A New Approach towards Network Security & Authentication

Ashoktaru Pal
Future Institute of Engineering & Management, India

Abstract— Since the early days of computers, authentication technologies have been used to protect the data inside computers. The commercialization of the Internet makes the authentication even more important [1]. The term "authentication" is much used in the context of computer security. It is also a term that causes much confusion. Failure to grasp the real meaning and the importance of "authentication" can seriously delay the adoption of security technology in general, authentication technology in particular. In this paper, we conducted a survey on major authentication technologies and found they can be related in a systematical way. Using this way to categorize authentication technologies can reduce confusion.

Keywords: Authentication, Security, Cryptography, Security Service, Attack and OSI

I. INTRODUCTION

Authentication is one of the most commonly used terms in computer security. It is also a term that causes much confusion. To most people, authentication is a process performed during the login process when a user submits credentials usually consisting of a username and a password. But in reality, the term has different meanings in different contexts. Academic documents do not help either. Searching for the keyword "authentication" at http://www.google.com, one can find about 800 links. Conducting similar search in the online bookstore Books24x7 shows that about 750 books mentioned the keyword "authentication". It is quite easy to compare the keyword discussed in any two of these documents and find they may represent totally different concepts. This paper intends to present the technologies in a more systematical way. This section discusses three aspects of information security and shows the role of authentication in these aspects. Section II gives an overview of the authentication process that introduces the players in the process, including Claimant, Authenticator Generator, Access Control Mechanism, and Verifier. Section III discusses the properties of authentication, including who sends authentication information, where the authentication information comes from, whether the authentication information is sent in a timely and unique manner, and how to authenticate yourself without revealing who you are.

Section IV describes four types of authentication technologies from cryptography perspective.

These technologies are used to authenticate one or more properties mentioned in Section III.

Section IV presents four design patterns for deploying authentication systems. Section V lists several important security systems and their association with OSI layers. Section VI concludes this paper.

There are three aspects of information security [4]

A. Security Attack

A security attack is any action that compromises the security of information owned by an organization. There are two types of security attacks: Network Attack and System attack.

B. Security Service

The services are intended to counter security attacks. There are five major security Services, including Authentication, Authorization, Integrity, Confidentiality and Non-Repudiation. Among these five services, authentication is probably the most confusing one [2, 4], and the most complicated one because it is related to the other four security services.

C. Security Mechanism

Security mechanism is to detect, prevent, or recover from a security attack. Cryptography provides the foundation to build mechanisms to prevent network attacks. There are three major cryptograph technologies. Their relationships can be explained with Fig. 1.

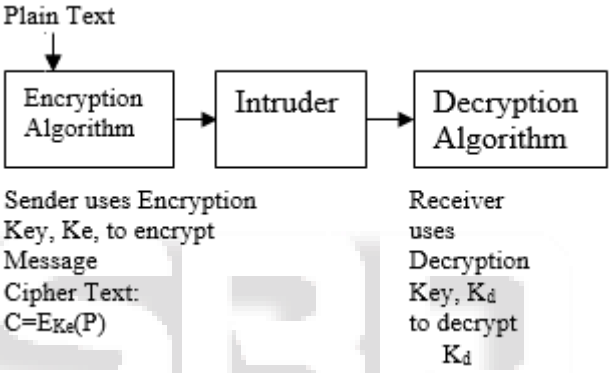

Fig. 1: Encryption and Decryption Using Symmetric Key

Note:

- For Symmetric Key Cryptography (i.e., Secret Key Cryptography): Ke = Kd.
- For Asymmetric Key Cryptography (i.e., Public Key Cryptography): Ke != Kd.

Symmetric Key Cryptography usually has a better performance than Asymmetric Key Cryptography. However, Symmetric Key Cryptography alone cannot be used in Internet because it is impossible that every Internet user keeps symmetric keys of all the other users he/she communicates with. In real application, Hybrid Key Cryptography is used. The Asymmetric Key Cryptography is first used to transmit a secret key which is called session key because the key is used only for one session. The session key is then used by Asymmetric Key Cryptography to transmit the message. Unlike the secret key used in Symmetric Key Cryptography, session key is not sent via out-of-band channel.

II. AUTHENTICATION PROCESS

Authentication is usually an interaction between two entities, which is called two party authentication. It is a process that verifies that entities are in fact who they claim to be.

Entities that may require authentication by computer systems include users, computers, and processes [3]. One entity (i.e., the Claimant) provides authentication information which includes its claimed identity and supporting information. The other entity (i.e., the Verifier) performs the

identity verification. In many cases two-party authentication is not scalable and secure. A third party (or more than one third party) is required for the authentication. These schemes are called trusted third-party schemes. Examples of third parties are Certificate Authority for Asymmetric Key Cryptography; and Key distribution Center for Symmetric Key Cryptography. The sequence of steps for an authentication process in a client/server environment is shown as follows:

1) In client side, the Claimant generates authentication information.
2) The authentication information is converted into an authenticator by cryptography algorithms. Authenticator is a value used by the Verifier in the server side to authenticate the Claimant.
3) The client sends the authenticator to the Access Control Mechanism which is located in the server side.
4) The Access Control Mechanism passes the authenticator to the server's Verifier.
5) The Verifier verifies the authenticator. To perform the verification, the Verifier applies an authentication function F to the authenticator and compares the result with the expected result [5].

F (authenticator) = expected result

There are two major types of F functions. The first type expects absolute result. Password Verification and challenge-response protocol belong to this type. Simple password verification may cause replay attack. Challenge-response protocol can prevent replay attack but may cause chosen-text attack because it reveals some partial information about the Claimant's secret. The second type expects probabilistic result. Authentication in this context is successful only with bounded probability, albeit possibly arbitrarily close to one [7]. Zero-knowledge protocol is an example of using the second type function [7, 9].

6) The Verifier passes the result to the Access Control Mechanism.
7) The Access Control Mechanism generates response based on the result.
8) The Access Control Mechanism sends the response to the client.
9) The client passes the response to the Claimant.

III. PROPERTIES OF AUTHENTICATION

As mentioned in the previous section, entities that may require authentication by computer systems include users, computers, and processes. This section describes an entity's properties, which are used by computer systems in an authentication process. The properties belong to different categories: who, when, where, and how. The "who" category can be divided further into three sub-categories, including something known, something inherent, and something possessed. If an authentication uses the properties belonging to the same category, we call it one-factor authentication. If the properties belong to two different categories, we call the authentication two-factor authentication.

A. Who

The "who" property is usually used to authenticate user entity.

1) Something known

This property is also called "Something you know". It is the most common property since the storage mechanism used is your own memory, making it one of the cheapest forms of storage [10]. Examples of this property include password, passphrase, passcode, passkey, and Personal Identification Numbers (PIN). This type of property is easy to deploy and manage, and supported by most systems. The downside is that it is relatively insecure.

2) Something inherent

This property is also called "Something you are". The property makes use of biometrics, such as handwritten signatures, fingerprints, voice, retinal patterns, hand geometries, and dynamic keyboarding characteristics [8]. Compared with "Something known" properties, this type of property is very hard to duplicate and cannot be forgotten because it comes with the Claimant. The downside is that it is not easy to replace a security system if an attacker manages to crack the system open (i.e. finds out how to "spoof" a finger or eyeball) [10]. Another issue for biometrics is that it is prone to sniffing and replay attacks.

3) Something possessed

This property is also called "Something you have". This is typically a physical accessory, resembling a passport in function. Examples include smart card, certificate, and time-variant password generator [8]. Compared with "Something known" properties, this type of property allow to have larger secret and the Claimant does not need to input it into the security system manually each time he or she wishes to use it. However, like "Something known" properties these properties may be lost or they may be transferred from one user to another one.

B. When

This property is to authenticate whether the authenticator is sent from one entity to another on a timely and unique manner. This property is used in Transaction Authentication to prevent message replay attack.

C. Where

This property is usually used in address-based authentication mechanisms to authenticate computer entity. Address-based authentication mechanisms assume the authenticity of a message on the basis of the originating address of the message. The addresses falls into three categories [12]: (1) Arbitrary addresses – Each entity is assigned a unique identifier. The device's software is configured to use the identifier; (2) Hard-wired addresses – The address is "hard-wired" into an entity; (3) Network enforced addresses – The entity is identified by a network address that is established and enforced by the network's carrier. This type of property faces several problems [11]. One problem is the reliability of calling addresses, as it is easy for an attacker to modify the address.

Another problem is the difficulty in maintaining a continuing association of a principal (a person or a piece of equipment) with a network address because address changes may occur frequently.

D. How

Authentications based on "who" and "where" always reveal some information about the Claimant. Zero-knowledge protocols are designed to address these concerns, by allowing a Claimant to demonstrate knowledge of a secret while revealing no information whatsoever of use to the Verifier. Thus, the authenticator passed from the Claimant to the Verifier is the knowledge of a secret, not the secret itself [7, 9].

IV. Types of Authentication

A. Entity Authentication

Entity authentication is also called User Authentication, Peer Entity Authentication, Identity Verification, and Identification [13]. It is provided for use at the establishment of, or at times during the data transfer phase, of an ongoing interaction [13]. While entity authentication may be informally defined as the process of verifying that an identity is as claimed, there are many aspects to consider. First, at the time of connection initiation, Entity Authentication assures that the two entities are authentic. Second, it assures that no third party can masquerade as one of the two legitimate parties at times during the data transfer phase.

B. Message Authentication

Message Authentication is also called Data Origin Authentication [14]. It provides data origin authentication with respect to the original message source (and data integrity, but with no uniqueness and timeliness guarantees). Unlike Entity Authentication, there is no Authentication Exchange for Message Authentication because Message Authentication is not for ongoing interaction; it is for a single message, such as a warning or an alarm signal. Authentication Exchange is a mechanism intended to ensure the identity of an entity by means of information exchange. Methods for providing Data Origin Authentication include the following:

1) message authentication codes (MACs)
2) digital signature schemes
3) appending (prior to encryption) a secret value, such as a salt value, to encrypted text.

C. Transaction Authentication

Transaction authentication denotes message authentication augmented to additionally provide uniqueness and timeliness guarantees on data (thus preventing undetectable message replay) [14]. The guarantee of uniqueness and timeliness is typically provided by appropriate use of time-variant parameters (TVPs). These include (1) random numbers in challenge-response protocols, (2) sequence numbers, and (3) timestamps.

Loosely speaking,

Message Authentication + TVP = Transaction Authentication.

D. Key Authentication

In Hybrid Key Cryptography, symmetric keys are required to be sent from one entity to another one. Key Authentication ensures that session keys are established between the correct entities. It is a special kind of Message Authentication. Instead of authenticating a message, session key is authenticated.

V. Design Patterns in Authentication Systems

This section describes architectural design patterns that often appear in the deployment of authentication systems. Based on the physical locations of the Claimant, the Access Control Mechanism, and the Verifier, the authentication deployment patterns can be categorized into four types: One Tiered, Two Tiered, Three Tiered, and Off-line authentications [6].

A. One Tiered Authentication

This deployment pattern is also called Local Authentication. In this pattern [6], the Claimant, the Access Control Mechanism, and the Verifier reside within a single physical security system. Examples of this pattern include stand-alone workstations and personal organizers like Palm-based systems. Since authenticator is not passed from the client to the server via network, this deployment greatly simplifies the system design and operations. One can directly use only one factor authentication property, such as biometrics or password, to implement authentication, no cryptography is required. The main issue for this authentication is its administration. Each security system represents a single point of service that must be individually administered.

B. Two Tiered Authentication

This deployment pattern is also called Direct Authentication. In this pattern [6], the Claimant resides in one security system; the Access Control Mechanism and the Verifier reside in a separate security system. Examples of this pattern include UNIX password mechanism and single-point LAN servers, like Microsoft's original LAN Manager and Novel Netware. This pattern yields the simplest architecture for authenticating remote users. The authenticator is sent (often in encrypted form) to the system's database of authorized users, a positive match grants access.

C. Three Tiered Authentication

This deployment pattern is also called Indirect Authentication [6]. In this pattern, the Claimant, the Access Control Mechanism and the Verifier reside in three separate systems. In Two Tiered Authentication, if a company runs a "server farm" for the user community, then the authentication yields a troublesome solution. If each server is an independent remote system with its own authentication mechanism, then administrators must perform every authentication maintenance task (that is, adding or revoking a user's account) individually on each server. Three Tiered Authentication solutions address the scalability problem with a single population of users but multiple points of service.

While One Tiered and Two Tiered design patterns combine authentication and access control mechanisms, the Three Tiered Authentication pattern extracts the authentication mechanism from the point of service and moves it to a separate authentication server.

Other components provide services or control access to resources but do not make authentication decisions. Instead, they authenticate people indirectly by contacting the authentication server when someone tries to log on.

D. Off-Line Authentication

Two Tiered and Three Tiered Authentications are for a client to authenticate a server. Off-line Authentication is the reverse, which is mainly for a server to authenticate several clients. Another difference among these deployment patterns is the usage of cryptography. Two Tiered and Three Tiered Authentications can use both Symmetric Key Cryptography and Asymmetric Key Cryptography, Offline Authentication, however, only uses Asymmetric Key Cryptography [6]. Public-key certification software follows an offline authentication pattern, which recognizes authorized users, and is stored in multiple locations throughout the system and is accessible offline. Adding users, however, is faster and easier than revoking them. Off-line deployment addresses the internal contradiction of truly practical, distributed authentication: a company cannot trust every device that needs to perform authentication. Some applications are so large or so broadly distributed (or cut off) that they can't rely on a centralized server for real-time authentication decisions. Yet the company may still want central authority over authentication. The best-known examples of such problems occur in consumer-oriented electronic commerce. Each vendor wants to assure customers that they are indeed talking to the vendor's computer. Yet the vendors can't automatically trust their customers or their customers' computers. Table 1 summarizes the features of authentication deployment patterns.

Property	One Tired	Two Tired	Three Tired	Off -Line
Protection Parts	Whole System	Points of service only	Auth--enti-cation Service only	Certification Authorities only
Biometrics safe	Yes	Not by itself	Not by itself	Not by itself
Crypto Used	None	Symmetric or Asymmetric	Symmetric or Asymmetric	Asymmetric only
Fault Tolerance	Low	Low	High-Low	High

Table 1: The Summary of Authentication Features

VI. SECURITY SYSTEMS

From OSI's perspective, the Authentication Service can only be applied to Application Layer, Transport Layer, and Network Layer [16]. Several security systems can be categorized on the basis of these three layers: (1) application layer systems, such as JAAS, Kerberos, S/MIME, PGP, SET; (2) transport layer systems, such as SSL and TLS; (3) network layer systems, such as IPSec. These security systems provide one or more Security Services, including Authentication Service. For the Authentication Security Service, each system use one or more Authentication Types.

VII. CONCLUSION

Authentication is one of the most important and complicated security services, yet it causes much confusion. The term "authentication" actually has different meanings in different contexts. In this paper, we conducted a survey of major authentication technologies and found they can be related in a systematical way:

- There are five major security services, including Authentication, Authorization, Integrity, Confidentiality and Non-Repudiation.
- Existing security systems can be mapped to OSI layers. Each system can provide one or more security services. But Authentication Service can only be applied to three OSI layers: application layer, transport layer, and network layer.
- Each Authentication Service can be realized by authentication technologies belonging to one or more authentication types.
- There are four major authentication types: Entity Authentication, Message Authentication, Transaction Authentication and Key Authentication. Each authentication type is to authenticate one or more authentication properties.
- There are four major categories of properties: who, when, where, and how. The "who" category can be divided further into three sub-categories: something known, something inherent, and something possessed.

Based on this way of categorization we can assess that the password mechanism most people use every day is an application layer authentication mechanism. It is part of Entity Authentication and is used at the time of connection initiation. The authentication is to verify the "something known" of "who" property. Another point we would like to make is the definition of authentication should depend on context. If one insists to have a generic definition of authentication, the following one is acceptable:

"Authentication is the process of determining the identity of a user or other entity."

REFERENCES

[1] Roger Clarke, "Authentication: A Sufficiently Rich Model to Enable e-Business", in http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel011019.html
[2] "X.800: Security Architecture for Open Systems Interconnection for CCITT Applications", in http://fag.grm.hia.no/IKT7000/litteratur/paper/x800.pdf, pp. 8-10.
[3] Mitch Tulloch, "Microsoft Encyclopedia of Security". Microsoft Press, 2003, pp. 31-32.
[4] William Stallings, "Cryptography and Network Security. Principles and Practices. Third Edition". Prentice Hall, 2003, pp. 4-16

