H2: Social Engineering

Hugh Anderson

***Abstract*—Points related to Social Engineering (Notes for DOTA, session 2).**

I. Social Engineering

A. Introduction

According to Wikipedia, Social Engineering, in the context of information security, refers to "psychological manipulation of people into performing actions or divulging confidential information". It is a type of confidence trick for the purpose of information gathering, fraud, or system access, and is often one of many steps in a more complex fraud scheme.

We have of course had confidence tricks played on us for centuries, and all of the following examples have had films made about them!

You may have heard of Frank Abagnale, who in the 1960s convinced people he was a university professor, a doctor, a lawyer, and (famously) a PanAm airline pilot. In amongst all this, he stole millions of dollars through various schemes. He eventually spent 5 years in jail (where he convinced his jailors that he was an undercover prison inspector), and currently has a security consultancy, and teaches at the FBI academy.

Another famous historical confidence trickster was Charles Ponzi. He promised clients a 50% profit within 45 days, or 100% profit within 90 days, buying discounted coupons in Italy and exchanging them for higher value stamps in the United States. Actually, Ponzi paid early investors using the money from later investors, "robbing Peter to pay Paul". Nowadays, any scheme of this structure is called a Ponzi scheme, and in recent times, Bernie Madoff was sentenced to 150 years in jail for stealing US$18B in a Ponzi scheme.

In the late 1970's Kevin Mitnick began attacking computer systems. His principal means of attack throughout his criminal career were dumpster diving[1], and social engineering. While engaged in computer hacking, he used cloned cell-phones to hide his location and copied proprietary software from telephone and computer companies, stole computer passwords, altered computer networks, and broke into and read private e-mails. He eventually briefly became the top fugitive on the FBI most wanted list, and when caught spent 5 years in prison. He is currently a computer security consultant.

B. Techniques for social engineering

Social engineering techniques are based on specific weaknesses of human behaviour. Human decision-making is often subject to cognitive biases [2]. An example of a cognitive bias is a common human trait that people making choices involving gains are often risk averse (particularly with the old), and with those involving losses, are often risk taking (particularly with the young). These biases are exploited to create attacks, typically to steal confidential information. Here are some Wikipedia-based definitions of some of the social engineering techniques:

> **Pretexting:** Pretexting also known in the UK as blagging or bohoing, is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (e.g., date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target.
> **Phishing:** Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN.
> **Vishing:** Phone phishing (or "vishing") can happen both ways - in the way we see in the lecture where a clever actor uses her skills to extract and manipulate someone, or using a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" information.
> **Baiting:** Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim. In this attack, the attacker leaves a malware infected floppy disk, CD-ROM, or USB flash drive in a location sure to be found, gives it a legitimate looking and curiosity-piquing label, and simply waits for the victim to use the device.

In September 2008, United States vice presidential candidate Sarah Palin's Yahoo email account was accessed by David Kernell, the son of a Democratic state representative. Kernell had obtained access to Palin's account by using Yahoo!'s account recovery for forgotten passwords. When the system

[1] At age 13, Mitnick found unused bus transfer slips in a dumpster next to the bus company headquarters, and convinced a bus driver to tell him where he could buy a ticket punch. After this he was able to ride any bus in Los Angeles for free. He learnt young!

asked questions to verify Palin's identity, Kernell found the details online: just her high school and birthdate, and then proceeded to publicly post Palin's emails. Kernell was charged and found guilty, and got one year plus a day in federal custody.

It is common in Singapore to receive phone calls at home or at work from "Microsoft Support Services" (or some similar non-existant company). They then proceed to tell you that their systems have identified that your computer is at risk; a virus, or a worm has infected it, and it needs to be remedied. From then on the conversation can go quite a few different ways - sometimes with them asking you to install a bit of software, or sometimes just asking for you to tell them details about yourself or your computer. In any case all these phone calls are fraudulent.

A particularly insidious attack is the one where your friend gets called by "the bank", and is told that you have applied for a loan. The "bank" then asks your friend details about you, to confirm/check if you are worthy to get a loan (I guess). Your friend divulges a lot of personal information about you, that "the bank" uses in a later attack (where they are better equipped to masquerade as you).

There are many other variations of social engineering attacks, but the above types clearly demonstrate the techniques.

C. Defences...

So, what are our defences against social engineering attacks? For us personally, protecting ourselves is a matter of becoming a little more cynical, a little more paranoid. It is a very sad tale, but, your friend was not mugged in London, and ...

- Microsoft Security Services is not calling you at home, and they do not know that your computer is infected.
- Neither the devout christian widow Mrs Fortunabe of Lagos, nor the wife of the Argentinian minister killed in the plane crash (see link), nor the lawyer acting for the late Dr Eldorado... really wants to be your friend.
- The story of the poor crippled boy is heartbreaking. But it is not true.
- The beautiful Albanian (woman/man - photo attached) does not like what s/he knows about you, and is not a beautiful Albanian (woman/man).

Ignore it all...

However, as IT professional people, we also want our systems to minimize the risk of successful social engineering attacks for our users/clients. When building new IT systems, what can we do to make them more resilient to social engineering? The Open Web Application Security Project [1] is a worldwide not-for-profit charitable organization focused on improving the security of software. The OWASP advice below is oriented to web based applications, but the advice is relevant in a wide range of systems, not just web-based ones.

According to OWASP.org, the big things we can do to improve our systems against social engineering are:

1) User education: teach your users/clients to engage in safe practices. This advice goes hand in hand with "do not train your users to engage in bad activities[2], and reduce risk by not sending email".
2) Feedback: make it easy for your users/clients to report scams or peculiarities they notice. Every such report should be responded to immediately by a human, not an automated innocuous response.
3) Interaction: Use schemes to increase trust, by ensuring your site is strongly located/branded (never redirect to other sites), and not asking for secrets when responding to your clients.
4) There are also technical issues, that we will discuss during this course:
   a) Do not use popups...
   b) Take care with iframes...
   c) use SSL...
   d) keep the address bar...

In summary then, eternal vigilance, cynicism, paranoia, and change your, or your client's behaviour, to reflect a more dangerous world. In short:

- You have not won €400,000 in the Euro lottery.
- Putting money in a paper bag and waiting cannot double your money.
- There is not a lot of dyed money that needs chemical treatment.

I am sorry that I am the one to have to tell you this.

REFERENCES

[1] The Open Web Application Security Project. http://www.owasp.org/. Accessed: 2016-07-14.

[2] Amos Tversky and Daniel Kahneman. *The Framing of Decisions and the Psychology of Choice*, pages 25–41. Springer US, Boston, MA, 1985.

[2] i.e. Do not make them click on emails! You might want to consider how you could manipulate your clients/users to become safer citizens.