MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKOV NATIONAL UNIVERSITY OF RADIOELECTRONICS

ISBN 966-659-088-3

Proceedings of East-West Design & Test Workshop (EWDTW'04)

Yalta, Alushta, Crimea, Ukraine, September 23 – 26, 2004

CONTENTS

NETWORK SAFETY. PROBLEMS AND PERSPECTIVES

VOLODYMYR NEMCHENKO

Kharkiv National University of Radio Electronics

vpn@narod.ru

Abstract. The necessity of the information protection for networks is shown. Analysis of certain types of the networks attacks is given. Principles of protection of the information in networks and perspectives are shown.

This paper analysis a state of arts in the Network Safety area. The problem is actual especially taking in consideration the escalating of the network attacks amount fixed daily in the Internet. This work estimates the situation with network safety. Summary classification of attacks with the analysis of the basic attacks types is given. Some characteristics of the main types of attacks are shown.

In reality today almost each server is exposed to the attack having place several times in day. The information from CERT (Computer Emergency Response Team) shows the distribution of an amount of the incidents registered in Internet coupled to a network attacks on years since 1988 (6 incidents) till today (137.529 incidents in 2003) [http://www.cert.org]. In total 319.992 cases of network attacks have been fixed during this period. The figure 1 presents this distribution.

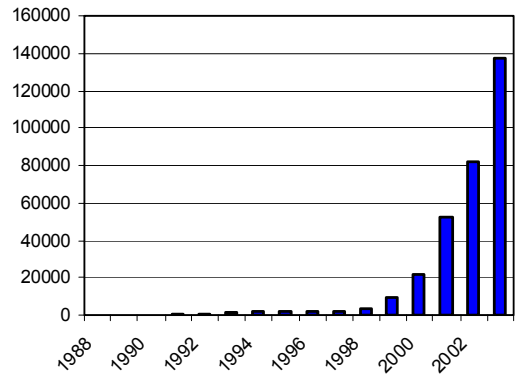

Fig. 1. Distribution of an incidents amount on years

The analysis of the literature shows that today there is no the uniform system permitting to classify possible network attacks. There is a lot of classifications not coupled with each other. In [1] a successful trying to realize systematization of all classifications is made. The brief characteristic of this classification is made in [2].

Before to proceed to the network protocols vulnerabilities reviewing we shall mark that all structures of Internet attacks are shown in this paper very schematically and they cannot be used by malefactors for a realization of real attacks. We use below only public data.

On the other hand, it is necessary to remember ancient wisdom – "who is informed that is armed". In this context the vulnerabilities network protocols knowledge allows users to be ready for any sort of attacks in the web.

Historically the basic network ideas came on 70 - 80th years of past century when it was not given the due attention to the questions of a network safety. The result is that practically all network protocols of ÒÑÐ/IP version 4 are vulnerable for attacks.

We shall examine now the basic types of network attacks.

Ethernet technology using in the LAN (Local Area Networks) uses the common bus topology. It means, that any information circulating on a one segment level can be intercepted and analyzed by any host of this segment. This property can be used by attacking host to pick up a confidential information from an attack victim host. This attack is classified as passive attack [2]. FTP and TELNET protocols are sensible to this attack type because they transmit an information without use of a cryptographic coding.

Another type of attack consists in the substitution of some network subject by another one. In this case when an attacking node sends to the victim a queries on behalf of another subject.

There are two possibilities of the organization of this type attacks. At first, the attacking node realizes the commands on behalf of a control network node, for example, on behalf of the server or of the router. Second, it is the attack realized through the virtual channel established by the TCP protocol. In this case the attacking node substitutes one of the trusted subject of a network.

The structure of the ARP false server attack (Address Resolution Protocol) is presented by the figure 2 on the Message Sequence Charts (MSCs) form.

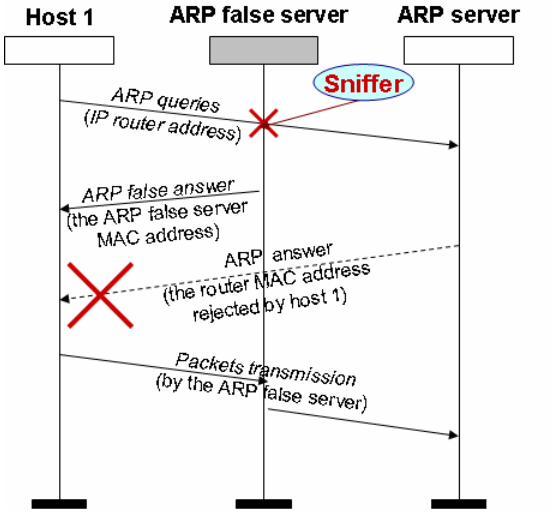

Fig. 2. Structure of the ARP false server attack

The main objective of this attack is to introduce the ARP false server between a host 1 and the real ARP server. As result, the transmitted information can be intercepted or forged by ARP false server.

The DNS server (Domain Name System) is used for transformation of a domain name to the IP-address. The basic vulnerability of the DNS server consist in the use of the UDP protocol (User Datagram Protocol) which is not protected against attacks.

There are some possibilities to realize a DNS attack. The figure 3 presents an example of the DNS false server attack structure.

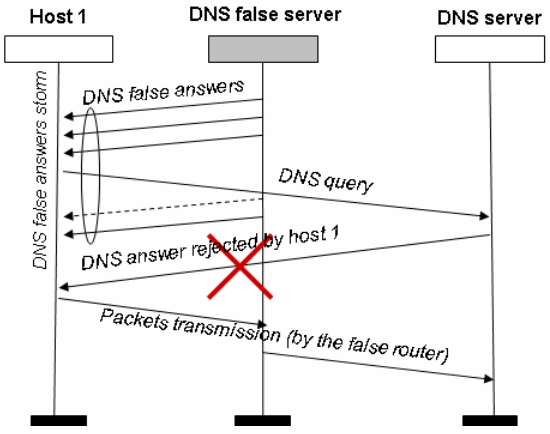

Fig. 3. Structure of the DNS false server attack

The malefactor connects the both nodes through the false router which address was received from the DNS false server. Thus the malefactor intercepts a link. Further all information exchange between hosts will be carried out through the false router, i.e. through the malefactor.

The routing on the network is carried out by such protocols as RIP, OSPF, etc., and the control of a routing is realized by protocols of ICMP family. In a case when a packet cannot be supplied to the destination node because of problems in a web the initial router receives a recommendation to redirect the route. A malefactor can take advantage and replace in the routing table the information concerning a default router. In this case we have the false router attack.

So, we stop our examination of the attack examples end we go on to the question concerning a perspectives of the network safety.

Today the Ethernet technology using a common bus topology is widely applied. Thus all hosts of the same segment have a possibility to gain any information circulating on a common bus. So, the malefactor can use a "sniffer" to intercept a confidential information.

Using a dedicated line segment topology permits to avoid this type of attack. In this case each host of segment should have a proper connection line with each host of the same segment. At the same time, the given structure has no property of flexibility and it is a bounded problem solution.

Other solution is the use of the network switch which connects all hosts of a segment by a dedicated lines. But for all that, in this case the main principle of a network construction - survivability is broken. I.e. if switch goes out of operation or is exposed to attack the functioning of all segment will be broken.

Another perspective to protect information in the web consist in the using of special Internet protocols of new generation. First of all we shall mark that the most protected protocol now is the TCP protocol. The initial TCP connection stage - handshake allows to lower considerably a possibility of attack but does not eliminates it completely [3]. Only use of special encryption methods allows to solve this problem practically. For this purpose it is possible to use the SSL standard (Secure Socket Layer). It is the

information encoding algorithm using the open key based on the Diffie - Hellman method [1].

This idea is embodied in the protocol stack of new generation TCP/IPv6. The formation of a cryptographic context is presented in the fig. 4.

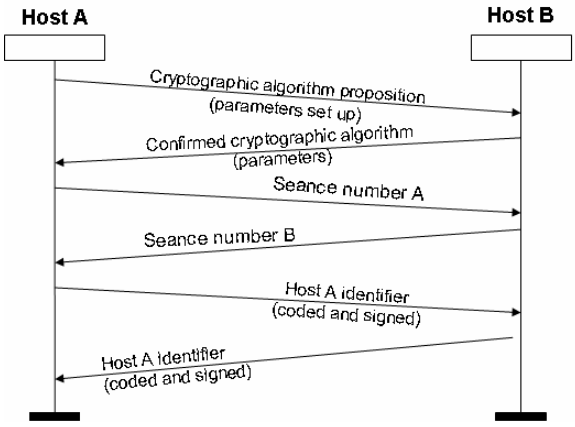

Fig. 4. The TCP/IPv6 cryptographic context formation

So, the use of a TCP/IPv6 stack protocols allows to lower a possibility of a network attacks.

Concerning a problem of routing attacks we note that this type of attacks is based on a IP address falsification of a host sending a packet. For solve this problem each router should test the IP address of the initial host and associate it with an appropriate subnet address. They must correspond each other. But in this case there is a problem of the packet header representation.

We shall mark that network safety contradicts always such web parameters as functionality, accessibility, velocity, etc. Therefore, before to undertake a safety measures it is necessary to determine the necessity level to guard the available information in each concrete case. It may be a price of the undertaken gains above a value of the defended information.

So, the present paper attempts to generalize the available information about the network safety and to show the development paths of this research area.

References: 1. *I. Medvedovsky, etc.* Attack against Internet DMK. 1999. **2.** *V. Nemchenko, A. Schaff.* Vulnerabilities and test of Internet protocols / Radioelectronika i Informatika. 2003, No.3, p. 194-195. **3.** Technical details of the attack described by Markoff in NIT. San Diego Supercomputer Center. 1995.

ELECTRICAL TEST IS NOT ENOUGH FOR QUALITY

BENGT MAGNHAGEN

JONKOPING UNIVERSITY, SWEDEN

bengt.magnhagen@ing.hj.se

Electrical test means Functional Test (FT), In Circuit Test (ICT) or Boundary Scan Test (BST) or even a combination of these technologies. However, with modern technology, like SMD (Surface Mounted Devices) technology, BGA (Ball Grid Array) components and extremely small component dimensions, electrical test alone does not meet the quality requierments.

Electrical test can not identify bad soldering and bad alignment of components, as examples. Missing decoupling capacitors and so on can not be detected because of it is hard to get physical access for testprobes. Do not forget that digital designs contains a lot of analogue devices!

The tutorial will discuss today test technology with equipment for ICT and BST as well as its pros and cons. And as the addition of this, Inspection. Inspection has traditonally been performed manually but this is not realistic today with board crowded by components. Today Inspection is performed by machine vision. Optical technique named Automated Optical Inspection (AOI) and more advanced X-ray inspection (AXI). AOI and AXI is not the future, it is here today.

EMC /EMI is also a growing challenge and some new ideas will be discussed how to test for these phenomenas.

Підписано до дру*у 9.09.т004. Формат 60*84$^{1}/_{8}$.

Умов. дру*. ар*. ууи4. Облі*.-вид. ар*. у0и0. Зам. № т-875. Тираж №0 прим.

Віддру*овано в навчальнофнау*овому видавничофполіграфічному центрі ХНУРЕ.

6№№6иХар*івипросп. ЛенінаиМ4.