International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.135-142
http://dx.doi.org/10.14257/ijsia.2016.10.4.14

Research and Analysis on Network Security Modeling

Kehao Cao

Henan Finance & Taxation College. Henan.GongYi.China
Corresponding E-mail:11862954@qq.com

Abstract

The integration of Internet and mobile Internet, Internet of things, will promote the wide application of the Industrial Internet and other vertical internet. Smart device manufacturing, smart Internet marketing will give people work and life led to profound changes and the experience. But all walks of network security problems will become increasingly serious. Traditional networks of a variety of viruses, hackers and other threats will expand the network to the new system, they caused the damage and the impact will be more dangerous and grim. Security Analysis researching work needs to extract network and system resources related to security as well as the security factors, so as to establish a security modeling for security analysis. In this paper, it takes the introduction of network security property as a cutting point, combined with the safety requirements and analysis on the level of safety requirements, discussing the structure of safety network platform as well as the main connection relationship modeling.

Keywords: *Safety network platform; Relationship modeling; Network security*

Introduction

Meanwhile rumors network, network underworld that intrusion ordinary people are also increasingly deepened. Global trend of Informationization, on information security in the world's struggle was intensified. Variety of new attacks and the protection technologies (such as an attack on the industrial control systems, unbounded browser, Internet brush votes, Anti-AntiVirus) emerge in endlessly. The new attack and protection methods (such as network ID, cloud security *etc*.) emerge in endlessly, implementation of infiltration and espionage via the Internet, is a great threat to the national security of new tools, especially the Snowden exposes United States listening project. Information network security has become the focus of the national security, military security, economic security and personal safety[1]. So it is necessary for the security problems brought by these new attacks and defense technology, the method of system analysis, to identify its brings on national security and social stability risk and impact, thereby cultivate network security and management personnel, to strengthen the security of key facilities.If in the industrial age is nuclear war as the Center, then the Internet era is based on Cyber-Warfare Centre, information and network security has become the United States one of the three core strategies. Especially after the 9.11 incident, the United States, Britain and other countries for information security professionals train very seriously, not only to raise it to a higher level, but also increase the input into the information security talent cultivation in colleges and universities[2]. United States Obama administration, strengthening information security as a revitalization of United States critical of economic prosperity and national security strategy, while strengthening the information security education and training of qualified personnel as security in cyberspace security strategy is focused on, in order to ensure that the United States controlled global information dominance [3].

ISSN: 1738-9976 IJSIA

The Attributes of Network Security

What system security assessment to consider is the security of the existed system, the main purpose of which is to test whether the target is known to change the penetration, therefore, it needs a simple, flexible and comprehensive model, so as to avoid the state of system space too complex as far as possible. At the same time, the model of safety network system security assessment should be general and feasible. The general feature refers that the elements of the model must be involved in the safety network system security requirements, while the feature of feasibility refers that the evaluation model of implementing safety network system in the economy and technology should be feasible, which can be seen in Figure 1.

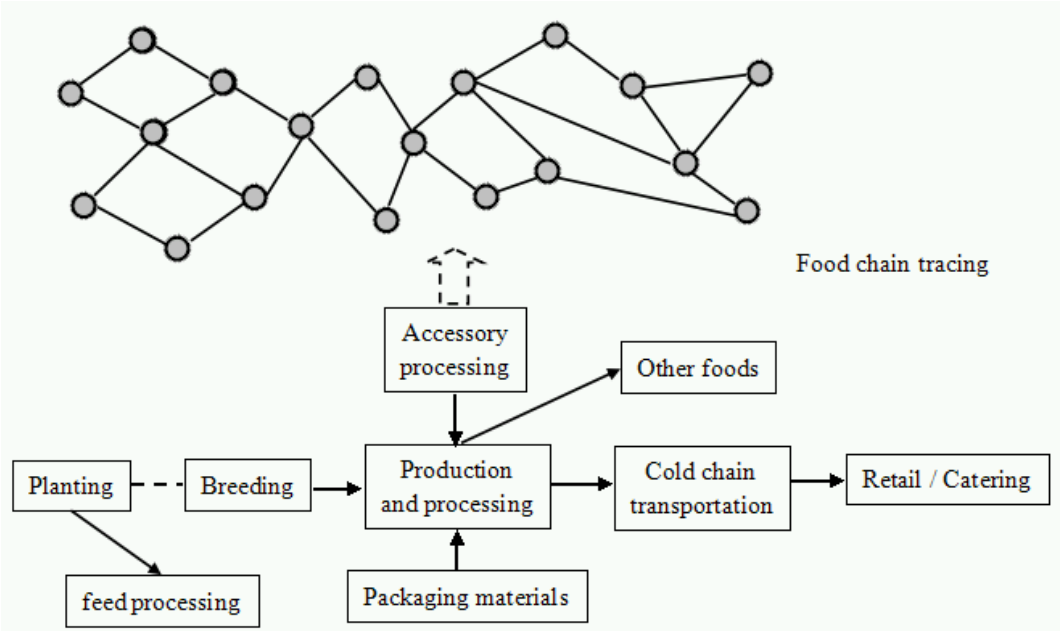

Figure 1. Schematic Diagram of Safety Network

Safety Requirements

Security requirement is a kind of security requirement of integrity, availability and confidentiality in the information of safety system. It mainly uses a series of security policy. Security policy is used to determine whether a subject can have access to a certain object, system user or process, such as discretionary access control strategy, mandatory access control strategy, organization's own specific policies and so on; the set of the security requirement made by the system is $R= \{r_1, r_2, \ldots r_p\}$, among them, r_i $(i = 1, 2, \ldots p)$ can represent the individual strategy.

Level of Safety Requirements

According to the different applications, the confidentiality (C), integrity (I) and availability (A) of system and other security requirements of the risk can be divided into different levels, taking the confidentiality of system as an example, the classification can be found in Table 1.

Table 1. Level of Confidentiality

Classification	Feature description
C1	Proving validity of the host computer
C2	Getting OS type and version number
C3	Getting application program and version information
C4	Detecting the presence of a target (file, directory, user, device, *etc*.) on the target host computer
C5	Reading the data from a user's specific file or non - sensitive memory space
C6	Reading the contents of multiple ordinary users' files or the data of the memory space
C7	Reading the contents of a particular privileged file (such as /*etc*/password, /*etc*/shadow) or system configuration file, or the contents of kernel and system processes
C8	Reading the contents of any privileged file or the contents of system configuration file, monitoring the system or network activity

From the view of the attributes of security of the system, they are independent, complementary and related [4-6]] .Firstly, independence means that every security attribute can be evaluated as a separate security quality, which is not conflicted with each other; while complementary can reflect that each security attribute can meet the needs of different users, which can be complement to each other. At the same time, it can reflect the whole needs of security network;the related feature means that the attacker wants to destroy some security attributes, at the same time, he also has the ability to destroy other security attributes, which also can affect the effect of the security attributes of the system on each of the attributes in different level.

The Frame of Safety Network Platform

Safety network tracing platform adopts the frame based on the network, which can receive the tracing information from the internal enterprise, the external enterprise by manual collecting information or automatically collecting information, it also can extract and trace information from the existed information system. The technical architecture of the platform can be shown in the figure, including four parts, namely, front terminal service, business logic, metadata framework, and extensible database. The extensible database contains whole information of the entire product chain from the farm to the table of consumer. The database itself may be a separate system, which also may be a collection of many systems. Any suitable database can be used to gather and store information of the product chain, which can be shown in Figure 2.

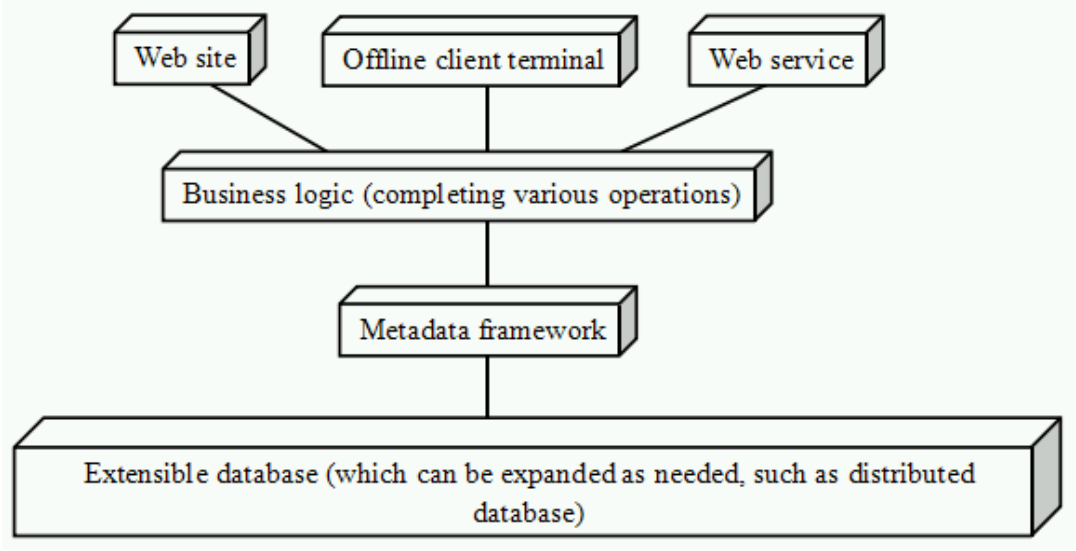

Figure 2. The Technical Framework of Traceability Platform

Tracing information can have access to the platform through the service subsystem and the offline client in the form of universal traceability structure to access the platform.[7].Firstly, data verification subsystem can determine whether the data accessing to the platform is normal in the syntax and semantics of the traceability structure; and then by the data decomposition (conversion) subsystem can transfer the traced back information into the structure and format that the database can be stored, then the data associated with the subsystem can complete the connection with the tracing information, for example, materials, the production equipment that are used, the environment, operating personnel, the related information of material detection [8].The data tracing subsystem, and the graphics displaying subsystem and other peripheral systems can take the tracing information as support, which can provide traceability information queries, the display of visualization traceability chain as well as other different application services.

The Equipment of Safety Network System

Safety network can be regarded as a collection of different functions of the host computers, these host computers can be divided into: router, switch, firewall, server, PC, and so on. In the safety network, these host computers are endowed with a unique identifier to indicate their identity, the only identity can be the IP address, MAC address and host name and so on. Taking the set of the device is $H=\{h_1, h_2,... h_m\}$, in h_i $(i=1, 2,... m)$, which can represent a single device.

A host computer of the safety network itself can contain many attributes, but in the network security analysis, it is not required to obtain all the attributes of the host computer. Among them, the attributes of the host computers that are related with the network security can be including: the operating system type and version of the host computer, the open service of the host computer and the corresponding information of the terminal, as well as the vulnerable information of the host computer.

Therefore, a host computer of security network can be represented in the following four parts (hostid,os, svcs, vuls). Among them, hostid is the unique identifier for the host computer in the network; while os is the operating system type and version information of the host computer; svcs is the list of host computer on the open web service; vuls is the list of the weakness of host computer, among the list, it may include the software that can be installed on the host computer, as well as the security flaw information, or the wrong environment configuration information.

Serious Shortage of Network and Information Security Professionals

Network and information security personnel, trained in network security technologies, information security education, know how computer technology, network management and information security knowledge and expertise to solve practical problems. They protect the security of information and ensure the smooth and safe running plays a fundamental and decisive role. But as a network security policy makers, programme implementers, Manager of network security, expertise in this field is still sorely lacking in the country, there is a big gap, particularly the high level of strategy and lack of professional and technical personnel. As of the end of 2011, China's culture of information security professionals a total of about 40,000 people, from our requirements for information security professionals in more than 50 million demands is difficult to narrow the gap. The next five years, the social requirements for information security professionals to increase by about 1.2 million people annually. Regardless of the school education and social training and social needs are very appropriate. Every year our country information security less than 10000 graduates, social training students count the quantity is less than 20000, the phenomenon of information security talent shortage exist for a long time [5]. Colleges and universities as the talent training base, of course, should take to carry out the research on the security of information and network technology, the popularization of information network security knowledge, the task of training talents of information security technology.

Current Situation of China's Network Information Security Education is not Optimistic

Personnel training plan, course system and education system is not perfect. Network information security technology is a comprehensive science, involves long-term accumulation of knowledge and the latest developments in computer technology, communication technology, mathematics and cryptography, and many other disciplines, but also social and legal issues involved. It covers a wide coverage of knowledge, technologies and methods to update faster, learning is difficult. At present, China's network and information security education training echelon Although initially formed from specialist to undergraduate to master's to doctoral, but because the set up time is short, there are differences in culture and the focus of each between universities, the emergence of diversified ideas of running schools. Different modes of thinking on the one hand reflects the advantages of disciplines of the school-running characteristics of universities and, in early development is a useful exploration and attempt; on the other hand, also reflects China's higher education system, lack of unified planning and guidance for information security training, has not yet formed a scientific and rational, hierarchical teaching mode. Embodied in the following two aspects:

1. The discipline of Chinese network information security training program, curriculum and educational system is still not perfect

Currently the community's overall lack of awareness of information security, information security disciplines lack systematicness, comprehensiveness, hierarchy and practice. The number of professionals in the field of information security, content and depth of talent is not enough. And most colleges and universities are additional network security-related courses in information security professional or network engineering and other professions. Curriculum is still dominated by traditional information security technology, focus on cryptography, firewalls, intrusion detection, and other simple safety theory and technology of knowledge imparting, lack of knowledge about network security management and network attack and defense techniques of explanation.

2. The curriculum and the teaching content is too scattered, the lack of systematic, the lack of practice relevant characteristic curriculum

Because of network and information security knowledge update faster, more involved in the field, making the school's teaching program is not scientific, curriculum does not reflect the characteristics of the information security discipline itself, curriculum design and teaching content is too scattered, difficult to constitute professional knowledge architecture. Course is difficult, more content, strong theoretical and systematic not enough. Experimental courses is insufficient, lack of experimental textbooks, the pertinence is not strong. Laboratory equipment is not enough, training projects not closely linked with network security management, lack of practical training base.

3. Teaching content, teaching methods cannot meet the teaching needs

With the development of information security awareness, information security professional has become an important part of major college computer teaching system. But the current teaching of information security, or too focused on theory studies lacking specific test case, or puts too much emphasis on a particular case while ignoring the complete training of information security knowledge; But currently of information security teaching, or too focuses on theory research and missing specific experiment case explained; or too focuses on a specific case analysis is ignored has information security knowledge structure of full introduced; or only focused on virus prevention technology is not explained related network offensive and defensive aspects of knowledge; or only focused on network offensive and defensive of General technology is failed to in-depth to hardware bottom, formed can't a full of information systems security solution programme. Furthermore, because of the information security and information industry closely related, the simple classroom and online teaching is not sufficient to reflect the current security technology development. The students' study of knowledge are still staying in the pure theoretical teaching or equipment application level, the theory and practice of operation combined with close enough, make the students not possess solid foundation of skills in learning. But as an information security professional talent, not only for deep understanding of theoretical knowledge, but also enhance practical ability. Experimental operation, deep understanding of knowledge and application of network and information security, enhance their employability and competitiveness.

Modeling of Main Connection Relationship

The whole Internet is set up based on TCP/IP protocol, so far, most of the current computer network system is based on this kind of protocol. TCP/IP protocol family has a lot of protocols, which can be divided into different levels. Followed by this specification, the connection between the network devices are distributed in different levels, once Ritchey has discussed about the safety analysis on the network connection relationship [9].According the the definition of protocol, in the link layer, the type of ARP data packets is spread within the local area network, the devices within network can capture the data message, the malicious subject can make use of this message to attack the TCP session. At the same time, the connection relationship between the host computers in this layer is also affected by network structure; if the network is connected by the hub, data packet is transferred by radio transmission, the malicious subject can capture all the packets on the network by setting the net with mixed mode, after having protocol parsing, it can have a sniff attack successfully. If network is connected by switches, the data packet transmission is transferred through the switch to the corresponding port, it will not carry on broadcasting, the traditional concept believed that individual users can only get the sent packets, which cannot get the entire network data packet, but in recent study, it showed in a certain exchanging network environment, through ARP cheating, it can monitor the network, but this type of attack requires a higher technical level [10]. The connection relationship between network devices in the data link layer are: ARP, HUB_Sniff, Switch_Sniff.

The protocol between the network layers is designed for the communication of network, each host computer on the Internet can be assigned with a different IP address, according to the ICMP protocol of the network layer, it can obtain network routing information such as purpose, time, and accessibility. As for network security, the attacks of denial service and distributed denial service can attack on the target system according to the layer protocol data packet structure. The connection relationship between network devices in the network layer exist: ICMP_ service type.

There are two protocols, namely, TCP and UDP in the transferring layer, each protocol has 65535 ports, which is assigned to different types of service and regarded as the conversation protocol between the end-to-end session of the host computer, while the connection relationship between network equipment can use the protocol and port to express, for example TCP_80, which means the target terminal is at the port 80 and it can provide TCP service. Namely, the connection relationship between network devices in the network layer exist: TCP (UDP) _ the number of the port.

Application layer can be responsible for the network to provide various services, each service type can provide support for the different application, while the application that can provide the same type of service can exist different security problems, in order to distinguish the difference, the users make personalization changes, in this paper, the connection relationship between the host computers in the application layer can be described as: TCP (UDP) _ the number of port _ the type of service _ the name of application, such as TCP_80_HTTP_IIS4. 0, it can refer that the target terminal based on TCP protocol is at port 80, using IIS4.0 to provide HTTP service.

In this paper, the various connection relationship of TCP/IP protocol which is closely linked with the security relations can be expressed as a collection, the network connection between the two devices of the network is a subset of the set. According to the realization of the network protocol, taking the network connection relationship between host computer and device as a set, namely, $Protocol=\{pro1, pro2, \ldots pron\}$, among them, $pro_i(i=1, 2, \ldots n)$, which can represent a relationship of a connection.

The connection relationship between the host computerscan use a triple set (Hsrc, Hdst, protocols)to express. Among them, Hsrc can represent the source, Hdst can represent the target of the host computer. While protocols is a subset of the set of connecting the source host computer and the target host computer. When there is no connection relation between source host computer and the target host computer, then the protocol is an empty set. When the source host computer is the same as the target host computer, then the connection relationship is the local connection, at the same time, $protocol = \{localhost\}$.

Conclusion

Application layer can be responsible for the network to provide various services, each service type can provide support for the different application, while the application that can provide the same type of service can exist different security problems, in order to distinguish the difference, the users make personalization changes.

References

[1] L P LSwiler, C Phillps, D Ellis. Chakerian. “Computer-attack graph generation tool[A]. Proceedings of the DARPA Information Survivability Conference and Exposition. Anaheim, California”, **(2000),** pp. 307-321.

[2] C Ramakrishnan, R. Sekar. “Model-based analysis of configuration vulnerabilities [J]”. Journal of Computer Security, vol.10, **(2002),** pp. 189-209.

[3] Y Z ZHANG, X C YUN, “A new vulnerbality taxomomy based on privilege escalation”. 2004 Sixth Internatioan Conference on Enterprise Information Systems Proceedings. Porto: INSTICC, **(2004)**, pp. 596-600.

[4] R. Ritchey, B O’Berry, S Noel. “Representing TCP/ IP connectivity for topological analysis of network security[A”, Proceedings of the 18th Annual Computer Security Applications Conference. San Diego, California, **(2002)**, pp. 25-31.

[5] C A Phillps, P Swiler. “A graph-based system for network vulnerability analysis. New Security Paradigms Workshop”, **(1998),** pp. 71-79.
[6] Anon; “outside hacker attack on China is becoming more serious”, more than half of attack from the United States. Xinhua net, .vol. 03, no. 10, **(2013)**.
[7] C Yan; “Snowden exposure USA network monitoring system: proficient in Chinese and Arabic”.Http://news.ifeng.com/world/special/sndxiemi/content-3/detail_2013_08/02/28186434_0.shtml,. vol. 8, no. 2. **(2013)**.
[8] Z Peng, L Jian, “The development of domestic and international information security”. Journal of Information Network Security, vol. 7, **(2011)**, pp. 84-85.
[9] L Shuxian, Z Guiding, “Analysis on information security of teaching mode of teaching and experiment innovation in specialty”, http://www.studa.net/Education/100529/16224111.html, vol. 5. no. 27, **(2010).**
[10] Z Yong; “Chinese information security professional talent gap of more than 500000”. Sohu IT, vol. 11. no. 28. **(2012)**.

Author

Kehao Cao. Lecturer Research direction: Computer analysis. Data mining

