# Lecture #20: Security (Attacks)

## *CS106E, Young*

---

*This set of notes includes some additions on Integrity Mechanisms from the last lecture that are not discussed in the CS105 Course Reader chapter I released on Monday.*

*This lecture we discuss how computers are attacked. We begin by discussing some of the results of attacks including installation of Spyware, Ransomware, and Adware, as well as the ability to turn a computer into a Zombie as part of a Botnetwork. We also discuss the mechanisms of Viruses, Worms, and Trojan Horses.*

*We turn to take a look at techniques used to get these programs on your computer (or to otherwise compromise your security). Chief among these techniques is Social Engineering, attacking the humans using or supporting the system, rather than the technical details of the system. Phishing and targeted Spear Phishing are two examples of Social Engineering.*

*We end the lecture with a look at some technical ways to attack a computer. These include SQL Injection, Cross-Site Scripting, Clickjacking, Exploiting Poor Sandbox Security, Drive-By Downloads, and Man-in-the-Middle attacks.*

---

**Security Mechanisms**

- Handout #10 "CS105 Reader Security" covers mechanisms for Confidentiality, Authentication, and Non-Repudiation, but doesn't really spend much time on Integrity.

- In addition to the material covered in that handout, here are a few mechanisms used for integrity. Note that most of these are for protection against accidental, non-malicious problems with data integrity, such as power surges affecting transmission of data over a network.
    - ***Error Correcting Code (ECC) Memory*** is special computer memory sometimes used on computer servers that can correct memory errors. If a bit within a byte is changed accidently, this memory will correct it. It does this by storing extra bits so a byte in ECC memory will be stored in 11 bits instead of 8, the extra 3 bits provide redundancy for error correction.
    - Checksums are numbers created by adding all the bytes in a file (and ignoring overflow). If a file is transferred over a network, the bytes in the file can be tallied and if the number attained does not match the checksum, the file did not transfer correctly.
        - Zip archives include a checksum, which can be used to ensure that the files have not been accidently modified.
    - Hashcodes are similar to Checksums in that they are numbers generated based on the bytes within a file. In contrast to Checksums however, they can protect against malicious modification of a file. With a good hash method, modifying the file in such a way that the hash stays the same should be extremely difficult.
        - Websites will sometimes post the Hashcode of a file and then provide several different websites that are hosting the file. If you download the file from another website, you can check the Hashcode of the file and compare it to the posted

Hashcode. If the Hashcodes match, you have a copy of the original file. If the Hashcodes don't match, either something went wrong with the download, or someone posted a modified file.

- Hashcodes you see on websites will be marked with names like MD5 or SHA512, which are the names of the hash functions used to create the hash.[1]

**Threats**

- See handout #10 for discussion on ***Spyware***, ***Adware***, and ***Zombies/Botnetworks***.
- In addition to the material covered there, here are a few additional points.
    - Spyware can now be used to turn on microphones and cameras on both computers and cell phones.
    - A new tactic used by some websites is to either replace advertising income or supplement it by using JavaScript running on your computer to help mine for Bitcoins when you visit their website.
    - In addition to their use for Spam and DDOS (Distributed Denial of Service) attacks, some Botnetworks are used for advertising click fraud, where they artificially inflate ad revenue by simulating clicking on specific advertisements. They can also be used for the opposite purpose, clicking on a competitor's advertisements costing them money, without actually having a real customer viewing the advertisement.
    - Some criminal organizations rent out Botnetworks.
- ***Ransomware***
    - In a ransomware attack, a malicious program encrypts all information on your hard drive and demands payment in order to access your own files.
- *Logic Bomb*
    - A logic bomb is malicious code installed on a computer that is waiting for something to trigger it.
        - This could be triggered by a particular date or when a particular file is read or modified.

**Propagation Mechanisms**

- A ***Computer Virus*** is a program that attaches itself to other programs.
    - The virus adds extra instructions to a program that is already installed on the computer.
    - In addition to carrying out some specific action (such as turning your computer into a zombie) these instructions are used to propagate the virus to other programs on the computer.
- A ***Worm*** is a program that propagates through the network.
    - For example, the ILOVEYOU worm made copies of itself, which it then sent to each of the email addresses in the victim's Microsoft Outlook contact list.
- A ***Trojan Horse*** is something that isn't what it purports to be (or that is what it purports to be, but also includes a hidden malicious component).
    - The Dalai Lama's computers were infected by an email with a document entitled "Translation of Free Movement ID Book for Tibetans in Exile.doc". The document included a malicious payload when opened.
    - The ILOVEYOU worm had a script attached claiming to be a "Love Letter". Instead of being a love letter it triggered the worm code described in the previous section.
    - The Bonzi Buddy program created a colorful animated gorilla on your desktop, but behind the scenes, the program also displayed advertisements while you were web browsing and tracked your web browsing habits.
- These mechanisms aren't necessarily independent of one another.
    - The ILOVEYOU worm first inserted itself on a computer as a Trojan Horse, but was also a worm.

[1] While the MD5 hashcode still appears on websites, this hash is no longer considered secure.

    - Computer viruses that attach themselves to files can also be worms propagating themselves across the network.
- We sometimes rate viruses and worms depending on how many *Zero-Day Exploits* they use.
    - A zero-day exploit is a vulnerability that is unknown and has not been used previously for an attack.
    - Many viruses and worms exploit vulnerabilities that are already known. Computer users who have not updated their computers will still be vulnerable to these attacks. But hopefully most computers will be updated and will block these attacks.
    - In contrast, someone who creates a virus or worm that uses a zero-day exploit can expect that all computers will be vulnerable to it.

**Attack Mechanisms**

We will now look at various attack mechanisms. First we'll look at Social Engineering, one of the most important ways to get into a computer system. After that, we'll take a look at some technical means of attacking computers.

**Social Engineering**

In social engineering, the hacker does not attack the technical vulnerabilities of a system, instead they attack the people in the system.

- For example, a hacker could call a company's tech support, claim to be the CEO and ask that they reset their account password.
- Hackers specializing in Social Engineering will gather information on the target and then try to impersonate the target with customer support.
- Hackers can drop a USB drive in the parking lot of a targeted company.
    - Department of Homeland Security discovered that some 60% of government employees would plug a USB drive they found lying in the parking lot into their computer. If the USB drive had a government logo on it, the percentage went up to 90%.

- As Kevin Mitnick (one of the most notorious hackers of the 80s and 90s) said: "There is no patch for stupidity."
    - Mitnick was known to specialize in Social Engineering in order to gain access to systems.

**Phishing**

- Phishing is a very common form of Social Engineering.
- In a Phishing attack, the hacker pretends to be someone else, such as your bank. They get you to carry out an action, such as clicking on a link in an email.
- Remember, recreating a website is as simple as copying the HTML and CSS files. Just because a link takes you to a website that looks exactly like your bank website, does not mean it really is your bank's website.

- ***Don't click on links on email messages.*** *If you receive an email from your bank or credit card provider that claims there's a problem, instead of clicking on the link, open the web browser and enter your bank's URL directly (don't copy the URL provided in the email). If in doubt, call your bank.*

- John Podesta, Chairman of Hillary Clinton's 2016 Presidential Campaign, received a Phishing email claiming his Gmail account needed to have its password reset. He clicked on the link, entered his password, and his email was hacked.

**Spear Phishing**

- In a Spear Phishing attack, a hacker specifically targets an individual and crafts an attack specific to that individual.

    - For example, the hacker might find out your job function and who you typically might receive email from.
    - The hacker might determine what sorts of mail messages you would expect to receive.
    - They would then craft an email that appeared to be from a coworker and which had a subject similar to the sort of emails they might send.

- The Dalai Lama's computers were infected via a Spear Phishing attack.
    - An email was received that purported to be from campaigns@freetibet.org. It included a Word Document entitled "Translation of Free Movement ID Book for Tibetans in Exile.doc".
    - Opening the Word Document infected the computer.

**Email is Completely Insecure**

- Remember the email system is completely insecure.
- It is very easy to forge the "from" field.
- It is also easy to setup a message such that replying to it doesn't go to the listed sender.
- Email is not encrypted. Any information that you send via email can be read by any computer that the email passes through on its way to the intended recipient.
- Don't trust your email.

**Technical Attacks**

Social Engineering is particularly important, both because it's one of the most prevalent ways to attack a computer, and it's the one that most of us are best able to prevent. So don't forget it, always keep it in mind when working with computer. However, we will now switch to looking at some example of how hackers can use technical means to attack a computer.

**SQL Injection Attacks**

We already looked at SQL injection briefly during the PHP and SQLite lecture. You'll recall that in a SQL injection attack, a malicious user enters SQL commands where the programmer is only expecting to see simple text.

To use the XKCD Example I showed in class if the user enters the name "Robert'); DROP TABLE Students;" where the programmer is only expecting "Robert", the attacker may modify the database.

Preventing a SQL Injection attack is simple, but the programmer must be careful and ensure that they "sanitize" all user inputs to ensure that they do not contain SQL commands.

**Cross-Site Scripting (XSS) Attacks**

A cross-site scripting attack works similar to a SQL injection attack. In this case, instead of injecting SQL commands for execution on a server, our attacker's objective is to get malicious JavaScript code inserted onto a webpage.

As with SQL injection, the attacker places code where the programmer was expecting only text. For example, suppose a commenting system on a webpage asks the user to enter their name. The string entered in the "name" text field is then displayed as provided directly by the user to other people who visit the webpage.

Now imagine what happens if I enter a <script> tag along with some malicious script in place of my name. If the program simply takes what I've entered and inserts it into other viewer's webpages they will execute my JavaScript code when they visit the webpage.

**Clickjacking**
In a clickjacking attack the user takes advantage of the ability to stick one webpage inside of another using the <frame> or <iframe> mechanisms. This is used in conjunction with CSS positioning to place elements wherever we want and CSS's ability to make elements transparent.

With clickjacking, I place one webpage on top of another webpage, but make the top webpage transparent. I then place items on the bottom webpage to get the user to click in certain locations. The user thinks they are clicking on the items on the bottom webpage, but instead they are clicking on the transparent top webpage.

As an example, I can have the bottom webpage include a form with a button to show the weather, and have the top webpage an Amazon product webpage. I position Amazon's "Buy-with-One-Click" button directly over the button to show the weather. The user clicks on the webpage thinking they are clicking on the button to show the weather, but they are actually buying something at Amazon.

The solution to Clickjacking is for a webpage owner, such as Amazon, to ensure that their webpages cannot be placed inside of <frame> or <iframe>. There are several methods to ensure that a webpage cannot be loaded inside a frame.

**Sandbox Security Failures**
Much of web browser security is based on the concept of Sandbox Security. The idea being that programs can run inside the sandbox (which has only limited access to the wider computer), but aren't allowed outside of the sandbox. So for example, JavaScript can change the color of webpages – that's part of what's in the sandbox – but it can't delete the files on a computer – those are outside of the sandbox.

There are several technologies related to web browsers that also rely on sandbox security. Java applets are Java programs that are designed to run on webpages. Java is supposed to provide sandbox security preventing them from doing anything malicious. Unfortunately Java's sandbox does not work very well, and letting web browsers run Java is very strongly discouraged by security professionals (in fact, as of this writing, most web browsers default to not allowing Java to run in the browser, the user can however, override this setting).

Adobe Flash also uses Sandbox Security. As with Java, many security professionals recommend not allowing Flash programs on webpages to run.

**Drive-By-Download Attacks**
While JavaScript, Java, and Flash are all supposed to run within a Sandbox, browser Add Ons or Extensions generally do not. They have free access to your entire computer and can generally do whatever they want.

A website (or email message) which uses a drive-by download attack either exploits a weakness in the web browser (or mail program) to automatically install something on your computer, or uses the gullibility of the user to get them to click and install an extension, add-on, or even a regular application all with a malicious payload contained within.

**Man in the Middle Attack**
A "man in the middle" attack is a technique used to spy on a user, gaining access to items such as their account name and password without their knowledge. For a man in the middle attack to occur the attacker must interpose their computer between the targeted user and the website (or other type of server) they are trying to communicate with. This might be

done, for example, by setting up a fake public WiFi network. When the victim logs onto the WiFi network all their network traffic passes through the attacker's computer.

In a man in the middle attack, the victim unknowingly passes their HTTP requests to the attacker, without realizing that they are not directly connected with the website they are trying to reach. The attacker sees the contents of the victim's request and passes it on to the requested website. The requested website passes the information back through the attacker and on to the victim. Neither the victim nor the website they are communicating with are aware that there is a third party listening in to all communications.

The attacker can see all traffic between the attacker and victim without the victim's knowledge. Depending on the attacker's objectives they can either continue to monitor the traffic (recording data such as account name and password for later use) or at some point they can modify the traffic.

If the victim is using a secure communication method such as HTTPS or SSH this does pose some difficulties for the attacker.

- The attacker might use a fake certificate (such as the ones generated when the Dutch DigiNotar Certification Authority was hacked), so that the victim thinks they are communicating with the actual website directly.
- The attacker might also simply count on the gullibility or laziness of the target.
  - For example, logging in to the Stanford Unix computers using SSH gives us the key of the computer we are communicating with and asks us if we want to continue before completing the login procedure. If we don't recognize the number, we should halt the login procedure to ensure that our login name and password aren't passed to a hacker. But how many of us have actually bothered to make sure the key is actually valid. With a man-in-the-middle attack, an attackers could pass us a fake key, and we would blithely enter our name and password to them. They would then use that data to actually login. We would have no idea that our data had been compromised.
  - Another approach might be for the attacker to ask the victim to accept a certificate for the correct website, but from a new untrustworthy Certification Authority that had allowed the creation of a fake certificate. Gullible users might simply click on the "Accept New Certification Authority" button when their web browser asks them to verify.

**Exploiting Internet Protocol Weaknesses**

Attackers can exploit how the Internet Protocol works for potentially nefarious purposes. For example, in 2010 China Telecom managed to route 15% of worldwide Internet traffic through China.

> *This incident affected traffic to and from US government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others.*