The IT security landscape, and Social Engineering

Hugh Anderson

***Abstract*—Points related to the IT security landscape, and Social Engineering.**

I. IT SECURITY

There are many aspects to "computer security". For example, look at the following items. Each one is related to computer security, but they cover a wide range of distinct subject areas:

- **Secrecy.** Much of modern-day commerce relies on secure transfer of information, and this security relies on exchange of secret keys. In addition, we often just want things to be secret, and encrypt documents to ensure this.
- **Insecurity.** Most computer systems are dangerously easy to subvert, and it is a scary world out there! Apart from an adversary gaining some level of control over your system, consider the insecurity you might feel when you sign a contract, and then the other party doesn't. Sometimes our concern is not with secrecy, but with subtleties like non-repudiation (you cannot deny that something happened afterwards).
- **Safety/control software and hardware.** Operating systems and distributed systems are complex entities, and various techniques for improving the security of such systems could be examined.
- **Assurance.** How can we convince ourselves (or our employer) that the computer system is to be trusted? Building assurance is best done by adopting standard, or formal methods to confirm, specify and verify the behaviour of systems.
- **Networks and protocols.** Some aspects of security are determined by the way in which we do things (the protocol), rather than what is actually done.
- **Mathematical, physical and legal.** Some aspects of computer security require an appreciation for various mathematical, physical and legal constraints.
- **Security models.** These models provide formal (read *mathematical*) ways of looking at computer security in an abstract manner. By adopting a formal security model and showing it to be secure, if your software components comply with the model, you can be sure of the security of your system.

Often the same security problems that occur in society re-occur today in computer systems: there are many examples of computer-based security activities that we can find by looking at society, or by studying history books. For example, confidentiality problems result in concerns about locks, and encoding. Integrity problems result in concerns about signatures, and handshakes. In each of these, we can see simple examples from society, and the computer-based versions follow the same lines (only a million times faster).

The History of Herodotus

For Histiæus, when he was anxious to give Aristagoras orders to revolt, could find but one safe way, as the roads were guarded, of making his wishes known; which was by taking the trustiest of his slaves, shaving all the hair from off his head, and then pricking letters upon the skin, and waiting till the hair grew again ... and as soon as ever the hair was grown, he despatched the man to Miletus, giving him no other message than this: "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Now the marks on the head were a command to revolt... [4]

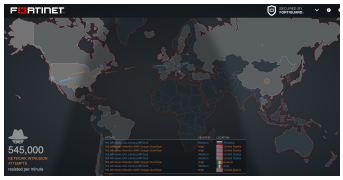
Histiæus ensured confidentiality by hiding his message in such a way that it was not immediately apparent, a technique so clever that it was used again by German spies in the 1914-1918 war. This sort of information-hiding is now called steganography, and is the subject of active research. Cæsar encoded messages to his battalions, a technique now called cryptography, and the use of agreed protocols between armies to ensure the correct conduct of a war is seen over and over again in history. Both of these activities (cryptography and protocol analysis) are active topics in the security area.

You will notice that we have begun with examples taken from the world of warfare, and throughout this course, you will find references to military conduct, procedures and protocols. This should not be a surprise to you given the nature of *security*.

A. The computer-based landscape

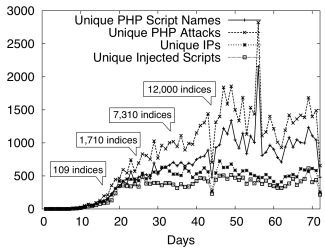
The landscape of IT security encompasses a wide range, from the world-wide to the microscopic. IT security can apply to governments, world bodies, organizations, small businesses, or even you, or things you barely notice around you.

Consider the infrastructure within a country providing the things we have become used to, for example, electrical power, sewage, water-on-tap, gas reticulation, the phone system. Most of these infrastructural elements run pretty well, but the results when they stop can be catastrophic[1]. Even when the infrastructure is working well, directed attacks can make your life hell. Not just you, but your company, your city, your country, your world.



You can view the landscape as that of "Information warfare". This "war" is going on every day, continuously, attacking every visible machine, both on and off the Internet. In the screenshot above, we see a real-time display of the Fortiguard threat intelligence system [1], monitoring Internet attacks as they happen.

[1] In 2000 I worked at the University of the South Pacific in Suva, Fiji during a coup, and some villagers sabotaged the Monasavu dam, cutting power to the entire country. For over three months we lived without power, although the electricity department did manage to get some generators going to provide 20 minutes of electricity to Suva every day. No phones, no shops open, no lights, eventually no water, no news, no TV - it was a scary time.



In the graph above, we see attacks on a web site that was set up using a new, never used before, Internet (IP) address [5]. As you can see, after about 10 days, the site got discovered, and the attacks started, growing quickly until stabilizing at about 1000 attackers per day. Individual attacks may last a few seconds, right up to continuous - all-day attacks.

In computer security, the term "attack surface" refers to the sum of all the different mechanisms (the "attack vectors") an unauthorized user (the "attacker") might use to gain access, or manipulate a system. In this course we will look at information warfare in detail, looking at these attack surfaces, and how to defend them. The list of surfaces that we will look at are, in order:

1) people: the ways in which people are manipulated.
2) complexity: complex systems are large, and may have a large number of attack vectors.
3) cryptography: underpinning much of our IT world is the use of cryptography. It may be possible to directly attack the cryptographic schemes.
4) underlying communication systems: many of our systems are constructed using physically remote devices, and the physical communication between them may be attacked.
5) high level communication systems: the Internet is based on the Internet Protocols (IP), which were not designed with security in mind.
6) web application architecture: these days, web based applications dominate the world, and they have well known structures, with a range of attack vectors,
7) machine architecture: sometimes attacks are directly on the machine's hardware, or operating system.

In addition, we will look at these surfaces within contexts of personal safety, organizational safety, and even infrastructural safety.

B. Frameworks

Because security is multi-faceted, it is difficult to find a way to think and reason about it. In this course, if we were just to list security issues, the list would have thousands of entries, and be chaotic. We need a framework in which to place our discussion, and begin to categorize the IT landscape.

What is a framework for thinking about this? Perhaps Ross Anderson's PIMA:

- Policy: what is supposed to happen - what are the rules,
- Incentives: what are the motives of all the participants,
- Mechanisms: what are the specific techniques being used,
- Assurance: what reliance can you place on each mechanism.

If we were to use a framework like this, whenever we consider a security issue, we look at it in the context of each of these four items.

Another framework: I asked a friend (Jeff Carr) who has worked for years in security at the level of large companies, and countries, and he came up with this framework, which reflects perhaps a "corporate" view, similar to the framework promoted by IBM [2]:

- Policy/Strategy: what are the policies or strategies that are being used?
- Legal Requirements: what are the legal requirements that bound the system?
- Assets: what is to be protected, and in what context - is it CIA (Confidentiality, Integrity, Availability) or some other issue?
- Risk management: can we view this clinically, statistically, as risk management? Perhaps we categorize our assets with respect to their importance and use this to aportion effort in securing the assets.
- Security architectures: what systems/architectures are used or appropriate for the system?
- Compliance: what level of compliance is mandated?

In this framework, there is perhaps less emphasis on mechanisms, and more on authority, and high level management views.

In our course, I will be (in order) looking at the current set of weak attack surfaces, and in each case, I will look at the issues for a particular surface from some viewpoint or other, and will try to use the appropriate *framework* words as needed.

C. Finally...

In any of these, you can see that there are a wide range of activities (and hence jobs): Information Security Engineer, IT Security Architect, IT Security Specialist, IT Security Analyst, Business Security Manager, Security Research (Technical). This is good for those of use who have an interest in security as an occupation - endless work in front of us. But perhaps overall it is bad for the world in general.

II. 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[2], 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 [6]. 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 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

[2] 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!

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 [3] 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[3], 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...

[3]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.

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 Fortiguard threat intelligence network. https://threatmap.fortiguard.com/. Accessed: 2019-08-15.

[2] The IBM Security Approach. http://www.ibm.com/security/. Accessed: 2016-07-15.

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

[4] Herodotus. The History of Herodotus. 440 B.C.

[5] Sam Small, Joshua Mason, Fabian Monrose, Niels Provos, and Adam Stubblefield. To catch a predator: A natural language approach for eliciting malicious payloads. In *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 171–184, 2008.

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