I.J. Education and Management Engineering **2012, 2, 74-80**
Published Online February 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2012.02.12

Available online at http://www.mecs-press.net/ijeme

Research of Network Security and Information Encryption

Wan Hongli

Computer Science and Technology Department, Neusoft Institute of Information, Dalian, China

Abstract

In the process of rapid development of the computer network, the network security has been paid more attention. The essential nature of network security is the information safety on the internet. Primary studies have been done in this paper on the aspects of information encryption technology and the network security strategy.

Index Terms: network security; information encryption; security strategy; network security algorithm;

1. Introduction

With the continuous development of the computer network, the global information has become the general trend of development of human beings. But due to the connection of computer network structure with the diversity, terminal and non-uniformity of distribution network interconnection of openness, etc, which feature of computer network is susceptible to hackers, malicious software and other bad behavior, so the online information security and confidentiality is one of the most important issues. Computer and network technology provide convenience to the people, but at the same time, security problems have emerged and become more and more serious. With the increasing popularity of computer applications, in particular, the rapid development of network technology, more and more security threat have appeared and information security has become a very important and urgent issue to be solved. Network information security has become the fifth security field after sea, land, air and space.

Event Log Monitoring, Management and Archiving Made Easy The enormous volume of system events generated daily is of growing importance to organizations whose business is required to record information for forensic purposes and the ever-growing reach of regulatory compliance. Increased threats to business continuity call for an approach that includes real-time monitoring of the network; and you also need the ability to analyze and report event data to address any incidents or security concerns.

* Corresponding author.
E-mail address: wanhongli@neusoft.edu.cn

2. Network security strategy

2.1 Net work security concept

Based on the analysis of network business's concept and features, "network security" is defined as follows: network security means the reliability, stability and real-time of business running on the network, the continuity of business processes and business operation's confidentiality and non-repudiation. Network security can be further described as follows: the integrity of network process sets and data sets, the running reliability and real-time of network process set, and the non-repudiation of processes running and writing operation on data set.

2.2 Physical security strategy

Ensure all kinds of equipments of computer network system of physical security are the premise of network security. Physics is to protect the security of computer network equipment, facilities and other media from the earthquake, flood, fire accident and unsuitable operation or error and various computer crime leads to destruction. Its purpose is to protect the computer system, web server, such as printers and communications link layer hardware entity network equipment from natural disasters and man-made destruction, etc.

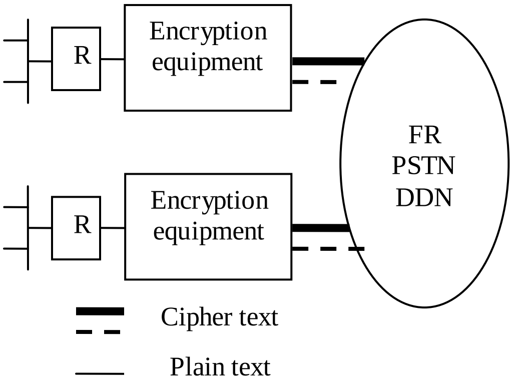

Fig 1. Encryption on link layer

The encryption on link layer do the encryption and decryption work by the point to point method. That is, deploy a link layer encryption equipment on every network point which has the requirement of access and encryption transitions. Implement the encryption and decryption procedure through the communications between the encryption equipment.

2.3 Access control strategy

Access control is the main task of the network resources that are not illegal use and visit. It is one of the most important network securities of the core strategies.

2.4 Firewall control strategy

Firewall is recently developed a kind of technical measure which is a protection of computer network security developed recently. It is a barrier to prevent the hackers on the network to access. It is a system of execution control strategy located between two networks, which to limit the external illegal users access to the internal network resources and the illegal authorized data transmission from internal to external. In network boundary on the corresponding established through network communication, monitoring systems to isolate external and internal network, to stop the external network intrusion, prevent the theft or damage effect on malicious attacks. Firewall system security defense ability, can resist all attack and penetration.

Firewall Analyzer helps network security administrators & IT Managers for bandwidth monitoring, and Firewall internet security events monitoring efficiently. The Firewall security events are, intrusion detection, virus attacks, denial of service attack, etc., anomalous behaviors, employee web activities, and web traffic analysis. It makes you visualize your enterprises network security. Capacity planning using trend analysis and detecting security compromises are some of the critical problems that are resolved using Firewall Analyzer. It generates admin reports, on all the firewall logs, addresses your network audit and regulatory compliance requirements. It monitors used/unused Firewall policies and policies can be optimized using Firewall settings. Employee web activities can be monitored with the help of proxy log analysis.

2.5 Information encryption strategy

Data encryption is the most direct and effective way to prevent the risk of network information. This technique is mainly guide users to set effective password in the process of the data transmit. Data encryption includes the line encryption and the point to point encryption. Each method has its own characteristics. Line encryption is mainly protecting the key encryption of the protected data information. Point to point encryption protects the sender of the information, closure the data when it attached to the TCP/IP using the data packages.

Table 1. Explanation of five properties of information security

properties	explanation
availability	The property of being accessible and usable upon demand
integrity	The property that data has not been altered or destroyed in an unauthorized manner
authentication	The provision of assurance of the claimed identity of an entity
non-repudiation	A service intended to protect against an entity's false denial of having participated in all or part of the communication
confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3. The concept of encryption

The basic process of data encryption is to process the original plaintext files or data according to an algorithm, making it unreadable piece of code, often referred to as cipher text, so that its content can only be shown only after entering the corresponding key through such means to protect data from unauthorized people to steal and read. The inverse of the process is the decryption process that is the process of translating encoding information into its original data[1].

Today's network social choose encryption with what we have no choice, but one that we know on the Internet file transfer, e-mail business dealings there are many factors of insecurity, especially for some large companies and a number of confidential documents transmitted over the network. And this insecurity is the base of the existence of the Internet--TCP/IP inherent in the agreement, including some services based on TCP/IP; the other hand, the Internet has brought unlimited business opportunities to so many businesses, the Internet connected the world together, toward the Internet means toward the world, which is undoubtedly the dream of a good thing for many businesses, especially for small and medium enterprises. In order to solve this contradiction, in order to open the door toward the world on the basis of secure, we have no other choice but data encryption and digital signature based on encryption technology. The role of encryption on the network is to prevent the privatized and useful information from being intercepted on the network and theft. A simple example is the transmission of password, computer passwords is extremely important, a number of security protection systems are based on password, in a sense the reveal of password means that its security system totally collapses[2].

4. The intra site automatic tunnel addressing protocol

The Intra Site Automatic Tunnel Addressing Protocol (ISATAP) allows computers that are configured to support ISATAP adapters to obtain an IPv6 address from the ISATAP server.

This ISATAP address is assigned to the ISATAP tunnel adapter on the system. When the ISATAP host want to connect to another ISATAP host, the communications are routed based on the IPv4 addresses of the source and destination, using the IPv4 header that encapsulates the communication. When the IPv4 packet reaches its destination, the IPv4 header is removed, and the IPv6 communication is exposed.

What's interesting is that if you have a single ISATAP server on your network, it will seem from an IPv6 point of view that you have a single hop network, in spite of the fact that the IPv4 header that encapsulates that communication might see 5 hops.

ISATAP assigns “real” IPv6 addresses that can be used by IPv6 applications right now. Even if you do not have a “native” IPv6 infrastructure (with IPv6 routers, DNS, DHCP, and client/server applications), you can still roll out IPv6 applications on your network today because ISATAP makes this possible for you. In a Direct Access deployment, the Direct Access server can and often does act as your ISATAP router. ISATAP makes it easy to deploy Direct Access because it removes much of the complexity inherent in a native IPv6 infrastructure and allows you to use Direct Access in an environment where you have IPv6 aware operating systems, network stacks, and client/server applications[3].

Table 2. Tunnel adaptor

Connection-specific DNS Suffix	corp.contoso.com
IPV6 Address	202:7ebe:9e9b:1:0:5efe:172.19.6.59
Link-local IPV6 Address	fe80::5efe:172.19.6.59%16
Default Gateway	fe80::5efe:172.19.6.60%16

There are going to be times when you do not have a public IP address, and you are behind a firewall or Web proxy on a private address IPv4 network that only allows outbound HTTP/HTTPS. That's a tough place to be, because you are limited only to servers that allow access to the HTTP protocol. However, in order to realize the goal of Direct Access, you should be able to connect to the corpnet regardless of your location, and that means you should be able to connect when your only option is HTTP. Direct Access clients support the IP-HTTPS protocol (IP over HTTPS). IP-HTTPS allows Direct Access clients to connect to the Direct Access server using HTTPS. This provides connectivity through firewalls that only allow HTTPS, and even through Web proxy devices. However, the Web proxy devices must not require authentication, because there is no provision in the Direct Access client that allows the client to forward credentials to an authenticating Web proxy server.

IP-HTTPS is the worst case scenario for the Direct Access client. There are two primary reasons for this:

The client needs to use processor cycles to encrypt the HTTPS communications in an SSL tunnel. This encryption is on top of the IPSec encryption that automatically used to protect the Direct Access communications between the Direct Access client and server. This double encryption duty is not required when using Teredo from behind a NAT device.

There is significant protocol overhead. The IPv6 packet is encapsulated in an IPv4, which is then encapsulated in an HTTP application layer protocol header, which is then encrypted with SSL. Your users will not be happy campers when using IP-HTTPS, at least they won't be as happy as your Teredo and 6to4 users. However, they will probably be more happy than your L2TP/IPsec VPN users, because your IP-HTTPS users don't have to manually establish their connections, and their overall end user experience is far superior than network layer VPN users. However, if they have to a lot of large file copies, they might want to move to a hotel that allows 6to4 or Teredo[4].

The IP-HTTPS 64 bit IPv6 address prefix is derived from a combination of a pre-define value, the public address of the Direct Access server, and a subnet ID. The 64 bit host ID is a randomly assigned value created by the Direct Access server. The combination of the prefix and host ID constitutes the complex IPv6 address.

Table 3. Tunnel adaptor IPHTTPS Interface

Connection-specific DNS Suffix	
IPV6 Address	202:ce49:7611:2:1429:515e:ef3d:4167
Link-local IPV6 Address	fe80::1429:575e:ef3d:4667%20
Default Gateway	fe80::466c:10dc:c879:44ef%20

Remember, IP-HTTPS is only used when the Direct Access client is behind a firewall or Web proxy that won't allow outbound access for Teredo connections. Teredo needs access to outbound UDP 3544. Many administrators might think that IP-HTTPS should be the preferred protocol since they are familiar with other HTTPS encapsulated protocols, such as RPC/HTTP, but the fact is that you want to avoid IP-HTTPS if you can.

5. DES encryption algorithm

The information security definition which defense objects are consist of data security, network security, and network business security can be described as follows: information security is theory and technology, which study how to protect hardware, software and data in computer network information systems, how to avoid accidental or malicious destruction, and how to ensure that the content of network information can't be disclosed, network services can't be interrupted and network business can running continuously and reliably. The new definition emphasizes on the three aspects of information security concept: data security, network security and network business security[5].

The principle of the DES algorithm is: DES will expressly divided into many 64-bit block size, each block with 64-bit key encrypt, actually, key by 56 data bits, and eight parity, so only 256 May password not 264.

Encrypt each block with initial encryption method, continuously 16 times complex replacement, finally back to their initial displacement of the reverse. The first step I is not directly use the replacement of the original keys, but by calculating the key Ki with the variable K and i. DES has such characteristics, and its decryption algorithm and encryption algorithm, except on the contrary Ki key sequence. DES is not really very safe. In fact, even if not using intelligent method, with the rapid, highly parallel processor, compulsory cracked DES also is possible.

6. RSA algorithm

6.1 Abbreviations and Acronyms

Public-key encryption methods of traditional and similar DES encrypted technique obsolete. Public-key encryption methods, encryption algorithm and encryption key is open, anyone can be converted into plaintext expressly. But the corresponding decryption keys are confidential (public-key encryption methods, including two respectively for encryption and decryption), and cannot be deduced from the encryption key, so even if unauthorized encryption person is also unable to carry out the corresponding decryption.

Public key encryption is initially thought by Diffie Hellman, and the most famous of Rivest is put forward, and the Adleman Shamir, now usually called RSA (the first letter in three inventor named)[6].

The method is based on the flowing two affects:

- Have a number of primes is fast algorithm;
- Has not yet found a qualitative factors of indicated algorithms.
- The working principle of RSA method is:
- Arbitrarily choose two different large prime Numbers and q, calculate the result of p = p * q;
- Choose a big integer e arbitrarily, e and (p-1)*(q-1) are co-primes, use the integer e as the encryption key word. Attention: it is easy to choose the number e, for example, all the prime number which is bigger than p and q are useful;
- Determine the decryption key d

$$d * e = 1 \mod (p - 1) * (q - 1) \quad (1)$$

The value of d can be easily calculated out according to e, p and q.

- Make the integer r and e to be public, but the integer d to be private.
- Encrypt the plaintext p to be a cipher text c, supposing p is an integer smaller than r.

The calculate algorithm is:

$$C = Pe \mod r \quad (2)$$

Deciphering the decipher text c to plain text p. The algorithm is:

$$P = Cd \text{ modulo } r \quad (3)$$

But according to r and e (not p and q) to calculate d is impossible. Therefore, anyone can explicitly to encrypt, but only authorized users (d) just can know plaintext for decryption.

7. Conclusion

The feedbacks of the results of assessing the network security policy based on security capability, as a reference to the security policy for effective adjustment, providing a more robust system and improve the safety. The correct security policy results from the correct understanding on the system security demands and effective assessment model, because the various security domain information subjects and objects have different security needs[7].

The wide application of computer network security and the increasingly serious threat to computer information confidential work put forward higher request, but it is absolutely safe computer network system is not zero, zero risk means that the network. Safety is the problem of computer network, the network secret lost eternal question, especially if we strengthen security concepts, optimize configuration, take effective safety technology, network behavior and strengthen information content protection, can reduce risk, as far as possible to play its biggest computer network[8].

On the basis of security domain and mainly aims at the security policy validity problem, we should proposes an assessment model of network security policy based on security capability, through the security domain partition and security domain policy establishment, analyzes the characteristics of the relationship between attributes, and calculates the network security capability.

References

[1] HongSheng Yan, XueLi Wang, Jun Yang. Computer Network Security and Defense[M]. Beijing: Electronics Industry Press,2007

[2] DENG Ju-long, Grey Forecast and Grey Decision, Wuhan:Huazhong University of Science and Technology Press,2002.

[3] Shuanghe. P, Zhen. H, Changxiang. S, “Security Protocol and Scheme for Inter-Realm Information Accessing”, Journal of Computer Research and Development, 2005,42(9), pp.1587-1593(in Chinese)

[4] Sheyner, J.Haines, S.Jha, R.Lippmann and J.Wing, “Automated Generation and Analysis of Attack Graphs”, In Proceedings of IEEE Symposium on Security and Privacy, Oakland, California, May 2002..

[5] Jason Thornton, Marios Savvides, and B. V. K. Vijaya Kumar, “An Evaluation of Iris Pattern Representations”, IEEE, 2007.

[6] Yu Shaojun. E-Commerce Security Analysis and data encryption technology. China's management of information technology (Integrated version), 2007. (in Chinese)

[7] D'Amico, A., Kocka, M., “Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned Visualization for Computer Security”, VizSEC 05, IEEE Press, 2005.10, pp. 110-112.

[8] Xiaobin, Tan; Yong, Zhang; Hongsheng, Xi, “Multi-Perspective Quantization Model for Cyberspace Security Situation Awareness”, Computational Intelligence and Security, 2007, pp. 853 – 857(in Chinese)