Technical sciences

UDC 004.77

Machusky Eugene
Doctor of Technical Sciences, Professor
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Svystun Roman
Student of the
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

ANALYSIS OF VOICE OVER INTERNET PROTOCOL ATTACKS DIRECTED AT IP TELEPHONY

Summary. *The organizational and technical problems of ensuring the protection of the communication channel via IP telephony against information leakage were analyzed. Possible attacks of this communication channel were considered and protection options based on available methods are proposed.*

Key words: *LAN, VoIP, communication channel, cipher.*

Introduction. Nowadays, more and more information is being transmitted via Internet network and telephones are no longer the exception. Now, making calls by using network is possible through a special protocol called Voice over IP (VoIP) that special IP phones use. As mentioned in [1], when IP phones first appeared, it was possible to contact only a small network of users using Skype service, which resembled the capabilities of regular phones. The biggest drawback for VoIP technology using IP protocol for data transmission, therefore inherits all its vulnerabilities. Addressing possible attacks on IP telephony by using

appropriate protection methods reduces costs in the event of information leakage through interception of voice messages. Types of attacks can be categorized as internal and external.

Internal attacks. For internal attacks, it is assumed that the intruder is on the territory of the object and tries to connect to the local area network (LAN). As basic as it gets this type of attacks allow intruders to listen to data (similar to wiretapping). Most common type of attack for corporate espionage.

Examples of internal attacks. Let's assume that the intruder trying to connect to the VLAN using his own device. Since the purpose of VLANs is to isolate local networks, not to protect them [2] the criminal does not care where to gain access to the LAN. Once intruder is connected, it will take moments to find MAC address for connected devices and use them for his masking (spoofing) and filtering of necessary packets. Figure 1 shows schematic of intruder connecting to local network by using cable, which was connected to IP phone.

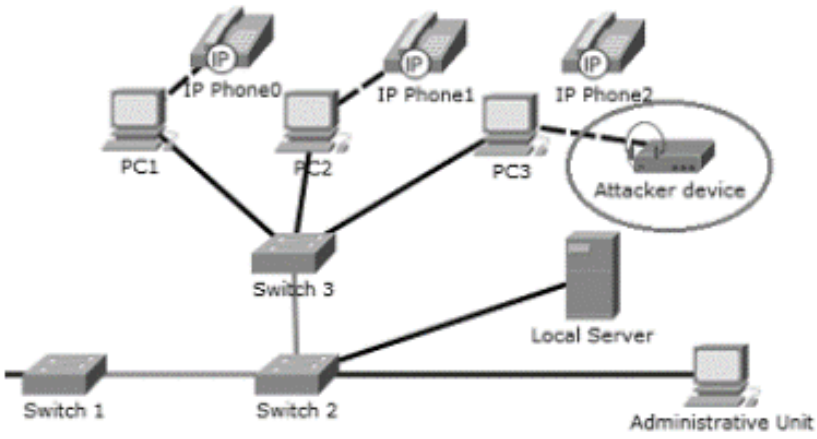

Fig. 1. Example of local connection of the offender

The second example for this type of attack is using devices, which already connected and in use. Without installed limitations on those devices, intruder can immediately interact with traffic: listening to conversations or contacting with said device to transmit already intercepted information.

External attacks. From connection perspective, external attacks can be categorized into two group types by direction of their attack: penetration of LAN from Internet and data channel interception as shown in Figure 2.

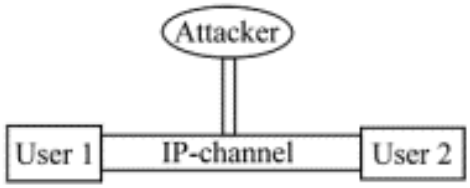

Fig. 2. Logical connection diagram

Examples of external attacks. Without proper device configuration (first and foremost firewall) and logical connection, LAN become vulnerable to external attacks. When intruder trying to reach data within LAN penetration attack occurs. For example, VLAN hopping attack uses double encapsulation of packets [3]. Figure 3 shows a diagram of a double encapsulation attack.

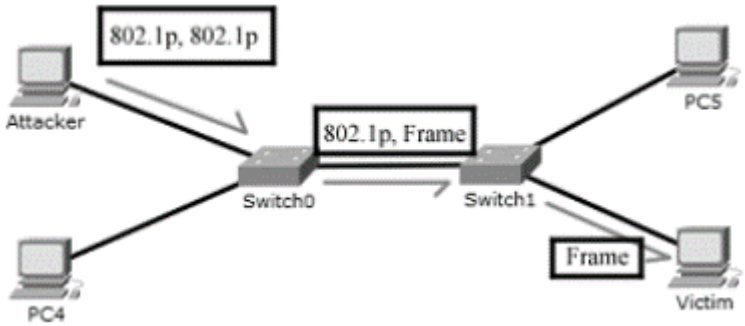

Fig. 3. Connection diagram of external attacks

The attacker sends the data. Then packets reach first switches, which see only one level of encapsulation, strip packet from it and forward it to the next. In this way, the end device receives a normal packet request, after which it sends a response packet to the intruder. Regardless of answer data in response packet, the criminal receives information that can be used to carry out the next step. A similar problem is unconfigured switches operating in trunk mode [4], which does not allow local networks to be isolated from each other. Due to this, the intruder is able to combine both multiple attacks into one.

Interception attack is more straightforward. It uses connection to a data line between VOIP call users. For example, when sender and receiver are physically located in different offices or LANs intruder able to "listen" their call when data line goes through device he connected to as shown in Figure 4.

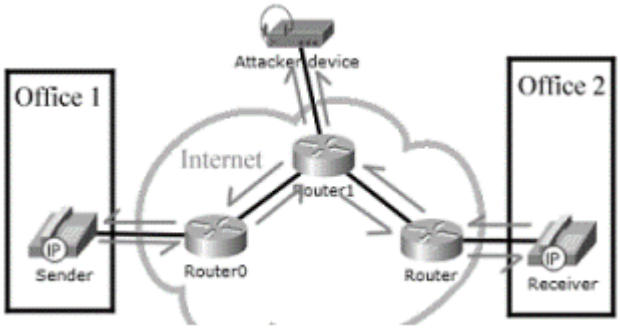

Fig. 4. Interception of data between two LANs

Overview of available protection methods. Methods to counter reaction for internal attacks. First line of defense against intruders is maintaining confidentiality by security system. User identification is the first method that comes to mind and for a good reason. It gives protection against bystanders in system. To connect into it, you will require to enter identification code. This method can support alarm triggering when incorrect sequence of symbols is typed. Using passwords is another method for protection and sometimes used as an alternative to identification. For example, if device being used by multiple employees in office at different work shifts. Those methods allow system to keep track of intruders in case they try to enter the system. To make sure that user is not an intruder who tries entering the system those methods should be combined for stronger authorization complex and thus maintaining overall confidentiality of system. There are many other examples for authorization which can be used in combination with identification, such as: ID cards, tokens, digital signature, fingerprints, iris and retina scan, facial scans, etc.

If by chance intruder managed to bypass first layer of security measures the second wall of defense will be system accountability and encryption. If intruder

reach system's second layer, we need to guarantee that he will be caught and stopped in time, before anything bad will occur. Encryption works wonders for this task and while there are no absolute uncrackable ciphers in existence, there are "practically" unbreakable, which are sufficient due to decryption time it would take (over 80 years to decipher).

Methods of countering external attacks. Attacks which aim to penetrate the LAN from the Internet are relying on a poorly configured protection system. Most responsible components for this type of attacks are firewall settings and logic behind device connections. Switches have their own logic for local VLAN connections. When two switches are connected, they form three VLAN zones: one between them and two more (from switch to another connected device). For defeating double encapsulation attacks we can connect firewall right between switches. A wall will be placed between external wide area network (WAN) and LAN, as shown in Figure 5.

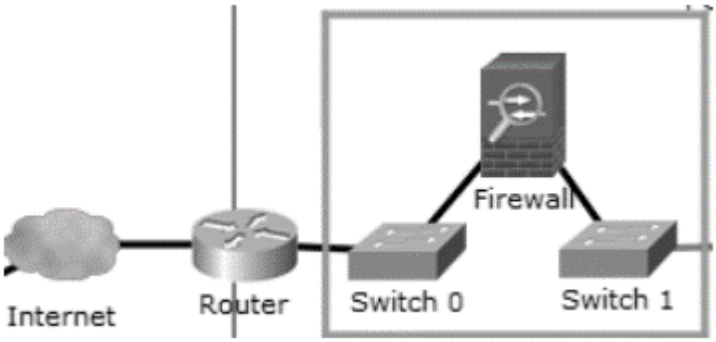

Fig. 5. VLAN demarcation scheme of switch networks

As firewalls provide resilience for system, they will also secure vulnerabilities of switches considering their configuration will be done properly, with awareness of problems that could appear. For switches it is important to disable dynamic trunking protocol (DTP) [5] and always change settings for VLAN [6] as they give intruder information to make their penetration attack more successful.

This leaves intruder only option, which is traffic interception from Internet, as shown in Figure 3. Again, data encryption provides information security in case of interception and modification attempts. Effectiveness of non-standard encoders with practically unbreakable ciphers [6] will greatly slow down data decryption, which in turn guarantee two things. First, that is information being transferred without any changes by intruders and second being encrypted so well, by the time it will be deciphered data inside the packet will lose all of its value to the intruder. Use of virtual private network (VPN) service is an alternative to just encryption method, that could be considered as upgrade. With VPN service working system's network form their own secured data channel between devices that undetectable by intercepting attacks, as shown in Figure 5.

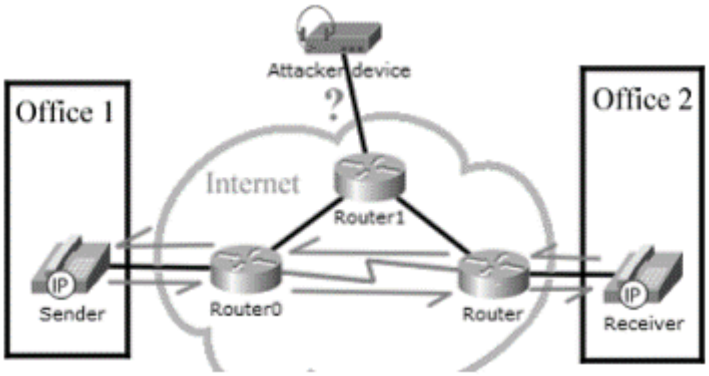

Fig. 6. Data transferred with using VPN

While this method creates secure data line by using secure Internet Protocol (IPsec) tunnel between devices [7], the price of such security method comes to transmission quality. As real-time voice data being transferred through VoIP channel it is important to have minimal delay for packets which VPN service only increase due to extra steps to achieve secure data transfer.

Conclusions. In this work attacks at VoIP channel were analyzed and counter methods were proposed. Securing voice channel requires a thorough combination of methods. Identification and password methods can be combined into comprehensive authorization method, which along with the VPN service, become first layer of defense. Second layer utilize encryption as stalwart

resistance to further intruder attempts of gaining vital information through VoIP channel. Despite the lack of absolute protection, practically unbreakable ciphers give data that being transferred enough duration to lose its value to intruder.

References

1. Renee C. H. Businesses move to Voice-Over-IP // Forbes. 2008. URL: http://bit.ly/3FMan5N
2. Farrow R. VLAN Insecurity. 2003. URL: http://rikfarrow.com/Network/net0103.html.
3. Hayvoronsky V., Novikov M. Information and communication system security. M. : BHV. 2009. ISBN: 966-552-167-5 (in Ukrainian).
4. Cisco. Cisco Nexus 5000 Series NX-OS Software Configuration Guide. 2019. URL: http://bit.ly/3Brdgq8.
5. Cisco. Configuration Examples Related to VLAN Features. 2012. P. 463-470. URL: http://bit.ly/3WdD6pi.
6. Alishov N., Zinchenko S., Alishov A., Sapunova N. Control, navigation and communication. 2017. P. 3–7. URL: http://nbuv.gov.ua/UJRN/suntz_2017_1_3 (in Ukrainian).
7. Kent S., Seo K. RFC4301: Security Architecture for the Internet Protocol. 2005. URL: https://tools.ietf.org/html/rfc4301