Lecture Overview

The world is a scary place, and everyone is out to get you.

I hope you leave this lecture a little bit paranoid and a lotta bit interested in the field of security.
In today's lecture, we will cover:
- What computer security is
- Goals of computer security: authentication, confidentiality, integrity, and availability
- Social engineering attacks and general advice
Computer security is the protection of computer systems and information from harm, theft, and unauthorized use.

You’ll find many different types and definitions of computer security (e.g. information security, network security, application security, etc.). These exact definitions are less important to us.
What is Computer Security?

The Computer Security Problem:
What is Computer Security?

The Computer Security Problem:

1) There is lots of buggy software out there.
What is Computer Security?

The Computer Security Problem:

1) There is lots of buggy software out there.

2) A lot of money can be made from finding and exploiting these vulnerabilities.
What is Computer Security?

To: Jonathan Kula

iMessage
Today 5:16 PM

How much do you think a zero-day is worth?

Idk I think it would depend on what platform and what kind of exploit

Oh hm, idk, maybe like an exploit on iMessage 😐😐😐

Would the user have to do anything in order to trigger the exploit??

Nope 👀 zero click

Hmmm........
Delivered
What is Computer Security?

The Computer Security Problem:

1) There is lots of buggy software out there.

2) A lot of money can be made from finding and exploiting these vulnerabilities.

A single zero-day exploit is estimated to be worth anywhere between $60,000 (Adobe Reader) to $2,500,000 (Apple iOS).
What is Computer Security?

A **threat model** is structured way to evaluate threats and risks to a system.
What is Computer Security?

A **threat model** is structured way to evaluate threats and risks to a system.

To develop a threat model, we ask: “**what is our bad guy trying to do**”

It's important to think about who our adversary might be and what our adversary has access to.
What is Computer Security?

Threat models are context dependent.
We can consider a general case where we have some user, who wants to be able to:

- Visit the Bank of America website
- Log into their bank account
- View information about their bank statement
- Wire money to another user

Let's consider how we can guarantee security throughout this entire process.
Goals of Computer Security

We can divide computer security into different goals:

1. Availability
2. Authentication
3. Confidentiality
4. Integrity
Availability

**Availability:** authorized users should always have access to their systems and data.

**Problem:** we want to prevent unauthorized users from preventing authorized users from using resources.
Availability

Let's experience something!

1. Open an alternate browser (that you don't normally use)
2. Visit TheAnnoyingSite.com and don't press any buttons
3. On the count of three... hold down the space bar!

Source: Feross Aboukhadijeh
https://github.com/feross/theannoyingsite.com
Availability

**DoS Attack:** Using up all of the resources is a way that an attacker can prevent other users from using the service.
Availability

DoS attack

DDoS attack

Source: UpGuard
Availability

DoS attacks are extremely prevalent!

**DDoS cyberattacks temporarily foreign ministry website**

**NYT, REDDIT, KICKSTARTER ARE ALL SUFFERING A DDoS ATTACK RIGHT NOW**

**Russia-linked Hackers Launch DDoS Attacks on Germany and U.S. Hospitals, Threaten Canadian**

**German airports hit with DDoS attack**

The websites of seven German airports were taken down by hackers
Availability

Sites prevent DoS/DDoS attacks by:

- Limiting how many times you can make a request
- Distributing servers across multiple access points
Goals of Computer Security

We can consider a general case where we have some user, who wants to be able to:

- Visit the Bank of America website
- Log into their bank account
- View information about their bank statement
- Wire money to another user
Authentication is used to verify that a user is who they say they are.

**Problem:** we want to prevent unauthorized users from gaining access to our systems.
Most users choose weak passwords
Most users choose weak passwords

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
<td>123456</td>
</tr>
<tr>
<td>password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12345678</td>
<td>12345678</td>
<td>qwerty</td>
<td>qwerty</td>
<td>12345</td>
<td>qwerty</td>
</tr>
<tr>
<td>qwerty</td>
<td></td>
<td>12345678</td>
<td>password</td>
<td>password</td>
<td>qwerty</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>12345</td>
<td>12345</td>
<td>1234567</td>
<td>1234567</td>
<td>password</td>
<td>1234567</td>
</tr>
<tr>
<td></td>
<td>123456789</td>
<td>123456789</td>
<td>12345678</td>
<td>12345678</td>
<td>12345678</td>
<td>12345678</td>
</tr>
<tr>
<td>letmein</td>
<td>sunshine</td>
<td>12345</td>
<td>111111</td>
<td>111111</td>
<td>111111</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12345678</td>
<td>1234567</td>
<td>iloveyou</td>
<td>123123</td>
<td>123123</td>
<td>iloveyou</td>
</tr>
<tr>
<td>iloveyou</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12345678</td>
<td>1234567</td>
<td>qwerty</td>
<td>iloveyou</td>
<td>1234567890</td>
<td>111111</td>
</tr>
<tr>
<td></td>
<td>football</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iloveyou</td>
<td>iloveyou</td>
<td>123123</td>
<td>123abc</td>
<td>1234567</td>
<td>123123</td>
</tr>
</tbody>
</table>

Source: 2017-2020 and 2022 data from SplashData, 2021 data from NordPass
Authentication

Most password guidelines do not provide good guidance.

Source: Attorney General of Texas Child Support, Telnet, PayPal, and many other sites.
Help: List of Password Rules

1. The password must be **exactly** 8 characters long.
2. It must contain **at least** one letter, one number, and one special character.
3. The **only** special characters allowed are: @ # $
4. A special character must not be located in the first or last position.
5. Two of the same characters sitting next to each other are considered to be a "set." No "sets" are allowed.
6. Avoid using names, such as your name, user ID, or the name of your company or employer.
7. Other words that cannot be used are Texas, child, and the months of the year.
8. A new password cannot be too similar to the previous password.
   a. Example: previous password - abc#1234, acceptable new password - acb$1243
   b. Characters in the first, second, and third positions cannot be identical. (abc****)
   c. Characters in the second, third, and fourth positions cannot be identical. (*bc****)
   d. Characters in the sixth, seventh, and eighth positions cannot be identical. (**234)
9. A password can be changed voluntarily (no Help Desk assistance needed) once in a 15-day period. If needed, the Help Desk can reset the password at any time.
10. The previous 8 passwords cannot be reused.
"WELL, THEY BANNED PASSWORD RE-USE. WHAT DO YOU EXPECT ME TO DO?"
Authentication

Choose the password!

secretword -or- s$cretw0rd
58 minutes
1 month

CoolWater -or- CfgWrylk
17 hours
19 hours

HorseHouseLake -or- s$cretw0rd
8 hundred thousand years
1 month

HorseHouseLake -or- HcdfyHatsrlpiq
8 hundred thousand years
23 trillion years

Source: https://www.security.org/how-secure-is-my-password/
Password Best Practices

- Complex is not necessarily strong (e.g. P@ssw0rd!)
- Choosing multiple random words may result in a stronger password, even if all words appear in a dictionary (e.g. horsestaplebattery)
- Check passwords against leaked breach data
- Don’t use the same passwords for all of your accounts!
- Length is the most important factor
Password Manager
Authentication

Password Manager

Use one. 😁
New Methods of Authentication

Something the user knows
New Methods of Authentication

Something the user knows → a password
New Methods of Authentication

Something the user knows → a password

Something the user has
New Methods of Authentication

Something the user *knows* → a password

Something the user *has* → a phone, a badge, a cryptographic key
Authentication

New Methods of Authentication

Something the user \textit{knows} \rightarrow \text{a password}

Something the user \textit{has} \rightarrow \text{a phone, a badge, a cryptographic key}

Something the user \textit{is}
Authentication

New Methods of Authentication

Something the user *knows* → a password

Something the user has → a phone, a badge, a cryptographic key

Something the user is → a fingerprint, face ID, biometric data
Authentication

That was MUCH easier than I expected! Why did I pull an ALL-NIGHTER studying?

Which final was it?

Not a final. He just signed up for TWO FACTOR AUTHENTICATION.
Goals of Computer Security

We can consider a general case where we have some user, who wants to be able to:

- ✔ Visit the Bank of America website
- ✔ Log into their bank account
- ☐ View information about their bank statement
- ☐ Wire money to another user
Confidentiality

When we communicate with one another over the Internet, we expose ourselves to privacy concerns.

Unless our data is somehow obfuscated (usually through encryption), we risk other people seeing what we are sending.
Confidentiality: only intended users should be able to read our data or information.

Problem: we want to prevent unintended users from reading information we send or that is stored on our systems.
Confidentiality
Confidentiality
Confidentiality
HTTPS and TLS

HTTPS (Hyper Text Transfer Protocol Secure) is used to send data between a web browser (e.g. Chrome running on your computer) and a website (e.g. Facebook).
HTTPS and TLS

**HTTPS** (Hyper Text Transfer Protocol Secure) is used to send data between a web browser (e.g. Chrome running on your computer) and a website (e.g. Facebook).

- ![Secure](https://crypto.stanford.edu/~dabo/cs255/)
- ![Not Secure](http://crypto.stanford.edu/~dabo/cs255/)
HTTPS and TLS

HTTPS (Hyper Text Transfer Protocol Secure) is used to send data between a web browser (e.g. Chrome running on your computer) and a website (e.g. Facebook).

All of the data is encrypted using an encryption protocol called TLS (Transport Layer Security).
Confidentiality

[WIRESHARK DEMO]
Confidentiality

Confidentiality Best Practices

Always (we mean, always) use HTTPS.

Use private messaging: Signal is the best, WhatsApp is okay, Telegram is bad.

iMessage is secure... unless you have iCloud enabled.
Goals of Computer Security

We can consider a general case where we have some user, who wants to be able to:

- Visit the Bank of America website
- Log into their bank account
- View information about their bank statement
- Wire money to another user
Integrity: only authorized users should be able to modify data or information.

Problem: we want to prevent unauthorized users from modifying information that we send or that is stored on our systems.
"Jonathan sends $1000 to account Akshay."

On its way to BANK OF AMERICA

| fg4s6yq8 | 71l2ta0 | 95bh08qw | ab459k1q | 5rtws2lp |
"Jonathan sends $1000 to account Akshay."

Jonathan sends $1000 to account Ayelet."
Integrity

[XSS DEMO]
We've already seen this!
We've already seen this!

```bash
chgrp staff ./secrets
chmod g+r ./secrets
```
We've already seen this!

```
chgrp staff ./secrets
chmod g+r ./secrets
```

**Access Control Lists (ACLs)** describe what access each user has for every file, folder, or program.

ACLs maintain integrity by ensuring unauthorized users can't modify files.
Virtual Machines are another way to preserve integrity is by ensuring that programs run within a confined ("sandboxed") environment.
Goals of Computer Security

We can consider a general case where we have some user, who wants to be able to:

- Visit the Bank of America website
- Log into their bank account
- View information about their bank statement
- Wire money to another user
Social Engineering
Social Engineering

Many security vulnerabilities are not technical vulnerabilities. Instead, they are vulnerabilities in how humans disclose information. These are known as social engineering attacks.
Many security vulnerabilities are not technical vulnerabilities. Instead, they are vulnerabilities in how humans disclose information. These are known as **social engineering attacks**.

Social engineering uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social Engineering

Many security vulnerabilities are not technical vulnerabilities. Instead, they are vulnerabilities in how humans disclose information. These are known as **social engineering attacks**.

Social engineering uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social Engineering

Phishing Attacks

A *phishing attack* occurs when an attacker masquerades as a trusted entity and tricks the user into giving away sensitive information such as credit card information or login credentials.
Social Engineering

Phishing Attacks

A **phishing attack** occurs when an attacker masquerades as a trusted entity and tricks the user into giving away sensitive information such as credit card information or login credentials.

This is often done using a duped email, text message, or having a user open a link.
Phishing Attacks

A *phishing attack* occurs when an attacker masquerades as a trusted entity and tricks the user into giving away sensitive information such as credit card information or login credentials.

This is often done using a duped email, text message, or having a user open a link.

**Example:** a spoofed email from it.stanford.edu. The email claims that the user’s password is about to expire and that the user needs to renew the password within 24 hours at a provided link.
Social Engineering

True Story Time
True Story Time

+27 87085101200668

Text Message
Today 4:06 PM

Good day, the Pawboost Rescue Squad has found a pet that matches your description. State: Healthy. Area: Randburg. Please reply with your email for info.
Social Engineering

Notice anything wrong?

Hey there!

https://www.apple.com

Secure Connection
Social Engineering

Real:

Cyrillic:
The Cyrillic representation uses punycode, which does break legitimate use cases.
Social Engineering

Best Practices Against Phishing

- Always double triple check that you aren’t clicking on links from suspicious or unknown emails.

- Check the URL bar and sender address to make sure they appear as you expect them to.

- Use two factor authentication. Even if an attacker has your username and password, they won’t have your smartphone...
Social Engineering

Ransomware Attack

A ransomware attack occurs when an attacker encrypts a user’s files and data, and then demands a payment (a “ransom”) in order to unlock the user’s files and data.
Social Engineering

Best Practices Against Ransomware

- Backups, backups, backups.
- Turn on a file encryption system. (Encrypted File System for Windows, FileVault for macOS, or dm-crypt for Linux)
- Get your devices up to date. Updates are important because they often contain patches, which are fixes to remedy discovered vulnerabilities.
- VPVs don't necessarily increase security; they change point of trust.
  - VPNs that are advertised on YouTube are almost completely useless; the VPN company can still see everything you do.
Other Advice

- VPNI  don't necessarily increase security; they change point of trust.
  - VPNI  that are advertised on YouTube are almost completely useless; the VPN company can still see everything you do
- Don't plug into random USB ports (at airports, coffee shops, etc).
Other Advice

- VPNs don't necessarily increase security; they change point of trust.
  - VPNs that are advertised on YouTube are almost completely useless; the VPN company can still see everything you do.
- Don't plug into random USB ports (at airports, coffee shops, etc).
- If an email causes a strong emotional reaction (fear, panic, etc.), be very careful with it—phishing emails are designed to do that.
- VPNs don't necessarily increase security; they change point of trust.
  - VPNs that are advertised on YouTube are almost completely useless; the VPN company can still see everything you do.
- Don't plug into random USB ports (at airports, coffee shops, etc).
- If an email causes a strong emotional reaction (fear, panic, etc.), be very careful with it—phishing emails are designed to do that.
- Embedded devices (e.g. phones) are generally more secure.
Other Advice

- VPNs don't necessarily increase security; they change point of trust.
  - VPNs that are advertised on YouTube are almost completely useless; the VPN company can still see everything you do.
- Don't plug into random USB ports (at airports, coffee shops, etc).
- If an email causes a strong emotional reaction (fear, panic, etc.), be very careful with it—phishing emails are designed to do that.
- Embedded devices (e.g. phones) are generally more secure.
- Again, use a password manager!