Information Security

Aniel Nieves-González

Fall 2015

Introduction I

We have emphasized the importance of data as strategic asset. Now, we'll focus on how to protect such data. Many companies have been the target of cyberattacks. For example:

1. Target and TJX (parent company of Marshalls, Home Good, etc.) were targeted by hackers who infiltrated the store's network via an insecure Wi-Fi base station.
2. At least 45.7 million credit and debit card numbers were stolen by the hacker and his gang who pilfered driver's licenses and other private information from an additional 450,000 customers.
3. TJX suffered under settlement costs, payouts from court-imposed restitution, legal fees, and more.
4. A number of factor played an important role in the TJX breach:

Introduction II

   1. *Personnel betrayal:* An alleged FBI informant used insider information to mastermind the attacks.
   2. *Technology lapse:* TJX used WEP, a less-secure wireless security technology known to be easily compromised. Many of the tools used by hackers can be obtained easily over the Internet.
   3. *Procedural gaffe:* TJX had received an extension on the rollout of mechanisms that might have discovered and plugged the hole before the hackers got in.

5. Information security must be a top organizational priority.
6. A constant vigilance regarding security needs to be part of individual skill sets and a key component in organizations' culture.
7. Edward Snowden Revelation have also a lot to teach us:
   - E. Snowden: A disgruntled employee, a traitor, or a patriot?

Introduction III

- In any case the NSA intrusion of the intranet of Google, Yahoo, and other companies is another type of attack. In what sense?
- *The Lavabit case:* Lavabit was a webmail service that whose focus was on privacy protection and security. It has to closed down after the Federal goverment ask them for the private keys (*vide infra*) of their service.

8. The Stuxnex case was also very important and fundamentally different than the attacks previuosly discussed. Why?
    - A physical component of Iran's nuclear facilites (centrifuges) were destroyed by either the US or Israel.

Motivation behind cyberattacks I

- Account theft and illegal funds transfer. Whereas some steal cash other harvest data to resell to third parties. Personal and financal data are sold over the Internet in black markets.
- Extortion: Pay us or we'll launch a DDoS attack, etc.
- Corporate espionage. Think about the accusations of the U.S. goverment to China about this subject.
- Cyberwarfare.
- Hacktivism.
- Revenge.
- Pranksters.

Some of this activites may be funded by international crime organizations. Think about the 2013 ATM cyberlooting in NYC.

Important concepts I

1. *Zero-day exploit.* A security vulnerability in a piece of software that is used to compromise a computing system. Remark: You don't have to be a security expert to get a hold on them, since they can be bought in the black market.
2. *SQL injection.* It is when an SQL instruction or command is inserted (injected) into a DBMS (and run by it) using an entryfield.
3. *Distributed Denial of Service (DDoS) attack.* It is an attack in which a server is tried to be overloaded by huge load of requests from clients. The goal is to crash the server with the load of requests.

Important concepts II

4. *Botnet.* It is a collection of inflitrated, linked, and remotely controlled computers used for nefarious activites like: sending spam, doing DDoS attacks, etc.
5. *Malaware.* It refers to all kinds of maicious software that seeks to compromise a computing system. There are different types of malaware:
    - *Virus.* Programs that infect other software or files and require an executable to spread. Typically they require direct action from a user to execute.
    - *Worm.* Programs that take advantage of security vulnerability to automatically spread. They do not need to be attached to an executable in order to spread.
    - *Trojans.* Exploits that try to sneak in masquerading as something they are not.
6. Malware is used to:

Important concepts III

- Recruit computers to build a botnet.
- *Malicious adware:* Programs installed without full user consent or knowledge.
- *Spyware:* Software that surreptitiously monitors user actions, network traffic, or scans for files.
- *Keylogger:* Type of spyware that records user keystrokes.
- *Screen capture:* Variant of the keylogger approach.

7. *Social engineering.* Con games that trick employees into revealing information or performing other tasks can be used to compromise a firm's security.

8. *Phishing attacks.* Phishing attacks refers to cons executed through technology. For example: an email y sent to you and ask you to click on some link. Spear phishing attack is when a specific group of users is targeted.

Important concepts IV

9. Dictionary attack. It is a type of brute-force attack in which a password, for example, is cracked by trying all words (and combinations of words) from a dictionary.
10. *Dumpster diving.*

SQL Injection

The SQL injection technique focus on a sloppy programming practice where software developers don’t validate user input.

- Web sites that don’t verify user entries and instead just blindly pass along entered data are vulnerable to attack.
- SQL injection compromise the integrity and security of a database and thereby of the data it contains.

Push-button hacking I

1. Tools have been created to make it easy for the criminally inclined to automate attacks.
2. There are tools available on the Internet that probe systems for the latest vulnerabilities, and then launch appropriate attacks.
3. The barrier of entry is becoming so low that literally anyone can carry out these attacks.
4. The tools are not bad, but the intentions might be. Examples of such tool are:
   - As primitives as ping or ncat..
   - As sophisticated as Network Mapper (nmap), Metasploit (penetrating testing tool), and Nessus (vulnerability scanner).

Passwords I

Sometimes, valuable data is secured by a thin layer: a password.

- Most users employ inefficient and insecure password systems. Many users:
  - Use the same password for different accounts.
  - Make only minor tweaks in passwords.
  - Write passwords down.
  - Save passwords in personal email accounts or on unencrypted hard drives.
  - Use passord suceptible to dictionary attacks.
- The challenge questions offered by many sites to automate password distribution and resets are usually easy to guess.
- Strong passwords, two-step authentication, and biometrics increase security.

Encryption I

Encryption is the scrambling (transformation) of data, making it unreadable to any program that doesn't have the descrambling password, known as a key. Mathematically, the process of scrabling and descrambling is carried out by a function.

- Extremely sensitive data –trade secrets, passwords, credit card numbers, and employee and customer information– should be encrypted before being sent or stored.
- Encryption is used in SSH.
- Encryption is also employed in virtual private network (VPN) technology, which scrambles data passed across a network.
- There is asymmetric and symmetric encryption:

Encryption II

- In symmetric encryption one key is used to encrypt and decrypt.
- In the asymmetric or public key encryption one key is for encryption (the public key) and another is for decryption (the private key).
- The first public key crypto system is RSA (Rivest-Shamir-Adleman). It based on the practical difficulty of factoring the product of two large prime numbers.

- Public-key encryption is the most commonly used.
- Certificate Authority is an entity that issues digital certificates. Such certificates certifies the ownership of a public key by the named subject in the certificate.
- Why we don't always encrypt?

How to protect ourselves? I

1. Strong passwords.
2. Encrypt as much as possible.
3. Keep your systems up to date in order to minimize the chance of being exposed by zero-day vulnerabilities.
4. Distrust everything and everyone in order to minimize the chance of getting caught by phishing schemes.
5. Lock down the network as much as *possible*.
    - *Firewall*. A Firewall is software or hardware that monitors and control incoming and outgoing network traffic based on predefined rules. All OS come with firewall software.
    - *Intrusion Detection Systems (IDS)*. An IDS (software or hardware) monitors a network looking for suspicious activities.
    - Use blacklists or whitelists.

How to protect ourselves? II

- Use software like denyhosts for services like ssh.

6. Back up data.
7. Have failure and recovery plans. While firms work to prevent infiltration attempts, they should also have provisions in place that plan for the worst.