Lecture #21: Security –
Defensive Measures and Practical Suggestions

CS106E, Young

This lecture we discuss strategies to defend computers against attacks. We discuss strategies corporations can use to protect themselves – as we see, some of these techniques can also be used by private individuals. Companies and individuals can use Firewalls to monitor and prevent certain types of Internet traffic. We take a look at how a company can create a Virtual Private Network (VPN) encrypting all traffic between their different geographic locations. VPNs can also be used by individuals for privacy and sometimes to get around regional locks. An Air Gap, which separates a system physically from the Internet, provides the best security.

While most email is not secure, secure email systems do exist. Similarly, much of web traffic is completely insecure, but using HTTPS (HTTP Secure) instead of HTTP guarantees the identity of the website you are communicating with and encrypts communications with the web server. As JavaScript can be used for malicious purposes, disabling JavaScript on random websites with a browser plug in such as NoScript or ScriptSafe can greatly enhance your security on the web (at the cost of some inconvenience).

Multifactor authentication can help prevent unauthorized access to your accounts, even if your password is stolen. Use of standard cell phone Text Messages (SMS) is no longer recommended as the SMS system is not secure and scammers have sometimes taken over phone numbers to intercept SMS messages. However, the use of Authentication Codes generally does provide good security. We also discuss the pros and cons of using Biometric data such as fingerprints. In addition to multifactor authentication, coming up with a cryptographically strong password helps protect your security. We discuss what makes a good password, using a pass phrase instead of a password, as well as using a Password Manager.

Laws are under consideration allowing companies or individuals to Hack Back, taking the fight to an attacker. We take a quick look at the implications.

Finally, we end the lecture by considering some practical steps one can take to improve their own personal security online.

Firewalls

- A firewall monitors network traffic between a computer or set of computers, and the wider Internet.
- Corporations often will not connect their computers directly to the Internet.
    - The Corporation's computers will form an internal network (sometimes referred to as an Intranet).
    - All Internet traffic into or out of the corporate Intranet will have to pass through a special computer that acts as a ***Firewall***.

        - The Firewall inspects all Internet traffic passing through it.
        - Firewalls can be configured with custom rules to determine what traffic can pass through.
            - We could configure the Firewall to allow only packets from certain applications through the Firewall.
            - We could only allow incoming traffic from certain specific computers or we could block traffic from certain computers.
                - For example, some companies will block access to si.com (Sports Illustrated).
            - We could scan traffic looking for specific keywords.

- Personal computers have special software provided by the Operating System sometimes referred to as a ***Personal Firewall***.
    - The Personal Firewall serves a purpose similar to a Corporate Firewall.
    - We tell the Firewall software which applications are allowed to send data outside of the computer.
    - We can tell the computer which applications we expect to receive data from the network.
    - When you install a new program and run it for the first time, your Operating System may ask if that program is allowed to send data out to the network.
    - If you receive a message asking to give access to a program and you have not recently installed software, you may have a virus on your computer.
    - Some programs that you might not expect need access to the network may request access to allow them to check in with their manufacturer for automatic updating.

Proxy Servers

- A proxy server is a computer that acts as an intermediary between two different computers.
- It can be used for a number of different purposes.
    - Stanford provides access to a number of different resources for free, such as the Medline database and Safari Online technical books.
        - Some of these resources determine whether or not someone can access them by checking the IP number of the incoming request.
        - If the request is coming from a Stanford IP number, the request is allowed, because Stanford has a contract with them.
        - If the request is not coming from an IP number in the allowed range, the request is denied.
        - This means that if you are living off campus and try to access these resources, you will be blocked – while Stanford IP numbers are allowed, other IP numbers such as Comcast IP numbers are not.
    - Stanford has a Proxy Server that will allow access to many of these resources.
        - When off campus, we contact the Stanford Proxy Server asking it to pass a request on to Medline or Safari Online.
        - The Proxy Server forwards our request.
        - The online resource checks the IP number of the request, and sees that it's coming from a Stanford IP number (because the Stanford Proxy Server has a Stanford IP number).
        - The request is allowed, and the data requested is sent back to the Stanford Proxy Server.
        - The Proxy Server forwards the data on to us.
    - This same technique can be used to access Sports Illustrated at a company that does not allow direct access. ***Warning:*** *if you get caught doing this, your Corporate IT department may be very angry with you.*

- Note that working with a proxy server does not imply any encryption, so for example, a request to si.com via a proxy would pass through a firewall, assuming the proxy server itself was not blocked, but a scan off the contents would reveal that it was a request forwarding to si.com. In contrast Virtual Private Networks, which we'll look at next guarantee encryption of all data.

Virtual Private Networks

- Virtual Private Networks (VPNs) were traditionally developed for corporations, but are now used by individuals. We'll start out by talking about their corporate use, but will look at personal use of VPNs once we've finished our corporate discussion.

- When all a company's computers are centrally located, they can be better protected from outside snooping. Traffic between the computers won't be snooped on, because the traffic only passes between computers within the company. Also, as we've seen, a company can place all their computers behind a Firewall.
- What happens if the company has multiple offices in different geographic locations though? Network traffic between those office locations must pass through the wider Internet.
- The company can create a Virtual Private Network connecting all the computers spread across the globe.
    - Traffic between office locations pass through special Gateway Computers.
    - The VPN gateway computer will completely encrypt the network traffic. The exact source computer and destination computer will be encrypted, as will the actual message contents.
    - Those outside the network will see network traffic passing between two gateway computers at the two office locations, but won't see any further details.
    - Computers outside of the network, such as sales personnel out on the road, can also connect to the VPN. Any network traffic to or from their laptop, when connected to the VPN, will be encrypted and passed to a VPN gateway before being forwarded to its actual destination.
- With a VPN our company can ensure that all data transmitted between offices and between our personnel on the road is completely encrypted and cannot be snooped on by outsiders.

- VPNs can also be used for private purposes.
    - If you use a private VPN, all your network traffic from your computer will be encrypted and passed to the VPN.
        - Your regular Internet Service Provider (ISP) will see that you're communicating with the VPN, but won't know what you're doing and where your Internet requests are ultimately going.
    - Private VPNs can have several uses.
        - They provide privacy, as your ISP is now allowed to sell information on your web browsing habits.
        - They can sometimes get around regional locks. Many VPN companies have servers around the world. Say you want to purchase an ebook in French, but the website you want to purchase it from only allows those in France to buy their ebooks. You connect to your VPN's French server, and go to the French website. It appears you're in France, so your purchase goes through.
        - Warning: some media companies (e.g., Netflix) don't allow use of VPNs or Proxy Servers. If you try to watch content on these services, you will be warned to turn off your VPN or Proxy Server.
        - VPNs can allow access through "The Great Firewall of China" allowing those with VPN access to read news articles and access websites prohibited to Chinese citizens.

- While historically China has allowed foreign nationals to use VPNs to access prohibited websites, such as the New York Times, restrictions have increased, particularly on private use.

Air Gap

- Placing computers on the Internet increases their risk of being attacked.
- One of the best ways to prevent an attack is to create an ***Air Gap***.
    - This means completely removing the computer or computers from the wider Internet so that there is a physical gap isolating them from the rest of the world.
    - With an Air Gap, someone would have to physically break in to the building housing the computers in order to access them.
    - Note that if your Air Gapped network includes WiFi, this means someone may still be able to access it from outside the building. This lowers your security.

Secure Email

- As we learned in the last lecture, the standard email system is completely insecure.
- There are several secure versions of email that are available. Some things to look at when thinking about secure email.
    - What does it actually mean for the email system to be secure?
        - Does the system prevent others from eavesdropping on your conversation (Confidentiality) or does it guarantee the identity of those you are communicating with (Authentication).
    - Some secure email systems are deliberately setup to support anonymity. These systems, for example, might make sure that messages sent with it do not include your originating IP address.
    - If your email messages are being stored encrypted on a server, who has the ability to decrypt those messages?
        - In some cases, for example, the data is encrypted, but the server owner has the ability to decrypt the messages upon receiving a government order.
        - Human rights leaders and dissidents may have concerns with these types of systems.

HTTPS / Secure Web

- The HTTPS (HTTP Secure) protocol is a secure version of the HTTP protocol.

- If you are using the standard HTTP protocol, all communication with the website is being sent in clear text (i.e., it is not encrypted). In addition, HTTP does not verify the identity of the party you are communicating with.

- In contrast, with HTTPS, the website you are communicating with must have a valid Certificate. In addition, communications with that website is encrypted.
    - Some websites only use HTTPS for their login page. On this type of website, all communication with the website, other than that initial login page can be eavesdropped on.
    - Some websites only encrypt the HTML file. For example, images or CSS files associated with a webpage might not be encrypted. This may trigger a web browser warning that the webpage is not fully encrypted.
    - Some websites support both the secure HTTPS and the insecure HTTP protocol for the same pages – encrypting takes processing power and can raise expenses, so they may try to have users use the insecure version. The HTTPS Everywhere plugin will force these websites to switch to the HTTPS protocol on all webpages if it is available.

Disabling JavaScript (No Script / ScriptSafe)

- Malicious JavaScript code is a common attack vector. Disabling JavaScript can prevent these attacks.
- Web browser extensions are available that will disable JavaScript.
    - On Firefox, the NoScript extension blocks JavaScript.
    - On Chrome ScriptSafe blocks JavaScript.

- Many webpage simply won't work correctly without JavaScript. These extensions will allow you to form a whitelist of websites that are allowed to run JavaScript on your computer.
    - Initially you will have to constantly tell the extension that you trust the website you are currently visiting, and that it is allowed to run JavaScript.
    - Over time, your whitelist will be filled with websites you regularly visit, and the extension will become less intrusive.
- While these extensions can be somewhat of a pain to use, security experts say that they will greatly enhance your security.
    - If you go far afield on the web, these extensions are strongly recommended.

Multifactor Authentication / Login

- In order to better protect an account, additional factors other than just knowing the name and password can be used.

- Many websites support "Two-Factor Authentication".
    - This often involves sending the user a text message when they first login from a new computer.
    - This means that the user would need to know the password (that's the first factor) and have their cell phone to receive the text message (that's the second factor).
    - Unfortunately, the cell phone network is no longer considered secure.
        - Standard cell phone text messages (which use the SMS system) are generally not encrypted.
        - The SMS system can also be spoofed, manipulating sender information.
        - Scammers have also transferred phone numbers without their original owner's knowledge. Once they've done this, the text message will go to the criminal's phone instead of to the original owner of the phone number.
    - Using cell phone texting-based two-factor authentication is still probably better than just using a password.

- Authentication Codes
    - As an alternative to receiving a text message, another authentication mechanism is to create a pseudo-random number.
        - In computer science, we don't actually generate random numbers, we generate pseudo-random numbers. This is a number that appears to be random, but we can reproduce the same sequence of pseudo-random numbers if we start our algorithm using the same seed number.
    - If both our remote device and the server we are connecting to shares the same seed number, both will generate the same sequence of pseudo-random numbers.
    - When logging in, if we enter the pseudo-random number given by our device, the server can check to make sure that it matches the next pseudo-random number in the sequence. If the two match, this verifies that we both share the same seed number.

    - Authentication codes are actually created combining the concept of a pseudo-random sequence along with the current time using a procedure called the TOTP (Time-based One-Time Password) algorithm.

    - This is how an authentication application such as Google Authenticator works.
    - Typically, these applications allow you to get access to the original seed number.
        - You will need this seed number if you change phones or for some reason need to delete and reinstall the application.

- Biometric Data
    - Biometric data such as fingerprints or retinal eye patterns can also be used as a means of identification.
    - Some security experts do have concerns with the use of biometric data.
        - If a system is based on biometric data, and your biometric data is stolen, you have no way of changing your biometric data.
        - For example in the Office of Personnel Management hack fingerprint data for over 21 million people was stolen.

Passwords vs. Passphrases

- Generally recommendations on passwords have been to have a long password (at least nine characters long, longer is better) and to make sure that the password includes lower-case letters, upper-case letters, numbers, and symbols such as % or @.
    - The objective is to make sure that anyone carrying out a brute-force attack (trying all the possible combinations of passwords) has to try a lot of combinations.
    - Obviously the longer your password is, the more combinations they need to try.
    - In addition, if you use upper-case letters along with lower-case letters, they'll have to double the number of possible combinations. Including numbers and symbols increases the possible combinations even more.

- Recently the idea of using a pass phrase instead of a password has taken hold.
    - A pass phrase consists of multiple words in the English language.
    - The idea here is that:
        - Pass phrases can be much longer than passwords and still be remembered.
        - There are many more possible words in the English language than the number of upper-case letters, lower-case letters, numbers, and symbols. So even if the attacker knows it's a pass phrase, and the pass phrase only consists of a few words, there are still many more combinations than in a password.

- One thing to be careful on when using a pass phrase. If you use an actual phrase that is grammatically correct and makes sense, you are greatly reducing the number of possible combinations.
    - Research has shown that pass phrases aren't typically as random as one might hope. Because of this, an attacker can greatly reduce the theoretical number of combinations they might have to try to get into a typical account.

Password Managers

- As an alternative to having to deal with remembering long passwords or coming up with a good random pass phrase, you can use a Password Manager.
- A Password Manager is a program that remembers your passwords for you.
    - Typically you can ask the Password Manager to create a cryptographically strong password for you that is truly random.
    - The Password will be saved by the Password Manager, and will be accessible on all your devices.
    - Web Browser plug ins will automatically retrieve the Password from the Password Manager when you visit a website.

AviD's Rule of Usability
"Security at the expense of usability, comes at the expense of security."

If you end up designing security guidelines for a company, keep this rule in mind. If you make security a burden for your employees, they are likely to work around your guidelines. This will reduce your overall security.

- For example, changing passwords every few months used to be considered best practice, but it isn't anymore. When passwords are changed frequently users can't remember them and end up writing them down or storing them, thus reducing security.

Active Cyber Defense Measures / Hack Back

- If an outside intruder is actively trying to get on your computer, what can you do?
- Taking active measures to fight the attacker is called ***Hack Back***.

- Under current US law, actively taking the fight to the intruder may be illegal.
    - There is a law currently under consideration in the US Congress to change this.
    - Security experts are divided on the wisdom of allowing this.

- Active measures can include:
    - Placing a beacon on data that is being stolen.
        - The data will send signals as it is moved to the attacker's computer. This will allow the defender to see where the data is being taken.
    - Using a dye packet.
        - In contrast to a beacon, which simply indicates where it has been taken, data with dye packet code inserted into it will actively attempt to destroy data where it has been taken.

- Concerns with active measures include:
    - Typically, the initial computers where data will be taken won't actually be the attacker's computers. They'll be computers of innocent users (with poor security) used as intermediaries to hide the attacker's true identity.
    - If we allow companies or individuals to strike back, they could start a cyberwar with another nation state. This problem is exacerbated by the fact that it's relatively easy to leave a false trail in cyberspace.

Recommendations for Personal Cyber Security

Keep Your Software Updated – Security holes in software are a major means of attacking your computer. Viruses are often simply copies of previously released viruses. Viruses based on Zero-Day Exploits are relatively rare. If your software is updated, most attacks will be blocked.

Use Different Passwords for Different Accounts – Don't use your banking passwords for a hobby bulletin board. Use different passwords for different accounts. Do not use your banking or email passwords for other accounts. If that other site has poor security and you use your email password on it, a hacker can now access your email.

Use a Password Manager or Make Good Passwords or Pass Phrases – Consider using a Password Manager. Otherwise, if you use a password, make sure it's at least nine characters long and includes upper-case letters, lower-case letters, numbers, and symbols. If you use a pass phrase, it should not be an actual phrase. Your best bet is to choose four or more words at random.

Use Multi-Factor Authentication when Available – Many services such as email and financial websites support two-factor authentication. Use this option when it's provided. As we discussed earlier, authentication by sending text messages via the standard cell phone text system (SMS) is no longer preferred, so choose the Authenticator option if it's available. However, even SMS-based two-factor authentication will dissuade an unsophisticated attacker.

Don't Fall for Phishing Scams – Don't click on links in email messages, even if they look legitimate. If you get an email claiming to be from your bank, don't click on the link. Instead go directly to your web browser and manually type in your bank's URL (don't copy it from the email). If in doubt, call in and talk to someone in person.

Block Java and Flash / Considering Blocking JavaScript – Java and to a lesser extent Flash are major means of attacking a computer via the web. JavaScript can also be used to exploit web browser vulnerabilities. You should definitely make sure Java is disabled in your web browser and should consider disabling Flash and JavaScript from random websites you visit. Only whitelist those websites that you trust.

Use Anti-Malware Software – Anti-Malware / Anti-Virus / Anti-Spyware software will keep an eye out for malicious software and block them before they can attack your computer.

To Learn More

Students have asked me for additional sources of information on topics in this course, and I often don't have good references to provide them that are at the appropriate level of technical detail for CS106E students. However, in this case, I do have a recommendation:

"Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare" an 18-lecture course by Professor Paul Rosenzweig, George Washington University Law School, is quite good and should be quite understandable for CS106E students. Professor Rosenzweig spends a bit less time on technical details than we have, but provides a lot of case studies, and spends a lot of time discussing policy questions. I originally discovered several of the case studies in the homework readings from listening to Professor Rosenzweig's lecture series. You can get this lecture series either from their producer, The Great Courses company, or from Amazon/Audible (which will generally be much less expensive – and in fact the course can be gotten for free if you've never used Audible before).

He also has a 24-lecture series entitled "The Surveillance State: Big Data, Freedom, and You" which is also good.