Portál pre odborné publikovanie ISSN 1338-0087

Social Engineering

Petrák Petr · Informačné technológie

17.12.2012

This paper deals with the social engineering issues and it introduces a definition of this term and brief distinction of technical and non-technical social engineering. There are also mentioned a history of techniques which has been used to gain valuable data since 1990s. To better understand of techniques of social engineering there are description of the ways how to get data – non-technically especially.

The authors suggest few possible solutions how to prevent and secure data of users and how to be more cautious when the user is logged in a computer. At the end of this paper, the authors hands out an opinion about the awareness of PC users and possible threats which they might deal with and the authors also introduce a view to the future connected with development of social engineering.

1. Introduction

To better understand this topic, it is essential to describe or define the term “Social engineering” – everyone, who has met with general security little bit deeper, understands this term as the way how to obtain confidential information, private data or any other secured details by non-technical ways. To get required information social engineers use the regularly intruding techniques – precisely they do not have to use a computer to crack in victim´s privacy but they use simple psychological techniques to get victim´s trust and obtain required data.

De facto, social engineers do not have to deal with complicated physical security e.g. firewalls, antiviruses, routers, etc. The popularity of social engineering has become higher since 1990´s when the development of information technologies became spread as well. There will be described few social engineering techniques in the following chapter. Socio techniques contain a various amount of ways how to get data and this chapter is going to show some of them.

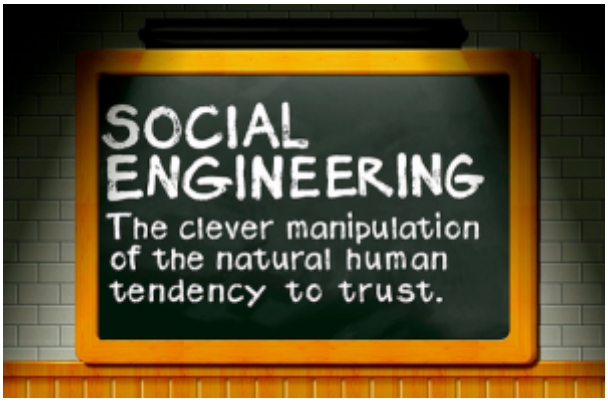

Figure 1. Social Engineering

2. Dumpster Diving

In this time, we still use printed and tangible form of our data or personal details – this means everything what is written on the sheet of paper. But sometimes this physically written data we do not use longer because it might have been transferred into a computer for easier management. But something must happen with the papered written ones – they are usually thrown away into dumpster and no one cares any longer what could happen with them. In better cases, these paper documents are shredded into thin strips but it is still not perfect and social engineers may find out a victim´s secured details by assembling of these stripes together, because even these stripes are thrown away as not shredded documents as well.

Because the dumpster is not being secured mostly, there is nothing easier to wait until someone is going to throw away a dust bin with shredded or even only creased sheets of documents and explore the dumpster up to bottom of it – it also means patient job to reassemble shredded documents but if a company, facility or an enterprise does not use the proper shredder they might risk revealing their personal data, e.g. invoices where is displayed names with addresses, telephone numbers and more confidential details. Not every sheet of paper should be shredded into small pieces (it depends on its importance and content) but people should realize what they considered for important and private.

3. Shoulder Surfing

This is the easier and cleaner form of socio technique compared to mentioned dumpster diving and it also provides the way how to find out details leading to another ones. Shoulder surfing can be described as spying the personal information, choices or mood beyond the victim´s back – of course this technique is used unintentionally by huge amount of people and they do not have to be called hackers (when someone is entering his or her password and someone else can see what is typing so it may be considered for certain way of shoulder surfing).

Shoulder surfers have easier job if their victims do not respect that they display much information unintentionally in order to be more aware and hide these “hints” instead – it is meant various kind of stickers, labels or tags which do not have to contain fully private details but they may display certain information which helps social engineers to create the suitable tactic how to grab more information from victim who is tracked. Shoulder surfing is not only the affair of securing our personal zone and social

engineers do not have to appear closely to their victim and stare at his or her PC desktop – to capture trusted data or get clue (in form of used applications on the computer). Which might help further cracking is to use camera and zoom in needed object. This can evoke lesser suspicion if the camera is properly hidden and the act of snapping does not take a long time.

With shoulder surfing is closely connected so called “tailgating”, which represents the way of tracking the victim in purpose to intrude into building when the victim enters as well – it is meant that social engineer could use slowly closing door and he or her can use the moment to intrude. The similar case is a intruding into group of employee during a short break when they are smoking outside (if there is not break room inside) and chatting – with suitable uniform, false badge and facility jargon it is easy to gain a confidence of employees and get in together into facility etc.

4. Disguising and Playroling

To strengthen the feeling of victim, that is not really tracked there serves a possibility to disguise for someone to whom victim could trust and pretend that disguised social engineer is not interested in victim´s privacy but he or she really do what he or she is disguised himself/herself as somebody who do not arouse the suspicion, e.g. repairer, maintenance man or new employee of company (if social engineer´s attack is aimed to company). The preparation is not underestimated but there might be a few clues how to reveal the cheater, even he or she might have badge, uniform or equipment, but the victim has to pay attention to every detail which might not fit.

5. Lockpicking

When the social engineer is unable to get the data directly via dumpster or tailgating, he or she must deal with some elements of security for example in form of lock on the door. This can be still considered for non-technical attack because the attacker do not need to use computer to encrypt a complicated password to crack into some database and grab information – to have a access in most cases it is sufficient to get over mechanical lock which can be penetrated with special bumped keys that enable to nudge internal pins as the original one (of course there is needed to use additional shimming features to unlocking).

Non-technical hackers can succeed with ordinary equipment e.g. aluminium can of Coca-Cola, toilet paper, electric toothbrush, straw or paper clip. People are also sure, that lock using number code are safe too, but even they can be penetrated with a stripe of metal from can and hacker is able to find out the lock combination when he hear the correct click of number wheel (hacker must go slightly and it may take some time).

6. Bypassing Electronic Security Devices

A various electronic security devices do not seem to be problems as well, because there are always few possibilities how to distract them. One of them – the passive infrared motion sensor activation is being used in the whole world – snaps everything which or who emits the heath, precisely its warmth is higher than 33.8 °C, so it is needed somehow to decrease temperature in order to become invisible for sensor – to

reach invisibility for a short time the authors of this publication mentioned in source wrote about using the neoprene until it absorb body heat and make him / her visible again.

The next security device, which is often placed to secure certain area, is a camera. Even this device is vulnerable to hacker´s attack, either it is equipped with infra sensor. Most of models of cameras can capture the picture with specific traits, especially it depends on light conditions – if there is too much light, camera is unable to capture the picture or video, everything will be recorded as very bright shine without details and this is case how to distract camera.

Intruder must be equipped with strong source of light, e.g. pocket laser or torch and its task is to aim to objective of camera in order to overflow with light – in this moment the camera is unable to capture and the intruder can go through secured area without problems. Electronic locks using number combination do not represent the cracking problem as well. In the case when intruder can take seat near the place which is secured with it and pay attention when victim will enter the code and he or she will not cover the lock with his or her body during entering the code.

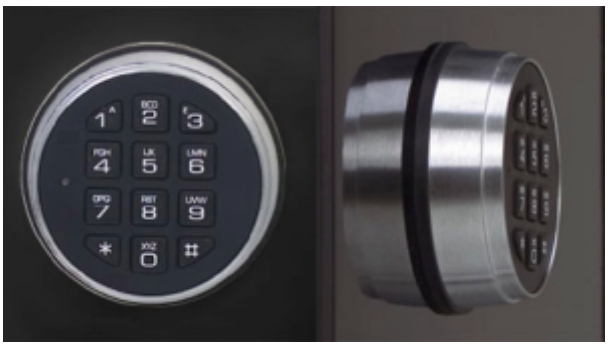

Figure 2. Electronic lock using number combination

A special part may represent kiosk, i.e. self-service machine which serves for customers on the airport, in shopping stores or in bureau – of course this is not a kind of security device but it represents the door to internal system which can be badly secured. Due to unexpected errors, the attacker can find out the version of operation system, running processes and determine following steps. If the kiosk is Microsoft Windows based and credentials are not sufficiently selected, so then it is easy to enter to the system.

7. Social Engineering Practically

The act of obtaining data must be supported by convincing behavior, disguise and insolence and social engineering covers roleplaying. Generally, it is cheaper way how to crack into victim´s system instead using expensive hardware methods. Johnny Long, the author of the publication about no-tech hacking claims, that two telephone calls suffice to get needed information or credentials which enable access to database or any secured files.

Roleplaying is connected with collecting data, social engineer must collect some information in order to create reason why he or she should be the one who will perform as someone, who is trusted – for example: when the attack is aimed to obtain

database which contains personal details like bank account numbers or the number of health insurance, so at first it is important to intrude to chosen company (this option could be even left out because clues leading to confusing the victim may be found on the internet, websites of targeted company) and find out the used software which enable the access to the database (every detail is valuable).

This is the first pretense to contact the company which is intended to attack. The social engineer will introduce himself / herself as IT support of software which is used by company and then he or she announces that there is some issue with software connected with, for example, last update and it may cause total collapse of system or corrupting the database. In order to be get trustworthy, the social engineer has to add more relevant information which confirm his or her identity, awareness about issue and he or she arouse the feeling of trustworthy itself. When the victim loses suspicion, he or she provides access via telephone as login name and password; the social engineer wins and gets the access. The simple way to get further is also to ask victim – some people happily provide many clues to reach the attacker´s target.

8. Recommendations Leading to Prevent from Social Engineering

To avoid or to reduce number of meeting with social engineers there is needed to recognize possible attacker. Unfortunately there is no strict rules how to recognize him or her correctly and people must pay attention when they reading something private in public, surfing in café or just working in their jobs. People may prevent from attack when they will abide certain rules, e.g.: do not let of no use papers or more precisely do not throw away in the bin – use shredder instead and make documents unreadable to prevent from capturing information. A good point to reduce of unwanted providing information is a removal of any stickers as logos, production key of OS or any other stickers giving information about the used software in your laptop, or any informative stickers on your car, for example.

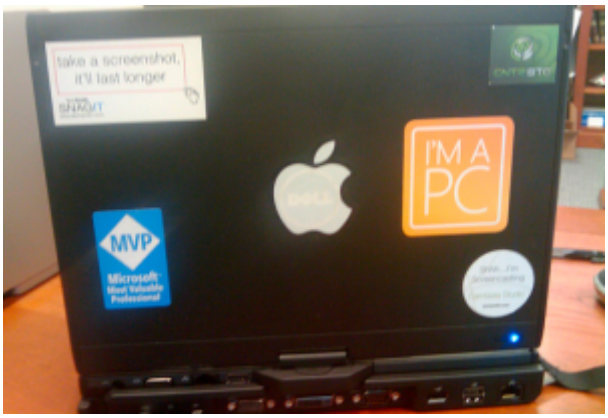

Figure 3. The typical example of incorrect notebook desktop – do not use stickers

With removal stickers can be connected the free displaying of working badges – this may unwontedly provide the information to attackers as well, so it is good to hide it – insert into pocket. People do not have to tend to be paranoid but they should also pay attention at anyone who is moving nearby their personal zone, when they are surfing with their laptop on the internet or they use it somehow and provide unintentionally some details as displayed application on their toolbars etc. To avoid displaying these details it is easy to hide this toolbar (fade out) and in addition, on laptops they will get

extra few lines in case small screens.

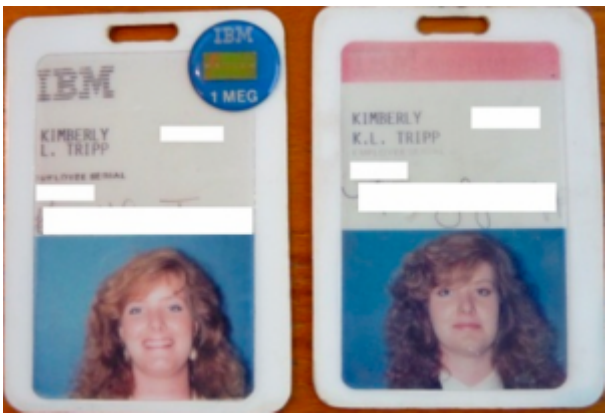

Figure 4. The example of facility badge

9. Conclusion

In this paper has been mentioned few social engineering techniques where are also outlined some features of them. Their description enables to understand better the substance and also there is introduced a few possible solutions how to reduce the threat of attacking by any social engineer. In addition everyone should realize that even the best antivirus or antispyware application cannot secure his or her data if there are social engineers who are able to crack into system just with two telephone calls or well written e-mail. Also, people need to realize what they consider for private property and what would be the best to hide it and what is unnecessary to keep it in secret.

The study of literature interested to non-technical hacking provided additional information at what an ordinary user or everyone should pay attention. This topic is more linked together with psychology and sociology than with information technology and if we want to understand better the intentions of social engineers and their steps, it would be great to be also interested in these sciences. Social engineering was the threat and still will be the threat, even in the future because it is based on human factor. Compared to computers, human beings cannot concentrate on too many things as computers and so human beings cannot pay attention at every detail perfectly. Computers are lesser vulnerable in this case but on the other hand the computer is programmed by human beings – this is like a vicious circle. [1, 2]

References

1. LONG, Johnny; MITNICK, Kevin. No Tech Hacking: A Guid to Social Engineering, Dumpster Diving and Shoulder Surfing. Syngress Publishing, 2008. ISBN 978-1-597-9-215-7.
2. BullGuard: What is social engineering [online]. [Cit. 2011-12-04]. Available from WWW: http://www.bullguard.com/bullguard-security-center/security-articles/what-is-social-engineering.aspx

---

Coauthor of this paper is David Vavra, Tomas Bata University in Zlin, Faculty of Applied Informatics, Department of Mathematics