Computer networking and sociotechnical threats

VLADIMIR SOBESLAV
Department of information technologies, Faculty of informatics,
University Hradec Kralove
Rokitanskeho 62, 500 03 Hradec Kralove
CZECH REPUBLIC
vladimir.sobeslav@uhk.cz

Abstract: - Digital communication technologies create the fundament of modern information technologies. The development of security application and system made more difficult to penetrate the information systems and computers. Social engineering opens the new possibilities for attacker trough vulnerabilities of human interaction in cyberspace. The aim of this paper is to analyse sociotechnical attacks from the perspective of computer networking. This paper is divided into two main parts. First part is focused on principles and categorization of sociotechnical attacks. Second part analyses the vector techniques in traditional computer network and we present penetration testing as a possible solution methods.

Key-Words: Digital communication technologies, sociotechnical attacks, computer networks, penetration testing.

1 Introduction
Securing computer networks is complicated and very important task for every organization or person using information technologies. This complication is caused of many factors. One of the most important is that the problems, threats and vulnerabilities are evolving dynamically in the time. Modern security technologies are getting more and more sophisticated and help to defence user privacy and systems covering following issues [3].

- Intrusion detection systems
- Intrusion prevention system
- Proactive based systems
- Hardware accelerate systems
- Real-time antivirus, exploits and spyware controls
- Artificial and heuristic approach

In conjunction of the security technologies development it is harder to break in to the system via uncovering the security hole, brute attacks, listen on the channel and other standard hacking techniques [8]. On the other hand, security solution has to be balanced with a needs and users limitation. This is one of the basic necessities while creating the security politics. If we ignore this rule we create the paradox of weakening systems. For example we cannot use Vernam cipher for every kind of symmetric authentication because of the cipher length. Therefore the security attitude has to be always compromised between the user and the technologies.

This assumption opens the possibility to use very old technics of psychological manipulation of individuals – Social engineering. The basic principles rely heavily on human interaction and often involve tricking other people to break normal security procedures. Social engineering is recently up today. Latest research shows the growth and success of this technics, it is one of the most successful intrusion technics [3]. This aim of this paper is to analyse the combination of technological approach and the principles of human behaviour in the area of IP networks.

2 Sociotechnical attacks
Sociotechnical attacks cover the combination of many technologies and the social approach of attacks. Pretexting is the basic method, perceived for the next step of attacks. [10]. Pretexting often involves a scam where the liar pretends the need of information in order to confirm the identity of the person he is talking to. After establishing the trust with targeted individual, the pretexter might ask a series of questions designed to gather key individual identifiers such as confirmation of the individual's social security number, mother's maiden name, place or date of birth or account number.
2.1 Spamming
This term covers the use of electronic system for collective unwanted information sending. There is no coherence between the acceptors and the content. The most widely used form is e-mail communication. More than 90% of all messages are spam [7]. Spam is broadcasted by the BOTNET, known as the network under the control of hackers. This category can be divided into the other areas.

- **Instant messaging** (also called „spim“) – based on presumption that the communication is not usually being deeply checked by firewalls or other intrusion detection systems.
- **Discussion forums and blogs** – historical part of the SPAM channels. Repeating multiple discussion text or automatic hypertext sending.
- **Mobile phones** – unwanted information via SMS. Used on selected markets by operators.
- **Online games** – similar channel to discussion forums. Information’s (cheats) are offered by third party subjects.
- **Spamdexing** – Fraudulent SEO technic for increasing value of HITS.4 algorithms

Phishing
Phishing is a method used for acquiring secret information of users such as username, passwords, credit card number etc. This basic category includes many forms taking the advantages of small success factor, but on the other hand of the huge number sent information. Following picture shows the common structure of phishing targets in Europe [6].

![Common structure of phishing targets](image)

Modern methods use the targeting approach for maximisation of the efficiency. The phishing information needs to be targeted more accurately according to the domains, languages or the area of interest. The internetwork offers this improvement of IP address localisation network, Autonomous system classification or domain name system association. IP spear phishing, whaling and vishing are the examples of advance phishing method.

- **IP Spear phishing** – based on the automatic or manual level of profilisation. IP addressing of autonomous system schemas are organised by IANA – the Internet Assigned Numbers Authority. For a consideration of this authorization spear, phishing systems can target the concrete areas or victim. E-mail can be automatically generated with appropriate coding, syntax and with the local context. Other sources of important information are the social networks, cookies or internet browsers history.
- **Whaling** – variation of spear phishing targeting the top management (executive officers, managers), financials or politics. This area of interest represents the possibility to acquire the information with high level of importance or financial liquidity. Positive whaling represents headhunting, security service operations or military services.
- **Vishing** – using the features facilitated by the VoIP (voice over IP) or direct access over the telephone system. Victim is directed to call the certain number. This method much more successful than the common types of phishing because this type of communication channel is much more confidential for the victims [2]. It allows the utilization of automatic telephone system feature called IVR (interactive Voice Response).

2.1.1 Pharming
Pharming method is very dangerous and malicious. The victim doesn’t have to notice any fragments of attack in contrast to common phishing methods. Pharming exploits the DNS records and doesn’t have to react on the substituted stimulus. Redirection of the traffic is based on retracing the legit URL record on counterfeit host usually under the control of attacker. Routing the traffic is the main feature of the internetworks. Gathering the statistics and security mechanism development is
very complicated. The research is traditionally built on the inference of phishing and other sociotechnical attacks [10].

2.1.2 Scareware
Anti-Phishing Working Group research claims that more than 50% of 18.5 mil testing computers were affected by malware [9]. Scareware usually installs the malware software products that produce frivolous and alarming warnings or threat notices, most typically for fictitious or useless commercial firewall and registry cleaner software. By the point of sociotechnical engineering view can be this group divided in two following subcategories.

Roguware – issue as a software cleaner or antivirus. According to Panda Software research the average income of this sort of malware is 35 million dollars per month.

Ransomware – hide certain features or parts of the system and informs the user by various ways. Disable an essential system service or lock the display at system start-up. Encrypt some of the user's personal files.

3 IP networks and vector technics
Social engineering consists of many methods and technics and therefore it represents various scientific areas such as psychology, sociology, informatics etc. By the networking point of view the communication can be divided in two main parts, logical and physical. Logical layer of the modern computer networks and internet is based on TCP/IP protocol stack and includes following sub-layers: application, transport and IP. The area of local networks and physical layer is typically represented by the ETHERNET technologies. Furthermore we discuss the vulnerabilities and threats of the most used variation of networking technologies in organisations. According to this kind of attacks are highly effective and dangerous.

3.1. ARP Poisoning
Address resolution protocol (RFC 826) provide the translation of logical networking IP addresses and physical media addresses. MAC addresses are used for routing and delivering data over the LAN switching segments. Therefore the sociotechnical use is limited by the broadcast domains and divided by routers and logical segments of IP layer [3]. Attacker answers the switch or computer the ARP resolution confirmation. The result is that the communication is forwarded to non-existent gateway or attacker computer. The first example is concerned as man in the middle attacks and the second one as denial of services.

3.2. MAC Flooding
MAC flooding techniques is focused on misuse of the switch device compatibility to change to hub mode. If attacker floods certain port of switch by huge number of MAC addresses, the device is losing the compatibility to manage data stream to appropriate destination. The device is significantly overloaded and the switch broadcast the communication to every active interface. The attacker is able to listen the data stream on link.

3.3. DHCP Spoofing
Automatic device address allocation helps the administrators to set the parameters of end user devices. DHCP server can be used for configuration of many parameters, gateway, DNS servers, Time protocols, server parameters etc. Due to security reasons are the servers often located in the different parts or under the control of access systems. This assumption creates the security paradox. As closer the trusted or fake DHCP sever is closer to the host than the attacker can overtake the configuration of host. Standard device configuration doesn't differ between the fake and trusted DHCP server. This vulnerability is very dangerous and it is not easy to uncover these activities [3]:

3.4. DNS SPOOFING
DNS records are being used for human interaction and addressing the internetworks, rather than IP addressing schemas. Every domain name matches one or more unique IP address. The goal of this kind of sociotechnical attacks is to insert fake information or change DNS response information between servers and client. The attacker use two main techniques described below.

DNS cache poisoning – attacker ask the DNS server for DNS information for servers unknown address. Server has to ask for this information the delegated server because the DNS system is hierarchical. With notification the attackers DNS server is able to send proper translation response and poison the DNS cache. The result is that the customer is redirected to another server, unsecure area etc.

DNS ID spoofing – the domain name system is able to use stat or stateless communication mechanism. This is represented on transport layer according to RMD ISO/OSI network model. Therefore in internetworks two protocol solution can be used
TCP an UDP. UDP is the most used solution. Proper DNS server has to hold the ID information because the UDP is stateless. ID information is pointed with the queries and responses with the client. DNS ID spoofing techniques allows the attacks to listen to the client queries, server answers and change the server response with fake information’s. Many variants of these attacks due to security mechanism exist. One of these security and data compromise examples is described on the following picture.

![Fig. 2: DNS SPOOFING EXAMPLE [1]](image)

3.5. Electronic communication
Electronic communication systems, such as chatting, sending email or presenting information via computer networks is the common way of sharing information’s. It helps the attacker to improve the confidentiality of the attacks. For delivering of electronic mail is responsible the SMTP serves, respectively the protocols. Email communication can be affected by the following issues:

- SMTP header changing
- Grammatical faults
- Dividing the words
- Non valid tags adjustment
- Graphical representation
- Misuse of MIME Formats

4 Penetration testing methods
Penetration testing is a method used for simulation of sociotechnical attacks. It can be held from inside or outside the organisation. The orientation level of targets may vary from the concrete thing to the whole organisation. Penetration testing can offer the result, overview of the security politics and uncover the security and vulnerabilities in computer systems.

4.1. Methods
A penetration test can be seen is a controlled process where a trusted third party security systems and experts perform the security verification by using methods, tools and socio communication styles that to perform the suspicious activities. Penetration testing consists of variety techniques and many organisations serve their own solution, ISECOM for example. The solution has to correspond with international standardisation methods and frameworks. ISO standardisation procedure in conjunction with Sociotechnical attacks are three following standardisation norms:

- ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security

Penetration testing can be carried in three possible ways according to the attacker knowledge of the infrastructure and skills. The main difference is in the systematics of methods [26].

![Fig. 3: Penetration test types](image)

- **Black box** - the penetration tester performs the attack with without the knowledge of the network infrastructure, security mechanisms and communication technologies of the target. Black box test is a non-systematic type of attack with no need of professional skills.
- **Grey box** - the penetration tester performs the attack with bounded information’s of the network infrastructure. Grey box is a systematic type of attacks, which is well prepared outside the organisations with limited access privileges.
- **White box** - the penetration tester performs the attack with complete information’s of the network infrastructure, security mechanisms and communication technologies of the target. White box I a type of systematic attack with the knowledge inside and outside the organisation.
According to the destructiveness of the penetration tests we can differentiate between destructive tests, which is fully check and confirm the weaknesses and non-destructive attempts to attest the weak parts of the systems. This kind of test is based on theoretical background, but on the other hand the organisation doesn’t risk the fault of information systems. Other possible penetration test differentiation is the inside/outside targeting. Inside target test are focused on internal staff in contrast to inside targeting approach.

5 Conclusion and acknowledgements
In this article we have tried to analyse the sociotechnical attacks from the representation of communication technologies and the networks security area. Sociotechnical attacks consist of plenty type of attacks. The categorisation in computer networks can be performed over the existing protocol stacks with a focus on the logical and networks layers. The development of sociotechnical attacks requires the changes in the critical networks services such electronic communication, the LAN technologies improvements.

This work and contribution we supported by the project of Specific Science Research “OVTE” Optimisation of virtualisation technologies in the education process.

References: