Security Issues in Distributed Systems – A survey

Kaltrina Nuredini[1]

[1]*Faculty of Contemporary Sciences and Technologies, SEE University, Tetovo, Macedonia*
Email: kn11284@seeu.edu.mk

ABSTRACT

One important technology area in which researchers are interested is distributed systems technology. Distributed systems in general involve the interaction between diverse independent entities using a common language and protocols to achieve different conventional goals. Enterprises are now particularly growing, involving data sharing among distinct participating entities with the need of distributed resources and computing. This internet growth has meant that many distributed systems are open to the world, from where this has brought to a major problem: certifying that such systems are secure. By this approach it is essential to cover security and protection in distributed environments. This report survey emphasizes this aspect that provides a literature review between the collected papers to discuss some general security issues. The key ideas and techniques involved at these systems are studied. It defines what a secure system is, observes security policies from security mechanisms including authentication and authorization as major processes. Considers encryption as a cryptographic technique that is useful for data confidentiality and privacy than similarly, access control as an important feature that enables authority is also assessed monitoring some proposal models. At the same time denials of service attacks attempting to prevent legitimate users from accessing services are described observing different scenarios.

Keywords: *Distributed Systems, security, access control, encryption, DDoS*

INTRODUCTION

As we move more and more to a connected world, computer systems are broadly used and are becoming more distributed in terms of geography as well as functionality. Distributed systems were admitted in academic and research communities in order to connect and collaborate. Enterprises are now growing the collaboration and data sharing among various cooperation entities, resulting in the need and use distributed resources and computing. Distributed systems entail the interaction between different independent entities, using common language and protocols and working toward a common goal. Simply defined a distributed system is where the CPUs are not in a single machine and to its users looks like an ordinary centralized system. With an extensive selection of distributed computing, security is a very critical and crucial issue that can hurt the enterprises and user communities in a massive way. Based on these considerations the aim of this paper is to describe the concept of security issues in distributed systems considering some important concerns during reviewing and evaluating research papers framed for security.

This paper is organized as follows. The next section briefly considers the main security issues in distributed systems involving security policy, authentication, authorization and access control. Within authorization it is prescribed the problem of distributed denial of service attacks. Next section elaborates distributed denial of service attack. Finally, the last section describes conclusion.

OVERVIEW OF SECURITY ISSUES IN DISTRIBUTED SYSTEMS

Security in distributed systems essentially can be divided in two important parts. The first part is the communication between users including secure channels more particularly: authentication, message integrity and confidentiality. The other part involves the access rights to the resources in distributed systems. It is important to define what a secure system is. One assumption is that security is absolute, but according to this security in physical world is never absolute because none of the safes are expected to resist attacks that can happen in the system. So from this point of view users must feel confident about the security but it cannot be said that the users are guaranteed of anything that can happen [1]. Clearly declaring that a system should be able to protect itself against all achievable security threats is not the way to actually build a secure system. It is almost understandable that *hosts* which are client desktops and low level servers need to be protected from malicious outside agents, then *applications* has assumed major importance and the design of them needs to be secure also services must achieve confidentiality and integrity.

As it is described security in such systems preserve a significant challenge for certain reasons. Different concepts are summarized for security in distributed systems. Security features can be defined depending on the environment in which applications are operating. Users must have some capabilities and policies that allow them easy access to the resources. It is important to name that security must be applied usually in all layers not in a specific one because it is difficult to understand and manage the system [4]. To analyze the various elements of IT security that can occur in the system a Metamodel is developed. In accordance with [2] good security system must use three main parts a *Core* of basic IT security concepts, *Countermeasures* and *Attacks*. There is described about assets, threats, security goals and also the focus was on Attacks. The Metamodel is applied in a real life using three attacks in distributed systems: Incorrect lookup Routing on Peer to Peer systems, XML bombs on Service Oriented Architectures and Black Hole attacks on Mobile ad hoc Networks.

SECURITY POLICY

The first thing that is needed is the description of security requirements or as called security policy. Defining a security policy is the design of language that can be used in a policy. This means that policy can be defined as roles applied to some humans for collaborative software development team and assigning the rights or authorization and obligation about the members on the team. Policies are performed as objects which can be members of domain. There are two types of policies. **Authorization policies** designate what actions a manager is permitted or denied to do to a set of objects and are comparable to security access protocol policies. **Obligation policies** determine what a manager must or must not to do to a set of objects [11]. As described in [4] authorization policy are usually used in database management systems with a view to ensure privacy of information however obligation policies are used either in association with authorizations in case to ensure the integrity of the system. For example if we take an obligation policy that defines an activity in order the manager to perform that activity there is no authorization policy that allows the manager to behave the specified activity. The policy should be clearly stated, the language should be able to express policies for a variety of systems, should be expressive in order the failures to express what the policy creator wants and should be easily to write, modify and understand. The PPL Policy programming language is a framework used for specification, verification and implementation of security policy. Subjects and objects are certainly defined with the use of PPL security that allows automatic distribution of policy implementation components [4].

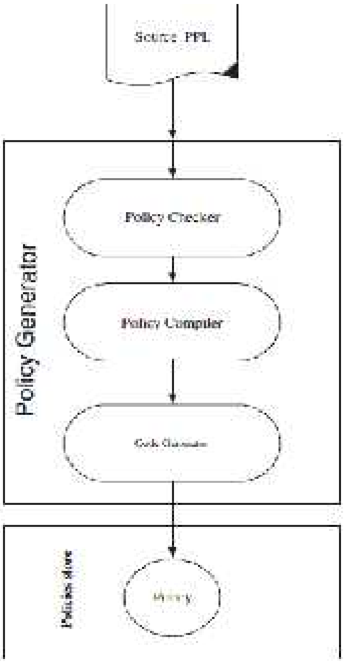

Figure 1 PPL development process

According to the figure 1, security policy is specified using the abstraction provided by the PPL language [4]. The policy is checked in order to detect potential conflicts that can occur. The policy needs to be translated into appropriate representation for usage. After a security policy has been laid down, now the concentration is on security mechanisms by which a policy can be enforced. These are some important security mechanisms:

- Encryption
- Authentication and
- Authorization

CRYPTOGRAPHY

Encryption is accomplished using cryptographic methods. This technique is employed for achieving confidentiality. The reason of using encryption is based on the idea of transforming a piece of text (plain text) into an encoded text (cipher text). An interesting advancement in the field of cryptography is identity based encryption (IBE). The notion of this is that the public key would be used to encrypt messages which can only be decrypted by the corresponding private key. With IBE, the sender can encrypt the message with any string that can be associated with the receiver and there is no need to obtain or store the receiver's public key. According to [9] it is introduced the architecture of scribe where uses IBE. Here the notion of IBE is described as the follows "If Alice wished to send Bob an encrypted email, there is no need for Alice to obtain Bob's public key certificate, instead Alice will be able to encrypt message to Bob using only his email address as the public key". Scribe delegate on the integrity of the master key to guarantee secure communications. By submitting a request to each machine holding a share the Master key operation can occur. To secure the master key is difficult in such systems because there are no trusted entities, the master key must be protected from generation to storage by a collection of nodes. With the use of Scribe it is provided an important service that helps authenticating nodes which are based on their public identity and delivers private keys. In accordance with this system we can conclude that it allows a secure and authenticated communication behind a distributed system.

AUTHENTICATION

Authentication is the process that defines who he/she is allowed to carry out an operation on a computer. According to [1, 4] authentication can be done in two environments: the Calling Agents (CA) and the Responsible Agents (RA). The authentication system is based on public key cryptography [1, 4]. With the use public key crypto-system, the specified system can improve matters. In this arrangement each member has its own (public key, private key) pair, in which the public key can be used by all members for sending confidential messages. To define authentication we will cover an important system that is widely used named as Kerberos. Besides a Kerberos it is described also SSL which both are widely used system components that support secure and authenticated communication. Kerberos is a security system that assists clients setting up a secure channel with any server that is part of distributed system. As it is described in [12] using Kerberos scheme Key Distribution Center (KDC) issues to clients short-lived credential as in Public Key scheme a Certificate Authority (CA) issues long lived credential – a public key certificate. When both clients and servers have such certificates they can authenticate to each other without further reference to a CA. Some methods are required to inform servers of revoked certificate because of long lived credentials. This is done by checking certificate validity or by distributing Certificate Revocation Lists (CRL's) to all servers periodically. The paper was concentrated on PKDA which was the proposed extension of Kerberos that requires the use of public key operations each time that a service ticket is required. According to PKDA, authentication between the Kerberos clients and servers using public key cryptography, the clients and the servers won't need to maintain symmetric keys with the KDC. It seems that PKDA is more important in usage than Secure Socket Layer protocol in agreement with [12]. SSL as a transport layer protocol can be used in conjunction with TCP-based client-server communications whereas Kerberos in application layer can be used in either UDP or TCP. This shows that the privacy of the client's identity in a Kerberos authentication can be protected. The integration of restricted proxies with Kerberos as it is described in [13] can be listed another authentication system-based on conventional cryptography. The use of proxies within an authentication mechanism can have several advantages. The first one is transparency and the second one is the authentication of a user that can be thought of as the granting of a proxy based from the credentials of the users, and the restrictions between the authentication server are placed.

AUTHORIZATION

Authorization is related to the problem of controlling access to resources. All the authorization of client must be distributed by server, which means the client can't authorize any other clients [3]. Authorization is also related to access control in which they specify whether a sequence of actions are permitted or forbidden to a specified object. Based on [13] authorization is implemented using restricted proxies. Proxy is defined as a token that allows one to operate with the rights and privileges primary to grant the proxy. The usage of proxy is beneficial from these reasons:

- Can be used by anyone that gets hold of it
- The individual can do anything that the granted could do on any service.

Restricted proxy is a proxy that places conditions during the usage. In this case the authorization server implemented using restricted proxy does not specify that a particular principal is authorized to use the specified service or access a particular object. The server grants a restricted proxy allowing the authorized client to act as the authorization server for the purpose to allow the client access the accurate object or service.

Access control

Access control is used after a process has been authenticated. Related to access control is preventing denial of service, described in the next section. Data does not need to perform access control because identification, authentication and authorization services are not relevant services required for data. These services are more related to users or agents [6]. There are some traditional access control models in distributed systems such as DAC, MAC and RBAC. According to these models any of these properties are not implemented on models.

- Credential are delegatable and delegation is recorded
- Decision mode
- Altering trust relationship during run-time events.

Based on these requirements Policy Domain Access Control (PDAC) was initiated. Distributed system consists of nodes and applications. At this context the node is abstract as a domain and this domain has ability of access control from where is named as Policy Domain. The access control scheme model can be as follows: first, client finds the server, than server creates a policy based on the operation that the client requests. Server stores this policy and signs it as a credential. This credential is issued direct to the client [10], see figure 2.

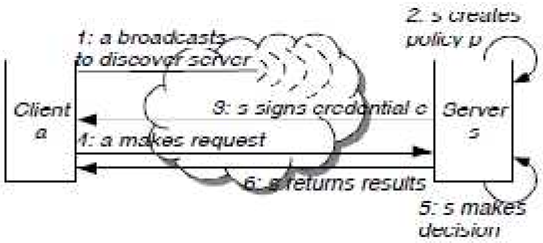

Figure 2 Local decision

There are two occurrences of delegation in PDAC. The first case is where credentials are not modified and the delegation is not recorded. The second case is where the credentials are modified and delegation is recoded [10], see figure 3.

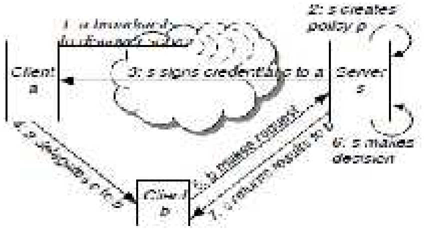

Figure 3 Delegation without modification

Sometimes server cannot make decision using its own state information, because the client who makes the request is new and it did no interaction with server before, or it is because information for the decision is damaged. In this case, server will cooperate with other servers to make a consensus decision.

Denial of service attack

Denial of service (DoS) attacks is becoming very important as distributed systems are opened up through the Internet. DoS occurs where accredited users are prevented from getting access to shared resources or services [5]. One of the deadliest forms of DoS attack is when attackers are distributed in nature. Such attack is called DDoS attack. In February 2000, the first major DDoS attack was waged against yahoo and then against eBay, Amazon, E*Trade, ZDnet and several other Web sites [7]. Primary victims are services, while systems that used to launch the attack are secondary victims. To solve DDoS problem there are many interpretations depicted below. One interpretation is an approach to detect bandwidth attacks by monitoring the arrival rate of new source IP addresses [8]. There are two scenarios for DDoS attacks defined as Typical DDoS attack and distributed reflector denial of service (DRDoS) attack. The first scenario is divided into two stages: compromise the systems that are available on the Internet and then install on them attack tool. This process is known as turning computers into "zombies". The second stage the attacker sends an attack command to the "zombies" through a secure channel to launch a bandwidth attack against the victim. DRDoS uses routers or web servers to attack [7]. There are two main classes of DDoS attacks naming the as flood attacks and amplification attacks.

- **Flood attacks** results in sending large volumes of traffic to a victim system, from where the victim system slows down, crashes or suffers from saturated network bandwidth.
- **Amplification attacks** involves the attacker sending messages to broadcast IP address in order that all systems in a subnet to send a reply to the victim system.

Attackers use many different DDoS tools to attack. These tools are easy to implement and can have unfavourable effects. The first one is Active DDoS Agent installation method that includes the attacker scanning the network for systems with known vulnerabilities, running scripts to break into the system and installing DDoS agent software. The second one is Attack network communication make use of encrypted communication within DDoS attack network. The last one is operating system supported which means that DDoS attacks are typically designed to be compatible with different operating systems [8].

CONCLUSION

Distributed systems form the backbone of the IT infrastructure and security is a key concern that must be approached with an accurate blend of theory and usefulness in enterprises. Nowadays are invented very different collaborative and data-sharing technologies from which they need to be protected. With the growth of them in an enterprise infrastructure increases the complexity. With the use of some research papers, here we investigate some primary security issues that can be taken into account in case to use distributed systems. It is described about security policies that can help interacting with the system in different manners. Nowadays most of organizations address security policies that help to notify how and what information is to be handled by organizations. With other words a policy can be defined as a plan designed to determine actions, decisions and other phenomena. The second section depicts encryption as a technique and the notion of IBE. In the encryption process IBE takes a completely new approach. With the use of IBE the data can be protected using an arbitrary string as a public key without the need of certificates. This technology requires the need for a key server that allows the controlling of decryption keys. The cryptosystem with IBE seems to be a good fit of use. After that section, next section describes authentication and authorization that are useful for accessing resources and achieving confidentiality in the system. Authorization itself involves access control as an important process for providing secure solution about some specified problems that can arise in the system. Access control involves DDoS involving different DDoS attacks from where attacker can use in the system. All issues described in previous sections are very important in such systems and their way of implementing and using them needs to be very serious in terms to achieve security.

REFERENCES

[1] Wulf, A.Wm, Wang Chenxi, Kienzle Darrell. A new model of security for Distributed Systems

[2] Miede, Andre,. Nedyalkov Nedislav. (2010). A generic Metamodel for IT security – Attack Modeling for Distributed Systems, International Conference on Availability, Reliability and Security

[3] He, Ming. Hu, Aiqun. Qiu, Hangping. (2009). Research On Secure Techniques of Trustworthy Distributed System, International Conference on Computer Engineering and Technology

[4] Hamdi, Hedi. Mosbah, Mohamed. (2009). A DSL framework for Policy-based Security of Distributed Systems, Third IEEE International Conference on Secure Software Integration and Reliability Improvement

[5] Demir, Omer. Khan, Bilal. (2010). Quantifying Distributed System Stability through Simulation: A case study of an Agent-Based System for Flow Reconstruction of DDoS Attacks, International Conference On Intellegent Systems, Modeling and Simulation

[6] Tillwick, Heiko. Olivier, S.Martin. A Layered Security Architecture: Design Issues

[7] Peng, Tao. Leckie Chrictopher. Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring

[8] Specht, Stephen. Lee, Ruby. Distributed Denial Of Service: Taxonomies of Attacks, Tools and Countermeasures

[9] Stading, Tyron. Secure Communication in a Distributed System using Identity Based Encryption

[10] Wu, Xian. Qian, Peide. Research on Policy Domain Access Control Model in Distributed Systems

[11] Sloman, Morris (1994). Policy Driven Management for Distributed Systems, Journal of Network and System Management, Plenum Press, Vol.2, No.4, p: 333-360

[12] Sirbu, Marvin. Chuang John. Distributed Authentication in Kerberos Using Public Key Cryptography

[13] Neuman, Clifford. Proxy-based Authorization and Accounting for Distributed Systems (1993), International Conference on Distributed Computing Systems.