Analysis on Computer Communication Network and the Framework of the Network Security Technologies

Fengquan Li

Xi'an International University, Xi'an Shaanxi, 710077

Keywords: Computer Communication Network; Framework of Security Technologies; Network Security

Abstract: As the popularity of the computer technology and the constant development of communication technology, the application of the information technology was utilized more widely. Under this background, the issue of network security is exposed gradually. Especially the communication network, it is the core part of the communication system, so it is very important in the whole system. At present, the issue of network security becomes stubborn so that it influences the daily work and life of the public. In order to strengthen the construction of information security, and improve the network security, it is necessary to deeply analyze the network security technology, and then to bring forward the targeted countermeasures. According to the relevant materials, the writer of this thesis takes the present situation of the computer communication network as the breakthrough point, and then discusses and analyzes framework of the network security technologies.

In the developmental trend of information technology, the network communication becomes more and more popular, but it also brings about some problems on the security field. In one hand, the network information technology privies the strong driving force to the development of the economy and the society, and most of the industries take the best of this technology and becomes stronger and stronger; but, in the other hand, we have to accept that there still are some defects which could bring about some serious problems. The communication network is suffering the security risks every minutes, no matter these risks are brought about by the defects of the network or the risks that are caused by the defects of the operation system on which the network is run, even the mistakes of the operators, these all could bring about serious threats to the whole communication system, such as the reveal of the confidential data, system failure, etc, they all could bring about the negative influences to the daily production and life of the public. Because of the importance and the specialty of the communication network, and because of the severe circumstance that we have to face, we must strengthen our vigilances to improve the security technology, and draw up some relevant safeguard policies, so as to construct the safe system and safeguard the network communication.

The current security problems in the computer communication network

At present, because of the weakness of the technology, we have to import some technologies and software, and this problem is serious. In the construction of information society, the database technology, the relevant hardware, CPU, and the gateway software are not created by us; these threaten the information security a lot. Because we have not master the core technologies, the network information system faces some risks such as the attacks of the viruses, even there are some

hidden channels that cause the reveal of the user's confidential information, it is easily to be attacked and be controlled by the outside attackers, and the system becomes very unsafe [1]. Specially, to the communication network, in the special circumstance that it is lack of the core technologies, the information network is easily to be wiretapped or to be monitored, even the more serious information security problems. At the some time, the maintainers often feel difficult on the subsequent maintenance because of the deficiency of the core technologies.

At present, as the constant development of the communication network, the information system is easily be attacked by the outside attackers, some hackers and criminals often attack the system via the network platform, they plant the Trojan viruses in the system and alter the data of the system after they have intruded into the system successfully. At the some time, they could wiretap and monitor the relevant information so that the network is badly threatened by the illegal attacks [2]. Because the network platform is complex and it is hard to find out the true attackers, once the network is attacked by the outside attackers, the bad results usually are serious; the system would not work regularly, even some more serious problems would be occurred.

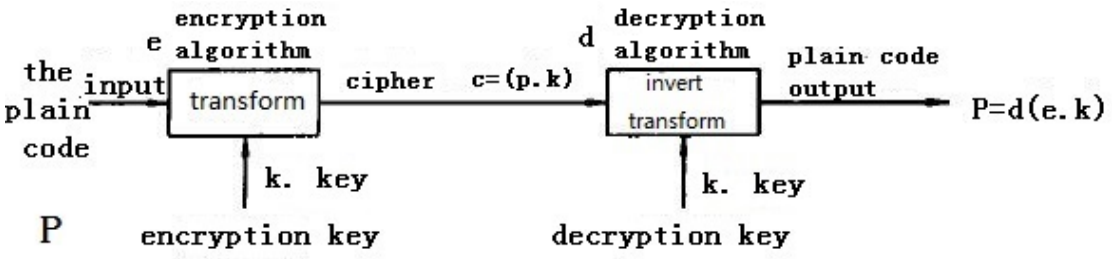
At present, there are many dangerous viruses, Trojans, and fishing websites in the network. These viruses usually are covert, complex, and they have strong destructive force; at the some time, they could easily be transmitted by the documents in the network such as Email so that the information system can be easily influenced by these viruses. The information system is so special that once it was attacked by the outside or the Trojan was planted in the system, the terminal equipment could be destroyed, the information of the users could be revealed, these threaten the safe of the system [4]. Furthermore, if the situation become more serious, the whole system could be down, this would bring about some more serious losses.

It is known that the information of the system is transmitted by the connections of the nodes, but the connections of the nodes could easily be attacked, so could the terminal equipments which exchange the information likes this way. In this situation, the information also could be revealed or altered, or it could be destroyed spitefully, it is very dangerous, and the information can not be safeguarded effectively. Once the attacks intrudes into one of the connections between the nodes or the sub-systems, the security problems can be brought about, and the communication system will be broken-down; it threatens the communication system badly.

The analyses on the framework of the security technologies of the computer communication network

It is a very important security method to encrypt the transmitting data via the network so as to safeguard the data, i.e., to ensure the data that is stored in the equipments or in the process of transmission can not be stolen illegally [4]. We call the data that haven't been encrypted "plain code", and we call the data that have been encrypted "cipher". The encryption process makes the plain code to the cipher is a function transformation process with the key (k) as the parameter, we call this process transformation; conversely, it is inverse transformation. In general, the encryption algorithm (e) and the decryption algorithm (d) usually are not confidential, but only add the parameter key (k) to the process can the encryption algorithm (e) and the decryption algorithm are right. Therefore, the safe coefficient of the data encryption is mainly depends on the security degree of the key (k). There are three types of the basic cipher; they are the Caesar Cipher, the Substitution Cipher, and Product Cipher. The Caesar Cipher is the cipher that to create the new code by changing the order of the plain code; the Substitution Cipher is a kind of cipher that to substitute the plain code with the other character or code so as to encrypt the plain code; the Product Cipher means encrypting the plain code more than two times so as to create the new cipher that would be more difficult to be

decrypt. In the realistic encryption process, people usually doesn't just use one kind of the cipher, but use the cipher that has been transformed for several times according to the three ciphers we have mentioned above [5].



When the communication network is threatened, it could be solved by the dynamic monitoring technologies or the static detection technologies. The dynamic monitoring technologies include: (1) Non-execution Stack Technology. When the system is threatened by the outside, the system could be protected by the stop stack. It should be noticed that although this method is effective, but if it is fail, the computer would be damaged irreversibly. (2) Non-execution Heap Technology. This kind of technology could protect the software by controlling the memory area where the stack and the data sections could stop the hackers' codes so as to protect the system. The Non-execution Heap Technology is usually used with the Non-execution Stack technology at the some time. (3) Memory Mapping Technology. It is to hide the codepages for improving the security of the software, and improving the functions of the firewall so as to stop the attacks from the hackers. (4) Sandbox Technology. This technology prevents the attacks by banning the IP address of the hackers; we must notice that if the virus that could damage the system has intruded into the system, this technology could be useless. (5) Program Explanation. This technology protects the system by embedding the new code; this technology need not to modify the primary code. The static detection technologies include: (1) Lexical Analysis. By comparing the segments of the information and the details of the programs, the system could find out the flaws and the virus. Because of the low error-tolerant rate, this technology has been eliminated gradually. (2) Rule Detection. When we set up the framework of the communication network, there may be many kinds of software that could support the network; if the software of the network become unsteady, we could detect these software and improve the security of the network by analyzing the individual software so as to avoid the flaws that are caused by the operators' mistakes [6]. By using these detective technologies, the security of the communication network could be sound, the communication system would work smoothly.

In order to strengthen the management of the communication network, we must be vigilant, monitor the network all the time, and detect the system according to the schedule, so as to find out the viruses and other risks and then to solve them. In order to safeguard the network communication, it is necessary to solve the existed problems timely and actively, and avoid the expansion of the viruses, or it will become stubborn. It is also necessary to check up the relevant data that are transmitted in the communication network and that are transmitted between the nodes, if there is any virus that exists in the system, we must solve it as soon as possible, so as to improve the tolerance and the stability of the system [7].

The core technologies that are related to the communication network determine the safe coefficient of the network. In order to improve the self-protection of the network, we must research and create the core technologies of ourselves. Above, we have mentioned that the core technologies

are usually imported directly or researched by more that one country, so the network may face some risks naturally. Therefore, we must strengthen the investment on the core technologies, try our best to research and create the new technologies, so as to ensure we master the competitive core technologies which are confidential, and avoid the hostile attacks and instabilities that are caused by the sufficiency of the core technologies. Only when we improve the technologies, prefect the communication network constantly, and improve the functions of the firewall and the safety of the transmission, could the communication network become safe and stable.

Conclusion

The communication network provides a lot of conveniences to the people during its constant self-development, no matter in the production field or the management field, or in our daily life; so to speak, it has changed our ways of communication. But, as the changes of the outside circumstance, the communication network faces various threats that from the inner and the outside, such as we does not master the core technologies, the risks of the viruses that are caused by the outside attack, and the risks of data transmission between the nodes, etc, these may make the network very unstable. In order to clean the circumstance of the network, and safeguard the safety and stability of the network, it is necessary to improve the security technologies and its framework, at the some time, to make some significant breakthroughs on the technologies, and to improve the stability of the system by utilizing the new technologies. We must not only using the advanced technologies such as the encryption technology, but also make some breakthroughs of the technologies, and make great progress by means of the technologies.

Acknowledgements

The Scientific Research Project of Shaanxi Provincial Department of Education, 2017: Research on the Trajectory Programming and the Mixed Force and Position Controlling System of the Acupuncture Robot that is Base on the Vision.
Project No. : 17JK1103

References:

[1]Dong Jialong. Research on the Applications of the Data Encryption Technology on the Security of the Computer Network Communication[J]. PC Fan, 2017,(09):14.

[2]Tian Xiali, Xiong Ying. Research on the Present Situation and the Developmental Trend of the Computer Network Communication[J]. Computer Programming Skills & Maintenance, 2016,(24):73-74.

[3]Zhang Yang. Research on the Problems of the Computer network communication and the Countermeasures in the New Times[J]. Computer Programming Skills & Maintenance, 2016,(24):74-75.

[4]Tian Boru. Deliberations on the security of the computer communication network and the protective strategy[A]. The Symposium II of the 2016 International Scholar Symposia that is organized by the periodical office of *Smart City* and the Sino American Academic Exchange Association on the Smart City and the Construction of the Information Technology, 2016:1.

[5]Zeng Qilong, Ruan Yi, Wu Jiayi. Exploration on the Application of the Data Encryption Technology in the Security of the Computer Network Communication[J]. China Computer & Communication(Theory Edition), 2016,(17):164-165.

[6]Hang Zhongshi. Exploration on the Data Encryption Technology That Is Applied in the Security of the Computer Network Communication[J].Science and Technology,2016,(22):8+55.

[7]Gu Xingshe. Research on the Security of the Computer Communication Network and the Relevant Technologies[J].2016,(05):77.