Summarization of Various Security Aspects and Attacks in Distributed Systems: A Review

Istam Shadmanov [1], Kamola Shadmanova [2]

[1,2] Information Technology, Bukhara State University, Uzbekistan
istam.shadmanov89@gmail.com, kamola.shadmanova94@gmail.com

Abstract

The modern world is filled with a huge data. As data is distributed across different networks by the distributed systems so security becomes the most important issues in these systems. Data is distributed via public networks so the data and other resources can be attacked by hackers. In this paper we define different security aspects including on the basis of authorization, authentication, encryption and access control for distributed systems.

Keywords: *distributed system, security issues, security threats, integrity, security services.*

1. Introduction

Nowadays, security threats are a growing concern since the complexity of the collaborative processes increases. Another way of looking at security in systems is that we attempt to protect the services and data from various threats and attacks, which are discussed in a section 2. The objective of this paper is to understanding of the various threats and security aspects associated with distributed system.

Security issues in modern distributed systems can roughly be divided into two parts. [1] The first part is the communication between users or processes, possibly residing on different machines. The principal mechanism for ensuring secure communication is a secure channel and more specifically, authentication, message integrity, and confidentiality. Confidentiality refers to the property of a computer system whereby its information is disclosed only to authorized parties. Integrity is the characteristic that alterations to a system's assets can be made only in an authorized way. In other words, improper alterations in a secure computer system should be detectable and recoverable. The second part is the authorization, which deals with ensuring that a process gets only those access rights to the resources in a distributed system it is entitled to. Authorization is covered in a separate section 3, dealing with access control. Secure channels and access control require mechanisms to distribute cryptographic keys, but also mechanisms to add and remove users from a system. Before starting our description of security in distributed systems, it is necessary to define what a secure system is. Security system, that enforces boundaries between computer networks, consisting of a combination of hardware and software that limits the exposure of a computer or computer network from attack.

The systems security requires the existence of the followings:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;

Integrity: that supposes avoiding data corruption and keeping data integrity;

Availability: which means ensuring that data and applications can always be accessed, regardless of any interferences, to authorized entities. [5]

These three concepts embody the fundamental security objectives for both data and for information and computing services.

2. Threats and attacks in distributed system

A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning).

There are some types of security threats to consider:

-interception, the concept of interception refers to the situation that an unauthorized party has gained access to a service or data. Interception happens when data are illegally copied, for example, after breaking into a person's private directory in a file system;

-interruption, refers to the situation in which services or data become unavailable, unusable, destroyed, and so on;

-modification, include intercepting and subsequently changing transmitted data, tampering with database entries and changing a program;

-fabrication, refers to the situation in which additional data or activity that would normally not exist are generated.

An attack on system security can drives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

2.1 Classes of attacks in distributed system

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. The following are common types of network attacks in distributed system as, A Passive Attack, An Active Attack, Syn Flood Attack, Password Attack, Distributed Attack, An Insider Attack and Phishing Attack:

A passive attack usually monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions.

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files or modification of data.

A distributed denial of service (DDoS) attack attempts to consume the target's resources so that it cannot provide service. One way to classify DDoS attacks is in terms of the type of resource that is consumed. Broadly speaking, the resource consumed is either an internal host resource on the target system or data transmission capacity in the local network to which the target is attacked. A simple example of an internal resource attack is the SYN flood attack. [6]

Figure 2.1 shows the steps involved:

1. The attacker takes control of multiple hosts over the Internet, instructing them to contact the target Web server.
2. The slave hosts begin sending packets, with erroneous return IP address information, to the target.
3. Each packet is a request to open a TCP connection. For each such packet, the Web server responds with a SYN/ACK (synchronize/acknowledge) packet, trying to establish a TCP connection with a TCP entity at a spurious IP address. The Web server maintains a data structure for each SYN request waiting for a response back and becomes bogged down as more traffic floods in. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

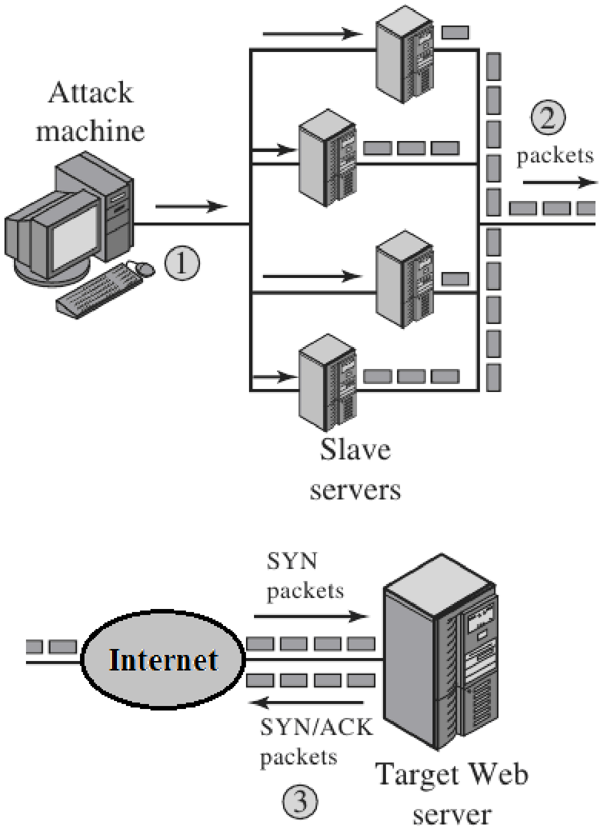


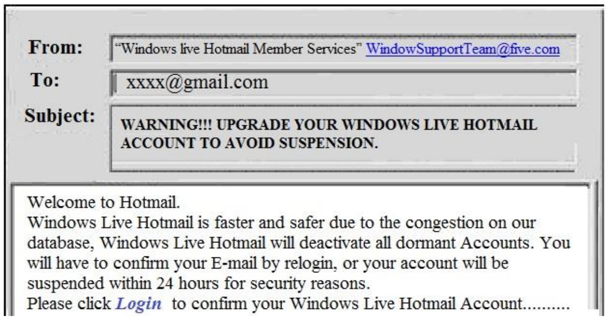
Figure 2.1 Distributed SYN flood attack

Password attack, an attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. In brute-force attack the attacker tries every possible combination of characters.

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

In phishing attack, the hacker creates a fake web site that looks exactly like a popular web site companies such as Facebook, Hotmail, Yahoo or consumer products companies. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. [2] When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site. An example of a phishing email posted as a warning on Microsoft's web site is shown in Figure 2.2.



From: "Windows live Hotmail Member Services" WindowSupportTeam@five.com
To: xxxx@gmail.com
Subject: WARNING!!! UPGRADE YOUR WINDOWS LIVE HOTMAIL ACCOUNT TO AVOID SUSPENSION.

Welcome to Hotmail.
Windows Live Hotmail is faster and safer due to the congestion on our database, Windows Live Hotmail will deactivate all dormant Accounts. You will have to confirm your E-mail by relogin, or your account will be suspended within 24 hours for security reasons.
Please click *Login* to confirm your Windows Live Hotmail Account..........

Figure 2.2 Example Phishing Email Message

Sometimes the phishing email advises the recipient of an error, and the message includes a link to click to enter data about an account. The link, of course, is not genuine, its only purpose is to solicit account names, numbers and authenticators.

Apart from attacks originated from external parties, many break-ins occurs due to poor information security policies and procedures, or internal misuse of information systems. Also, new security risks could arise from evolving attack methods or newly detected holes in existing software and hardware. But a system must be able to limit damage and recover rapidly when attacks occur.

2.2 Security Issues in Distributed system

The informatics security is an important issue that must be analyzed in order to identify security requests, to discover possible vulnerabilities or threats and to avoid loss of information [4].

For enforcement of security, the distributed system must have the following additional requirements:

- It should be possible for the sender of a message to know that the message was received by the intended receiver;
- It should be possible for the receiver of a message to know that the message was sent by the genuine sender;
- It should be possible for both the sender and receiver of a message to be guaranteed that the contents of the message were not changed while it was in transfer.

The secured implementation of distributed systems has been generated lot of critical issues. Some of these are as follows:

- Identification of methodology which access the security level in any system;
- Application of middleware in distributed system security;
- Application of web services in security purposes;
- Monitoring of the system security;
- Development of security metrics;
- Integration of techniques, like Cryptography etc., for secure distributed data communication.

3. Methods of the solution on security issues

In the context of distributed systems security is oriented on collaborative side, which means that security components cooperate to achieve a common goal, represented by vulnerabilities elimination. There are some broad areas of security in distributed systems:

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Encryption
- Digital Signature
- Nonrepudiation

Authentication. A fundamental concern in building a secure distributed system is a authentication of local and remote entities in the system. The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Access Control. In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links and the prevention of unauthorized use of a resource. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality. Confidentiality is the protection of transmitted data from passive attacks and unauthorized disclosure. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Data Integrity. As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. A connection - oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only. The integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation.

Encryption. The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithms and encryption keys. A security related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender. (Figure 4.1)

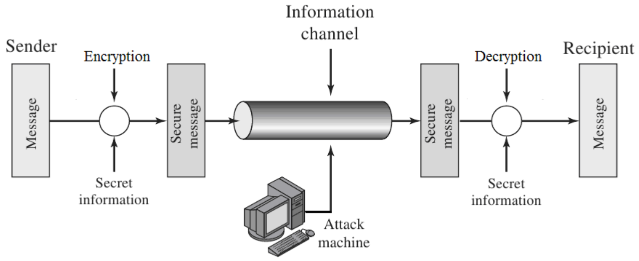


Figure 3.1 Example For Message Security

Digital Signature. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g., by the recipient. Digital information can be signed, producing digital certificates. Certificates enable trust to be established among users and organizations. [3]

Nonrepudiation. Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message. In such cases a notary is used to register messages, that neither of the participants can not back out of a transaction and disputes can be resolved by presenting relevant signatures or encrypted text.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

4. Conclusion

In order that the users can trust the system and rely on it, the various resources of a computer system must be protected against destruction and unauthorized access. Enforcing security in a distributed system is more difficult than in a centralized system because of the lack of a single point of control and the use of insecure networks for data communication. Authentication, access control, notarisation, data confidentiality, data integrity, digital signature etc. are well-studied and used methods of secure distributed systems.

References

[1] Andrew S. Tanenbaum, Maarten Van Steen, “Distributed systems Principles and Paradigms”, 2nd ed., Upper Saddle River, NJ, USA: Pearson Higher Education, 2007, pp. 377-389.

[2] Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, “Security in computing”, 5th ed., USA, Pearson Education, Inc., Massachusetts, January 2015, pp. 300-304.

[3] George Coulouris, Jean Dollimore and Tim Kindberg, “Distributed System- Concepts and design”, 5th ed., USA, Addison- Wesley, Massachusetts, 2012, pp. 481-483.

[4] I. Ivan, C. Ciurea, “Security of Collaborative Banking Systems”, Proceedings of the 4th International Conference on Security for Information Technology and Communications, November 17-18, 2011, Bucharest, Romania.

[5] Manoj Kumar, Nikhil Agrawal, “Analysis of Different Security Issues and Attacks in Distributed System A-Review”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[6] William Stallings, “Cryptography And Network Security Principles And Practice”, 5th ed., NY, Pearson Education, Inc., 2011, pp. 809-812.

First Author -ISTAM UKTAMOVICH SHADMANOV

1. 2013-UP TO NOW - TEACHER OF THE DEPARTMENT OF INFORMATION TECHNOLOGY
2. 2011-2013 MASTER`S DIPLOMA ON APPLIED MATHEMATICS AND INFORMATION TECHNOLOGY
3. 2007-2011 BACHELOR`S DIPLOMA ON APPLIED MATHEMATICS AND INFORMATICS
4. NUMBER OF PAPERS- 9.

Second Author-KAMOLA SHADMANOVA UMED QIZI

1. 2012-UP TO NOW – STUDENT OF THE DEPARTMENT OF INFORMATION TECHNOLOGY
2. NUMBER OF PAPERS- 2.