Annales UMCS Informatica AI XIV, 2 (2014) 31–45
DOI: 10.2478/umcsinfo-2014-0010

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Authentication Mechanism Based on Adaptable Context Management Framework for Secure Network Services

Mariusz Sepczuk[1]*

[1] *Institute of Telecommunications, Warsaw University of Technology, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland*

Abstract – A system, which uses context information is a new trend in IT. A lot of researchers create frameworks, which collect some data and perform actions based on them. Recently, there have been observed more and more different security solutions, in which we can use context. But not each works dynamically and ensures a high level of users quality of experience (QoE). This paper outlines what the context information is and shows a secure and user-friendly authentication mechanism for a mail box in cloud computing, based on using contextual data.

1 Introduction

Nowadays, we can observe that quantity of different kinds of data increases very fast. This information can be divided into many categories. Each data gives us details about a surrounding word. Some of them can be interpreted completely in a new way, because they depend on the context of particular information. Generally, we can say that the context it is information, which describes a user. For many people the first thing (and usually only this one), which associates with the user's context data, is a localization. And it is a good intuition. We have a lot of context information, even grouped into some categories. But the context data are something more. They are very helpful in reasoning about totally new information. It is especially powerful, when we want to decide how to adapt systems to the dynamically changing environment. In this paper it is shown how to use and adapt contextual information in security. The paper is structured as follows. Section 2 explains what is a context, how we can categorize and classify the context. Section 3 includes general information about an authentication mechanism and its association with the context data. Section 4 describes how to

*msepczuk@tele.pw.edu.pl

use a context security framework to create the authentication mechanism based on the contextual data. Section 5 shows a practical example of created authentication mechanism. Section 6 relates to the previous research about context-aware authentication. Section 7 includes comparison of existing context-aware authentication mechanisms, discussion about them, conclusion and future works.

1.1 Context Information Definition

At first, let us explain what the context information is. In [**17**] Schilit describes a context-aware system as a system, which can adapt to dynamically changing location, but also associated with a type of device, people relations and time. Moreover, he determined three major aspects of context: where you are, with whom and what resources are in your neighbourhood. He has also emphasized that the context is more than just your position, but it includes more information, which changes in time. In [**9**] the author claims that the context information are the answers to the question beginning with: Who? Where? What? When? Another, but a similar definition of context is shown in [**21**]. Context is a description of dependency between context states and their interpretation by the system and can be user, application or device oriented. Many other papers describe what the context is, but, in general, they include categories of the context, not exact definition. Using one of these terms we can have a problem with making decision whether new information is the context information or not. A simple and universal definition is created by Wrona in [**22**]. According to him the context data is information, which can describe state of entity. In this definition we do not qualify what categories could be exactly the context, but only specify information that characterizes entity.

1.2 Context Information Categories

All context data can be divided into two subclasses: internal and external. We talk about the internal context when we keep in mind everything which is associated with a user: his/her name, look, behaviour, childhood, etc. The external context data consists of environment in which a user is, so here we have information about location, temperature, etc. Naturally, that division is not permanent. In some situations information about localization could be the internal subclass (especially when we refer each data with GPS coordinates) and other categories could be external. It is flexible and depends on entity which we want to describe. Earlier, in the text, I have just mentioned about context categories, like a localization, a user and etc. Below is a description of some of them (a reader of this paper probably knows what each category means, but just in case I will describe it).

A system context defines a computing system in which all applications are run. This includes the data about type of device (e.g. mobile phone), type of network (e.g. LTE network), CPU, MAC and IP address, bandwidth, communication with other devices, protocols, etc. This category includes the data from the ISO OSI model, too.

An user context describes all data about the exact person. Thus, here we have information about the user's whole life, identity like a name, surname, ID or user's age. Furthermore, it refers to the information about medical and educational history, features of appearance (i.e. colour of eyes, iris, skin, shape of face, etc.), biometric data, knowledge about current user's goals, position at work or school, user's relationship, family, information of body and psychic conditions, etc. An environmental context refers to the context information about physical environmental, which was not discovered by a user and system categories. In this class of context we can find data about temperature, precipitation, weather conditions, atmospheric pressure, humidity, etc.

A temporal and spatial context consists of information about time, like hour, minute, second, part of day, part of year and localization, like geographic coordinates (e.g. GPS system). An activity context describes data about occurrence and when it happened. Here we can match events like entering to building or leaving a meeting.

And finally, a device context in which we have information about battery lifetime, profile and activities of device, current location, etc.

1.3 Context Data Classification

Besides the context categories, we have a model of classification which includes their features (see Fig. 1).

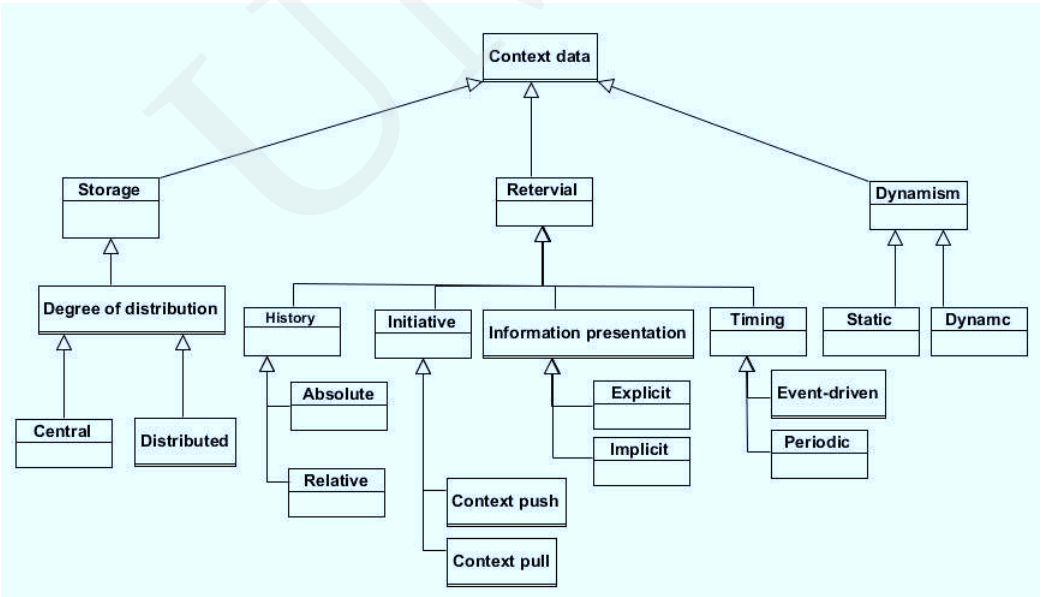

Fig. 1. Classification of context data

When we consider the context information we keep in mind three aspects: storage of context, retrieval of context and its dynamics. The storage refers to the degree of data distribution: central or distributed. In the central, the context information is stored

in one location, like database or Hidden Markov Model. In the distributed data are stored in a few places. Data also can be put in neural networks [**15**] or decision trees [**16**]. The second property is retrieval which includes different aspects of retrieving of context information like:

- history,
  - absolute - only present data are important for context; previous context information is no longer used,
  - relative - context information depends on past, present and future data; thus, it is important to store it in the repository for later retrieve; obviously a lot of data take more space and its retrieving is time consuming,
- initiative,
  - context-pull - the system receives context information without sending first requests; first devices send data to the system,
  - context-push - the system first sends a request to get new context information,
- information presentation,
  - explicit - context information is the same as raw data from CIP, so we do not need to use a context model to translate raw data to the context data; this kind of information is called low- level data,
  - implicit - the system gets context data which was earlier translated by a context model; this kind of information can be called high-level data,
- timing,
  - event-driven - the system gets context information when an event happens; so if something happens the system receives information about that and only in that situation,
  - periodic - the system receives context information periodically, according to an established schedule.

The last property is a dynamics. The system can be located in the environment, which changed overtime, so context information changes dynamically. On the other hand, the environment can be static and the context information never changes or changes very slowly.

1.4 Why Context Data?

Now it is the right time to ask and answer the question: Why can context data be useful? Is it really necessary to use? Obviously, the answer is positive. Having knowledge about context could it be really useful when we want to associate it with the provided service. The contextual data could be fundamental information in the reasoning process. The main goal of reasoning is to get totally new information (e.g. about actual conditions the system environment) and based on them correctly adapt the system. As a result, the system can work properly with the optimal usage of resources, power and etc. Of course, the contest data can be used in different kinds of services, therefore a good idea is to take advantage of them in the security mechanism.

This approach can be effective when we want to ensure a right level of protection of service. In this paper a model of a chosen security mechanism based on the context data-authentication is proposed. A created solution can be used to identify a user who wants to sign up to his/her e -mail box in a cloud computing, but this solution can work in other environments, too. But, at first, it is good to remind what an authentication is, what kind we can use and how we can connect it with context.

2 Authentication

An authentication is a process of verifying identity of entity. The entity is defined as people and devices. This mechanism confirms or not entitys identity without checking the permission for using resources. The main purpose of critical services, like an online bank account or e-mail account, is to provide the authentication mechanism with a proper level of protection and at the same time ensure user's satisfaction (process of user's identity should not be too complex and too long).

2.1 Classification of the Authentication

General classification of the authentication methods focuses on features, which each protocol can use for to identification [**2**] :

- something you know - it refers to the information which only the dedicated user has, like private key or password,
- something you have - it refers to a subject which is in the user's possession, like a generator of codes (token) or a key to a lock,
- something you are - it refers to biometric factors, like fingerprints or hand geometry.

In most IT systems and networks we can find a few main types of authentication. They are:

- one- way authentication - in this method only one side, usually a client of application, confirms your identity using login and password,
- two-party authentication - in this method both, a client and a server, sides have to confirm your identity. It could be done in two phases (two-phase authentication) when one of the sites confirms identity, then the second does the same or in one phase (one-phase authentication) when a client and server authenticates at the same time,
- trusted third-party authentication - this type makes us of the third party, which has high level of reputation. The third party verifies identity of a client and after right confirmation a client can show this confirmation to a server and based on it correctly authenticates,

- single sign on authentication - the idea of this is to minimalize a number of written authentication data, like password. When a user correctly authenticates to a server, each server should believe in that operation and not ask about authentication again.

2.2 Types of Authentication Protocols

Based on the lists in the previous section, we can enumerate a wide range of authentication protocols used nowadays, like Password Authentication Protocol (PAP) [**11**], Challenge Handshake Authentication Protocol (CHAP) [**18**], Shiva Password Authentication Protocol (SPAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) [**23**], Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)[**24**], Extensible Authentication Protocol (EAP) [**1**], RADIUS [**14**], KERBEROS [**12**], DIAMETER [**5**], etc. Furthermore, when we consider web application, we should notice that we have a special group of HTTP authentication protocols, like basic access authentication or digest access authentication [**8**]. As we can see, we have many types of authentication mechanisms. Choice of protocol depends on a lot of factors, like type of network, type of device, type of service, in the broad sense of the environment. We can not use them everywhere. We can not use the same authentication mechanism in sensor (e.g. because of a lack of power) and the users PC. We have different requirements of authentication in the sensor networks [**20**], another in the mobile network [**6, 19**] and alternative in the public network, like the Internet. In [**3**] Anderson shows that not always we should provide a very strong security mechanism. We should adapt a level of protection of service to the situation in which service must work. Thus, it is a good idea to connect the context data with the security mechanism to provide adequate authentication mechanism with adequate parameters, like length of ciphers key or hash function. This is especially important in the dynamical environment where context changes very fast and in some cases it is needed to change a security mechanism in the provided service (e.g. the use of stronger cipher). Using contextual information we can offer proper mechanism/protocol with proper parameters and at the same time ensure satisfaction of the user. In the next section an idea of authentication mechanism based on context data is presented.

3 General Description of Adaptable Context Management Framework for Secure Network Services

The created solution is based on the framework from paper [**10**]. The main goal of the framework is adapts security mechanism to the users context. The framework works in two modes:

- training- in which collects data and decides about a chosen proper security mechanism, which assures an excepted level of protection,

- working- in which monitors the user and his environment and decides if it is necessary to change authentication mechanism/parameters of mechanism and return to the training mode.

At the beginning the framework works in the training mode and it starts to gather a raw context data from entity. Raw means that the Context Data Acquisition layer, the first layer of framework, does not verify its usefulness, it checks only structure of data (e.g. if data have a correct format and range). That situation continues until the second layer, Context Identification, starts its action. In the second layer the framework determines which context categories can be helpful in authentication, and creates a new proper format for them (it is required when we want to reuse the context data by many entities). Afterwards, the Context Adaptation layer checks reliability of context information with help from the Experience resources layer. This layer provides references to entity reputation. Moreover, the Adaptation layer can report a problem to the Consultation and Communication layer, which decides what to do in error situations. In the end, based on the collected contextual information, the framework selects an adequate authentication mechanism with right parameters (e.g. kind of hash function etc.) and sends it to the entity. At that moment transition between the training and working mode proceeds. In the working mode the framework monitors the entity context and a current level of protection. Each time when entity wants to authenticate to other services, the framework checks if actual parameters are sufficient for the earlier provided authentication mechanism. If not, at first the framework tries to change parameters of identification mechanism (e.g. change a hash function, increase length of using key, etc.) and if it is not enough again it tries to change the authentication mechanism. Naturally, there can be a situation in which the entity changes its state and the framework is unable to determines an apposite level of protection. In that case (and other similar ones) transition between working and training mode is necessary to decide about a right level of protection.

4 Example of Context-Aware Authentication Mechanism

Based on the framework from [**10**] we can built many security mechanisms which use the context data to provide a proper level of service protection. In this paper an idea of authentication mechanism is presented. The chosen use case is associated with a real life situation, which is access to mail box. the user, who is waiting at the bus stop, wants to get access to his/her e-mail in cloud computing using a mobile phone (see Fig. 3).

Furthermore, he/she has installed on the mobile application which helps with context information collecting. An agent of context data acquisition gathers from the device such information as a location of user, a type of device, an Internet Protocol address of device, a Media Access Control address of device, an users name, a surname, an age and an ID and puts them in the data repository (framework works in a training mode). Afterwards, the agent selects only these data, which are necessary for authentication:

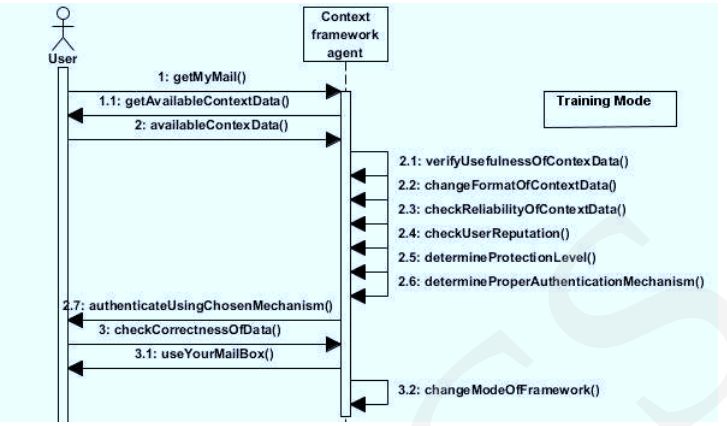

FIG. 2. Training mode of framework in the authentication mechanism

a location, an user ID, a type of device, an Internet Protocol address of device and transforms raw context data to the OWL format [**13**]. At the same time the agent confirms reliability of the gathered information and checks the users reputation. Based on this, using reasoning mechanisms the agent calculates that the best authentication mechanism in this situation will be an user's name with a password using the SHA-256 hash function. the user gets information about an authentication mechanism and correctly authenticates to e-mail service (framework starts to work in the working mode). However, after 15 minutes the user again wants to log in to his/her e-mail account (see Fig. 4). At the same time a frameworks agent notices that the user changes localization in which there are many hotspots. The agent decides not to change the authentication mechanism, but only chooses the hash function to SHA-384. The user does not feel any difference about the authentication.

At the end of the trip, the user at last gets to the airport and waits 1 hour for the flight. While waiting the user once again wants to read his/her e-mail. The framework agent detects the change of localization and finds out that the user is at the airport. In this environment, the agent can not immediately specify a level of protection of the authentication mechanism which should be delivered to the user. Thus, it determines that it must find new context information and with that knowledge provides a right identification mechanism. the agent communicates with other airport agents, as a result, it gets data about the users neighbourhood. That information helps to calculate a required level of protection and choose a right authentication mechanism (see Fig. 5) (framework switches to the training mode). Now the user again tries to log in with the password, which uses SHA-384, but besides he or she is asked about his/her mothers name. That information was given by the user during the e-mail registration process. When the user's name, password and her/his mothers name are correct, he/she can read the mail box.

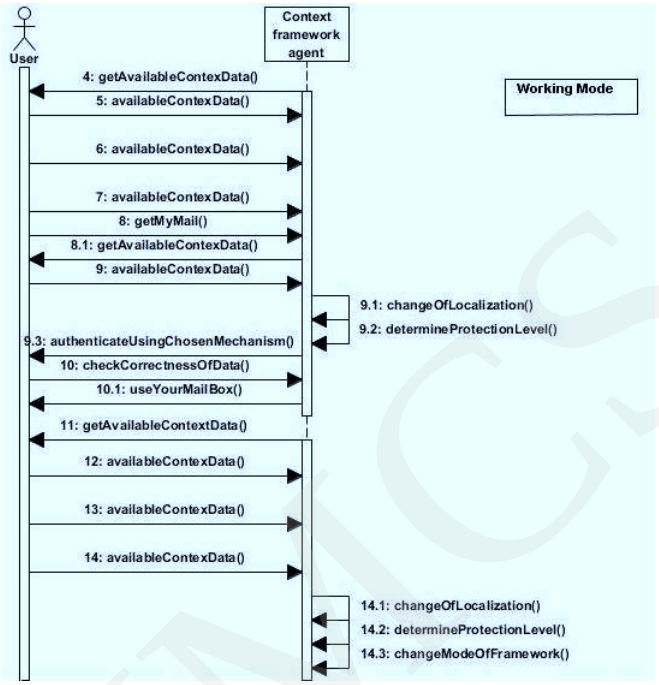

FIG. 3. Working mode of framework in the authentication mechanism

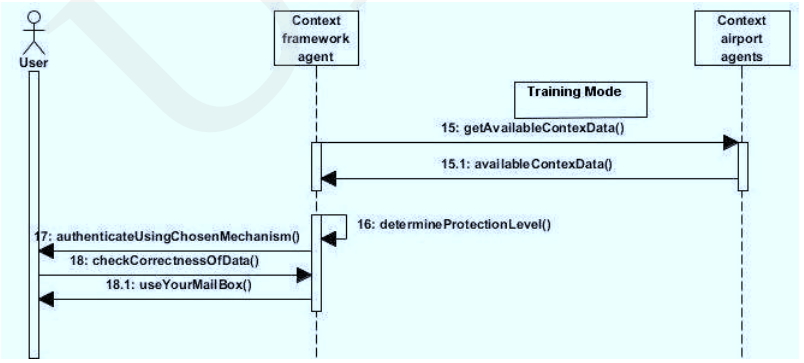

FIG. 4. Training mode of framework in the authentication mechanism during searching new context data

5 Related Works Concerning the Context-Aware Authentication

The main goal of the paper to show how to use the context with security mechanism, especially with an authentication. Several approaches for the context security have been described, but not all of them ensure a proper level of management of authentication

mechanisms. In [**25**] the authors showed a contex-aware authentication framework in which an authentication depends only on QR Codes and RFID. In that approach the framework uses history of the users authentications (date, result and context). Moreover, the solution emphasises that the users behaviour (patterns) is a good and reliable context factor. The pattern of behaviour is a very popular way how to use context with security mechanism. Much research focuses on habits of people. Paper [**31**] introduces this idea. Rocha shows a solution which uses only a spatio- temporal context with users mobile behaviour . The solution control users authentication on mobile devices based on the spatio- temporal context data (this allows to create model of the users behavior which includes events, goals and tasks as a part of the users activity). A lot of solutions used context in smart places. The example of this we can find in [**26**]. The authors present solution which can be used in the conference rooms or meeting rooms. Sensors using RFID or Bluetooth scanner detect devices and specify level of authentication, which determine probability that device is in a given area. A very similar idea is described in [**27**], where authentication depends on probability that the user is in that localization. Many solutions use mathematical calculations to associate them with a level of security. The example of this is considered in [**28**]. Park shows framework called COBAR which uses an authentication mechanism based on confidence of an users authentication level (ACI). The ACI is calculated based upon users history and divided into 5 categories. One of the problems connected with context and security is to ensure compatibility with the earlier mechanisms. Paper [**29**] tries to solve this problem. It includes a model for the context-aware multi-factor authentication, which is sufficiently generic to integrate any kind of application that needs authentication services. The author shows how to use context data to improve Single Sing On authentication. Moreover, solution solves a problem of flexibility in the dynamic environment. Next the example of context authentication is shown in [**30**]. Nishiki presents a distributed system based on authentication and access control agents characterized by autonomic policy decision, network federation and dynamic access control for context-aware services. A system tries to ensure an appropriate level of security and it was achieved by creation of authentication policies based on users preferences and his/her context. One of the most popular approaches to context authentication is described in [**32**]. The solution called CASA: Context- Aware Scalable Authentication which chooses an appropriate form of active authentication (e.g., typing a PIN) based on the combination of multiple passive factors (e.g., a users current location) for authentication. Furthermore, CASA is a generic probabilistic framework that enables the selection of appropriate active authentication factors given a set of passive authentication factors.

6 Conclusion and Discussion

In section 6 the examples of context-aware authentication mechanisms are given. Naturally not all of them use context data in the same way. Table 1 includes the

comparison of described papers and some general features of every solution. The explanation of each feature is located below:

- management of authentication - level of management of authentication mechanisms based on context data (how important context if for choosing authentication mechanism)
- easy addition of a new security mechanism - in easy way we can add to the proposed solution a new security mechanism and it will work with contextual information
- context model - which context categories are used by solution
- decision about important category- solution is able to decides which context information is more important in current situation
- flexibility - solution is able to adapt to the dynamically changing environment
- use of historical data - how big impact on the reasoning process the users historical data (e.g. statistic, patterns, etc.) have
- modes of work - defines modes in which solution can works
- ensuring QoE - solution takes into account the users satisfaction from the authentication mechanism

As we can see in Table 1 the created solution is better than other in categories ensuring QoE and modes of work. One of the main goals of the framework from paper [**10**] is to create mechanism which will be users perception oriented. Every security solution based on that framework inherits that feature, so automatically they have a high level of users QoE which is important especially nowadays. Another value in the solution are two modes of work. Each mechanism based on the framework from paper [**10**] can work in two modes: training in which i learns abtout actual environment conditions and working in which it observes changes of environment. It is especially important when we consider dynamically changing environments - some solutions are be able to react properly to some behaviours which results in providing a security mechanism with an inadequate level of protection. Moreover, the proposed solution allows easy management of authentication mechanism based on properly chosen context data.

The systems based on context data become more and more popular. Context data is information which we can use to reason about entity state and action and based upon that adapts system to a new environment. It means that we can use context to create a protection mechanism. In this paper there is described an authentication mechanism which uses the context information to provide a proper level of authentication. The mechanism can be used in the mobile environment (but not only), which nowadays is so popular. Moreover, solution dynamically adapts to the users state and chooses a good identification solution. It is necessary to provide a right security solution, which works using less resources, power, etc. and at the same time with a high level of protection and always user-friendly (a big rate of users satisfaction). Summing up, the created context authentication protocol could be applied in dynamically changing environment, where we expect fast, proper and the flexible solution. In this paper it is assumed that

reasoning mechanism is built in the context of agents actions, so I do not consider this process in the paper. But of course, reasoning in the systems based on context data is a very good research area, so the future work will be concentrated on other context security mechanisms, measurement of users satisfaction (when he/she uses the contextual mechanisms) and comparison the results with other security solutions.

Table 1: Comparison of context-aware authentication mechanisms

		Features							
		Management of authentication mechanisms	**Ease of adding a new security mechanism**	**Context model**	**Decision about important category**	**Flexibility**	**Use of historical data**	**Models of work**	**Ensuring QoE**
Existing solutions	**Proposed solution**	high	high	depends on situation	high dynamism	high	high	training, working	high
	[25]	low	low	localization	low dynamism	medium	high	basic	medium
	[26]	low	low	localization	low dynamism	medium	low	basic	high
	[27]	medium	low	localization, time	low dynamism	high	high	basic	medium
	[28]	high	high	situation	high dynamism	high	low	basic	medium
	[29]	medium	high	no model	low dynamism	high	low	basic	medium
	[30]	medium	high	situation	medium dynamism	high	low	basic	medium
	[31]	low	low	localization, time	low dynamism	medium	high	basic	medium
	[32]	high	high	depends on situation (but no general localization)	high dynamism	high	high	basic	high

References

[1] Aboba B., Blunk L., Vollbrecht J., Carlson J., Levkowetz H., Extensible Authentication Protocol (EAP), RFC 3748 (2004).
[2] Andress J., Identification and Authentication, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (2011).
[3] Anderson R. J., Security Engineering: A Guide to Building Dependable Distributed Systems (2008).
[4] Allen R., Hunter L. E., Dinerman B. J., Routing and Remote Access Service (Remote Access) (2006): 141–189.
[5] Fajardo V., Arkko J., Loughney J., Zorn G., Diameter Base Protocol, RFC 6733 (2012).
[6] Fitzek F., Munari M., Pastesini V., Rossi S., Badia L., Security and authenticationconcepts for UMTS/WLAN convergence (2003).
[7] Flordi L., Information: A Very Short Introduction, UK, Oxford (2010).
[8] Franks J., Hallam-Baker P., Hostetler J., Lawrence S., Leach P., HTTP Authentication: Basic and Digest Access Authentication, RFC 2617 (1999).
[9] Gwizdka J., Whats in the Context?, Toronto, Canada (2000).
[10] Kotulski Z., Sepczuk M., Sitek A., Tunia M.A., Adaptable context management framework for secure network services (to appear) (2014).
[11] Lloyd B., Simpson W., PPP Authentication Protocols, RFC 1334 (1992).
[12] Neuman C., Yu T., Hartman S., Raeburn K., The Kerberos Network Authentication Service (V5), USA (2005).
[13] OWL - Web Ontology Language, http://www.w3.org/TR/owl-features
[14] Rigney C., Rubens A., Simpson W., Willens S., Remote Authentication Dial In User Service (RADIUS) (1997).
[15] Rojas R., Neural Networks, Tokyo, Japan (1996).
[16] Rokach L., Maimon O., Data Mining with Decision Trees: Theory and Applications (2014).
[17] Schilit B. N., Adams N., Want R., Context-Aware Computing Applications (1994).
[18] Simpson W., PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, Day-Dreamer (1996).
[19] Tsay J., Mjolsnes S. F., A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols (2012).
[20] Vogt H., Exploring Message Authentication in sensor networks, ETH Zurich (2005).
[21] Winograd T., A Human-Centered Interaction Architecture, http://graphics.stanford.edu/projects/iwork/old/papers/humcent/ (1999).
[22] Wrona K., Gomez L., Context-aware security and secure context-awareness inubiquitous computing environments, France (2005).
[23] Zorn G., Cobb S., Microsoft PPP CHAP Extensions, RFC 2433, Microsoft Corporation (1998).
[24] Zorn G., Microsoft PPP CHAP Extensions, Version 2, RFC 2759, Microsoft Corporation (2000).
[25] Goel D., Kher E., Joag S., Mujumdar V., Griss M., Dey A. K., Context-Aware Authentication Framework, San Diego, CA, USA (2009): 26–29.
[26] Lenzini G., Trust-Based and Context-Aware Authentication in a Software Architecture for Context and Proximity-Aware Services, The Netherlands (2009).
[27] Hulsebosch R.J., Bargh M.S., Lenzini G., Ebben P.W.G., Iacob S.M., Context Sensitive Adaptive Authentication, Kendal, England (2007): 23–25.
[28] Park S., Han Y., Chung T., Context-Aware Security Management System for Pervasive Computing Environment, Roskilde, Denmark (2007): 20–24.
[29] Miranda L. H. F. M., Context-aware multi-factor authentication, Lisbona, Portugal (2009).
[30] Nishiki K., Tanaka E., Authentication and Access Control Agent Framework for Context-Aware Services, Trento, Italy.

[31] Rocha C.C., Lima J.C.D., Dantas M.A.R., A2BeST: An adaptive authentication service based on mobile user's behavior and spatio-temporal context, Brazil (2011).

[32] Hayashi E., Das S., Amini S., Hong J., Oakley I., CASA: Context- Aware Scalable Authentication, Newcastle, UK (2013): 24–26.