ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

Authentication Techniques in Computer Networks

Gulshan Kumar[1], Anjala[2], Jyoti Sharma[3]

Assistant Professor, Shaheed Bhagat Singh State Technical Campus, Feorzepur, Punjab, India[1,2,3]

Abstract - The Internet has emerged as one of the most convenient and widely used media for exchanging information. The Internet of today is faced with many challenges. One of the most intimidating challenges is to ensure security. Pursuing authentication through applicable mechanisms becomes a complex issue. Like other network applications, security issues have become the core issues to be settled. Among other security issues, authentication and access control are the two main fields of security issues, which must be resolved to protect information and computing systems against unauthorized access. This paper explores three authentication techniques, i.e. (i) Private key Cryptosystems (ii) public key cryptosystems (iii) Biometric based authentication and suggest/propose which technique will protect the privacy to authenticate users in an appropriate manner. Finally, the paper presents the comparison of various authentication techniques. The paper will help the readers in better understanding of different techniques and explore the field.

Keywords- Access control, Authentication, Cryptography, Biometric identification

1. INTRODUCTION

Computer industry has created an array of identification and authentication technologies like userID/Passwords, One Time Password, Biometrics, Smartcards, Secure Socket Layer, Lightweight Directory Access Protocol, Security Assertion Markup language (SAML), OpenID and CardSpace address varying business and security requirements [1]. Each organization adopts one or more of these technologies to secure information against misuse and un-authorized access. In a networked environment, users are granted access to the network only when they provide their access information (e.g. User name & password) securely to check and validate their identity. If a person can prove that he is, also knows something that only he could knows, it is reasonable to think that a person is he who claims to be. The purpose of personal authentication is to ensure that the rendered services are being accessed only by a legitimate user. All Network users aim to access information and transfer data safely. To make certain secure transmission of information between the parties; a group of challenges must. We detain these challenges to three areas: data Integrity, authentication and privacy.

1.1 Data Integrity: Data Integrity refers to the consistency and accuracy of data to ensure that unauthorized parties are prevented from modifying data Authentication. As a result, the data which is received must be to be the same as the data sent. Protecting data transmission process is required to avoid any intentional or unintentional changes of these data. Any damage or decline of data will affect the feasibility of these data or information; it becomes not beneficial and not safe to use. Data can use multiple techniques such as encryption.

1.2 Authentication: Authentication is the process of verifying if a user or entity or device is who claims to be. In other words, it's a combination of verification and Identification[3]. Authentication falls into three categories:-

- The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question), pattern)
- The ownership factors: Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)
- **The inherence factors**: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier). The most important technique is as described below.

Biometric Authentication: On the other hand, bequeath true user authentication. It is concerned with identifying a person based on his/her behavioral or physiological characteristics. This is of great help especially for

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

illiterates. Behaviors biometric can be gait, speech, signature and keystroke analysis, whereas physiological biometric uses face, ear, finger-print, voice, finger geometry, palms, hand veins, hand geometry, iris matching and recently brain waves are used exclusively.

1.3 Privacy: Privacy refers to secure and valuable data which should not be available unless the parties concerned are allowed to do so. Many techniques can be used to maintain and improve user privacy such as cryptography techniques, passwords and firewalls. In an unsecure situation, it is easy to break through privacy in several ways.

2. NEED AUTHENTICATION

Most organizations used their first Web applications to offer generally available information over the public Internet, intranets, and extranets. Successfully managing and securing corporate Web resources has become a more complex challenge as Web use has matured. Organizations that need their employees to access their intranets remotely through the Internet, or that want to automate their supply chains through extranets, should consider the security and management concerns that are unique to these situations.

To take advantage of the Internet, organizations are providing Web-based access to confidential information. With these configurations, internal and external users with varying needs and permissions should be able to access different resources maintained in the corporate intranet—and users should be able to access only information for which they are authorized. Adding to the complexity of the problem, few organizations have the luxury of building their information systems from scratch. Most companies need tools that can blend new technology with their existing systems to provide security to all resources and applications accessed through the Web.

There are several key requirements that should be met in order to manage information securely on a corporate intranet. First, the identity of an individual wishing to access the intranet should be authenticated. Authentication is the process of verifying that a requester has been issued a unique identifier and knows the secret (for example, a password or PIN) that is associated with that identifier.

This process is complicated when employees or business partners access information from multiple computers and, often, from remote locations over the Internet. Users should be able to authenticate from a Web browser or a wireless device (cell phone or PDA), with no client software requirements. In addition, there are often hundreds of Web servers in a large enterprise, and users need access privileges for each server they access. This can lead to many problems: users must remember passwords for many servers, administrators need to manage the access controls for each individual server, and many separate entries must be added or removed when a user's access privileges change or when employees join or leave the company. As shown in the figure below, a central location that maintains security policy offers a solution that:

- Lets the organization manage access controls for all of these servers centrally
- Presents users with a single sign-on to the Web space
- Greatly simplifies security management
- Enhances the user's experience and increases productivity.

3. AUTHENTICATION PROCEDURE I

Authentication is the process which allows a sender and receiver of information to validate each other. If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple. The simplest form of authentication is the transmission of a shared password between entities wishing to authenticate each other.

4. BASIC CONCEPTS

Before delving into authentication techniques used so for, it will be useful to establish some basic definitions here.

- AUTHENTICATION: Authentication means enabling the network to only admit the authorized users to have access to its resources. It provides the way where the claimed identifier is verified by the access control mechanisms through some means.
- ACCESS CONTROL: The discipline in which mechanisms and policies are established that restrict access to the computer resources only to correct users.
- IDENTIFICATION: It is a way where a resource claims (or is identified through other means) a specific and unique identifier.
- AUTHORIZATION: Which determines the privileges associated with authenticated identity.

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

- SECURITY: The ability of a system to protect data, services and resources against misuse by un-authorized users.

- PRIVACY: The ability of a system to protect the identity and location of its users from un-authorized disclosure.

- SMART CARD: A small pocket sized plastic card used to make payments and store personal information and which can be read when connected to the computer system. It is widely used a hardware token in financial transaction systems, especially in Internet based.

- E-VOTING: E-voting is also known as Electronic Voting, an electronic means of casting a vote and electronic means of counting votes. It can involve transmission of ballots and votes via telephone's private computer network or the Internet.

5. AUTHENTICATION PROCEDURE II

Authentication is the process which allows a sender and receiver of information to validate each other. If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple [9]. The simplest form of authentication is the transmission of a shared password between entities wishing to authenticate each other.

6. AUTHENTICATION TECHNIQUES

Cryptography provides an easy way for the transmitter and receiver to define a subset of valid messages that the transmitter can construct and the receiver can verify [10].

Two types of cryptosystems are available:-

i) Private key cryptosystems

ii) Public key cryptosystems: A more traditional technique that complements the two cryptographic methods is

iii) Biometric Systems

6.1.Private Key cryptosystems: Symmetric encryption (also called private-key encryption or secret-key encryption) involves using the same key for encryption and decryption. Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys).

6.2.Public-key cryptosystems: Public-key cryptosystems also known as asymmetric cryptography is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. The term "asymmetric" from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both.

➢ **Digital signatures:** Digital signatures in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as any manipulation of the message will result in changes to the encoded message digest, which otherwise remains unchanged between the sender and receiver.

➢ **Hash Functions:** A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data are often called the message, and the hash value is often called the message digest or simply the digest.

The ideal cryptographic hash function has four main properties:

- It is easy to compute the hash value for any given message

- It is infeasible to generate a message that has a given hash

- It is infeasible to modify a message without changing the hash

- It is infeasible to find two different messages with the same hash.

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for more general functions with rather different properties and purposes.

6.3. Biometric Systems: Biometrics is an authentication technique that uses fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. Since it is more difficult for a malicious hacker to gain access to a person's biometric data. Biometrics can be used for both physical access to corporate buildings and internal access to enterprise computers and systems. Biometrics are most often used as a form of authentication in a broader two-factor or multifactor authentication system

7. COMPARISON

The following table compares different techniques of authentication.

	Private-key cryptosystems	Public-Key Cryptosystems	Biometric Systems
Speed	High	Low	High
Memory Requirement	64 bits of secret key	400-500 bits of secret key	9 bits to megabytes depends on the application
Reliability	Good	Very good	Good
Security Level	High	High	Reasonable
Convenience	Convenient	Convenient	Not in all applications
Availability	Export restrictions	Export restrictions	Available

Table 1. Comparison of authentication techniques

8. CONCLUSION

In this paper, we presented the authentication techniques and concludes that Biometric-based authentication technique is more convenient, safe and reliable. This system is a pattern recognition system in which a person is recognized based on features derived from specific psychological or behavioral characteristics that the person possesses, which are harder to be theft or stolen. In the future, we planned to explore literature and implement the authentication technique.

REFERENCES

[1] Noor, A. (2008, March). Identity protection factor (IPF). In Proceedings of the 7th symposium on Identity and trust on the Internet (pp. 8-18). ACM.

[2] Khan, H. "Comparative study of authentication techniques", International Journal of Video & Image Processing and Network Security Vol:10 No:04,2012

[3] Masadeh, S. R., Azzazi, A., Alqaralleh, B. A., & Ali, M. A. (2014). A NOVEL PARADIGM IN AUTHENTICATION SYSTEM USING sWIFI ENCRYPTION/DECRYPTION APPROACH. International Journal of Network Security & Its Applications, 6(1).

[4] Web reference:
http://www.infosec.gov.hk/english/promotion/files/Script_common_authentication_methods_US.pdf, Accessed on 29-10-2014.

[5] Data encryption standards(DES), National Bureau of standards (u.s.), Federal information processing standards publication 46, national Technical information service.

[6] Guibing, Guo, Z. Jie, and J. Vassileva. "Improving PGP Web of Trust through the Expansion of Trusted Neighborhood." Web Intelligence and Intelligent Agent Technology (WI-IAT) (2011).

[7] Ramamohanarao, K., Gupta, K. K., Peng, T., & Leckie, C. (2007). The curse of ease of access to the internet. In Information Systems Security (pp. 234-249). Springer Berlin Heidelberg.

[8] Zhang, Yuqing, and Dehua Zhang. "Authentication and access control in p2p network." In Grid and Cooperative Computing, pp. 468-470. Springer Berlin Heidelberg, 2004.