Globus An International Journal of Management & IT
A Refereed Research Journal
Vol 6 / No 1 / Jul - Dec 2014 ISSN: 0975-721X

A STUDY ON DIGITAL SIGNATURE: EMERGING TECHNIQUES FOR NETWORK SECURITY

Sayed Khasim*

Importance of Computer Networking

A computer network is a connection of two or more computers through a cable or wireless connection. Networking enhances effective communication among memers of an organization or a company. With appropriate software, each computer user can communicate with other members or staff of an organization or company. Computer network gives users the opportunity to use remote programs and remote databases either of the same organization or from other enterprises or public sources. The importance of having a computer networks are really numerous. Thus, it is a necessity for every organization or company. It makes effective communication possible and helps to eliminate unnecessary waste of time and duplication or resources. Computer networks will help every organization to - reduce cost by sharing hardware and software resources; reduce cost; and increase flexibility and efficiency of any given organization. Computer network allows the user to share data with other users in a network. The user can also setup a central system wherein common files and folders which are frequently used by all the users can be stored. All the users within the network can easily access those files. Instead of taking backups from individual computer, the user can take data backup from the central system. Thus the computer network provides scalability. It is also reliable to sue a network as it uses mirroring and redundancy.

A. Types of Networks Based on Physical Scope

1) Local area network (LAN)

This is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards also provide a way to create a wired L using existing home wires (coaxial cables, phone lines and power lines).

2) Personal area network (PAN)

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines telephones, PDAs, scanners, and even video game consoles. -A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and Fire wire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

3) Home area network (HAN)

A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a Digital Subscriber Line (DSL) provider. It can also be referred to as an office area network (OAN).

4) Wide area network (WAN)

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

5) Campus network

A campus network is a computer network made up an interconnection of local area networks (LAN's) within a limited geographical area.

The networking equipments (switches, routers) and transmission media (Optical fiber, copper plant, cabling etc.) are almost entirely.

In the case of a University campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls.

*Research Scholar, Sunrise University, Alwar, Rajasthan

Why is Network Security Important

Network security is very important to protect confidential documents against misuse of the system. There are a number of drawbacks that can arise if network security is not launched properly, some of which include

A. Violation of Confidentiality

Every business has some information that is required to be kept confidential from other competitors and even from their own employees.

B. Damaging Data

Data is an important and valuable asset for any company or sole proprietor as it is the core of what your information is based on. Therefore backup scripts are also set for the data to be stored on other available media. If the data is damaged by any means, then the victim will face severe loss and can cripple the business severely.

C. Manipulation of Data

When data is hacked, the hacker often leaves behind a token of accomplishment which shows how easily your network can be accessed without proper network security.

Even riskier than all this is the manipulation of data in which the data is changed with another type. Anything, and everything and other users do with the machine, could be discovered, disseminated, altered, stolen and/or destroyed.

This does not mean that any of these bad things will occur, only that the potential exists, and that it does happen. You may have information concerning other people on your machine that could cause damage to them, You may be legally responsible for such damages in some situations.

How We Can Secure Our Network?

A. Network Security Tools Include

1) Antivirus software packages

These packages counter most virus threats if regularly updated and correctly maintained.

2) Secure network infrastructure

Switches and routers have hardware and software features that support secure connectivity, perimeter security, int Tusion protection, identity services, and security.

Dedicated network security hardware and software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

3) Virtual private networks

These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

4) Identity services

These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

5) Encryption

Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

Techniques that are Used to Secure a Network

A. Cryptography

Cryptography is the science of writing in secret code and is an ancient art. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes just about any network, particularly the Internet.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically -used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, the all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

1) Types of Cryptographic Algorithms:

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.

Hash Functions: Uses a mathematical transformation to irreversibly encrypt information.

2) Public key algorithms (RSA)

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adelman. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

3) Key generation algorithm

- Generate two large random primes, p and q, of approximately equal size such that their product n pq is of the required bit length, e.g. 1024 bits.
- Compute n pq and (Q) phi = (p-l)(q-l).
- Choose an integer e, 1 < e < phi, such that gcd(e, phi) = 1.
- Compute the secret exponent d, 1 <d < phi, such that ed 1 (mod phi).
- The public key is -(n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.
- n is known as the modulus.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

4) Digital signature

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and aprivate key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

5) Services of Digital Signatures

Authentication: Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context

Integrity: If a message is digitally signed, any change in the message after signature will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Non-repudiation: Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature. This is in contrast to symmetric systems, where both sender and receiver share the same secret key, and thus in a dispute a third party cannot determine which entity was the true source of the information.

References

1. Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
2. Akyildiz, I. F., Su, W., Sankara Subramaniam, Y, and Cayirci, F., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2012, pp. 3 93-422.
3. Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005,pp. 407-411.
4. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.
5. Under-coffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca./—angiezIpersonalIpaper/sensor-ids.pdf
6. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., - "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2012, pp. 521-534.
7. Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless ensor Networks", Proc. Eighth IEEE International Symposium on Computers