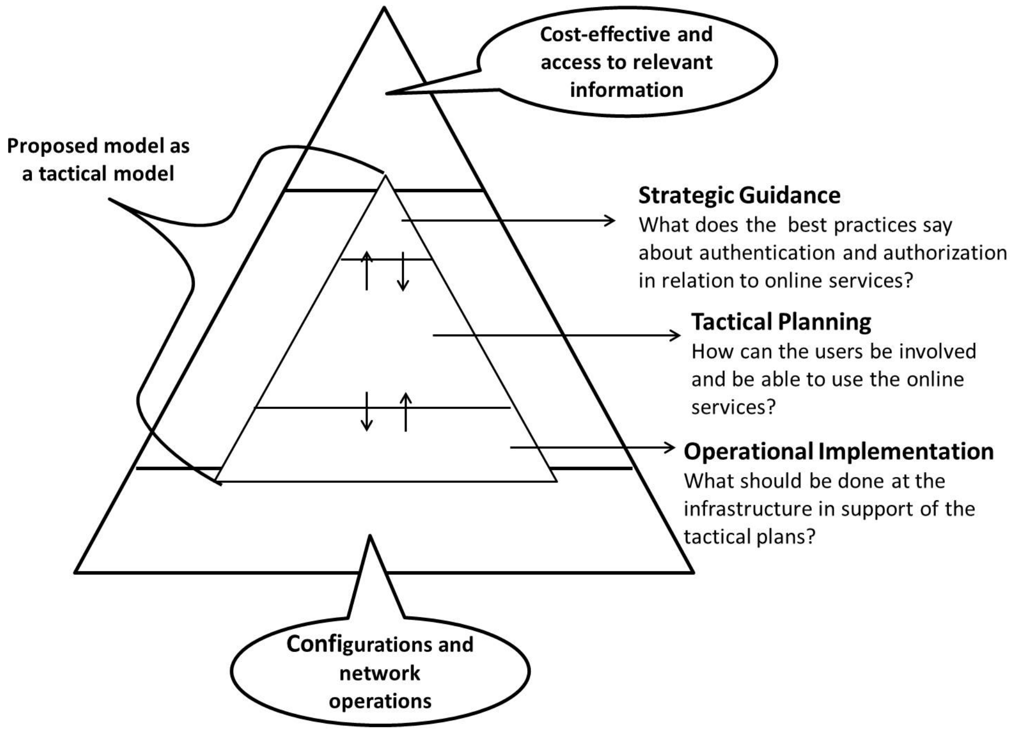


Figure 9.1: Positioning of the Model

This is considered as the primary contribution of the dissertation. The second contribution was in the form of journal, conference and poster papers(These are attached on the CD ROM). For each of these papers, valuable feedback was obtained from various expects in the field of this research study. This proved to be valuable as they also contributed during the development stages of the proposed multi-faceted model. Prior to this research study, a model to support authentication and authorization for online services was lacking. This research study tries to address this problem based on the existing literature, argumentation, theories, best practices, standards and management frameworks.

The following section discusses the research limitations and future directions.

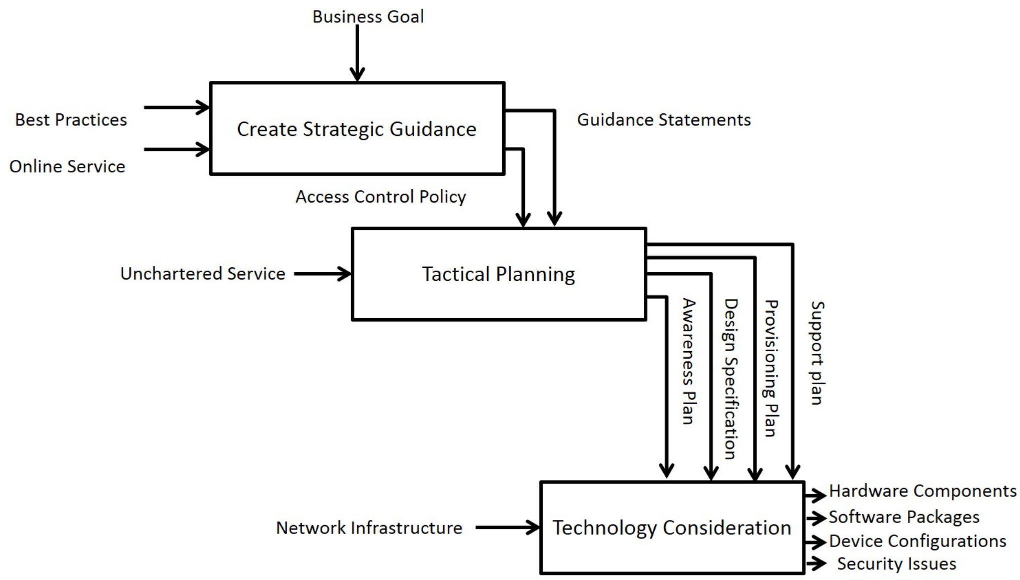


Figure 9.2: The Multi-faceted Model Layers

9.3 Limitations and Future Directions

Although the research aimed to develop a model that is not environmentally specific, some limitations were faced. The proposed multi-faceted model was demonstrated by addressing a problem on the eduroam facility, implying that it could possibly work for any other facility that offers online services and requires users to be authenticated and authorized. However, a limitation of the proposed model is that, it considers a single use case scenario. Therefore, there remains doubts about whether the proposed model can be generalized to other systems such as Cloud computing as such environment might possess effects and risks dissimilar to eduroam.

Future directions may include considering other use case scenarios or facilities similar to eduroam. Furthermore, since the proposed multi-faceted model is silent about the technical issues and implementations that might be present, it could be a good idea to implement it on the actual system for online services. In other words, if the decision from the proposed model considers implementing Shibboleth, then Shibboleth should be implemented in a real life context.

9.4 Final Words

In closing, the model was developed and found to be effective and satisfactory when it was applied to eduroam (the use case). As the results of this research study stands, it can be confirmed that all the aims that were initially stated were achieved and nothing was left out.

References

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). *Extensible authentication protocol (EAP)* (Tech. Rep.). RFC 3748, June. http://www.hjp.at/doc/rfc/rfc3748.html. (Accessed: June 9, 2015)

ACE. (n.d). *Considerations on technology solutions.* Retrieved 25 July 2016, from https://aceproject.org/ace-en/topics/et/eta/eta01/default

Bao, Y., Song, J., Wang, D., Shen, D., & Yu, G. (2008, Nov). A role and context based access control model with UML. In *Young computer scientists, 2008. icycs 2008. the 9th international conference for* (p. 1175-1180).

Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., & Vaniea, K. (2009). Real life challenges in access-control management. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 899–908). New York, NY, USA: ACM.

Bhoj, P., Singhal, S., & Chutani, S. (2001). SLA management in federated environments. *Computer Networks*, *35*(1), 5–24.

Blansit, B. D. (2007). Beyond password protection: methods for remote patron authentication. *Journal of electronic resources in medical libraries*, *4*(1-2), 185–194.

Bolle, R. M., Nunes, S. L., Pankanti, S., Ratha, N. K., Smith, B. A., & Zimmerman, T. G. (2004, November 16). *Method for biometric-based authentication in wireless communication for access control.* Google Patents. (US Patent 6,819,219)

Botha, R. A. (2008). *CoSAWoE-A Model for Context-sensitive Access Control in Workflow Environments.* (Unpublished doctoral dissertation).

Cain, M. (2003). Cybertheft, network security, and the library without walls.

The Journal of Academic Librarianship, *29*(4), 245 - 248.

Cánovas, Ó., Gómez-Skarmeta, A. F., López, G., & Sánchez, M. (2007). Deploying authorisation mechanisms for federated services in eduroam (DAMe). *Internet Research*, *17*(5), 479–494.

Clinch, J. (2009). ITIL V3 and Information Security. *Best Management Practice*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

de Groot, C. (2004, April). *TERENA Annual Report 2003.* https://www.terena.org/publications/files/terena_final_2003.pdf. (Accessed: June 1, 2014)

Dropbox. (n.d). *Using Dropbox at Work.* https://www.dropbox.com/team?_tk=left_nav_team. (Accessed: December 1, 2015)

Duffy, J. (2001). The Tools and Technologies Needed for Knowledge Management. *Information Management*, *35*(1), 64.

eduroam. (2015a, March 3). *About eduroam.* https://www.eduroam.org/index.php?p=about. (Accessed: June 1, 2015)

eduroam. (2015b). *Where can I eduroam?* https://www.eduroam.org/index.php?p=where. (Accessed: June 14, 2015)

eduroam. (n.da). *Simple,Secure and fast network access for students,reseachers and staff.* https://www.eduroam.org/downloads/docs/eduroam-brochure-it-managers.pdf. (Accessed: July 14, 2015)

eduroam. (n.db). *What is eduroam?* https://www.eduroam.org/. (Accessed: May 31, 2015)

Erdos, M., & Cantor, S. (2002). Shibboleth-Architecture DRAFT v05. *Internet2/MACE, May*, *2*, 33.

Fang, X., Sheng, O. R. L., & Chau, M. (2007, October). Servicefinder: A method towards enhancing service portals. *ACM Trans. Inf. Syst.*, *25*(4). Retrieved from http://doi.acm.org/10.1145/1281485.1281488 doi: 10.1145/1281485.1281488

Fen, Y., Zhen, H., Liu, J., et al. (2009). A Mandatory Access Control Model with Enhanced Flexibility Multimedia Information Networking and Security. In *Proceedings of the inernational conference on digital object identifier* (pp. 120–124).

Florio, L., & Wierenga, K. (2005). Eduroam, providing mobility for roaming users. In *Proceedings of the EUNIS 2005 conference, manchester.*

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, *13*(2), 159–190.

GEANT. (n.d). *Make yourself@home with eduroam.* `http://www.geant.net/Services/UserAccessAndApplications/Pages/eduroam.aspx`. (Accessed: July 06, 2015)

Greenfield, D. (2007). *ITIL, COBIT, and ISO 17799 provide a blueprint for managing IT services.* Retrieved from `http://www.informationweek.com/standards-for-it-governance/d/d-id/1062203?page_number=1`

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*(2), 337–356.

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. In *Information security for south africa (issa), 2012* (pp. 1–8).

Harrington, R. J., & Ottenbacher, M. C. (2009). Decision-making tactics and contextual features: Strategic, tactical and operational implications. *International Journal of Hospitality and Tourism Administration*, *10*(1), 25-43.

Huai, J. (2010). Design Service Level Agreements in Outsourcing Contracts. In *4th International Conference on Management and Service Science (MASS)* (pp. 1–4).

Hulsebosch, R., Salden, A. H., Bargh, M. S., Ebben, P. W., & Reitsma, J. (2005). Context Sensitive Access Control. In *Proceedings of the tenthACM symposium on access control models and technologies* (pp. 111–119).

Hunnebeck, L. (2011). *ITIL service design.* TSO.

Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative market research: An international journal*, *3*(2), 82–90.

Internet2. (n.d.). *Trust and identity in education and research: Collaborative to the core.*

ISACA. (2013). *COBIT 5 process assessment model (PAM).* Author.

ISO/IEC27002. (2013). *Information technology - Security techniques -*

Code of practice for information security controls. International Organization for Standaedization/International Electronical Commission (ISO/IEC).

Jaferian, P., Rashtian, H., & Beznosov, K. (2014). To authorize or not authorize: helping users review access policies in organizations. In *Symposium on usable privacy and security (soups).*

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, *43*(2), 618–644.

Kim, J., & Lee, J. (2002). Critical design factors for successful e-commerce systems. *Behaviour & Information Technology*, *21*(3), 185–199.

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems (TOCS)*, *10*(4), 265–310.

Lee, G.-G., & Lin, H.-F. (2005). Customer perceptions of e-service quality in online shopping. *International Journal of Retail & Distribution Management*, *33*(2), 161–176.

López, G., Cánovas, Ó., Gómez-Skarmeta, A. F., & Sánchez, M. (2008). A proposal for extending the eduroam infrastructure with authorization mechanisms. *Computer Standards & Interfaces*, *30*(6), 418–423.

Mikesell, B. L. (2004). Anything, anytime, anywhere: proxy servers, shibboleth, and the dream of the digital library. *Journal of library administration*, *41*(1-2), 315–326.

Milinović, J. R., Miroslav, Winter, S., & Florio, L. (2008). *Deliverable DS5. 1.1: eduroam service definition and implementation plan.* `https://eduroam.org/downloads/docs/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf`. (Accessed: June 8, 2015)

Mooi, R. D. (2014). *A model for security incident response in the South African National Research and Education Network* (Unpublished master's thesis). Nelson Mandela Metropolitan University.

Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic Computation & Economic Cybernetics Studies & Research*, *43*(1), 16.

Needleman, M. (2004). The Shibboleth authentication/authorization system.

Serials Review, *30*(3), 252–253.

NMMU. (n.d). *Wireless Network: eduroam.* http://wifi.nmmu.ac.za/eduroam. (Accessed: July 07, 2015)

OGC. (2007). *Itil: Service operation.* Crown.

or Buy, B. (1999). *bidorbuy,Online Platform where Buyers and Sellers Meet.* http://www.bidorbuy.co.za/help/3981/About_Us. (Accessed: December 7, 2015)

Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring Role-based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security (TISSEC)*, *3*(2), 85–106.

Osterwalder, A., et al. (2004). The business model ontology: A proposition in a design science approach.

Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers.* John Wiley & Sons.

Paschoud, J. (2004). Shibboleth and saml: at last, a viable global standard for resource access management. *New review of information networking*, *10*(2), 147–160.

PCI. (2014). Information Supplement: Best Practices for Implementing a Security Awareness Program. *PCI Data Secicurity Standard (PCI DSS) Version 1.0*, 27.

Pinxteren, B. V. (2013, December). *TERENA COMPENDIUM of National Research and Education Networks in Europe.* https://www.terena.org/publications/files/TERENA-Compendium-2013.pdf. (Accessed: May 13, 2015)

Rangarajan, S., Takkallapalli, A., Mukherjee, S., Paul, S., & Miller, S. (2004). Adaptive VPN: Tradeoff between security levels and value-added services in virtual private networks. *Bell Labs Technical Journal*, *8*(4), 93-113. doi: 10.1002/bltj.10089

Ridley, G., Young, J., & Carroll, P. (2004, Jan). COBIT and its utilization: a framework from the literature. In *System sciences, 2004. proceedings of the 37th annual hawaii international conference on* (pp. 1–8 pp.).

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In *Modeling & simulation, 2008. AICMS 08. second asia international conference on* (pp. 749–753).

Saint-Germain, R. (2005). Information security management best practice based on iso/iec 17799. *Information Management*, *39*(4), 60.

Sandholm, T. (2005). Service level agreement requirements of an accounting-driven computational grid. *Royal Institute of Technology, Stockholm, Sweden, Tech. Rep. TRITA-NA-0533*.

Sandhu, R., Bhamidipati, V., & Munawer, Q. (1999). The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security (TISSEC)*, *2*(1), 105–135.

SANReN. (n.d.). *Overview.* `http://www.sanren.ac.za/overview/`. (Accessed: June 1, 2015)

SANReN. (n.da). *eduroam – Eduroam administrators and operations list.* `http://lists.sanren.ac.za/cgi-bin/mailman/listinfo/eduroam`. (Accessed: July 20, 2015)

SANReN. (n.db). *Where can i eduroam: List.* `http://www.eduroam.ac.za/list`. (Accessed: July 07, 2015)

Schutz, R., McLaughlin, S., Daeleman, T., Luoma, M., Peuhkuri, M., Carlen, P., & Haines, J. (2013). Protected Core Networking (PCN): PCN QoS and SLA definition. In *Military Communications and Information Systems Conference (MCC)* (pp. 1–9).

Shamdasani, P., Mukherjee, A., & Malhotra, N. (2008). Antecedents and consequences of service quality in consumer evaluation of self-service internet technologies. *The Service Industries Journal*, *28*(1), 117–138.

Spens, K. M., & Kovács, G. (2006). A content analysis of research approaches in logistics research. *International Journal of Physical Distribution & Logistics Management*, *36*(5), 374–390.

Tan, L., & Wang, N. (2010). Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (icacte)* (Vol. 5, pp. V5–376).

Tekeni, L., Botha, R., & Thomson, K. (2016). An overview of access control practices: Guidance from itil, cobit 5 and iso/iec. In *Information institute conference, las vegas, nv. march 29-31.*

Tekeni, L., Thomson, K.-L., & Botha, R. A. (2014). Concerns regarding service authorization by ip address using eduroam. In *Information* *security for south africa (issa), 2014* (pp. 1–6).

TENET. (2012). *eduroam National Policy for South Africa.* http://www.eduroam.ac.za/eduroam/static/pdf/eduroam_SA_policy.pdf. (Accessed: July 20, 2015)

TENET Board. (2012, December). *eduroam National Policy for South Africa.* http://www.eduroam.ac.za/eduroam/static/pdf/eduroam_SA_policy.pdf. (Accessed: June 9, 2015)

TERENA. (2003). *Activities: eduroam.* https://www.terena.org/activities/?action=set_filters&filters[topic_id]=*. (Accessed: July 20, 2015)

TERENA. (2004, December 15). *EduRoam Goes Global.* http://www.terena.org/news/archive/2004/newsflash163.pdf. (Accessed: March 8, 2014)

TERENA. (2010, April 28). *Reaserch and education networking FAQ-general.* https://www.terena.org/activities/development-support/r+e-faq/general.html. (Accessed: March 26, 2015)

TERENA. (2011). *eduroam Compliance Statement.* https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf. (Accessed: June 14, 2015)

TERENA. (2012, May, 24). *eduroam celebrates a decade of providing secure roaming internet access for users.* https://www.terena.org/news/fullstory.php?news_id=3162. (Accessed: June 1, 2015)

Thomas, R. K., & Sandhu, R. S. (1997). Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. *DBSec*, *113*, 166–181.

Verma, M. (2014). *Comparison of IT governance framework: COBIT, ITIL and BS7799.* Retrieved 19 April 2015, from http://www.slideshare.net/meghnaverma3956/comparison-of-it-governance-frameworkcobit-itil-ds?related=5

Von Solms, R., Thomson, K.-L., & Maninjwa, M. (2011a). Information Security Governance control through comprehensive policy architectures. In *Information Security South Africa (ISSA)* (p. 1-6).

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011b). Information security governance control through comprehensive policy architectures. In *2011 information security for south africa* (pp. 1–6).

Von Solms, R., & von Solms, S. B. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 408–412.

von Solms, S. B. (2005). Information security governance compliance management vs operational management. *Computers and Security*, *24*(6), 443 - 447.

Wang, H., & Osborn, S. L. (2007). Discretionary access control with the administrative role graph model. In *Proceedings of the 12th acm symposium on access control models and technologies* (pp. 151–156).

Whitman, M., & Mattord, H. (2013). *Management of information security.* Cengage Learning.

Wierenga, K. (2002). *Initial proposal for (now) eduroam* (Tech. Rep.). `http://www.terena.org/activities/tf-mobility/start-of-eduroam.pdf`. (Accessed: April 3, 2015)

Wierenga, K., & Florio, L. (2005). Eduroam: past, present and future. *Computational methods in science and technology*, *11*(2), 169–173.

Wierenga, K., Winter, S., Arends, R., Poortinga, J. R., Simonsen, D., & Sova, M. S. (2006). Deliverable DJ5. 1.4: Inter-NREN Roaming Architecture: Description and Development Items. *GN2 JRA5, GÉANT*, *2*.

Willens, S., Rubens, A. C., Rigney, C., & Simpson, W. A. (2000, June). *Remote authentication dial in user service (RADIUS)* . `https://tools.ietf.org/html/rfc2865`. (Accessed: June 8, 2015)

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. *NIST Special publication*, *800*, 50.

Winter, S., Kersting, T., Dekkers, P., Guido, L., & Papageorgiou, S. (2008, Octomber). *Deliverable DJ5. 1.5, 3: Inter-NREN Roaming Infrastructure and Service Support Cookbook-Third.* `http://www.darenet.dk/sites/default/files/uploads/eduroamCookbook153.pdf`. (Accessed: June 9, 2015)

Yamaguchi, I., Suzuki, T., Goto, H., & Sone, H. (2010). Centralized authentication system for location privacy protection and low operational cost of large scale wlan roaming. In *Applications and the internet (SAINT),10th IEEE/IPSJ International Symposium* (pp. 297–299).

Yuan, E., & Tong, J. (2005). Attributed Based Access Control (ABAC) for Web Services. In *Web services, 2005. icws 2005. proceedings. 2005 ieee* *international conference on.*

Zhou, L., Varadharajan, V., & Hitchens, M. (2012, June). Trusted administration of large-scale cryptographic role-based access control systems. In *Trust, security and privacy in computing and communications (TrustCom), 2012 IEEE 11th international conference on* (p. 714-721).

Zhu, F. X., Wymer, W., & Chen, I. (2002). It-based services and service quality in consumer banking. *International Journal of Service Industry Management*, *13*(1), 69–90.

Part IV

Appendices

Appendices

During this research study four papers, one for a journal and others for conferences were prepared. These are attached below, following are the full references.

Tekeni, L.; Botha, R.A; & Thomson, K.-L., "*A multi-faceted model for IP-based service authorization in the eduroam network*", SAIEE African Research Journal, Volume 106, No 2, pages 83-92.

Tekeni, L.; Botha, R.A; & Thomson, K.-L, "*An Overview of Access Control Practice: Guidance from ITIL, COBIT5 and ISO/IEC 27002*", Information Institute Conferences, Las Vegas, March 29-31, 2016

Tekeni, L.; Thomson, K.-L.; & Botha, R.A., "*Concerns regarding service authorization by IP address using eduroam*", Information Security of South Africa (ISSA), Johannesburg, August,2014.

Tekeni, L.; Botha, R.A; & Thomson, K.-L, "*An overview of authentication and authorization approaches used in federated domains*", Southern Africa Telecommunication Networks and Applications Conference (SATNAC) 2014, Port Elizabeth, South Africa.

A MULTI-FACETED MODEL FOR IP-BASED SERVICE AUTHORIZATION IN THE EDUROAM NETWORK.

Luzuko Tekeni*, Reinhardt A. Botha† and Kerry-Lynn Thomson‡

* *School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, e-mail: s210083719@live.nmmu.ac.za*

† *School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, e-mail: ReinhardtA.Botha@nmmu.ac.za*

‡ *School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, e-mail: Kerry-Lynn.Thomson@nmmu.ac.za*

Abstract: Eduroam provides a facility for users from participating institutions to access the Internet at any other participating visited institution using their home credentials. The authentication credentials are verified by the home institution, while authorization is done by the visited institution. The user receives an IP address through the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. While this provides great flexibility, it competes with security: access may be wrongfully provided or denied to services that use IP-based authorization. This paper enumerates the risks associated with IP-based authorization in the eduroam network by using Digital Library access as an example. The tension between security and flexibility suggests that a multi-faceted approach to the problem is needed. This paper presents such a multi-faceted model that can be used holistically to consider options for IP-based authorization.

Key words: eduroam, authorization

1. INTRODUCTION

In the current generation, the number of users who connect to the Internet using mobile devices has increased significantly [1]. Most mobile users would like to get connectivity everywhere, including at home and at educational institutions. The TERENA (Trans European Research and Education Network Association) proposed a service for WLAN roaming between educational institutions and research networks [2]. This WLAN roaming service is called eduroam (EDUcation ROAMing). Eduroam provides users (researchers, teachers and students) with Internet access using their home credentials at any institution around the globe which participates in eduroam. This access occurs with minimal administrative overhead [3, 4].

Institutions see eduroam as beneficial to them as academic staff members and students frequently travel between institutions. These students and academic staff members can use their home institution credentials to login at visited institutions that participate in the eduroam service. In eduroam, the authentication credentials are verified by the home institution, while authorization is done by the visited institution [5]. The student or academic staff member receives an IP address in the range of the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize via an IP address of the visited institution may include access to services that are not allowed at the home institution.

In eduroam there is no specific policy in place regarding how authorization should be handled at the visited institution. The NREN (National Research and Education Network) of a country must sign the eduroam compliance statement [6] in order to be part of the eduroam federation. The unavailability of the eduroam authorization policy is due, possibly, to mismatch and scalability issues at the institutional level, as well at national or global levels. However, at the institutional level, the basic and acceptable access policy approach that most of the institutions are following is that the visited institution denies access to their local resources to the users who are not part of the domain [7], while it only grants them access to the Internet using the network infrastructure of the visited institution. To facilitate flexibility and ease-of-maintenance Internet-based services may use IP-based authorization.

This paper enumerates problems with IP-based service authorization in the eduroam network. Further, the paper proposes a multi-faceted model to address the problem. There are many services that authorize users via an IP address when connecting to the Internet using eduroam and it is impossible to analyze all of them. To provide focus, therefore, this paper will primarily consider Digital Library Service Providers.

The rest of this paper is organized as follows. Firstly in Section 2. an overview of the eduroam service is given. Since this paper addresses the problem of IP-based authorization, Section 3. introduces the IP-based authentication and authorization process that can be encountered when roaming between institutions. Thereafter, Section 4. illustrates the problem using Digital Library access as an example. Section 5. analyzes the risks in much more detail. This is followed by considering the interaction between stakeholders and possible technologies that can help in Section 6.. However, not all solutions are suitable for all circumstances. Therefore Section 7. propose a multi-faceted model that can help in deciding how to address the problem. Section 8. discusses how the model can be used when considering a decision. Finally, Section 9. concludes the paper and provides the next step to future work.

2. AN OVERVIEW OF EDUROAM

This section provides a general overview of the eduroam service. It does so by considering its history and by providing an overview of the infrastructural components necessary to implement the eduroam service.

2.1 The Origin

The eduroam service started as an idea of combining a RADIUS-based infrastructure with IEEE 802.1x protocol for roaming Internet access across institutions in Europe [8]. The actual eduroam service started in 2003 within the TERENA Task Force on Mobility, TF-Mobility [9]. During that time many institutions showed an interest in eduroam by joining. Those institutions were from the Netherlands, Finland, Croatia, the United Kingdom, Portugal and Germany [10]. Gradually, other NRENs in Europe began joining what was then named eduroam [1]. In December 2004, Australia became involved and was the first non-European country to join eduroam [11]. According to the eduroam website [12], eduroam "is now available in 69 territories worldwide", but is only available at certain locations within those countries, as long as their NRENs have signed the eduroam Compliance Statement [6].

2.2 The Infrastructure

The eduroam infrastructure is based on hierarchically organized RADIUS proxy servers [13] and the IEEE 802.1x protocol [4]. This initiative makes use of three levels of RADIUS proxy servers, namely: the Top-level server (Confederation), National-level servers (Federation) and Institutional-level servers (Edge) [3]. The Top-level server acts as the bridge between National-level servers for global communication, while the National-level server is responsible for connecting institutions within the country. Every institution wanting to join eduroam connects to its National-level server and deploys a dedicated server for eduroam.

Figure 1 shows a User who wants to connect to eduroam at `institution_A` (visited institution), whose home institution is `institution_B` (home institution). In this case, the supplicant software of the user contacts the Access Point (AP) using 802.1x with EAP (Extensible Authentication Protocol) protocol.

The EAP protocol provides integrity and confidentiality to protect the transportation of user credentials throughout the hierarchy of RADIUS servers [14]. Then the AP contacts its local RADIUS server for authentication. The RADIUS server examines the realm part of the username, and as it

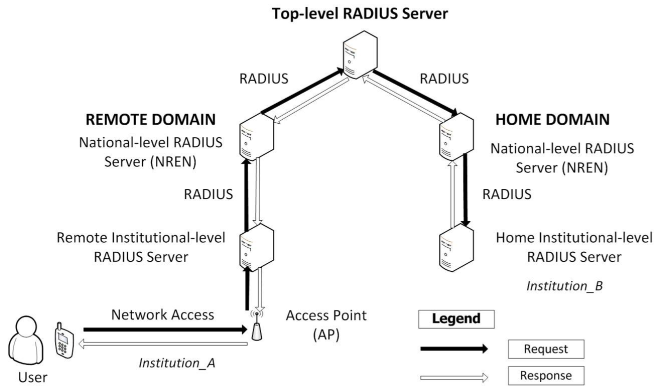


Figure 1: eduroam Infrastructure

is not a local realm in this example, the RADIUS server then proxies the request through the hierarchy of RADIUS servers until `institution_B` is reached. The RADIUS server of `Institution_B` decapsulates the EAP massage and verifies the credentials of the user. It can either accept or deny the request by proxying the results in the reverse order using the same path. The AP at `institution_A` informs the user of the outcome (accept or deny) and the connection is established (if the response is accept).

At the time of writing (late 2014) the South African NREN handled about 10000 (non-unique) authentication requests per day (personal communication, S Miteff, 5 Jan 2015). The next section briefly explains the IP-based authorization process.

3. IP-BASED AUTHORIZATION PROCESS

Some services, such as Digital Libraries, at universities use an IP address to authorize users. This presents a potential problem when using eduroam. Figure 2 shows home and visited institutions and their Service Provider. In this example, before a user can be given any kind of access, the IP-based process for authentication and authorization must first take place. The user then roams between the two institutions using his or her home institutional credentials.

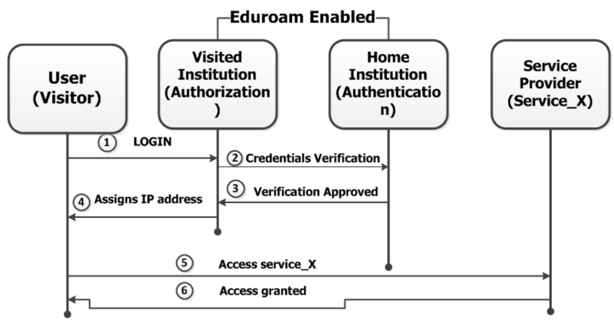


Figure 2: IP-Based Process

When the user reaches the visited institution and connects to eduroam, the following happens:

1. The user tries to login at the visited institution using his or her home credentials.

2. The visited institution examines the realm part of the username and sees that the user belongs to the home institution. Then it sends the user credentials through the hierarchy of RADIUS servers for authentication (verification) to the home institution.

3. The home institution decapsulates the message and verifies the users credentials. It can either accept or deny the request by sending back the response to the visited institution.

4. The visited institution receives the response and grants internet access if the results are positive (accepted), and it assigns an IP address to the user. This IP address can be assigned from a general pool of IP addresses or from a special pool of IP addresses used for roaming users.

5. The user accesses the Service Provider's resource (`service_X`) of the Service Provider using the IP address assigned by the visited institution.

6. The Service Provider verifies the validity of the IP address and gives permission (or not) to the user based on the IP address provided by the visited institution.

This approach certainly alleviates administration, but may have interesting side-effects on the experience of the roaming user.

4. PROBLEM IDENTIFICATION

This section explains the effects that IP-based authorization can have on the expoerience of roaming users. To illustrate, this section uses "Digital Library access" as an example of a service. This section firstly uncovers what the typical legal agreement between universities and Service Providers stipulates. Thereafter, an example is considered where the authorization may contravene these stipulations.

A Service Level Agreement (SLA) is "an agreement between an IT Service Provider and a customer." [15]. Expectations between Service Providers and their customers are typically governed through Service Level Agreements (SLAs).To understand the stipulations between Digital Library providers and universities three Service Level Agreements were reviewed. The gist of these agreements was all the same. Figure 3 shows an extract from the South African Library Consortium Site License Agreement with Emerald.

Of particular interest is the mention of "walk-in users". Walk-in users should only be able to access Licensed Material from computer terminals within the Library premises. This implies that the users must be within the physical premises of the Library to access the service.

"Authorised Users" means individuals who are authorised by the Licensee to access the Licensee's information services whether from a computer or terminal on the Licensee's Secure Network, or off site via a modem link to a valid IP address on the Licensee's Secure Network and who are affiliated to the Licensee as a current student, faculty member or employee of the Licensee. Persons who are not a current student, faculty member or an employee of the Licensee, but who are permitted to access the Secure Network from computer terminals within the Library Premises ["Walk-In Users"] are deemed to be Authorised Users, only for the time they are within the Library Premises. Walk-In Users may not be given means to access the Licensed Material when they are not within the Library Premises.

Figure 3: Emerald Licence Agreement

In a world with wireless Internet and eduroam, this SLA can be considered fairly antiquated. Eduroam users visiting from another institution would not be classified as walk-in users if they accessed the licensed material through their eduroam -authenticated device and may thus breach the SLA. This is assuming that the eduroam users access the Service Provider using an IP address from a pool that has access. On the other hand, if visiting eduroam users are allocated to IP pools that don't have access, the value of roaming authentication is decreased as they will also not have access to services they have access to at their home insitution.

What can be seen here is tension between flexibility and security. The flexibility offered by IP-based authorizaion comes at the expense of security. More secure solutions will mean more effort on the part of stakeholders and will thus reduce flexibility. The rest of this paper considers this flexibility-security tension and proposes a multi-faceted model to help us to decide on a road ahead.

The next section will consider the risks in more detail.

5. RISK ANALYSIS

The previous section pointed out that IP-based authorization may be problematic. This section examines the risks associated with IP-basedc authentication from the vantage point of Digital Library services.

According to [16, 17] risk can be defined as the possibility of an undesired outcome or the absence of the desired outcome to a service. It "is a future event that may or may not occur" [16]. This paper explores the risks from different stakeholder perspectives: the Users, the Service Providers, and Libraries at universities. Each of these risk perspectives is expounded on next.

5.1 The Users

As discussed, when Users visit a particular institution, they could have access to services that they normally do not have when they are at their home institution. These Users can be regarded as 'happy' users, because they have access to services to which they are not subscribed. However, the opposite could also be true. Users may have access to certain services at their home institution that become unavailable to them at a visited institution. These Users could be regarded as 'unhappy' users. In these scenarios, the situation can be seen as unfair to some of the users, while others are enjoying the benefits of accessing services that are not available to them at their home institution. This could impact the users either positively or negatively, depending on the specific circumstances.

To further clarify this, consider the South African academic landscape. Table 1 below shows a comparison of digital Libraries available at selected South African Universities and Research Institutes. Note that, for brevity, only a few selected digital Libraries at each institution are shown. Further, as this is merely illustrative, the names of institutions are not used. The selected institutions participate in eduroam in South Africa.

Table 1: Digital Libraries at Institutions

Comparison of eduroam Institutions			
Digital Libraries	Institution1	Institution2	Institution3
Access Engineering	✓	✓	✓
Access Pharmacy	✗	✗	✓
AccessScience	✗	✓	✓
ACM	✓	✓	✗
African Journals	✓	✗	✗
Biomed Central	✓	✗	✓
Emerald	✗	✓	✓
IEEE Xplore	✓	✓	✓
ISI Web of Knowledge	✗	✗	✓
LexisNexis Academic	✗	✗	✓
Sabinet	✓	✓	✓
SAGE	✓	✓	✓
ScienceDirect	✓	✓	✓

Based on Table 1, the risk varies depending on the institution that the User is visiting. For example, if the User visits Institution1 from Institution3, that User can access the ACM database; whereas at Institution3 he or she does not have access to the ACM database. While users from Institution3 will be very happy with the situation (as they have more access), users from Institution1 visiting Institution3 will be less happy as they do not have access to the database that they usually have when at the home institution. Table 2 summarizes the two risks to users.

Table 2: Risks Facing Users

Risks	**Description**
1A	Users cannot access material they legally have access to
1B	Users could have access to material that they should not have

5.2 Service Providers

The Service Providers are responsible to provide a particular service to the Users. In this context, the Service Providers could find themselves in a position of losing a portion of their income when the users access the service. In other words the user might visit the institution just to access the service that is unavailable while he or she is at the home institution. On the other hand the user might unsubscribe to a particular service intentionally because he or she knows that the service is available to the neighbors and he/she could just go and visit in order to access it. To some extent Service Providers depend on the honesty of the clients to whom they provide the service. If an authorization issue exists in the side of the client, the Service Provider is at risk. The situation needs to be controlled by the clients because if the Service Provider sets an SLA, there is no assurance that the clients will enforce the SLA effectively. Table 3 summarizes the above-mentioned risks.

Table 3: Risks Facing Service Providers

Risks	**Description**
2A	Loss of income when unauthorized users are accessing the service
2B	Service misuse by institutions

5.3 Libraries at universities

Many Libraries at universities use an IP address to authorize users. This presents a potential risk when using eduroam. The eduroam user is given an IP address when visiting a particular institution which gives him or her access to services that could be unavailable at the home institution. This would result in an unauthorized user gaining access to certain services of the visited institution. Furthermore, the visited institution might breach the SLA if these users access the Licensed Material through their own devices andnot on the Library Premises as stated on the license agreement in Figure 3 above. Libraries, therefore, run the risk of being held legally liable. Libraries also do not want to subscribe to unused (and therefore unnecessary) services.

So if at `institution_X`, the library staff members capture their online database usage for the purpose of terminating the contract if an online database is not used, visitors accessing these databases through eduroam may result in incorrect statistics being captured. This could lead to the Library not terminating the use of an online database. At first this risk may seem negligible, but it is worth remembering that services in this category (possible cancellation) are already little used. Hence, even a small number of visitors accessing the service could multiply the number of accesses thereby rendering the service in the expensive, but needed, category. There is no tracking of users and their activities in the current eduroam infrastructure and, therefore, it is impossible to assess the extent of visitor user access.

Universities have thousands of users to manage, potentially including several visitors. Keeping track of registered users and visitors could be challenging in this environment. Service Providers are also at risk as their services could be misused by the visitors since they know they are not paying for it. However, maintaining access records on an individual level rather than at an institutional level is certainly more costly. Table 4 enumerates the main risks discussed in this section that affect Libraries at universities.

Table 4: Risks Facing Libraries at universities

Risks	Description
3A	Libraries might breach the SLA if users (visitors) are accessing the licensed material from their own devices
3B	If Libraries are capturing their online database usage, visitors may lead to incorrect statistics captured. Therefore, this could lead to unnecessary service subscription, which is only used by visitors
3C	Service misuse by visitors

5.4 Risk analysis summary

To summarise the risks affecting the users, Service Providers and Libraries at universities, consider table 5 below.

Table 5: Risk analysis summary

Summary			
Risks	**Users**	**SP**	**LB**
1A: Cannot access	-	x	x
1B: Could access	+	-	-
2A: Loss of income	x	-	-
2B: Service misuse	+	-	-
3A: Breaching SLA	x	x	-
3B: Unnecessary service and incorrect statistics	x	x	-
3C: Same as **2B**	+	-	-

+ = *Positive Impact* **-** = *Negative Impact* ***X*** = *Not Applicable* ***SP*** = *Service Providers* ***LB*** = *Libraries*

As shown in Table 5 if the users cannot have access to a particular service at the visited institution, it affects them negatively. However if they do have access to a resource they normally do not have, it affects them positively. Service Providers and the Libraries at universities are both potentially negatively affected by this situation, albeit not at the same time. The Service Providers are at risk of losing money owing to missed sales opportunities. Libraries also miss opportunities for patrons to pay membership fees for access to resources. Breaches to SLAs negatively impact Libraries as they open up the possibility of legal action. In addition libraries may not be able to trust usage record, for example, not knowing how many access requests really originated from a specific institution.

Although this section did not try to quantify the risks to the various stakeholders, it did show that there are risks. The question now is how to address these risks. The next section considers the relationships among stakeholders and discusses various possible technologies and issues to be considered.

6. THE RELATIONSHIPS AMONG STAKEHOLDERS

The various stakeholders have different relationships among them. Figure 4 abstractly depicts these relationships.

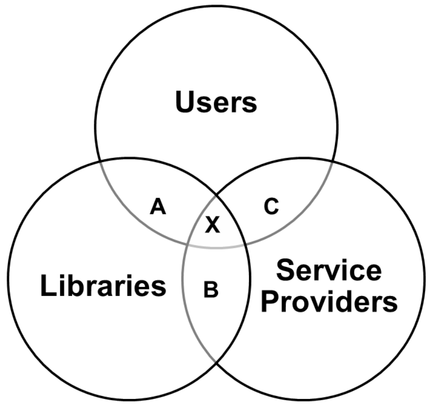


Figure 4: The Relationships among Users, Libraries and Service Providers

Each relationship, as seen in Figure 4, will be briefly described to illustrate how the previously identified risks are mapped and addressed along with possible solution for each. Eduroam in each country is managed and monitored by its NREN [18]. The NREN rolls-out the eduroam service to the interested institutions who want to have the eduroam service on their campus. In Figure 4, as marked by "X", the point of intersection among the Users, Service Providers and Libraries represents where the NREN is placed. The following subsections look at the relationships among the Users, Service Providers and Libraries at universities. Each relationship introduces technologies or actions that might help address the issues. Note that these technologies are not new. On the contrary, they are currently used in various ways by the relevant stakeholders. The discussion in the next section serves to introduce the technologies and actions. Section 7. will combine them into a multi-faceted model that allows us to argue more easily the effect of choices we make in using IP-based authorization in eduroam.

institution.

6.1 Users and Libraries

Consider first the relationship between Users and the Libraries as marked by "A" in Figure 4. According to risks **1A** and **IB** Users cannot access material they legally have access to (at their home institution), when they visit another institution because the visited institution has no subscription to the same material. However, if the users are from the visited institution going to the opposite institution, they could have access to material to which they should not have, because the opposite institution has subscription to the material. A possible solution to this involves the use of a Virtual Private Network (VPN) tunnel. A **VPN tunnel** provides a complete data privacy and integrity for Users who access the network from outside their Intranet in a secure manner [19]. For instance, by enabling VPN between the user and the home institution, a secure tunnel will be established. This will help to improve the IP-based level of security as highlighted by risk **3A**. In other words, this is adding another layer of security to the IP-based authorization process. Figure 5 shows how a VPN tunnel between the user and the Service Provider in the eduroam network can address the risk of a user not having access to services when visiting institutions.

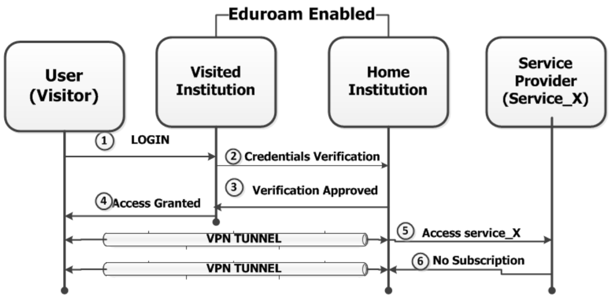


Figure 5: VPN Tunnel in eduroam

However, this only addresses the risk from the perspective of a user not having access to something to which he or she normally has access.

Figure 5 depicts the use of a VPN tunnel. Steps 1 to 3, 5 and 6 were described in Figure 2. Step 4 secures the IP address that is normally assigned by the visited institution to access a service. However, access to the service is obtained via the VPN tunnel being established to allow one-to-one communication rather than consulting the visited institution. Access to Service_X is now requested from the home institution, and not from the visited institution.

This approach eliminates the risk identified by **3C** which concerns service misuse by visitors. For technology-savvy users, the use of VPN could be a straightforward concept for them to understand and be able to VPN back to their home institution when visiting others. However, for non-technical users it may not be as straightforward. Hence, training sessions should be provided to educate users with regard to how to connect to the eduroam service at visited institutions and how to VPN back to the home institution.

6.2 Libraries and Service Providers

The relationship between the Libraries and the Service Providers is marked by "B" in the diagram: In the SLA analysed earlier, it was highlighted that Libraries might breach the SLA if the visitors access the licensed material from their own devices (as described in risk **3B**) and the Service Providers may lose a bit of income (risk **2A**). Their service could be misused by the users of the institution (risk **2B**).

As a possible solution to this, the Libraries must engage the Service Providers in connection with the SLA presented to them. It is very important to understand that eduroam has been introduced far more recently than the SLAs. It might happen that it is not of great concern to the Service Providers that visitors are being given access to their service, or it may require an adjustment of the SLA. The SLA presented in Section 4. Figure 3 needs to be revised by the authorized entities. Another option is that the Libraries can consider joining existing federations or consortia that provide more controlled access. These can be country-wide federations which also come with policies on how a service can be accessed.

6.3 Service Providers and Users

The relationship between the Users and the Service Providers is marked by "C" in the diagram. When the user accesses online material such as Digital Libraries, the "identifier" is merely an IP address [20]. However, IP addresses are easy to spoof. Hence, federated identity domain technologies need to be investigated to determine how the attributes of the User can be transported in order to provide access control to the website of the Service Provider. Even though a high-level analysis of risk involved may not identify major risks it is worth noting that possible controls may already exist to address this situation. Since the issue here is really that of the identity of a user to be used from outside the institution, solutions may exist in different environments.

One way to solve this is to use **virtual direct dialing** into a campus server through L2F (Layer Two Forwarding) protocol using PPP/SLIP (Point-to-Point Protocol/Serial Line Interface Protocol) connections [21]. A remote user will be given an IP address of the institution to his/her personal device through L2F protocol which provides virtual direct dialing service into protected (Private) networks through the Internet (Public) Service Providers [22]. Figure 6 shows a high level overview of the virtual dialing approach.

As can be seen in Figure 6, the remote users will connect to the NAS (Network Access Server). These NASs can be geographically located anywhere around the world [22]. In turn they connect through the Internet. The Internet will check whether the user is dialing-up (is this case it is). Then the L2F protocol will take control using

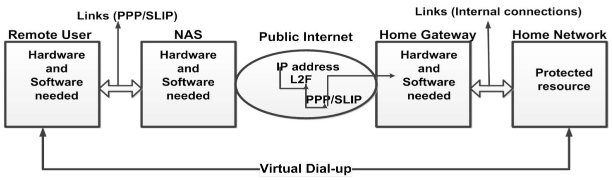


Figure 6: Virtual Dialling Approach

PPP/SLIP communicating with the home gateway of the user and the user will have access to the licensed material. However, this approach suffers from many disadvantages [21]. Hardware and software packages are required to setup this kind of communication and the solution can be expensive to deploy. Furthermore, it has a limited calling area. In other words, if a remote user is located far away, this might not work. Clearly this approach has several disadvantages that are particularly problematic for a large-scale network.

Another technology, a **Web proxy**, was therefore considered. According to Duke and Yu [21] "The Web proxy is designed primarily to secure an Intranet, to control and monitor employees access to the Internet". Web proxy servers are normally placed outside the firewall of a company. In this context, visitors accessing the Internet using eduroam can be forced to go through a Web proxy server which will restrict them from accessing the licensed material. However, this will inconvenience legitimate users at the home institution when they connect to the Internet using eduroam. Hence, network administrators needs to figure a scalable way to implement these proxy servers. Figure 7 illustrates how a Web proxy works between a user and an institution holding the required service.

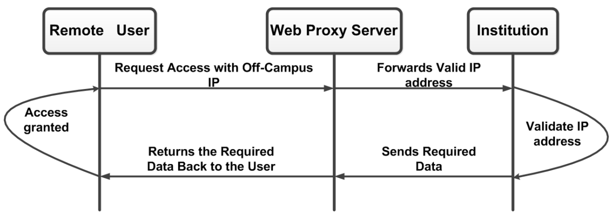


Figure 7: Web Proxy Server at Institution

The remote user tries to access licensed material using a proxy-enabled browser. The request is directed to a proxy server located on campus. When the proxy server receives the request and forward it to the institution, the institution validates that the IP address came from the proxy and authenticates the request. Thereafter, an inside system returns the data to the proxy server, which in turn, sends the retrieved data back to the remote user. But this only solves the problem of visitors accessing the licensed material at the visited institution. The above discussed approach might suffer in terms of the distance coverage area. In other words, at times it could be very difficult to reach the proxy server over a long distance. Since the problem here involves federated identity management domains, the use of Shibboleth could solve the problem.

Shibboleth acts as an intermediate third party between the home institution and the Service Provider on behalf of the visited institution as shown in Figure 8 [20]. Figure 8 shows a high-level view of how Shibboleth could be used in eduroam.

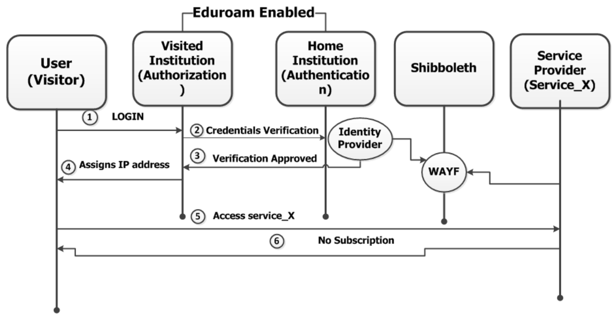


Figure 8: Shibboleth in eduroam

A Where Are You From (WAYF) database will be used to identify the user and once that it is done, the Service Provider will be able to access the attributes of the user from the Attribute Authority (AA) at the home institution of the user. The AA is the database that stores the attributes of the user located at the home institution under the supervision of the Identity Provider (IdP). Shibboleth will be able to identify services that are allowed at the home institution for the user, using SAML (Security Assertion Markup Language) [23] query request/response messages. This will, however, require services to evaluate SAML attributes in order to do authorization. Shibboleth works well if an institution forms part of a federation. Federated identity management allows users to hand out identity information dynamically across the distributed domain of the federation. On the negative side Service Providers also need to co-operate and do authorization based on SAML attributes.

From the above discussion it is clear that several potential solutions exist, each with its own advantages and disadvantages. The next section introduces a multi-faceted model that can be used to argue about these different options in a more holistic way.

7. A MULTI-FACETED MODEL

Before introducing the model components in sub-section 7.2, sub-section 7.1 first positions the model conceptually.

7.1 Conceptual positioning

It has become commonplace to think about business in terms of strategic, tactical and operational decisions. To understand where the proposed model fits, two important assumptions that have been made must be considered.

Firstly, the proposed model assumes that participants in the eduroam network have made the strategic decision to provide cost-effective access to relevant information and services to users while travelling. Of course, what exactly "cost-effective access" means to each particpating university may differ vastly.

Secondly, the proposed model assumes that the underlying network operations are in place and that they are being configured and managed by the various NRENs.

In the bigger picture our model is therefore conceptually positioned as a tactical model, as shown in Figure 9. Decisions in the proposed model will certainly be influenced by the strategic direction assumed by participating universities, but it is not overly concerned with the operations of the underlying network. This does not mean that the proposed model might not influence the strategic direction, nor does it mean that decisions made will not influence the operations. However, its focus is on making tactical decisions to manage the tension between flexibility and security when considering IP-based authorization decisions.

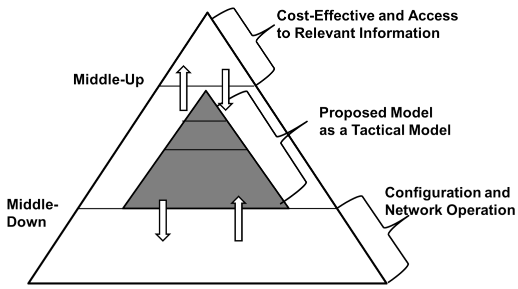


Figure 9: Positioning of the Model

As an example consider a tactical decision to implement federated identity management technologies such as **Shibboleth**. This will clearly impact the configuration of the network devices and the operation of the network - an operational concern. The proposed model, however, is deliberately silent in terms of operational implementation issues. Similarly, strategic decisions such as the joining of federated identity consortia should be with the view of supporting a bigger strategic view in order to allow access to relevant information to all users, even while they are traveling.

7.2 Model Components

This section briefly discusses the components that constitute the proposed model. The model will consider the decisions that must be made at each layer of the model. Figure 10 presents the proposed model.

The model is made up of three main components. These are: Strategic decisions, Tactical planning and Operational implementation. Each of the components represents various decisions that must be made. These decisions are multi-faceted in that various options are available, but these choices are not independent. A choice made for one component influences the choices for other components.

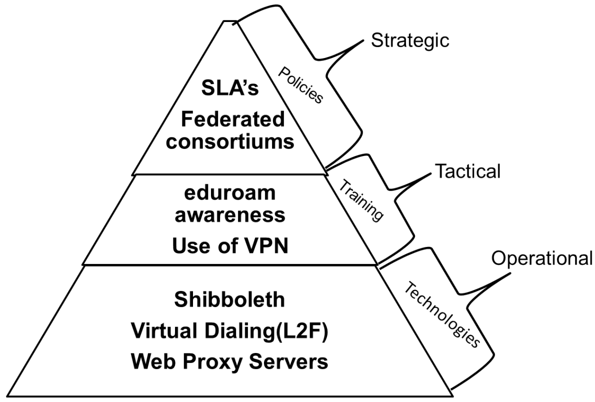


Figure 10: The Multi-faceted Proposed Model

The next sub-sections briefly consider the nature of each of the components by positioning some of the issues revealed in Section 6. within the model components.

Strategic decisions:

Strategic decisions are made to guide the direction an organization takes. In order to provide access to relevant information to researchers, certain decisions need to be made. These decision are often embodied through policies [24] and agreements with suppliers and partners. The SLA between the university library and the Digital Library Service Provider is an example of such an agreement. One way to reduce risk would be to engage Service Providers in terms of the definitions used in these agreement in order to bring the SLA in line with modern trends regarding access to electronic information. Another issue to consider is the joining of federated identity provider consortia, such as InCommon.

Tactical Planning:

After the strategic decisions have been made, plans must be put in place to ensure that the strategic choices can actually be implemented feasibly. This may involve project planning activities that inter alia include raising awareness of the strategic direction and training in the use of technologies. In the current context, users may often be unaware of eduroam and the advantages it holds to them. If the institution makes VPN access available to users, some may lack the skills to use the VPN access effectively, and will thus require training.

Operational implementation:

Decisions related to the operational implementation of the underlying infrastructure should also be made. For example, do the institution allow VPN access to its resources? The use of technologies such as web proxy servers, virtual direct dialing, and Shibboleth as discussed in section 6.3 are all operational implementation decisions that must be made.

From the multi-faceted perspective of the model none of these operational implementation option represents a panacea. Instead the interplay between the three components in this essentially tactical model ensures a balanced view that will enhance future decision-making. The next section discusses how the proposed model can be used to aid in decision-making.

8. DISCUSSION

With a multi-faceted model it is important to strike a balance between different, sometimes opposing concerns. This is also the case in this model which proposes three components to be considered when addressing the risks associated with IP-based authentication. The proposed multi-faceted model allows us to think holistically about the implications of our decisions. For example consider two cases, one from a technological perspective and the other from a strategic perspective: using Shibboleth as underlying authentication technology and strictly enforcing SLA requirements.

8.1 Technological decision: Using Shibboleth

Firstly, consider a decision to deal with IP-based authorization issues through the use of Shibboleth. Clearly this is a decsion aimed at the operational implementation of a technology. Deciding to go that route one will have to consider the tactical planning required. This would include project planning, but also what training need to be put in place on a technical level. Furthermore, how will awareness of the advantages to our user-base be raised? Finally the impact on strategy must be considered. Will we, or perhaps should we, join specific federated identity management consortia. Also what kind of cooperation agreements must be put in place with Service Providers? In the case of digital libraries, will the provider support Shibboleth authorization? Clearly, it is not just a case of "just implementing Shibboleth".

8.2 Strategic decision: Enforcing SLAs

Consider another decision: reducing the risk on the institution by ensuring that visitors cannot access online libraries illegally. Operational implementation may be by means of managing different IP pools for visitors and not using the same web proxy to exit to the Internet. For our own users who may encounter similar measures at other institutions we would need to allow them secure access to their home network through a VPN. However, such decision would require tactical planning in terms of raising awareness regarding eduroam and the possible issues that users may have while traveling. It further requires tactical planning regarding implementing training programs to help end-users understand the concept of a VPN and to teach them how to use it while traveling. Again, thinking about the decision from multiple facets uncover the fact that it is not just as simple as applying technical measures to apply the SLA requirements more strictly.

These two decision cases demonstrated that the multi-faceted model can be used to ensure that the various facets impacted by (or that impact) the decision are considered. Of course many more options can be considered, but will be thought of in the same manner as were the two illustrative cases.

9. CONCLUSION

This paper discussed the origin of the eduroam service and its components. It showed that it certainly helps with the flexibility of Internet access. However, it also highlighted that problems can be experienced when services use IP-based authorization. Several potential solutions exist to address the problem if the relationships between the various role players are considered. However, the tension between flexibility and security ensures that a purely technical solution may be more evasive than is immediately evident.

The paper therefore proposes a multi-faceted model for considering decisions regarding IP-based authorization in the eduroam network. Decisions regarding one facet have a direct implication on the other facets. This paper drew on online Digital Library providers as a case study. This is but one example of a service that might be appropriate in the eduroam environment. Other services, for example, collaboration services or grid computation services may expose other risks. However, the model does not exclude any particular risk, but requires us to think not only of the operational implementation issues, but also of the tactical planning issues and the strategic decisions that are impacted. Thinking around the various facets will lead us to better consider the risks involved.

Information technologies change at a rapid rate. The proposed model positioned several existing technologies, but any new technologies or risks could similarly be positioned. This ensures that the model has utility amidst a fast-changing landscape.

The proposed model did not make any claims regarding completeness, but does claim to provide a more holistic view on authorization problems which are often considered technical issues. Future work could include expanding the model to other security problem spaces outside of the authorization places. Furthermore the interplay between different stakeholders, as well as between the different facets of the models, warrants further investigation.

The proposed model recognizes that the 'non-technical' security implications in large scale computer networks such as created by the eduroam services are not clearly understood and it therefore set off, as a prudent first step, to address these issues. The sheer scale of eduroam definitely amplifies what can otherwise be considered minor problems.

REFERENCES

[1] K. Wierenga and L. Florio, "Eduroam: past, present and future," *Computational methods in science and*

technology, vol. 11, no. 2, pp. 169–173, 2005.

[2] K. Wierenga, "Initial proposal for (now) eduroam," Tech. Rep., 2002.

[3] K. Wierenga, S. Winter, R. Arends, J. R. Poortinga, D. Simonsen, and M. S. Sova, "Deliverable DJ5. 1.4: Inter-nren roaming architecture: Description and development items," *GN2 JRA5, GÉANT*, vol. 2, 2006.

[4] J. R. Milinović, Miroslav, S. Winter, and L. Florio, "Deliverable DS5. 1.1: eduroam service definition and implementation plan," 2008. [Online]. Available: https://eduroam.org/downloads/docs/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf

[5] Ó. Cánovas, A. F. Gómez-Skarmeta, G. López, and M. Sánchez, "Deploying authorisation mechanisms for federated services in eduroam (DAMe)," *Internet Research*, vol. 17, no. 5, pp. 479–494, 2007.

[6] TERENA. (2011) eduroam compliance statement. [Online]. Available: https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf

[7] T. Watanabe, S. Kinoshita, J. Yamato, H. Goto, and H. Sone, "Flexible access control framework considering IdP-Side's authorization policy in roaming environment," in *Computer Software and Applications Conference Workshops (COMPSAC), 2012 IEEE 36th Annual*. Swissotel Grand Efes Izmir, Turkey, 2012, pp. 76–81.

[8] TERENA. (2012) eduroam celebrates a decade of providing secure roaming internet access for users. [Online]. Available: http://www.terena.org/news/fullstory.php?news_id=3162

[9] Eduroam. (n.d) About eduroam. [Online]. Available: https://www.eduroam.org/index.php?p=about

[10] D. Olesen. (2003) Terena annual report 2003. [Online]. Available: http://www.terena.org/publications/files/terena_final_2003.pdf

[11] TERENA. (2004) Eduroam goes global. [Online]. Available: http://www.terena.org/news/archive/2004/newsflash163.pdf

[12] Eduroam. (n.d) Where can i eduroam? [Online]. Available: https://www.eduroam.org/index.php?p=where

[13] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (RADIUS)," 2000. [Online]. Available: http://www.hjp.at/doc/rfc/rfc2865.html

[14] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," RFC 3748, June, Tech. Rep., 2004. [Online]. Available: http://www.hjp.at/doc/rfc/rfc3748.html

[15] C. Rudd, V. Lloyd, and L. Hunnebeck, *ITIL Service Design*. TSO, 2011.

[16] E. S. Chia, "Risk assessment framework for project management," in *2006 IEEE International Engineering Management Conference*. Bahia, Brazil, Sept 2006, pp. 376–379.

[17] P. Smith and G. Merritt, "Proactive risk management," in *Controlling Uncertainty in Product Development, New York, USA*. Productivity Press, 2002.

[18] eduroam. (n.d) eduroam infrastructure. [Online]. Available: https://www.eduroam.org/index.php?p=about

[19] S. Rangarajan, A. Takkallapalli, S. Mukherjee, S. Paul, and S. Miller, "Adaptive VPN: Tradeoff between security levels and value-added services in virtual private networks," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 93–113, 2004.

[20] M. Erdos and S. Cantor, "Shibboleth architecture draft v05," *Internet2/MACE, May*, vol. 2, 2002.

[21] J. K. Duke and X. Yu, "Authenticating users inside and outside the library," *Internet Reference Services Quarterly*, vol. 4, no. 3, pp. 25–41, 1999.

[22] A. J. Valencia, "Virtual dial-up protocol for network communication," Jun. 29 1999, US Patent 5918019. [Online]. Available: http://www.google.com/patents/US5918019

[23] S. Cantor, I. J. Kemp, N. R. Philpott, and E. Maler, "Assertions and protocols for the oasis security assertion markup language," *OASIS Standard (March 2005)*, 2005. [Online]. Available: https://www.oasis-open.org/committees/download.php/10391/sstc-saml-core-2.0-cd-02g-diff.pdf

[24] R. Von Solms, K.-L. Thomson, and M. Maninjwa, "Information security governance control through comprehensive policy architectures," in *Information Security South Africa (ISSA), 2011*, Aug 2011, pp. 1–6.

An Overview of Access Control Practices: Guidance from ITIL, COBIT 5 and ISO/IEC 27002

L. Tekeni; R. Botha; and K. Thomson
School of Information and Communication Technology
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
E-mail: {Luzuko.Tekeni;ReinhardtA.Botha;Kerry-Lynn.Thomson}@nmmu.ac.za

Abstract

Access control is one of the oldest aspects of information security. Several IT (Information Technology) best practices, guidelines, frameworks and standards discuss access control. Although these documents discuss very similar concepts, not all of the access control issues are discussed at the same level of detail. Therefore the purpose of this paper is to provide a holistic view of access control as described by the major IT best practices, management frameworks and standards. The ITIL (Information Technology Infrastructure Library) lifecycle access management activities are used as a framework. Further, the access control views from COBIT 5 (Control Objectives for Information and Related Technology) and ISO/IEC 27002 (International Organization for Standardization) are integrated into this framework.

Introduction

Information security is important to any organization. Organizational processes, networks and systems are valuable assets (ISO/IEC27002, 2013); therefore they need to be protected. Organizations need to ensure that their security is effective and adequate at all times (Saint-Germain, 2005). Access control is one of the oldest aspects of information security in an organization. Its main purpose is to manage the provision of user access rights to ensure that resources can be appropriately shared between properly authenticated users. Consider an example of access control decision making as illustrated in Figure 1.

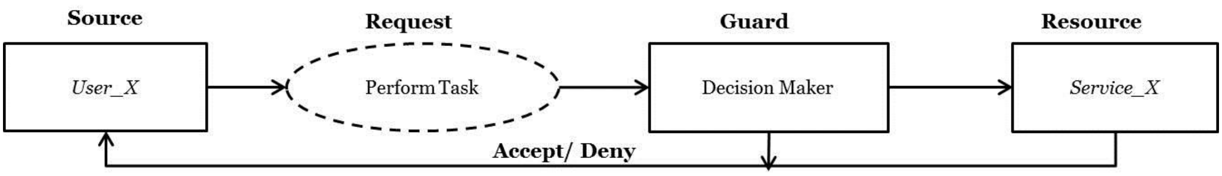


Figure 1: Access control decision making (based on Lampson, Abadi, Burrows, & Wobber, 1992)

In Figure 1 the `Source' (User X) requests access from the `Guard' (Decision Maker) to perform a specific task on a particular `Resource' (Service X). In order to make a decision the `Guard' needs to know the `Source' of the request to determine the identity. This is called authentication. Furthermore, the `Guard' must also verify the access rules associated with the required `Resource' by the `Source'. This is called authorization (Lampson et al., 1992). Therefore, once the `Guard' completes authentication (Who is accessing?) and authorization (What can be accessed?), the decision is made to either `Accept' or `Deny' the required `Resource'.

However this happens when the user attempts to access a particular resource: thus a *run-time* decision. Furthermore, this decision is based on a set of access rules which must be created first. Therefore, there is also an *administration-time* activity of setting up those access rules. Considering administration of access control separately from the operational access control to ensure that the policies and objectives are not compromised is not a new idea (Sandhu, Bhamidipati, & Munawer, 1999). We, therefore, must consider the activities both from a *run-time* and *administration-time* perspective.

As can be expected access control to information systems has been discussed by many, including in IT best practices, management frameworks and standards. Among these, the most commonly used are ITIL (OGC, 2007), COBIT5 (ISACA, 2013) and ISO/IEC 27002 (ISO/IEC27002, 2013). Although ITIL is considered as best practice guidelines, COBIT 5 as a management framework, and ISO/IEC 27002 as a standard, we will collectively refer to them as frameworks. While all these frameworks discuss access control, each discusses issues from a unique perspective. However, not all of the access control issues are discussed at the same level of detail. Hence, this paper provides a holistic view of access control practices by integrating the views from ITIL, COBIT 5 and ISO/IEC 27002. The ITIL lifecycle access management activities are used as a framework to structure the discussion around the access control lifecycle.

Firstly, this paper introduces ITIL, COBIT 5 and ISO/IEC 27002. Secondly, an approach that will be used through the analysis of access control views is provided, along with the ITIL lifecycle access management activities. Furthermore, the access control views found from COBIT 5 and ISO/IEC 27002 are integrated into the ITIL lifecycle access management activities. Thereafter, the main access control themes found from these three frameworks are discussed. Finally, remarks and the conclusion of the paper are stated.

Introducing ITIL, COBIT 5 and ISO/IEC 27002

Many organizations are under pressure to control access to their business systems and services. Organizations should use IT best practices, guidelines, frameworks and standards as guidance when implementing access control. ITIL, COBIT 5 and ISO/IEC 27002 all discuss the concept of access control. However access control views are scattered through the frameworks. This could make it challenging to use them during access control implementation.

Much research has been done in an attempt to integrate them (Sahibudin, Shari, & Ayat, 2008). Furthermore, the access control issues are not discussed at the same level of detail. To understand the differences, think of these three in this way: COBIT 5 discusses what to monitor and control, ITIL clarifies how to go about implementing the processes for performing that, while ISO/IEC 27002 discusses the process for securing those services (Greenfield, 2007). As the focus of this paper is the analysis of access control views within ITIL, COBIT5, and ISO/IEC 27002, the following subsections focus not only on an overview of these frameworks, but also provides a direction with which the information concerning access control views can be located within them.

ITIL

Information Technology Infrastructure Library (ITIL) is a best practice guidelines introduced by the Office of Government Commerce (OGC) situated in the United Kingdom (UK), to provide best practices for IT service management in an organization (Nastase, Nastase, & Ionescu, 2009). This framework discusses issues related to different entities such as "people, processes and infrastructure technology", to provide cost effective and high-quality IT services (OGC, 2007). ITIL comprises of five publications, namely (Verma, 2014): Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

Service Strategy discusses the concept of identifying market opportunities for new services, while Service Design is concerned with developing a strategy into a designed document (Greenfield, 2007). On the other hand, Service Transition deals with the implementation of the activities laid down by the Service Design and Service Operation focuses on the operational side to ensure that services are delivered. Furthermore, Continual Service Improvement provides consistence between the other four publications. It focuses on how the service can be improved over time (Verma, 2014).

In ITIL, the access management process is described in the Service Operation publication. Views are clearly defined in the access management section (4.5) as lifecycle activities.

COBIT 5

COBIT 5 is a management framework developed by ISACA (Information Systems Audit and Control Association) for IT governance and IT management (Sahibudin et al., 2008). This framework defines 34 control objectives in a hierarchy of processes and domains (Ridley, Young, & Carroll, 2004). These processes are subdivided into four domains: Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Evaluate, Direct and Monitor (EDM) (Greenfield, 2007). Under each domain, the process objectives, key activities, input, output, performance measures, Work Product (WP) and Best Practice (BP) are discussed.

There is no specific section that discusses access control views in this management framework. However, access control views could be found in any of the four domains mentioned above. During the integration of access control views in COBIT 5, the Deliver and Support domain discuss more access control views than the other domains.

ISO/IEC 27002

This is an information security standard introduced by International Organization for Standardization (ISO) and by the International Electro-technical Commission (IEC) for information security management (Sahibudin et al., 2008). The main purpose of this standard is to provide guidelines and general principles for "initiating, implementing, maintaining and improving information security management in an organization" (ISO/IEC27002, 2013). The three areas of information security, Confidentiality, Integrity and Availability, are covered in this standard. Furthermore, the standard contains 14 security control clauses in which access control is included (ISO/IEC27002, 2013). Each of these 14 clauses defines a number of main security categories in them.

Although access control views are primarily found in section 9 under the access control clause, other sections also make references to access control related views.

Table 1 below highlights key differences and similarities between these frameworks.

Table 1: Differences and Similarities between ITIL, COBIT 5 and ISO/IEC 27002

Parameters	ITIL	COBIT 5	ISO/IEC 27002
Purpose	IT Service Management	IT Governance	Information Security Controls
Created by	OGC	ISSACA	ISO/IEC
Targeting	Lifecycle of IT Services	34 Processes and 4 Domains	14 Security Control Clauses
Access control details	SOP: Access Management	Within those 4 Domains	Section 9: Access Control

Next consider how we analysed these frameworks.

Analysis Approach

As pointed out earlier, access control must be considered from both an *administration-time* and a *run-time* perspective. Clearly access control is not a once-off activity, but requires administration to be done from time to time, and the actual access control decision is made every time an attempt to access a resource is made. This nature of access control is best acknowledged by ITIL which view access management activities as part of a lifecycle. We therefore decided that structuring our analysis according to the ITIL access management activities will ensure a holistic view.

Figure 2 conceptually positions the access management activities identified by ITIL in terms of *administration-time* and *run-time* perspectives.

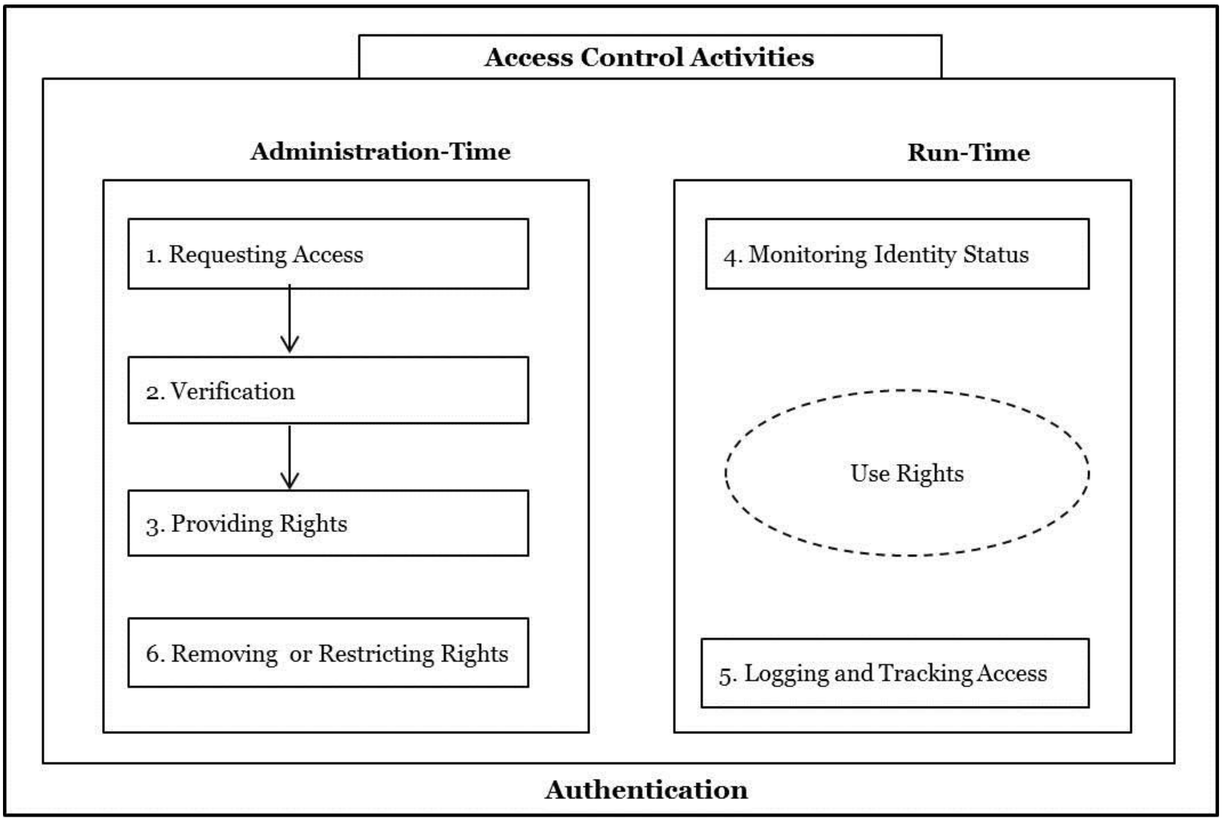


Figure 2: Activities for Access Control Analysis

The first three activities, namely, ‘Requesting Access’, ‘Verification’, and ‘Providing Rights’, ensure that users will receive the access rights they require. The ‘Monitoring Identity Status’ and ‘Logging and Tracking Access’ activities continually takes place to ensure that access rights reflect the business requirements and are not misused. Anomalies and changes to business requirements may in turn trigger some of the administration-time activities. Finally, the ‘Removing or Restricting Rights’ activity ends the lifecycle of the access rights.

Access Control Analysis

This section looks at what guidance is available regarding access control views by using ITIL lifecycle access management activities as a framework. The discussion integrates material from ITIL (OGC, 2007), COBIT 5 (ISACA, 2013) and ISO/IEC 27002 (ISO/IEC27002, 2013). In order to facilitate easier integration of the views, the following cross-referencing mechanisms are used:

- For ITIL specific concepts, the reference would indicate the ITIL lifecycle and the relevant section in the lifecycle documentation. For example (SOP, 11.4) refers to Service Operation Processes section 11.4.

- For COBIT 5 specific concepts, the reference would indicate the framework and the process number. For example (COBIT 5, BAI06-BP1). The references will use the acronyms introduced in section 2.

- For ISO/IEC 27002 specific concepts, the reference would indicate the standard and relevant section in the documentation. For example (ISO/IEC27002, 8.1).

- Where a statement relates to more than one document the reference would be combined, separated by a semi-colon.

Activity 1: Requesting access

The first step towards gaining access to resources is requesting access. Users (Employees, Contractors and Visitors) could request access to a specific service or a set of services. These requests may originate from different sources. ITIL (SOP, 4.5) identifies four sources, namely HR (Human Resource) Management, a Service Request by the user, RFC (Request for Change), and a request from the Manager. Whenever someone is hired HR is required to initiate a request. The request is based on the user's business job requirements and access policies of the organization (IS0/IEC 27002, 9.2.2). The HR department must verify the user's identity and should ensure that his/her job requires the services being requested. To accomplish such a goal the request should be automated. In other words, HR systems for allowing access to information systems and services should be in place prior to employment (ISO/IEC 27002, 9.2.1).

This applies to the current services, but when there is a new service being deployed in the organization, the RFC will initiate the request. Such requests could happen when there are large upgrades to the system that affect a large number of user access rights within a particular group of users (SOP, 4.5.6). It is thus imperative that the change management processes consider the impact of user access.

General service requests, which may also include requests to access a service/system, are handled by the IT service desk. Such service requests should be classified and prioritized in order to assess the risks they might pose to the organizational processes and services (COBIT 5, DSS02-BP1). These requests must be recorded as they could help in future investigations (ISO/IEC 27002, 12.4). Some requests may not come from the user, but could originate from the manager of a particular department. This could happen when the manager assigns an internal user to perform a task that requires more access rights than currently available to that user. The request will then be channelled via the service desk.

Once a request is received, the next step is to verify that the user is who he/she claims to be and that he/she really needs the access. The next activity will discuss the verification process.

Activity 2: Verification

Verification according to ITIL is an administration-time activity that follows requests for access. It involves two actions. Firstly, the requester must be authenticated to ensure that he/she is who he/she claims to be (SOP, 4.5.5.2). Secondly, it must be ensured that he/she really needs the service (COBIT 5, DSS05-WP6). The process is illustrated in Figure 3.

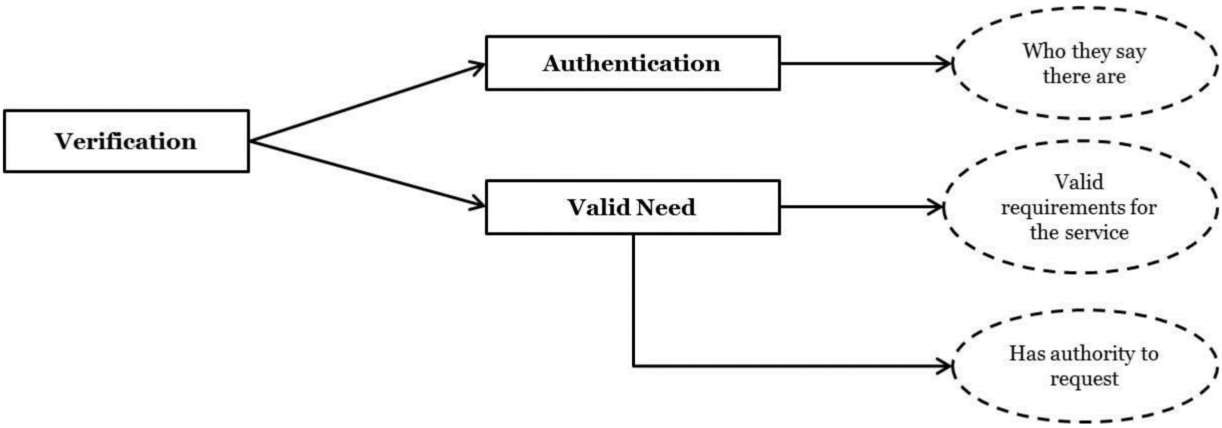


Figure 3: The Verification Process Activity

Sometimes the need might be validated from the fact that the requester is not the grantee, and that the requester has the authority to request this. Other times, if the requester is the grantee, logical mechanism such as usernames and passwords might not be sufficient. In that case physical mechanisms such as a user visiting the Service Desk with a suitable identification document may be required. However, for an indirect request, where a manager might request access for his/her users, a username and a password might still be acceptable as this is really just an execution of the manager's rights to request access.

Where the access request deals with sensitive services other verification mechanisms such as hardware tokens (e.g. smart cards) and biometrics (e.g. fingerprints or signatures) (SOP, 4.5.5.2), may be required.

Once the request has been verified the user could be provided the access rights required. This is further discussed in the next activity.

Activity 3: Providing rights

As soon as the verification process is complete the user is eligible to be given access rights in order to perform his/her day-to-day activities (ISO/IEC 27002, 9.2.2). Access rights are provided according to the user's job requirements and should be used for business purposes (COBIT 5, DSS06-02). One of the challenges in providing access rights arises when the user holds multiple access rights for different tasks. These multiple access rights could conflict with one another (SOP, 4.5.5.3). For example, a user needs to log the total number of hours worked per day for the purpose of calculating the salary earned (Task 1). However, Task 2 requires the user to approve the number of hours logged. This could be seen as a potential conflict or conflict of interest. However, such conflict can be avoided by carefully designing roles (SOP, 4.5.5.3).

At present most organizations are implementing the concepts of role-based access control when providing access rights to users (Bao, Song, Wang, Shen, & Yu, 2008). Role-based access control provides two steps: firstly, mapping roles to access rights and secondly, mapping users to their roles (Zhou, Varadharajan, & Hitchens, 2012) as depicted in Figure 4.

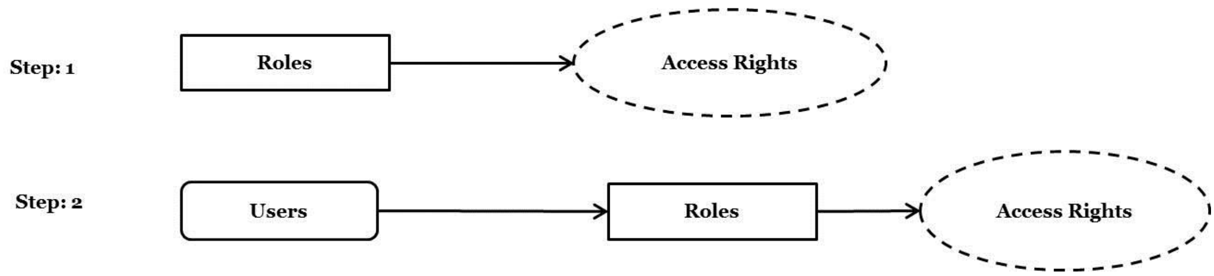


Figure 4: Role-Based Access Control Mappings

This makes the provision of access rights much simpler than providing each user access rights that are not mapped to a particular role. Since the user might have two or more roles assigned to him/her, each of the roles assigned should be recorded and documented (COBIT 5, DSS05; ISO/IEC, 9.2.2).

Activity 4: Monitoring identity status

In the previous activity users were mapped to their roles according to their business needs and requirements. As users continue in these roles changes to the roles may be required, and changes to access rights might arise (SOP, 4.5.5.4). It then becomes challenging to monitor the user's identity status or changes. Access control should cater for prevention of redundant user IDs and accounts (ISO/IEC 27002, 9.2.1), keep track of the date and time of changes, the type of change, the type of file accessed and also the program used to execute the change (COBIT 5,EDM03) when doing monitoring. The changes should be explicitly authorized by the appropriate authority prior being approved (ISO/IEC 27002, 12.1.1, 12.1.2).

A change could be triggered by the user changing his/her password. In this case automated tools could be useful to monitor such a change and automatically update the involved database or systems. Of course these changes could be legitimate or illegitimate. If the change is legitimate the records on the database will show that the user is actually active on the system. Whereas if the change is illegitimate, the database probably needs to integrate with intrusion detection tools which will lookout for passwords changing at the same time or odd patterns in passwords.

Today most organizations use tools, such as intrusion detection tools (COBIT 5, DSS05-BP7), to monitor their systems (Vigna, Gwalani, Srinivasan, Belding-Royer, & Kemmerer, 2004). Although changing the password of the user could be seen as minor, “big” changes such as job changes, promotions or demotions, transfers, resignation or death, dismissals, disciplinary action, and retirement (SOP, 4.5.5.4) can be challenging to monitor if automated tools are not in place.

It is of interest to discuss disciplinary action and dismissals. These might bring harm to the organization's valuable assets due to user's behaviour during the disciplinary action or dismissal period. In serious cases of misconduct, user access rights, duties and privileges should be temporarily suspended (ITIL: SOP, 4.5.5.4; ISO/IEC 27002, 7.2.3) and if necessary, he/she can be escorted off the organizational premises. Similarly, during suspension, all access should be restricted until the employee is ready to resume duties. And again, automated tools should be in place to re-activate the access rights revoked when appropriate.

Activity 5: Logging and tracking access

Threats originate not only from the outside world, but internal users can initiate threats unintentionally if policies are not followed. Users could breach the policies or misuse the organization's resources (SOP, 4.5.5.5). However, this can be minimized by implementing intrusion detection tools for tracking and logging user activities (ISO/IEC 27002, 12.4.1; COBIT 5, DSS05-BP7; ITIL: SOP, 4.5.5.5). When the user is suspected of resource misuse the logged files could help to speed up the investigation process (IS0/IEC 27002, 12.4.1; COBIT 5, DSS05-WP9). Even when there is a change in a user's identity or role, the change needs to be logged and be kept for the minimum duration period specified by the organization's security policies (ISO/IEC 27002, 9.2.5).

Access control should not only track unauthorized user access activities, but also track authorized user activities (ISO/IEC 27002, 19.2.5). A user can be given access rights to execute a task but never uses them. This could bring harm to the organization. For example, if a user has legitimate access rights and chose not use them, the access rights get compromised by the third party. This introduces vulnerability to other organizational systems unnecessarily. This activity is also accountable for making sure that the user access rights that were provided in activity 3 are properly used for their purpose. Clearly this activity should also be utilized when there is a change within the organization and those changes must be logged at all times.

Activity 6: Removing or restricting rights

Activity 3 discussed the concept of providing access rights to users. This activity is responsible for revoking those rights whenever the need arises. The process of removing or revoking access rights can take place when the user is dismissed, dies or resigns (ISO/IEC 27002, 7.2.3; SOP, 4.5.5.6). Removing rights needs to be performed in a timely manner to prevent unauthorized access by the dismissed user. Having the user de-registration procedures in place (ISO/IEC 27002, 9.2.1), which should be developed by information security management, could speed up the process.

The removal of the access rights process does not mean the user access rights should be completely erased as these could be needed again. Rather, the access rights should be deactivated. The same for restricting access rights to the user. Restricting access rights could be triggered when the user has changed roles, is under the disciplinary process or is on temporary leave for a short period of time (COBIT 5, APO07; ITIL: SOP, 4.5.5.6; ISO/IEC 27002, 7.2.3). However, a record of access rights should still be kept until the user is ready to resume his/her duties (COBIT 5, EDM03).

Discussion

The previous section identified six ITIL lifecycle access management activities and used them as a framework when integrating access control views found in ITIL, COBIT 5 and ISO/IEC 27002. This section serves to uncover the main access control themes found in these frameworks as discussed in section 2. Each of the six ITIL lifecycle access management activities are illustrated in Table 2 to highlight these main access control themes.

In Table 2, if minimal information is provided in a framework regarding a chosen theme, the (✓) will be shown. Furthermore, the (✓✓) shows that the framework has detailed information regarding the chosen theme. If the table entry is empty, there is no information contained in a framework for the chosen theme.

Table 2: A Summary of access control themes from COBIT 5, ITIL and ISO/IEC 27002

ITIL Activities	Access Control Themes	COBIT 5	ITIL	ISO/IEC 27002
Requesting Access	Automate access requests		✓✓	✓✓
	Classifying and prioritizing requests	✓✓		
	Record and document access requests	✓	✓✓	✓✓
	Originating sources of requesting access		✓✓	✓
Verification	Authentication	✓	✓✓	✓✓
	Verifying business needs		✓✓	✓✓
Providing Rights	Designing of roles		✓✓	✓✓
	Record and document roles		✓✓	✓✓
Monitoring Identity Status	Changes to access rights		✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓
	Prevention of redundant user IDs			✓✓
Logging and Tracking Access	Log files	✓	✓✓	✓✓
	Intrusion detection tools	✓✓	✓✓	✓✓
	Proper use of access rights	✓✓	✓✓	✓
Removing and Restricting access	Resignations		✓✓	✓✓
	Suspensions	✓	✓✓	✓✓
	Dismissals	✓	✓✓	✓✓

As can be seen in Table 2, many similarities exist between ITIL and ISO/IEC 27002. Where ITIL provides detailed information regarding a theme, similar detailed information is often provided in ISO/IEC 27002. For example, as can be seen in Table 2, both ITIL and ISO/IEC 27002 discuss the theme of 'Automate access requests' and that these requests should be recorded and documented at all times. The same applies to 'Verification' and 'Providing Rights' activities where 'Authentication' and 'Designing of roles' are also discussed. Similarly, when no information is provided for a theme in ITIL, no information is provided in ISO/IEC 27002 most of the time. For example, 'Classifying and prioritizing requests' is not detailed in either ITIL or ISO/IEC 27002. However, it is not always the case that information provided by ITIL is also provided by ISO/IEC 27002. For example, as shown in Table 2, ISO/IEC 27002 discusses the theme of 'Prevention of redundant user IDs' while ITIL does not.

Conversely, COBIT 5 addresses some of the themes which are not discussed in either ITIL or ISO/IEC 27002. For example, as shown in Table 2, the theme of `Classifying and prioritizing requests' under the 'Requesting access' activity is discussed by COBIT 5 but not by ITIL or ISO/IEC 27002. Where ITIL and ISO/IEC 27002 discuss a theme, COBIT 5 does not always provide information for that theme as can be seen from Table 2. For example, Table 2 highlights that information is not provided by COBIT 5 for certain themes such as 'Designing of roles' and 'Record and document roles' under the theme of 'Providing Rights'. Therefore, it can be determined that COBIT 5 is not as detailed as ITIL and ISO/IEC 27002 in terms of access control.

Based on this discussion, it can be argued that a combination of ITIL, COBIT 5 and ISO/IEC 27002 gives a more comprehensive view of access control as themes that are not covered in one framework or standard are covered by another framework or standard.

Conclusion

Access control is a critical feature in any organization, as valuable assets must be protected. This paper has shown that access control is well established, as it is discussed in ITIL, COBIT 5 and ISO/IEC 27002. However, not all of the access control issues are discussed in the same level of detail. No framework should be used in isolation when implementing access control in organizations. Therefore, it can be argued that a combination of ITIL, COBIT 5 and ISO/IEC 27002 gives a holistic view of access control as themes that are not detailed in one framework are detailed by another framework. Consider an abstracted holistic view of access control summary illustrated in Figure 5.

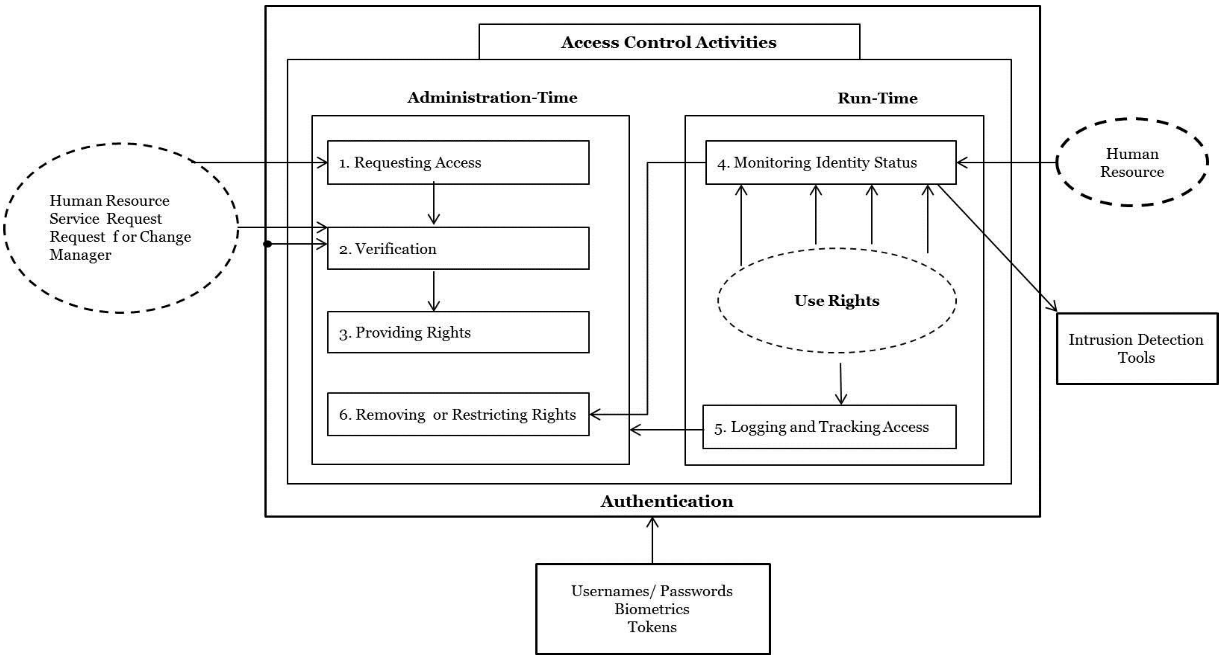


Figure 5: Summary: A holistic view of access control

In Figure 5, as previously mentioned, access requests might originate from any of the four sources identified by ITIL (SOP, 4.5). Thus the request needs to be authenticated and it must be verified that the request originating from the HR (for example), as illustrated by the three arrows pointing to the 'Verification' activity in Figure 5, before the required access rights are provided. Of course, the first three activities ensure that the requester will receive the access rights he/she requires (*administration*-time).

Whenever someone changes a job, resigns, retires, dies, is dismissed or is under the disciplinary process, the HR is notified. These needs to be monitored and necessary actions must be taken, as shown by the arrow from the 'Monitoring Identity Status' to the 'Removing or Restricting Rights' in Figure 5. These changes should be monitored using 'Intrusion Detection Tools' (*run-time*) as argued by COBIT 5 (COBIT 5, DSS05-BP7).

Further, the access rights provided should be tracked and logged as shown in Figure 5. Finally, the administrators of these access rights might need to look at the log files when performing some administration activities, as illustrated by the arrow between 'Logging and Tracking Access' and 'Removing or Restricting Rights' in Figure 5.

This paper could be useful for people involved with access control. The paper provided a holistic view of access control that has been built through analysing ITIL, COBIT 5 and ISO/IEC 27002. The integrated view frames access control in terms of the ITIL access management activities. Access control should not be a once-off effort, but a continuous one. Access rights should be managed across its lifecycle: access rules must be developed and requested (*administration-time*), used and the use monitored (*run-time*), and eventually revoked (*administration-time*). It is also important that access control does not stand alone, integration with organizational systems, such as the HR systems, as well as with other security services, such as authentication and intrusion detection services. Cross references in section 4 provides pointers to additional details regarding specific issues in the integrated view.

Acknowledgements: This work is based on the research supported in part by the South African National Research Network (SANReN).

References

Bao, Y., Song, J., Wang, D., Shen, D., & Yu, G. (2008). A role and context based access control model with UML. *The 9th International Conference for Young Computer Scientists* (pp. 1175-1180). Washington, DC, USA.

Greenfield, D. (2007). *ITIL, COBIT, and ISO 17799 provide a blueprint for managing IT services.* Retrieved 22 April 2015, from http://www.informationweek.com/standards-for-it governance/d/d-id/1062203?page number=1

ISACA. (2013). *COBIT 5 process assessment model (PAM)*

ISO/IEC27002. (2013). *Information technology - Security techniques - Code of practice for information security controls*. International Organization for Standardization/International Electronical Commission (ISO/IEC).

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems (TOCS)*, *10*(4), 265-310

Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic Computation & Economic Cybernetics Studies & Research*, *43*(1), 16.

OGC. (2007). *ITIL: Service operation*. London: TSO (The Stationary Office).

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* (pp. 8-pp). Big Island, HI.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *2008 Second Asia International Conference on Modeling & Simulation* (pp. 749-753). Kuala Lumpur, Malaysia

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60-66.

Sandhu, R., Bhamidipati, V., & Munawer, Q. (1999). The ARBAC97 model for role-based administration of roles. *ACM Transactions on Information and System Security (TISSEC)*, *2*(1), 105-135.

Verma, M. (2014). Comparison of IT governance framework: COBIT, ITIL and BS7799. Retrieved 19 April 2015, from http://www.slideshare.net/meghnaverma3956/comparison-of-it-governance-frameworkcobititil-ds?related=5

Vigna, G., Gwalan, S., Srinivasan, K., Belding-Royer, E. M., & Kemmerer, R. (2004). An intrusion detection tool for AODV-based ad hoc wireless networks. *20th Annual Computer Security Applications Conference* (pp. 16-27). Tucson, AZ.

Zhou, L., Varadharajan, V., & Hitchens, M. (2012). Trusted administration of large-scale cryptographic role-based access control systems. *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 714-721). TBD Liverpool, United Kingdom.

Concerns Regarding Service Authorization by IP address using Eduroam

Luzuko Tekeni, Reinhardt A.Botha And Kerry-Lynn Thomson
School of Information and Communication Technology
Nelson Mandela Metropolitan University
P.O.BOX 77000, Port Elizabeth 6031
E-mail:(Luzuko.Tekeni, Kerry-Lynn.Thomson, ReinhardtA.Botha)@nmmu.ac.za

***Abstract*—Eduroam is a secure WLAN roaming service between academic and research institutions around the globe. It allows users from participating institutions secure Internet access at any other participating visited institution using their home credentials. The authentication is verified by the home institution, while authorization is done by the visited institution. The user receives an IP address in the range of the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize via an IP address of the visited institution may include access to services that are not allowed at the home institution, due to legal agreements. This paper looks at typical legal agreements with service providers and explores the risks and countermeasures that need to be considered when using eduroam.**

I. Introduction

In the current generation, the number of users who connect to the Internet using mobile devices has increased significantly [1]. Most mobile users would like to get connectivity everywhere, including at home and at educational institutions. The TERENA (Trans European Research and Education Network Association) proposed a service for WLAN roaming between educational institutions and research networks [2]. This WLAN roaming service is called eduroam (EDUcation ROAMing). Eduroam is a secure WLAN roaming service between academic and research institutions around the globe [3]. It provides users (researchers, teachers and students) with secure Internet access at any eduroam participating visited institution using their home credentials with minimal administrative overhead [4]. Institutions see eduroam as very beneficial, as the exchange of students and academic staff members between institutions is very common. These students and academic staff members can use their home institution credentials. In eduroam, the authentication is verified by the home institution, while authorization is done by the visited institution [5].The student or academic staff member receives an IP address in the range of the visited institution, and accesses the Internet through the firewall and proxy servers of the visited institution. However, access granted to services that authorize via an IP address of the visited institution may include access to services that are not allowed at the home institution, due to legal agreements. This paper explores the risks involved and looks at legal agreements with service providers when an institution uses eduroam.

The rest of this paper is organized as follows. Section II looks at the background of the eduroam service. Section III provides an overview of the eduroam service as well as its components. Section IV looks at the IP-based authentication process and the underlying problems that can be encountered when roaming between academic institutions. Section V illustrates the example of a legal agreement between a client and a service provider and provides a brief description of a possible illegal case. Section VI provide a discussion of some possible risks, their impact and possible controls. Finally, section VII concludes the paper and serves as an introduction to future work..

II. The origin Of Eduroam

The eduroam service started as an idea of combining a RADIUS-based infrastructure with IEEE 802.1x protocol for roaming Internet access across institutions in Europe [6]. The actual eduroam service started in 2003 within TERENA's Task Force on Mobility, TF-Mobility [7]. During that time many institutions showed an interest in eduroam by joining. Those institutions were from the Netherlands, Finland, Croatia, United Kingdom, Portugal and Germany [8]. Gradually, other NRENs (National Research and Education Networks) in Europe began joining what was then named eduroam [1]. In December 2004, Australia became involved and was the first non-European country to join eduroam [9]. According to the eduroam website, eduroam "is now available in 68 territories worldwide" [10], but is only available at certain locations within those countries, as long as their NRENs have signed the eduroam Compliance Statement [11]

III. Eduroam Service and Components

The eduroam infrastructure is based on hierarchically organized RADIUS proxy servers [12] and the IEEE 802.1x protocol [4]. This initiative makes use of three levels of RADIUS proxy servers, namely: Top-level server (Confederation), National-level server (Federation) and Institutional-level server (Edge) [3]. The Top-level server acts as the bridge between National-level servers for global communication, while the National-level server is responsible for connecting institutions within the country. Every institution wanting to join eduroam connects to its National-level server and deploys a dedicated server for eduroam.

Figure 1 shows a user who wants to connect to eduroam at `institution_A` (visited institution), whose home institution is B (home institution). In this case, the users supplicant software contacts the Access Point (AP) using 802.1x with EAP (Extensible Authentication Protocol) protocol. The EAP protocol provides integrity and confidentiality to protect the transportation of user credentials throughout the hierarchy of RADIUS servers [13]. Then the AP contacts its local RADIUS server for authentication. The RADIUS server examines the realm part of the username, since it is not a local realm, then proxies the request through the hierarchy of RADIUS servers until `institution_B`

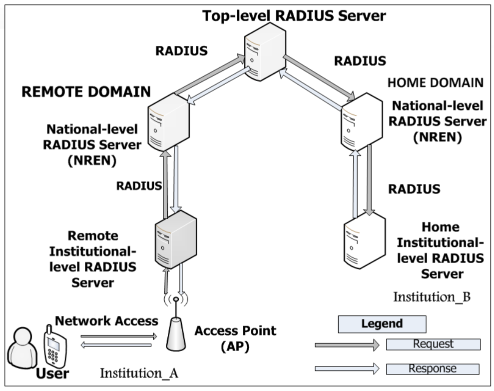


Fig. 1: Eduroam Infrastructure

is reached. `Institution_B` RADIUS server decapsulates the EAP massage and verifies the user's credentials. It can either accept or deny the request by proxying the results in the reverse order using the same path. The AP at `institution_A` informs the user about the outcomes ('accept' or 'deny') and the connection is established (if the response is 'accept').

IV. IP-Based Authorization Process

Some services, such as digital libraries, at universities use an IP address to authorize users. This presents a potential problem when using eduroam. Figure 2 shows home and visited institutions and their service provider. In this example, before a user can be given any kind of access, the IP-based process for authentication and authorization must take place first. The user then roams between the two institutions using his or her home institutional credentials.

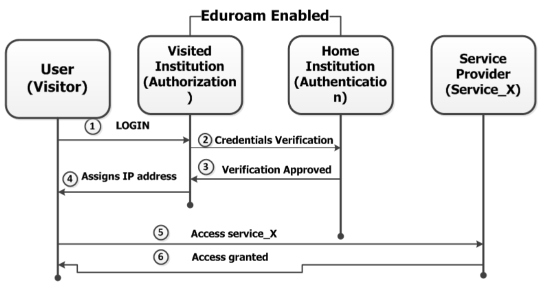


Fig. 2: IP-Based Process

When the user reaches the visited institution and connects to eduroam, the following happens:

1) The user tries to login at the visited institution using his or her home credentials.
2) The visited institution examines the realm part of the username and sees that the user belongs to the home institution, and then sends the user credentials through the hierarchy of RADIUS servers for authentication (verification) to the home institution.
3) The home institution decapsulates the message and verifies the users credentials, it can either accept or deny the request by sending back the response to the visited institution.
4) The visited institution receives the response and grants internet access if the results are positive (accepted), and assigns an IP address to the user.
5) The user accesses the service provider's resource (`service_X`) using the assigned visited institutional IP address.
6) The service provider verifies the validity of the IP address and gives permission to the user based on the provided IP address (visited institutional IP address).

This would result in an unauthorized user gaining access to certain services of the visited institution.

V. Case Description

This section is divide into two subsections, the first subsection looks at the legal agreement example which was extracted between the home institution and the service provider and the second subsection explores illegal case based on the example provided in subsection V-A.

A. Legal Agreements

The increase and growth of the Internet and online services has forced organizations to outsource certain online services such as online databases [14]. When an organization outsources a particular online database service, a contract between the organization and the service provider is signed. This contract is called a Service Level Agreement (SLA) [15]. "SLA is a contract between a user and a provider of a service specifying the conditions under which a service may be used" [16]. Three of the Service Level Agreements were reviewed and all of them state a similar definition but one is used as an example below in figure 3. This was extracted from the Consortium License Agreement between the home institution and the service provider.

> "**Authorised Users"** means individuals who are authorised by the Licensee to access the Licensee's information services whether from a computer or terminal on the Licensee's Secure Network, or off site via a modem link to a valid IP address on the Licensee's Secure Network and who are affiliated to the Licensee as a current student, faculty member or employee of the Licensee. Persons who are not a current student, faculty member or an employee of the Licensee, but who are permitted to access the Secure Network from computer terminals within the Library Premises ["Walk-In Users"] are deemed to be Authorised Users, only for the time they are within the Library Premises. Walk-In Users may not be given means to access the Licensed Material when they are not within the Library Premises.

Fig. 3: Service Level Agreement

The main concept that needs to be highlighted in figure 3 is the "Walk-In Users" (visitors). According to figure 3 above, walk-In Users are only able to access Licensed Material from computer terminals within the Library premises. In other words the users must be within the physical premises of the Library, but this SLA is too antiquated because most users are using their mobile devices to access the wireless. This statement specified on the SLA needs to be reviewed by the authorities. Eduroam users from another institution could breach the SLA if they accessed the Licensed Material from their own devices not on the Library Premises. The next section looks at this situation in more details of breaching the SLA through the introduction of eduroam.

B. Illegal Access

An illegal case can be defined as one of the two agreed entities breaking the agreement and this is often referred to as breaching the SLA [17]. In many cases the SLA is viewed from the service providers perspective. In other words, a breach would be constituted if the service provider cannot provide the level of service agreed upon for the customer to meet its goals [18]. Before eduroam, if a user visited a particular institution, he or she would be given a guest account. This would make the visitor known on the physical premises.

Eduroam is advantageous in that it reduces the amount of work to be done by network administrators, allows easy and secure Internet access at any place around the globe. However many risks also came along especially to services that authorize via an IP address. The main focus of this paper is the concern of breaching the SLA to library services that authorize via an IP address when eduroam is implemented. Figure 4 below shows a situation when a user is at home institution using eduroam.

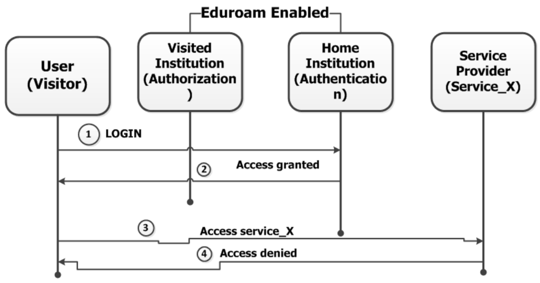


Fig. 4: Eduroam Access at Home Institution

When the user accesses eduroam at the home institution and tries to access a service which the institution does not have access to, the following happens:

1) The user tries to login at the home institution using his or her credentials and the EAP message is carried to the home server.
2) The home institutional server decapsulates the message and verifies the users credentials, sees that the user is the home user, assigns an IP address and grants Internet access.
3) The user accesses the service provider's resource (`service_X`) using the assigned IP address.
4) The service provider verifies the validity of the IP address and discovers that the received IP address has no subscription to access the service then denies access to the user.

If the user does not have access to `service_X` at home (home institution) but when visiting a particular institution that has subscription to the same service, the user is able to access that service without requesting authorization to it. Section V-A in figure 3 clearly states that "Walk-In Users"(visitors) are deemed to be authorized users only if they are using computer terminals or workstations within the Library Premises, meaning their presence is noticed. But the current eduroam infrastructure is lacking proper authorization mechanisms to those IP services and tracking of eduroam users.

VI. Discussion

Eduroam is a new service that has been recently integrated to the existing networks in academic institutions and research networks in many countries around the world. Academic institutions and research networks have policies in place that govern how the access to the Internet services can be granted, now that eduroam is implemented possible risks arises. The subsections below take a closer look at the identified risks, the impact that they might have and as well as some possible controls that could be used.

A. Possible Risks

According to [19] [20], risk can be defined as the possibility of an undesired outcome or the absence of the desired outcome to a service. It "is a future event that may or may not occur" [19]. For this paper we explore the risks from different perspectives: the Users, Service Providers, and Libraries at universities. Each of these risk perspectives are described below:

Users: when users visit a particular institution, they could have access to services that they normally do not have when they are at their home institution. These users can be regarded as happy users because they have access to services that they are not subscribed to, but the users from the visited institution to the home institution could be faced with the challenge of not having access to services that they normally do when they are at their home institution, these type of users can be regarded as unhappy users. In this case, the situation can be seen as "unfair" to some of the users while others are enjoying the benefits of accessing services that are not available at home.

Service Providers: The service providers are the ones that are responsible to provide a particular service to the users. In this context, the service providers could find themselves in a position of losing their income when the users are accessing the service. In other words the user might visit the institution just to access the service that is unavailable while he or she is at home, on the other hand the user might unsubscribe to a particular service intentionally because he or she knows that the service is available to the neighbors and could just go and visit to access it, in this way the service provider might find themselves faced with a big challenge if the situation is not controlled.

Libraries: Many libraries at universities use an IP address to authorize users. This presents a potential risk when using eduroam. The eduroam user is given an IP address when visiting a particular institution which gives him or her access to services that are normally unavailable at home. This would result in an unauthorized user gaining access to certain services of the visited institution and the visited institution might find themselves breaching the SLA if these users access the Licensed Material from their own devices not on the Library Premises as stated on the license agreement in figure 3 above. Libraries therefore run a risk of being held legally liable.

Libraries also do not want to subscribe to unused (and therefore unnecessary) services. So if at `institution_X`, the librarian staff members are capturing their online database usage for the purpose of terminating the contract if an online database is not being used. Visitors accessing these databases through eduroam may lead to incorrect statistics captured. This could lead to the library not terminating the use of an online database. At first this risk may seem neglible, but it is worth remembering that services in this category (possible cancellation) is already little used-even a small number of visitors accessing could multiply the number of accesses thereby rendering the service in the expensive but needed category. There is no tracking of users and their activities in the current eduroam infrastructure and therefore it is impossible to assess the extent of visitor user access.

B. Impact

The impact helps to identify the probability of the risk, how vulnerable is the service to the identified risk and whether the immediate actions are needed or not. For each of the identified risks above, their impact is analyzed below.

Users: The impact on users could be positive or negative, depending on the specific circumstances. To understand this statement consider the South African Academic landscape. Table 1 below shows a comparison of digital libraries available at selected South African Universities and Research Institutes. Note that for brevity only a selected of the digital libraries at each institution is shown. As this is illustrative the names of institutions are not used. Selected institutions participate in eduroam in South Africa.

Comparison of Eduroam Institutions			
Digital Libraries	Uni1	Unit2	Unit3
Access Engineering	No	Yes	Yes
Access Pharmacy	No	No	Yes
AccessScience	No	Yes	Yes
ACM	Yes	Yes	No
African Journals	Yes	No	No
Biomed Central	Yes	No	Yes
Emerald	No	Yes	Yes
IEEE Xplore	Yes	Yes	Yes
ISI Web of Knowledge	No	No	Yes
LexisNexis Academic	No	No	Yes
Sabinet	Yes	Yes	Yes
SAGE	Yes	Yes	Yes
ScienceDirect	Yes	Yes	Yes

TABLE I: Comparison of Digital Libraries at institutions

Based on the results shown in table 1, the risk varies depending on the institution that the user is visiting. For example, if the user visits the Unit1 from Unit3, that user can access the ACM database whereas at Unit3 he or she does not have access to the ACM database. While users from Unit1 will be very happy with the situation (as they have more access), users from Unit1 visiting Unit3 will be less happy as they do not have access to the database that he or she usually has when he or she is at the home institution.

Service Providers: Service providers will view this as a risk since it has a potential impact on their business.To some extent service providers are depending on the honesty of their clients that they provide the service to. If an authorization issues exist at the client side, the service provider is at risk. The situation needs to be controlled by the clients because if the service provider sets an SLA, there is no assurance that the clients will enforce the SLA effectively.

Libraries at Universities: Universities have thousands of users to manage, potentially including several visitors. Keeping track of registered users and visitors could be challenging in this environment. The advantages of eduroam infrastructure undoubtedly exceeds the possibility of misuse. This situation does not affect the institutions only, even the service providers are included, their service could be misused by the visitors because they know they are not paying for it, but maintaining access records on individual level rather than institutional level is certainly more costly.

C. Possible Controls

Even though a high-level analysis of risk involved may not identify major risk it is worth noting that possible controls may already exist to address this situation. While the situation needs to be further analysed, two ways are highlighted here.

One possible way of controlling the risks as described in subsection VI-A and their impact described in subsection VI-B, involves the use of a Virtual Private Network (VPN) tunnel. A VPN provides a complete data privacy and integrity for users who access the network from outside their intranet in a secure manner [21]. For instance, by enabling VPN between the user and the service provider, a secure tunnel will be established. This will help to improve the IP-based level of security. In other words, adding another layer of security in the IP-based authorization process. Figure 5 shows how a VPN tunnel between the user and the service provider in eduroam network can address the risk of a user not having access to services when visiting institutions without access to the required service. However, this only address the risk from the perspective of a user not having access to something that he or she normally have and others. Refer to figure 2 for step one to three and step five to six for their descriptions; the fourth step improves the IP address that is normally assigned by the visited institution to access a service. Meaning the user will now make use of the tunnel being established to allow one-to-one communication rather than consulting the visited institution as it can be seen in figure 2. The benefits that the unauthorized user was enjoying will now

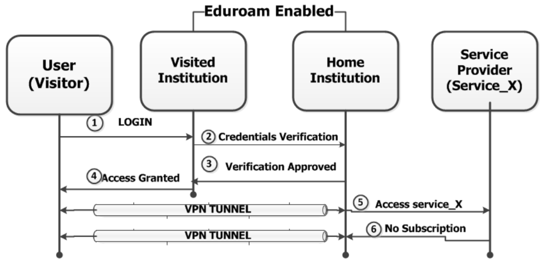


Fig. 5: VPN Tunnel in Eduroam

be controlled by the tunnel.

Since the issue here is really that of a users identity to be used across institutions, solutions may exist in the federated identity management space. A possible solution may be to introduce technologies such as Shibboleth, which will act as an intermediate third party between the home institution and the service provider on behalf of the visited institution as shown in figure 6 [22]. Figure 6 shows a high-level view of how Shibboleth could be used in eduroam. A Where Are You From

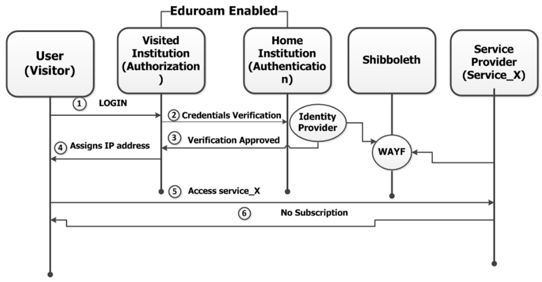


Fig. 6: Shibboleth in Eduroam

(WAYF) database will be used to identify the user and once that it is done, the service provider will be able to access the users attributes from the home institution. Shibboleth will be able to identify services that are allowed at the home institution for the user, using SAML (Security Assertion Makeup Language) [23]. This will, however, require service to evaluate SAML attributed to do authorization

VII. CONCLUSION

This paper, discussed the origin ot the eduroam service and its components. The eduroam initiative has proven to be more secure and scalable [7] by making use of a hierarchically organised RADIUS servers and IEEE 802.1x protocol with EAP protocol. Eduroam is being used in many countries with many benefits and advantages. However, this paper argues that authorization can be a problem for services that do IP-based authorization. We analysed an example of an SLA between the home institution and the service provider to revealed that eduroam authorization potentially allows us to breach the SLA with some digital libraries (or other services) that authorize via an IP. The paper discussed possible risks and their impact. Finally some possible controls were mentioned. Future research will investigate possible solutions in more details. This will contribute towards securing services that authorize via an IP address in the eduroam service. While it may be argued that the risk is neglible, eduroam is growing, as more and more institutions and NRENs and their constituents are joining in. It may therefore be prudent to address this issue before the scale of eduroam turns a molehill into a mountain.

REFERENCES

[1] K. Wierenga and L. Florio, "Eduroam: past, present and future," *Computational methods in science and technology*, vol. 11, no. 2, pp. 169–173, 2005.

[2] I. Yamaguchi, T. Suzuki, H. Goto, and H. Sone, "Centralized authentication system for location privacy protection and low operational cost of large scale wlan roaming," in *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*. IEEE, 2010, pp. 297–299.

[3] K. Wierenga, S. Winter, R. Arends, R. Poortinga, J. R. DFN, D. Simonsen, M. Sova, and M. S. DFN, "Deliverable dj5. 1.4: Inter-nren roaming architecture: Description and development items," *GN2 JRA5, GÉANT*, vol. 2, 2006.

[4] M. Milinović, J. R. DFN, S. Winter, and L. Florio, "Deliverable ds5. 1.1: eduroam service definition and implementation plan," 2008.

[5] Ó. Cánovas, A. F. Gómez-Skarmeta, G. López, and M. Sánchez, "Deploying authorisation mechanisms for federated services in eduroam (dame)," *Internet Research*, vol. 17, no. 5, pp. 479–494, 2007.

[6] TERENA. (2012) eduroam® celebrates a decade of providing secure roaming internet access for users. [Online]. Available: http://www.terena.org/news/fullstory.php?news_id=3162

[7] Eduroam. (n.d) About eduroam. [Online]. Available: https://www.eduroam.org/index.php?p=about

[8] D. Olesen. (2003) Terena annual report 2003. [Online]. Available: http://www.terena.org/publications/files/terena_final_2003.pdf

[9] TERENA. (2004) Eduroam goes global. [Online]. Available: http://www.terena.org/news/archive/2004/newsflash163.pdf

[10] Eduroam. (n.d) Where can i eduroam? [Online]. Available: https://www.eduroam.org/index.php?p=where

[11] TERENA. (2011) eduroam compliance statement. [Online]. Available: https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf

[12] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," 2000.

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz *et al.*, "Extensible authentication protocol (eap)," RFC 3748, June, Tech. Rep., 2004.

[14] J. Huai, "Design service level agreements in outsourcing contracts," in *Management and Service Science (MASS), 2010 International Conference on*. IEEE, 2010, pp. 1–4.

[15] R. Schutz, S. McLaughlin, T. Daeleman, M. Luoma, M. Peuhkuri, P. Carlen, and J. Haines, "Protected core networking (pcn): Pcn qos and sla definition," in *Military Communications and Information Systems Conference (MCC), 2013*. IEEE, 2013, pp. 1–9.

[16] T. Sandholm, "Service level agreement requirements of an accounting-driven computational grid," *Royal Institute of Technology, Stockholm, Sweden, Tech. Rep. TRITA-NA-0533*, 2005.

[17] Z.-Z. Yau, "Design of sla management framework with case," 2005.

[18] A. Aleem and C. R. Sprott, "Let me in the cloud: analysis of the benefit and risk assessment of cloud platform," *Journal of Financial Crime*, vol. 20, no. 1, pp. 6–24, 2012.

[19] E. S. Chia, "Risk assessment framework for project management," in *Engineering Management Conference, 2006 IEEE International*, Sept 2006, pp. 376–379.

[20] P. Smith and G. Merritt, "Proactive risk management: Controlling uncertainty in product development. 2002."

[21] S. Rangarajan, A. Takkallapalli, S. Mukherjee, S. Paul, and S. Miller, "Adaptive vpn: Tradeoff between security levels and value-added services in virtual private networks," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 93–113, 2004.

[22] M. Erdos and S. Cantor, "Shibboleth architecture draft v05," *Internet2/MACE, May*, vol. 2, 2002.

[23] S. Cantor, I. J. Kemp, N. R. Philpott, and E. Maler, "Assertions and protocols for the oasis security assertion markup language," *OASIS Standard (March 2005)*, 2005.

An Overview of Authentication and Authorization Approaches used in Federated Domains

Luzuko Tekeni, Reinhardt A. Botha and Kerry-Lynn Thomson
School of Information and Communication Technology
Nelson Mandela Metropolitan University, P.0.BOX 77000, Port Elizabeth 6031
E-mail: {Luzuko.Tekeni, ReinhardtA.Botha, Kerry-Lynn.Thomson}@nmmu.ac.za

***Abstract*—Access control is a critical feature in a federated identity management environment. Various approaches of access controls are widely deployed and proposed within the federated identity management domains. This paper provides a high-level overview of access control approaches that have the capabilities to extend their functionality beyond the campus network.**

***Index Terms*—Federation, Identity, Access control**

I. Introduction

In the environment of academic and research institutions, mobility is becoming a requirement for resource sharing and collaboration. Academic staff members, researchers and students access online resources regardless of the location. While research and academic users are enjoying the benefits of having access to online resources using Single Sign-On (SSO) services in federated domains their network administrators and service providers are faced with the challenge of identifying them (Authentication) and controlling access (Authorization) to resources in remote locations.

Many networks use IP addresses or usernames and passwords to authenticate and authorize users to online resources. These approaches however, do not scale well in federated domains. Hence in this paper, we provide a high-level overview of authentication and authorization approaches that have the capabilities to extend their functionality beyond the campus network. In this paper, authentication and authorization will be referred to as access control.

This paper is organized as follows. Section II provides an abstract overview of the access control approaches commonly used in federated domains. Section III demonstrates a scenario of access control when a user is visiting a remote domain from his or her home domain using attribute-based mechanisms to access `service_X`. Finally, section IV concludes the paper.

II. Existing Possible Solutions

Several aspects of federated approaches to online resource sharing, have been addressed by several projects [1] which are not bound by location. Examples of projects are eduroam [2], eduGAIN [3], Shibboleth [4] and the InCommon [5] federation. The idea is that authentication is verified at the home domain by the Identity Provider (IdP) and the authorization is carried out at the remote domain by the Service Provider (SP) of the resource. These approaches have similar goals to access control such as Single Sign-On (SSO) Capabilities, protecting user privacy, and providing fine-grained access control in research and high education communities. The option of requesting user attributes using the OASIS Security Assertion Markup Language (SAML) framework [6] as the protocol request/response message seems to be the best way to go. These federated approaches are briefly explained below.

A. eduroam

eduroam (EDUcation ROAMing) is an inter-institutional roaming service developed by TERENA (Trans European Research and Education Network Association) to provide secure Internet WLAN access across campuses in research and higher education institutions in Europe, using a hierarchy of RADIUS servers with IEEE802.1x protocol [7]. The eduroam service has now spread its wings to other continents as well [8]. In each country eduroam is monitored by the NRENs (National Research and Education Networks). However, the current deployed service addresses only authentication while lacking authorization mechanisms.

B. eduGAIN

It is a service established under the umbrella of the GEANT project to join together identity federations, and allows the exchange of information such as Identity, Authentication and Authorization (AAI) between federations and have the ability of identifying the user's (visitor) home domain by making use of a Metadata Database [3].

C. Shibboleth

Shibboleth is an initiative based on an open source software package developed by Internet2/MACE. It emphasizes user privacy protection [9] and has the ability to request user attributes between federations using SAML. In Shibboleth, the user's home location is discovered by making use of a "Where-Are-You-From" database.

D. InCommon Federation

It is a USA-based initiative that not only provides trust relationships and privacy protection over user information, but also offers certificates, assurance program and multifactor authentication services in research and higher education institutions, and their partners [5].

III. Attribute-Based Access Control

All of the above federated approaches use attributes to control access. The attributes can be a name, role and department of the user [10]. Figure 1 illustrates the steps in the process:

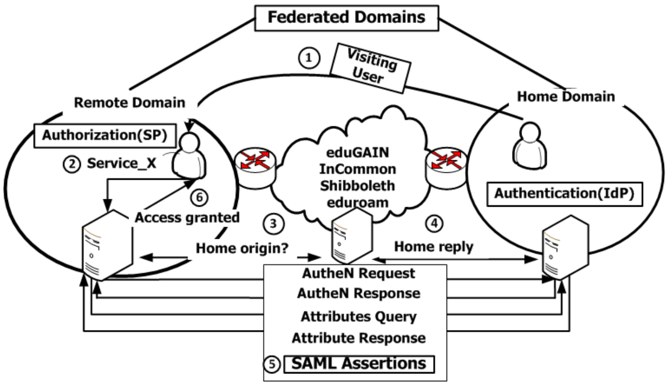


Fig. 1: Federated Domains

1) The user visits a remote domain that is participating in a federation.
2) Then, the user tries to access `service_X` at the remote domain.
3) The remote domain server will redirect the user request to a server, a ”Where-Are-You-From” with database to discover user’s home domain.
4) This server will in turn redirect the user for authentication if not authenticated already to his or her home domain.
5) The IdP at the home domain verifies the confidentiality (credentials) of the user and then the SAML protocol takes place, to exchange user information assertions.
6) Finally, the user is either allowed or denied access to `service_X` based on the attributes supplied.

IV. Conclusion

In this paper we looked at existing solutions that can be implemented to provide fine-grained access control in federated domains and some of these solutions can be integrated with minor modifications. A brief illustration of how a user accesses a service at the remote domain was provided. The South African National Research Network (SANReN) should consider deploying one of the approaches discussed in section II above to the eduroam service as it is under their control, to provide authorization mechanisms.

References

[1] G. López, Ó. Cánovas, A. F. Gómez-Skarmeta, and M. Sánchez, “A proposal for extending the¡ i¿ eduroam¡/i¿ infrastructure with authorization mechanisms,” *Computer Standards & Interfaces*, vol. 30, no. 6, pp. 418–423, 2008.

[2] Eduroam. (n.d) About eduroam. [Online]. Available: https://www.eduroam.org/index.php?p=about

[3] GEANT. (n.d) About edugain. [Online]. Available: http://www.geant.net/service/eduGAIN/about_edugain/Pages/AbouteduGAIN.aspx

[4] Shibboleth. (n.d) What’s shibboleth? [Online]. Available: http://shibboleth.net/about/

[5] InCommon. (n.d) Incommon federation. [Online]. Available: http://www.incommonfederation.org/federation/

[6] T. Wisniewski, E. T. Nadalin, S. Cantor, I. J. Hodges, and N. P. Mishra, “Saml v2. 0 executive overview,” 2005.

[7] K. Wierenga and L. Florio, “Eduroam: past, present and future,” *Computational methods in science and technology*, vol. 11, no. 2, pp. 169–173, 2005.

[8] TERENA. (2004) Eduroam goes global. [Online]. Available: http://www.terena.org/news/archive/2004/newsflash163.pdf

[9] M. Erdos and S. Cantor, “Shibboleth architecture draft v05,” *Internet2/MACE, May*, vol. 2, 2002.

[10] OASIS. (2009) Xacml overview, extensible access control markup language (xacml). [Online]. Available: http://xml.coverpages.org/xacml.html

Luzuko Tekeni recently completed his BTech (IT) degree in the School of ICT at the Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, and is presently studying towards his MTech(IT) at the same institution. His research interests include federated identity management, and networking.

Reinhardt A. Botha and Kerry-Lynn Thomson are professors in the School of ICT at Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.