Cybersecurity

Cybersecurity

Cybersecurity: set of techniques to protect the **secrecy**, **integrity** and **availability** of computer systems and data against threats.

- Secrecy or confidentiality: only authorized people should be able to access or read specific computer systems and data.
  - E.g. data breaches, where hackers reveal credit card information, is an attack on secrecy
- Integrity: only authorized people should be able to modify or use systems and data.
  - Hackers who learn your email password and then send emails masquerading as you is an attack on integrity.
- Availability: authorized people should always have access to their systems and data.
  - **Denial of Service(DoS)** attacks: Hackers overload a server with fake requests rendering the server slow or unaccessible. This is an attack on the service's availability.

Attack Vectors

To achieve those three goals, security experts need a formal definition of who the “enemy” is. This specification is called a **threat model**.

Many types of cybersecurity breaches that affect the three principles of security fall into different **attack vectors**:

- Phishing Attacks security
- **SQL injection**: use Structured Query Language(SQL) to send database manipulation code through username/password text fields.
- **DDoS** Attacks: **Distributed denial-of-service (DDoS)** attacks impact information availability. The attack comes when a bad actor creates a slew of traffic requests on a website at once in order to crash it or severely cripple it for a period of time.

An **attack vector** is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

Phishing Attacks

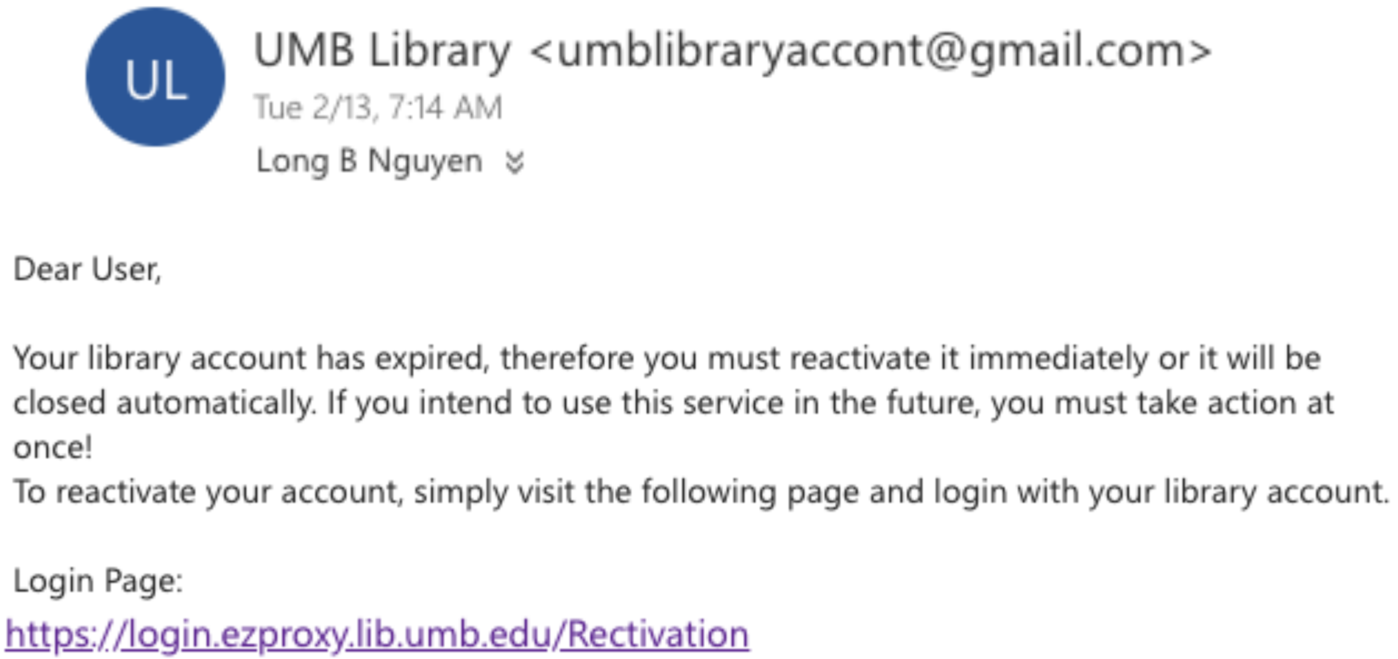
Phishing attacks: a hacker impersonate either a legitimate person or a corporation through an email that asks the user to take an action that would give the phisher an access point to critical data or information.

  - Phisher spoofs the logo or website of a well-known corporation or individual so their email request appears legitimate.
  - Contact HR department, posing as a trusted source, to get info(W2, SS#, etc..)

- To avoid a phishing attack:
  - Pay attention to anything that may be slightly wrong with an email, including misspellings, strange syntax, or logos that have been slightly altered.
  - Never to click on a link within an email. For example, if an employee is contacted by their bank and encouraged to reset a password, it’s best to go directly to the bank’s website.

A Personal Example of Phishing

Can you spot indicators that this is a phishing email?



UL

UMB Library <umblibraryaccont@gmail.com>

Tue 2/13, 7:14 AM

Long B Nguyen

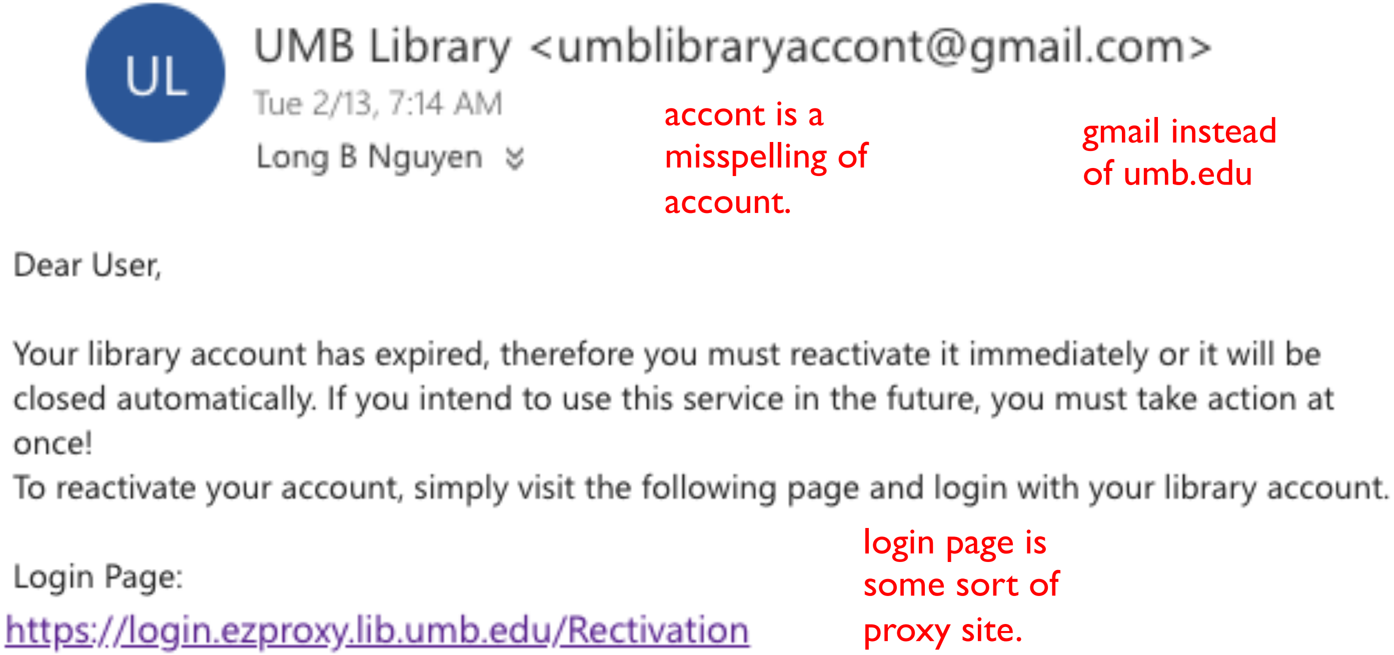
Dear User,

Your library account has expired, therefore you must reactivate it immediately or it will be closed automatically. If you intend to use this service in the future, you must take action at once!
To reactivate your account, simply visit the following page and login with your library account.

Login Page:
https://login.ezproxy.lib.umb.edu/Rectivation

A Personal Example of Phishing

Can you spot indicators that this is a phishing email?



UL

UMB Library <umblibraryaccont@gmail.com>

Tue 2/13, 7:14 AM

Long B Nguyen

Dear User,

Your library account has expired, therefore you must reactivate it immediately or it will be closed automatically. If you intend to use this service in the future, you must take action at once!
To reactivate your account, simply visit the following page and login with your library account.

Login Page:
https://login.ezproxy.lib.umb.edu/Rectivation

accont is a misspelling of account.

gmail instead of umb.edu

login page is some sort of proxy site.

misspelling

Coding Injection

hackers can use text fields to inject code to manipulate database info on the server.

Enter username: ‘john’; DROP TABLE users;

Enter password: ‘password123’

The SQL command DROP TABLE users; instructs the SQL database to delete all users.

- This is the reason why special characters like semicolons are not allowed in text fields. Client-side Javascript will catch this error and block it from being sent to the server.

With more sophisticated attacks, hackers can add new admin accounts, get access to confidential data.

Security

Security boils down to two questions:

- Who are you?
- What should you have access to?

Access should be given to authorized people and refused to the wrong people.

To differentiate between authorized/unauthorized personnel, we use **authentication,** the process by which the computer understand who it’s interacting with.

Authentication

There are three types of **authentication**.

- What you know: based on a secret knowledge known only to the real user and the computer. For example, username and password.
- What you have: based on the possession of a secret token that only the real user has. For example, a physical key and lock.
- What you are: based on YOU! You authenticate by presenting yourself to the computer.
  - **Biometric authenticators**: e.g. fingerprint readers and iris scanners.

What You Know

Username/Password

- Easy to implement, can be compromised if hackers can guess or find out.
- Some are easy for humans to figure out: e.g. 1234 or 1111
- Computers can try to **brute force** all password combinations. For example, a 4-digit ATM pin only as 10,000 combinations. 0000 to 9999.
  - Some systems will lock you out after 3 failed attempts.
  - But what if hackers have taken over many thousands of computers, trying a random pin like 1056 even once on thousands of computers can gain access to one or more bank accounts.
  - A famous successful brute force attack = The Fappening(See slide #24)
- Many websites now requires upper/lower case, numbers and special symbols to explode the number of combinations.
  - An 8-digit pin has 100,000,000 combinations. But an 8-character password has 600 trillion combinations.

LastPass and KeePass can store passwords safely

Chrome browser can also store it securely on the cloud

Nand Mirroring

One ineffective type of attack is brute forcing login credentials, e.g. try all combinations of passwords.

most systems defend against this type of attack by locking the user out after a certain number of tries.

Nand mirroring is one hack around this.

- attach wires to memory chip and make a perfect copy of its contents.
- try some password combinations, if the system is locked up, reflash the memory with original copy thereby resetting it and allowing the hacker to try new passwords immediately.
- nand mirroring was effective, for example, on an IPhone 5C.

What You have

What you have: based on the possession of a secret token that only the real user has. For example, a physical key and lock.

- You can open the door if you have the key.
- Avoid the problem of being guessable.
- Harder for remote attacker
- But can be compromised if hacker is close by: keys can be copied, phones can be stolen, even locks can be picked.

What You are

- what you are: based on YOU! You authenticate by presenting yourself to the computer.
    - Biometric authenticators: e.g. fingerprint readers and iris scanners.
    - secure but can be expensive.
    - data over sensors varies over time.

- what you know and what you have methods are **deterministic**
    - **deterministic**: always predicting the same output from a given input.
    - if you know the password or have the key, you’re granted access 100% of the time, if you don’t, you’re granted access 0% of the time.

What You are

- biometric authenticators are **probabilistic**
  - **probabilistic**: element of chance is involved, different output may come from the same input.
  - if lighting is bad or you’re wearing glasses, there’s a chance that the system won’t recognize you.
  - Or worse, it can recognize someone who is not you! (Your twin)

- biometric authenticators can’t be reset
  - what if your hacker compromises your fingerprint?
  - it’s possible to forge an iris by capturing a photo

Access Control

- After authentication comes **access control**.
    - specification on who should be able to see, modify and use what.

- **permissions** or **Access Control Lists(ACL)**, which describes what access each user has for ever file, folder and program on the system.
    - For example, share a google doc. Some users can only read it; while others can modify it.

Permissions

read: allow user to see contents of file.

write: allow user to modify contents of the file

execute: allow user to run the file.

You have set some of these settings(read/write) when you share documents through Google docs, for example .

Permissions

For organizations with users of different access privilege(spy agency), it’s important to configure permissions correctly to ensure secrecy, integrity and availability.

Say there are three levels of access: public, secret, top secret. There are 2 rules of read/write.(Bell Lapdula Model)

- People shouldn’t be able to “read up”, e.g., if you are only cleared to secret files, you shouldn’t be able to read top secret files. But you should be able to access secret and public files.
- People shouldn’t be able to “write down”, e.g. if someone has top secret clearance, they can read/write top secret files but cannot write down to secret and public files. Why?
    - This guarantees that there is no accidental leakage of top secret information to secret and public files.

There are other models(Chinese Wall or Bida Model)

Hackers

white hats: hackers hired to evaluate systems security, find bugs and security holes in software.

black hats: malicious hackers who intend to steal, exploit, sell private data.

- Blackhat(2015); Chris Hemsworth.

  (not sure if I can believe Thor is a hacker.)

why hackers hack:

- for curiosity and amusement
- for monetary gain(**cybercriminals**)
- promote a political or social goal(**hacktivists**)

How Hackers Hack

most common way hackers get into a computer system isn’t by hacking; it’s by tricking people into letting them in.

social engineering: a person is tricked into revealing confidential information.

- most common type of attack is phishing. For example, an email from Bank of America asking to reset the password by clicking on a link to a Bank of America clone site. Login credentials is compromised if account holders attempt to log on.
- even if less than 1% of success rate, a million phishing emails can possibly yield thousands of accounts.
- **pretexting**: an attacker called a company and pretend to be from the IT department and convince a user to configure their computer in a compromising way.

Malware

emails can be a common delivery mechanism for **trojan horses**, programs that masquerade as harmless attachments, like a photo, but actually contain malicious software, called **malware**.

malware can take on many forms.

- some steal confidential data(**spyware**)
  - install keylogger, that records all your keystrokes and send them to a remote source.
- others encrypt data and demand a ransom(**ransomware**)
- **virus**: attach itself to a file or program and harm your computer if opened.
  - delete files, slow down computer
  - requires human interaction(running or opening the file)
- **worms**: similar to virus but can self-propagate without user interaction.

The Melissa Virus

the Melissa virus spread like wildfire back in 1999.

- the virus was contained in a Word document called LIST.DOC
- contains passwords to a number of adult websites and was named after a Miami dancer.
- if opened, the virus sent a copy of itself to the first 50 contacts in the users' Microsoft Outlook address book (as an email attachment
- if one of the 50 recipients of that email opened the attachment, 50 new people would receive a copy of the virus.
- The email traffic generated by this virus was enough to jam corporate networks, so much so that many large companies had to shut down their email services to protect themselves.
- it wasn't until someone actually opened up the infected Word document that the virus was actually able to do anything, so users could protect themselves from the virus simply by ignoring or deleting the email.

Worms and Botnets

When a new bug is discovered in a system, it’s called a **zero day vulnerability**.

- black hat hackers rush to exploit this before white hat hackers can patch the bug.
- This is why it’s important to update your software. These downloads are security patches.

If a bug is left open on enough systems, hackers can write a program that jumps from computer to computer automatically, called **worms**.

- worms are destructive because of their ability to self-propagate.
- If a hacker can take over many computers, they can be used together to form a **botnet**. Botnets can be used to send large volumes of spam, using other computer’s power and electricity and launching DDoS attacks.

The Conflicker Worm

The Conflicker worm, first detected in November of 2008, created one of the largest botnets in the history of the Internet.

- The worm targeted vulnerabilities in the Windows operating system, and it was able to infect over ten million computers.
- it attacks banks and national defense networks, causing millions in damages.
- while difficult to remove at first, software utilities can now remove it.

ILOVEYOU Worm

The ILOVEYOU worm spread in 2000.

- While the Conficker worm created a huge botnet, the ILOVEYOU worm instead destroyed lots of files on infected computers.
- the worm targeted JPEG, MP3 and other important files.
- To spread itself to other computers, ILOVEYOU utilized both IRC, an early form of instant messaging, as well as email.
- ILOVEYOU one-upped the Melissa virus by emailing everyone in a user's address book, rather than just the first 50.

The Fappening

The Fappening was a successful brute force attack to obtain logins to Apple's iCloud service in 2014.

- Used Python script called "iBrute".
- Tried common passwords "jordan1", "charlie1", etc..
- Perpetrated through "Find My iPhone" app.
- iCloud did not take the precaution of blocking those accounts in which a login with repetitive attempts was being made.
- Intimate photographs of celebrities were hacked and published
- CEO Tim Cook forced to apologize and promise an improvement in security.
- Apple took a big financial and reputation hit right before iPhone6 was launched.

Sessions

When you log on a site, it uses cookies to remember you as you navigate to its different pages.

Logging on starts a browsing **session** that lasts until you log out or the session expired.

Each session has a unique identifier, usually generated randomly.

- Mike and Sara log on to their facebook accounts, Mike is given a session ID ABC123 and Sara the ID ABC456. This info is stored in a text file called a **cookie**.
- If the browser needs to inform who you are to the server, it reads the contents of this cookie file and sends the ID session without asking you to log in again.
- This can be done using the HTTP protocol.

HTTP Cookie Header

- The HTTP request for a session ID uses the **GET** method.
  - **GET**: requests data from a specified source
  - **POST**: sends data to a specified source.
- The HTTP cookie header looks something like this:

```
GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4
```

- This session ID, for example, is `5153d29ed84c4`.
  - The PHP part of the cookier refers to the web programming language PHP.

HTTP Cookie Header

```
GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4
```

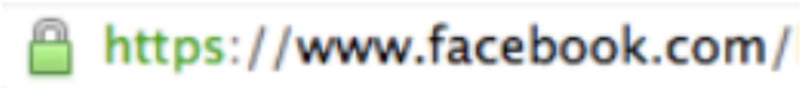
The HTTP header above is transmitted as readable text and unfortunately can be read easily by programs such as Wireshark and TCPDump.

Hackers who have access to the session ID can hijack the session and be able to have unauthorized access.

To transmit secure session IDs, HTTPS is used.

HTTPS

Sites like Facebook and Google use HTTPS to transmit information such as session IDs. Note the green padlock below.



https://www.facebook.com/

HTTPS is the protocol that combines HTTP with **Transport Layer Security(TLS)**.(also called **TLS/SSL**, **Secure Socket Layer(SSL)** is the older standard)

Sending session IDs with HTTPS look like this instead:

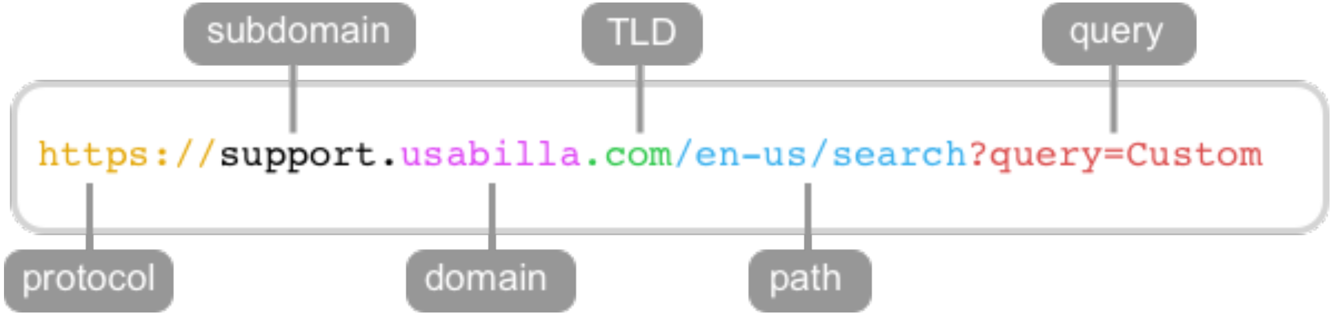
d2VsbCBhcmVuJ3QgeW91IGNsZXZlcg

In addition to HTTPS, wireless security protocols such as **WEP, WPA and WPA2** are used to encrypt network traffic.

- WEP has been cracked. WPA2(Wi-Fi Protected Access 2) is the newer version of WPA and is the current standard for wireless connection.

Uniform Resource Locator(URL)

Uniform Resource Locator(URL) also known as a web address is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.



the www is one of many subdomains(www., secure., blog., webmail.)

Some URL may include a port number.

Uniform Resource Locator(URL)

The URL can have **query string parameters** to send additional information to the server.

- after the path, ? begins a query string.
- Uses key-value pairs.
- Uses + for string concatenation.
- Uses & for multiple parameters.

Example: The following URL has three query parameters.

http://www.example.com/products/search/?q=chinese+food&sessionID=1234&p=true

Above, q is the key and “chinese food” is the value.

Try to use query string parameters to search for something without going to the Google homepage.

Cross-Site Request Forgery(CSRF)

- Hackers can use sessions and URLs to exploit users. One such attach is **cross-site request forgery(CSRF).**
- A user who logs into his bank account on a browser tab and then visit CNN still has not logged out of his bank account!
- Suppose you log into your bank account and transfer your money to a savings account(#67890). A possible URL:

https://bank.com/money/transfer?to=67890&amount=100

- That URL doesn't need to include the account number the money is coming from, since the server assumes that the account you're currently logged into is the source of the funds.

Cross-Site Request Forgery(CSRF)

- A hacker can send out a phishing email, asks the user to log on to his bank account and click on a link to reset his password:

https://bank.com/password/reset

- The URL above, however, actually redirects to:

https://bank.com/money/transfer?to=12345&amount=100

which transfers money to a different account(#12345).

- Most banks safeguards from such CSRF attacks by generating random tokens.

https://bank.com/money/transfer?to=67890&amount=100&token=8549ba93417cdef85

Homework

1)Read and reread these lecture notes.

2)Read:

- https://www.huffingtonpost.com/2012/06/08/linkedin-password-leak-infographic_n_1581620.html
- https://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet
- http://fortune.com/2017/06/22/cybersecurity-hacks-history/

3)Net neutrality:

- http://theopeninter.net/
- https://arstechnica.com/tech-policy/2011/01/huge-isps-want-per-gb-payments-from-netflix-youtube/

References

1) Part of this lecture is a recap of the following an episode from PBS Crash Course in Computer Science series.

PBS Crash Course in Computer Science. Cybersecurity. Retrieved from https://www.youtube.com/watch?v=bPVaOlJ6ln0

2) Computer Science E-1 at Harvard Extension School

Understanding Computers and the Internet by Tommy MacWilliam. Retrieved from http://cse1.net/video?v=lectures/6/lecture6