ISOM 5280
Threats & Attacks

HKUST
BUSINESS SCHOOL
香港科大商學院
WORLD CLASS IN ASIA

MSc

Prof. Weiyin Hong

Department of ISOM, HKUST Business School

Fall 2024

Reading

- [WM], Chapter 1 and 2
- Paying attention to security news in the media helps!

Table of Contents

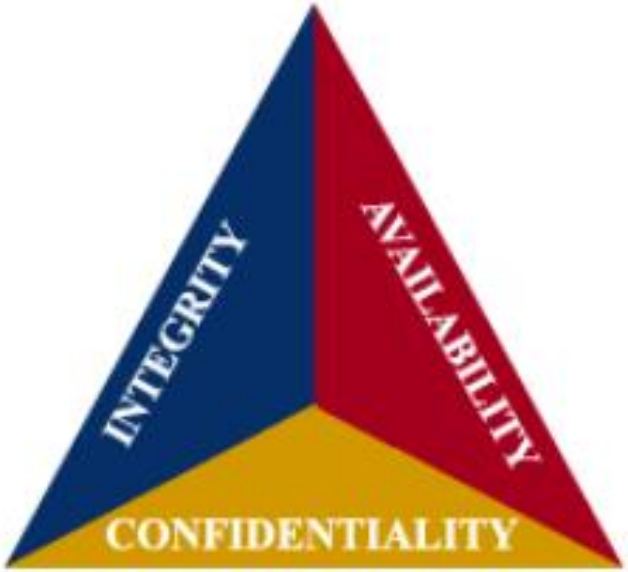
The CIA Triad

Common threats

- Malware
- Communication interception
- Social engineering
- Software flaw
- Service interruption
- Others
- Emerging threats (e.g. AI)

The CIA Triad

Examine Threat from The CIA Triad



- Threat is an event that can cause negative impact to an organization.
  - Confidentiality is a set of rules that limits access to information.
  - Integrity is the assurance that the information is trustworthy and accurate.
  - Availability is a guarantee of reliable access to the information by authorized people.

Mapping attacks to CIA Triad

	Confidentiality	Integrity	Availability
Malware			
Ransomware			
DDoS			
…			
…			
…			
..			

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

Emerging Threats

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

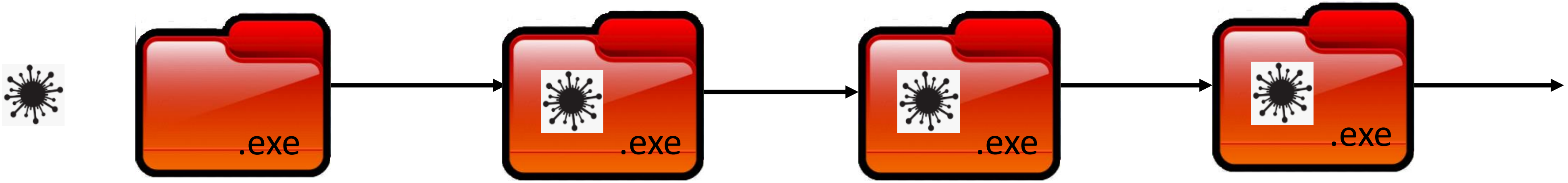
Emerging Threats

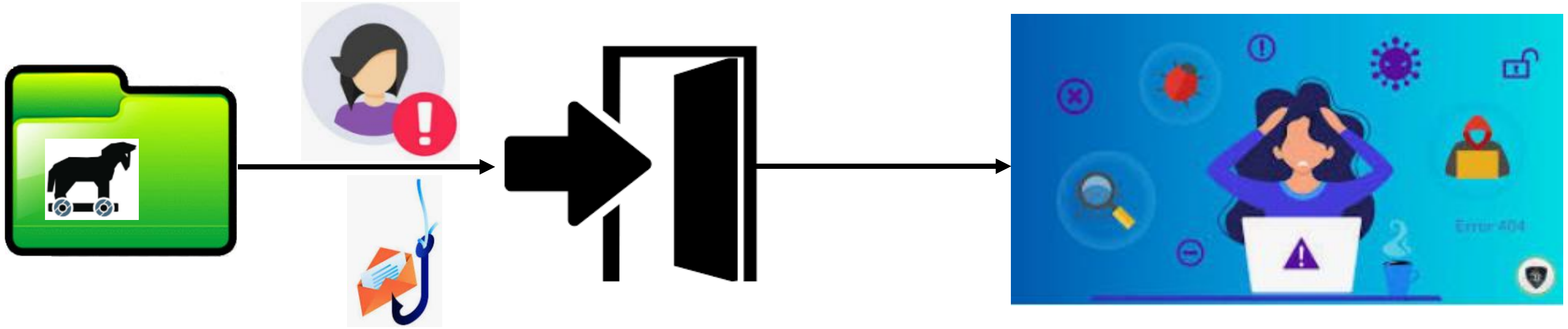
© Prof. Weiyin Hong 2024

Malware

- Virus: replicates by attaching to some executable files; aims to modify files or damage systems
- Worm: similar to virus, with the additional “strength” that it can survive and replicate on its own without the need to attach to something else
- Trojan horse: disguises its real purpose and is installed by users inadvertently
- Ransomware: a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

Virus/Trojan Horse





Worms

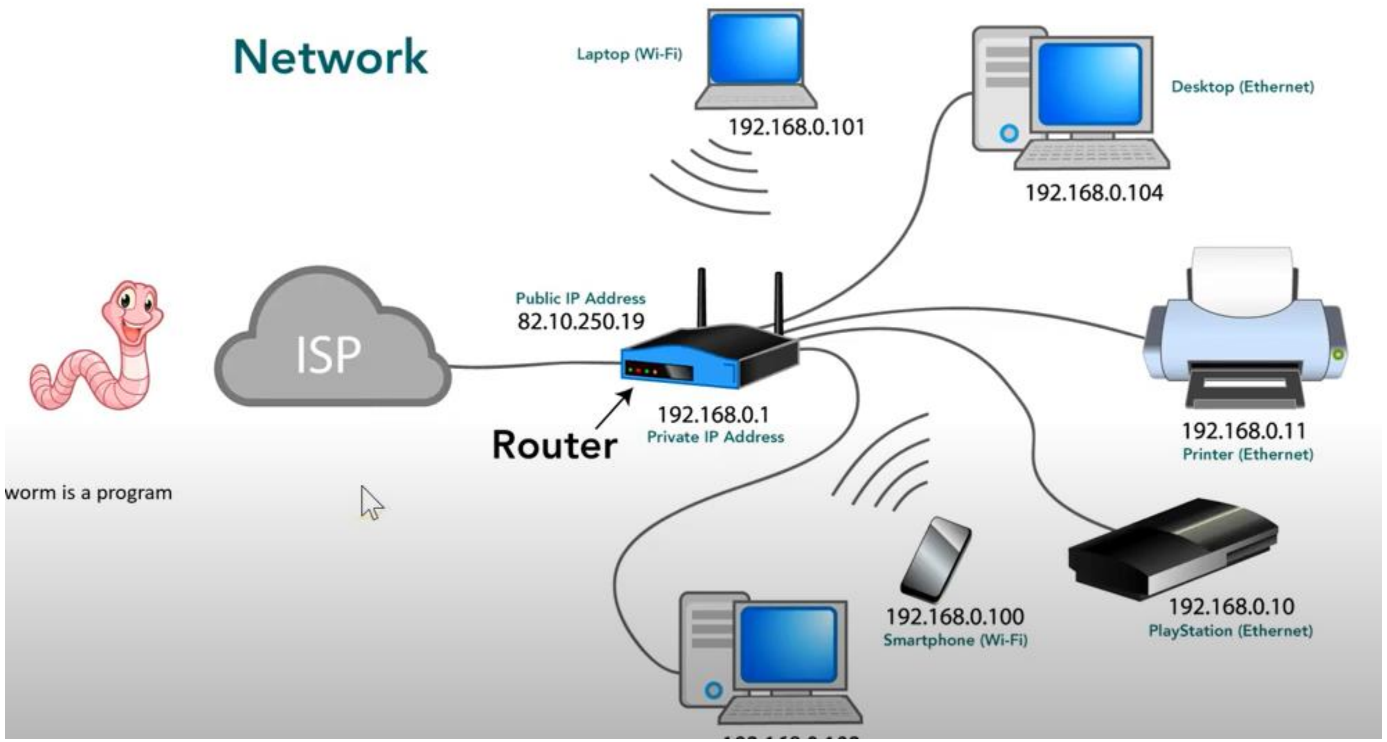


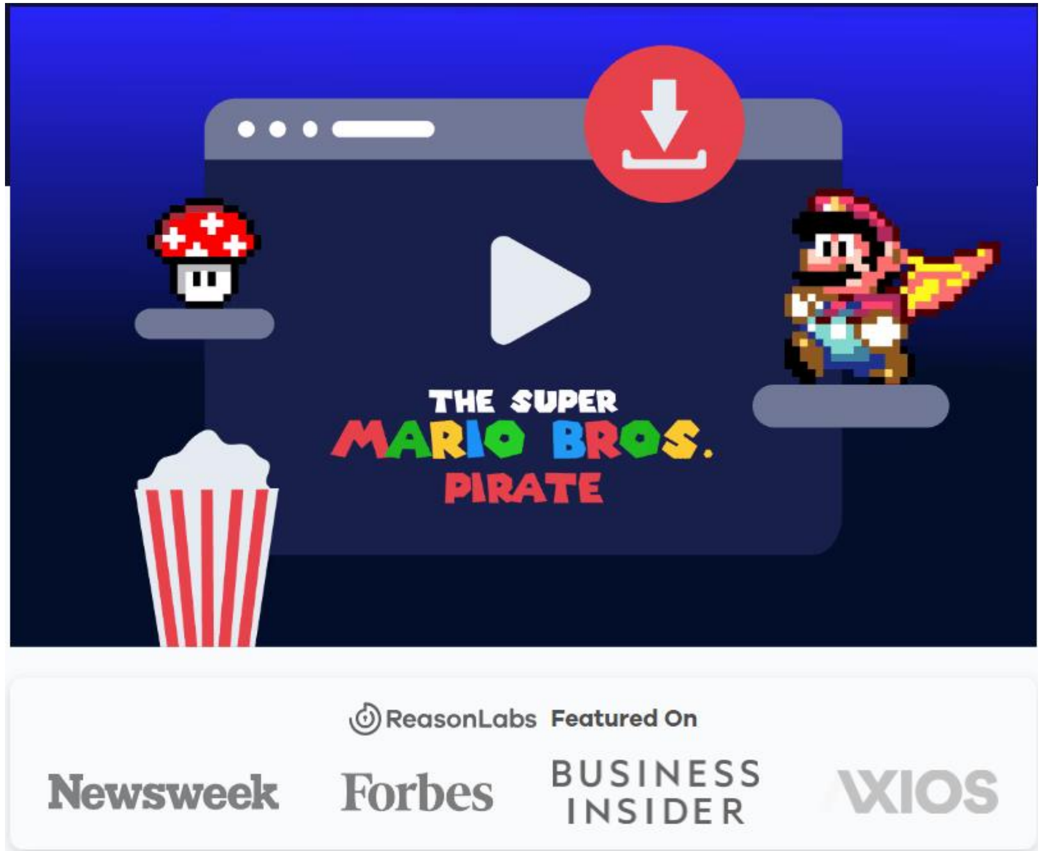
Image Source: Mr. Powell's Computer Science Channel

- Self replicating and exploring
- May carry other payload
- Causing congestion
- May carry good intention
- Taking actions without consent

So…

1. Which one of three doesn’t replicate itself? Trojan
2. Which one can clog the Internet? Worm
3. Which one(s) must “live off” other legitimate files? Virus and Trojan
4. Which one spreads the fastest? Worm

TRUE STORY



How The Trojan Affects Users

Browser hijacking changes the settings of a user's web browser without their consent. They usually change a user's homepage or their default search engine. They also might install unwanted applications or add-ons. The objective of a browser hijacker is often to redirect a user's searches to a different engine or to display unwanted ads, which in turn can generate a profit for the cyber attacker.

The malicious extension is hijacking the users' web search functions by giving itself numerous sensitive browser permissions. Because it's a local extension, it can't be removed from the Google Chrome Web store. Moreover, it's not supervised or inspected by the Google Chrome Web store team and therefore is not bound by security restrictions.

The Trojan replaces the primary browser DLLs to control the default search bar and injects its own DLL by writing to the AppInit registry key. We can also infer that because of the wide effort put into the distribution of the Trojan and the evasion techniques used by the attacker, the extension may execute further actions after an update or a period of time.

Countermeasures?

1) Update OS and patches
2) Install antivirus software
3) don't download files from an untrusted network or website
4) Make sure your browser's set to request your permission before running pop-ups, files, or programs from the internet.
5) Don't open files from people you don't know, or files from people who may not have a reason to message you directly
6) Regular backups of critical data must be made and stored on preferably read-only media such as CDs and DVDs.
7) Scan external storage devices on an isolated machine .

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

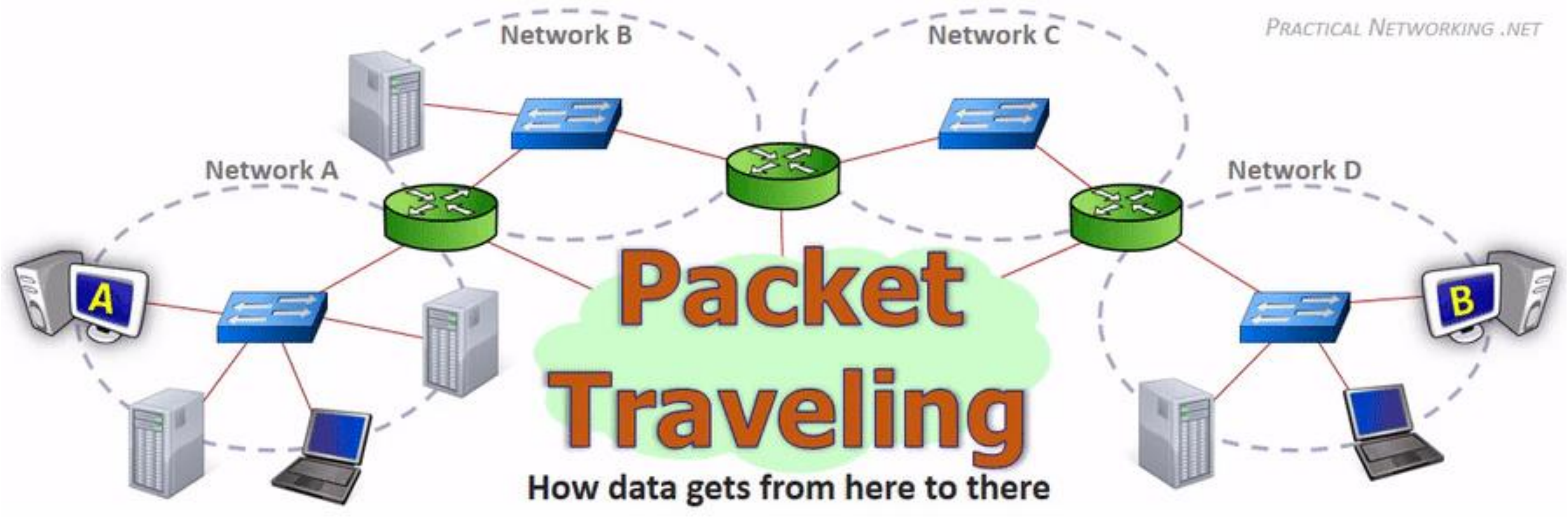
Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

Emerging Threats

© Prof. Weiyin Hong 2024

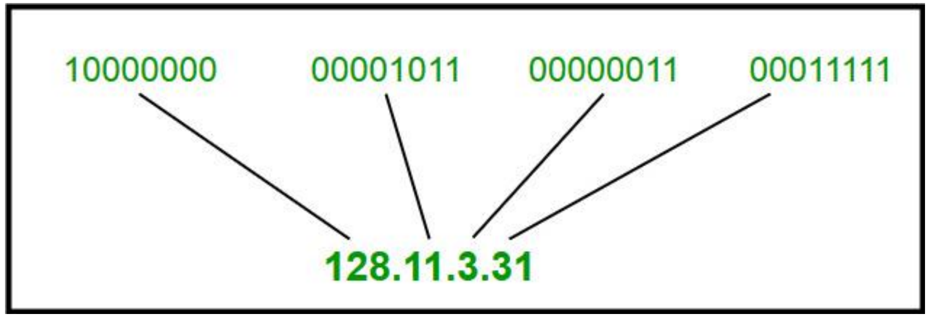
How Data Transmitted Over the Internet



Data are transmitted in the form of packets
A large piece of data will be broken into multiple packets

Types of IP Addresses: IPv4 and IPv6

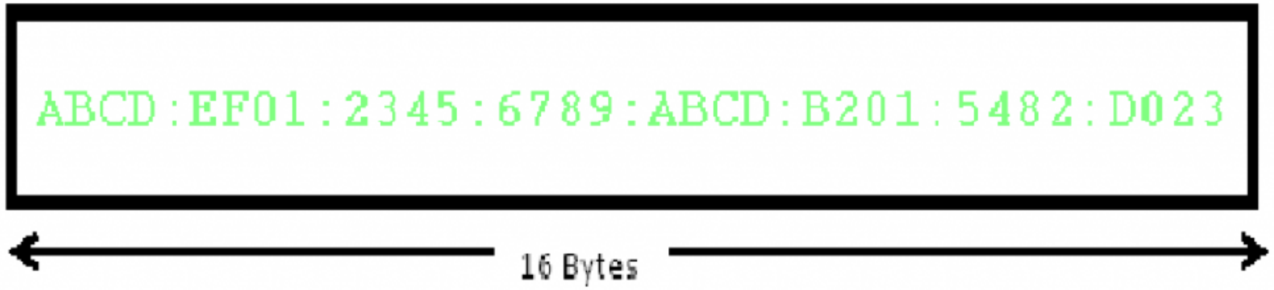
IPv4



10000000 00001011 00000011 00011111

128.11.3.31

IPv6



ABCD:EF01:2345:6789:ABCD:B201:5482:D023

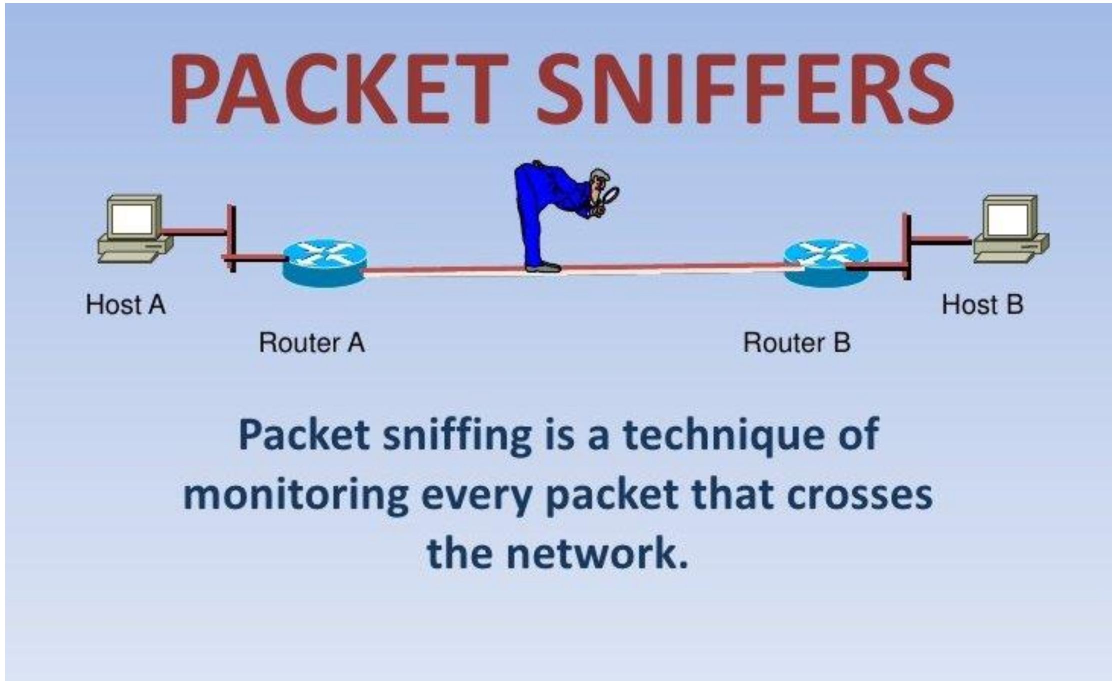
16 Bytes

Seems quite different from URL we typically use, e.g., www.google.com?

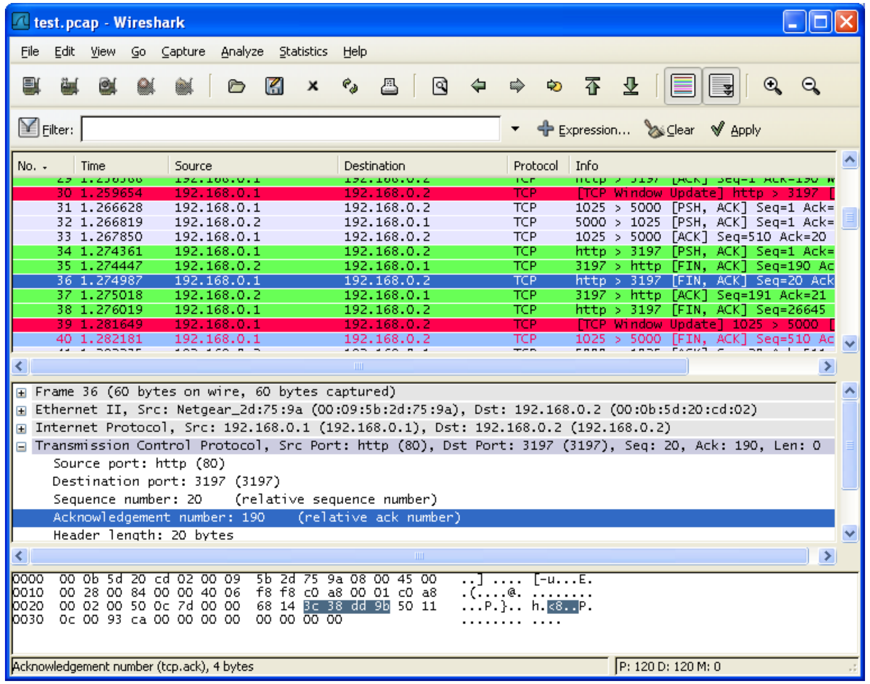
What can someone do to your package?

© Prof. Weiyin Hong 2024

1) Packet Sniffer



Packet sniffing is a technique of monitoring every packet that crosses the network.



```
No. - Time      Source        Destination   Protocol Info
   30 1.259654  192.168.0.1   192.168.0.2   TCP      [TCP Window Update] http > 3197 [
   31 1.266628  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [PSH, ACK] Seq=1 Ack=
   32 1.266819  192.168.0.2   192.168.0.1   TCP      5000 > 1025 [PSH, ACK] Seq=1 Ack=
   33 1.267850  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [ACK] Seq=510 Ack=20
   34 1.274361  192.168.0.1   192.168.0.2   TCP      http > 3197 [PSH, ACK] Seq=1 Ack=
   35 1.274447  192.168.0.2   192.168.0.1   TCP      3197 > http [FIN, ACK] Seq=190 Ac
   36 1.274987  192.168.0.1   192.168.0.2   TCP      http > 3197 [FIN, ACK] Seq=20 Ack
   37 1.275018  192.168.0.2   192.168.0.1   TCP      3197 > http [ACK] Seq=191 Ack=21
   38 1.276019  192.168.0.1   192.168.0.2   TCP      http > 3197 [FIN, ACK] Seq=26645
   39 1.281649  192.168.0.1   192.168.0.2   TCP      [TCP Window Update] 1025 > 5000 [
   40 1.282181  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [FIN, ACK] Seq=510 Ac
```

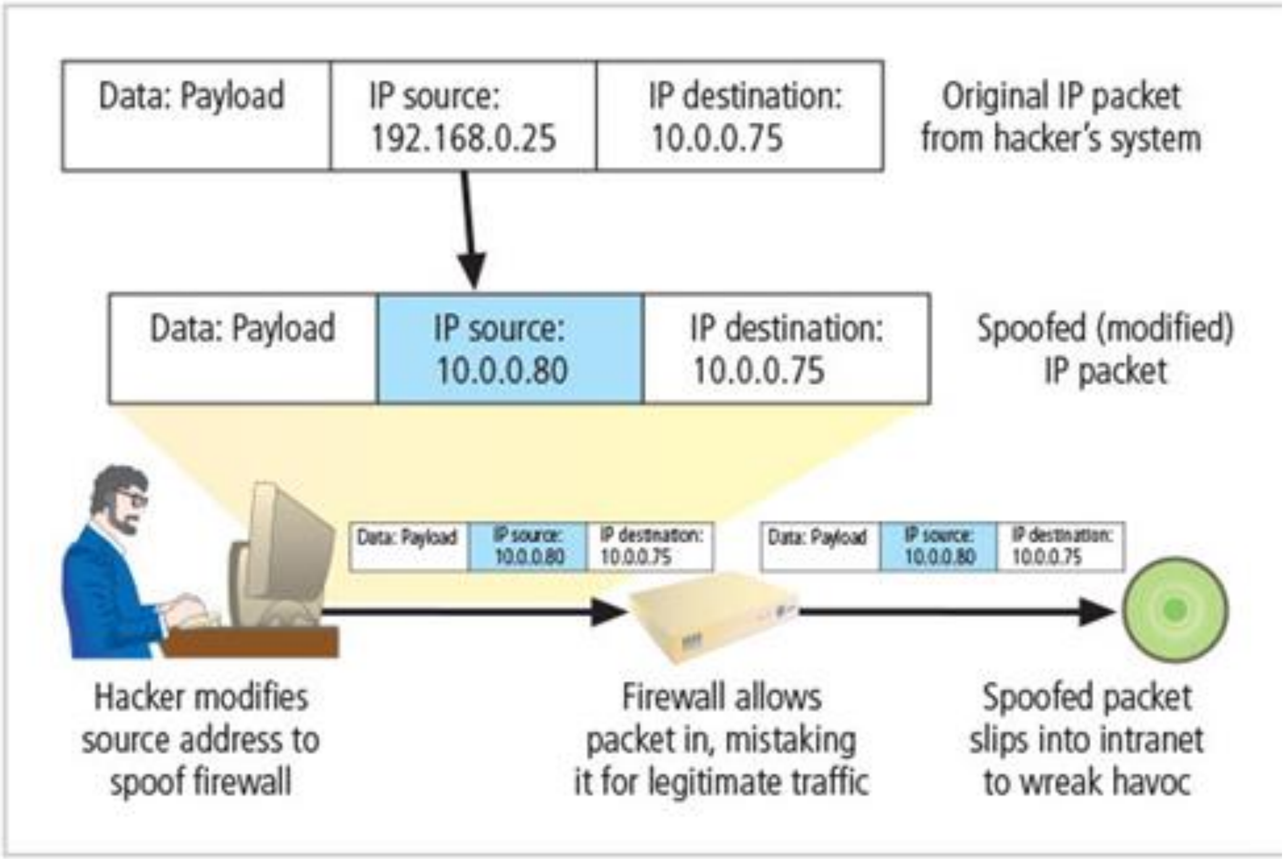
```
⊞ Frame 36 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, Len: 0
    Source port: http (80)
    Destination port: 3197 (3197)
    Sequence number: 20    (relative sequence number)
    Acknowledgement number: 190    (relative ack number)
    Header length: 20 bytes
```

```
0000  00 0b 5d 20 cd 02 00 09  5b 2d 75 9a 08 00 45 00   ..] .... [-u...E.
0010  00 28 00 84 00 00 40 06  f8 f8 c0 a8 00 01 c0 a8   .(....@. ........
0020  00 02 00 50 0c 7d 00 00  68 14 3c 38 dd 9b 50 11   ...P.}.. h.<8..P.
0030  0c 00 93 ca 00 00 00 00  00 00 00 00               ........ ....
```

Acknowledgement number (tcp.ack), 4 bytes   P: 120 D: 120 M: 0

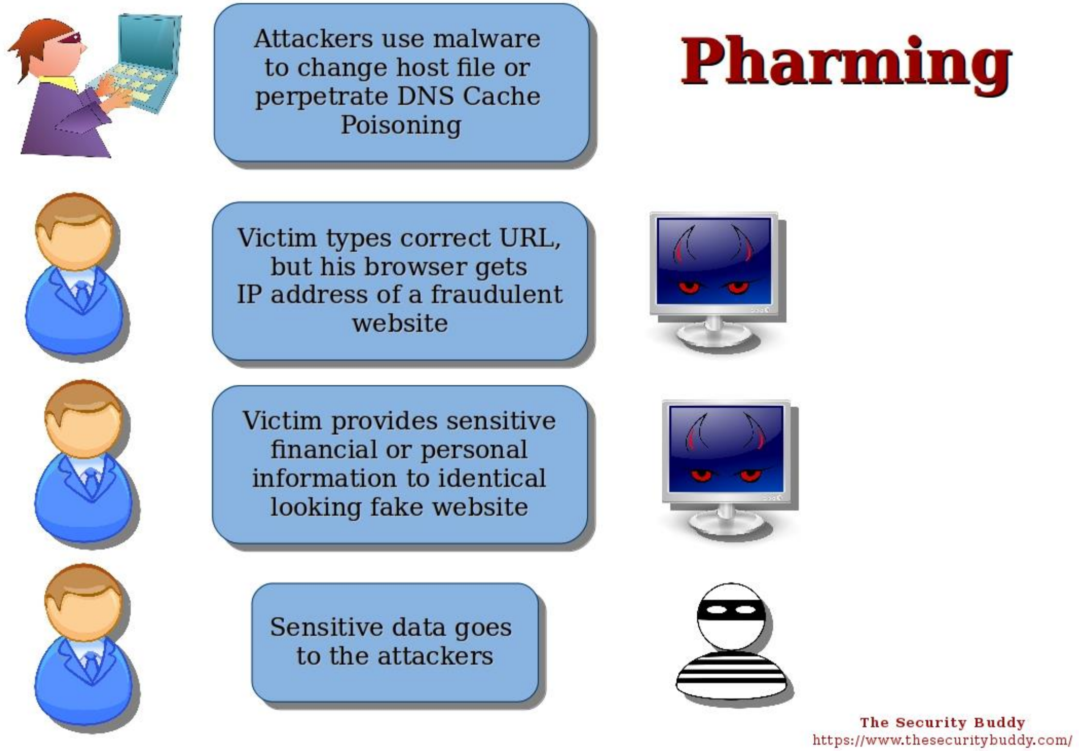
© Prof. Weiyin Hong 2024

2) IP Spoofing


Data: Payload
IP source: 192.168.0.25
IP destination: 10.0.0.75
Original IP packet from hacker's system
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Spoofed (modified) IP packet
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Data: Payload
IP source: 10.0.0.80
IP destination: 10.0.0.75
Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking it for legitimate traffic
Spoofed packet slips into intranet to wreak havoc

Source: [WM], chapter 2

3) Pharming



Pharming

Attackers use malware to change host file or perpetrate DNS Cache Poisoning

Victim types correct URL, but his browser gets IP address of a fraudulent website

Victim provides sensitive financial or personal information to identical looking fake website

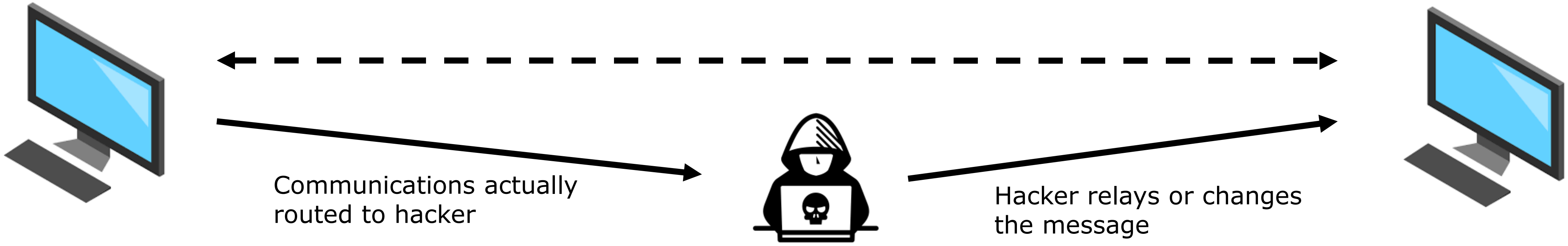
Sensitive data goes to the attackers

The Security Buddy
https://www.thesecuritybuddy.com/

https://www.youtube.com/watch?v=20FAWUVo3as

4) Man-in-the-Middle Attack

- Attacker places him/herself in the middle of communication between two targets
  - e.g., by compromising the network routers in either/both targets' networks
  - May relay, modify, or even block communication contents entirely


Communications actually routed to hacker
Hacker relays or changes the message

Man-in-the-Middle Attack

TRUE STORY

- Internet Service Provider **Comcast used JavaScript to substitute its ads** for advertisements from third-party websites. This kind of MitM attack is called code injection. The web traffic passing through the Comcast system gave Comcast the ability to inject code and swap out all the ads to change them to Comcast ads or to insert Comcast ads in otherwise ad-free content.

Q & A [www.menti.com]

- **Which one is the hardest to detect but easiest to defend against?**

- **Sniffing**

Countermeasures?

- firewall
- intrusion detection system
- prevent malware be installed

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Phishing
- Vishing

Social Engineering

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

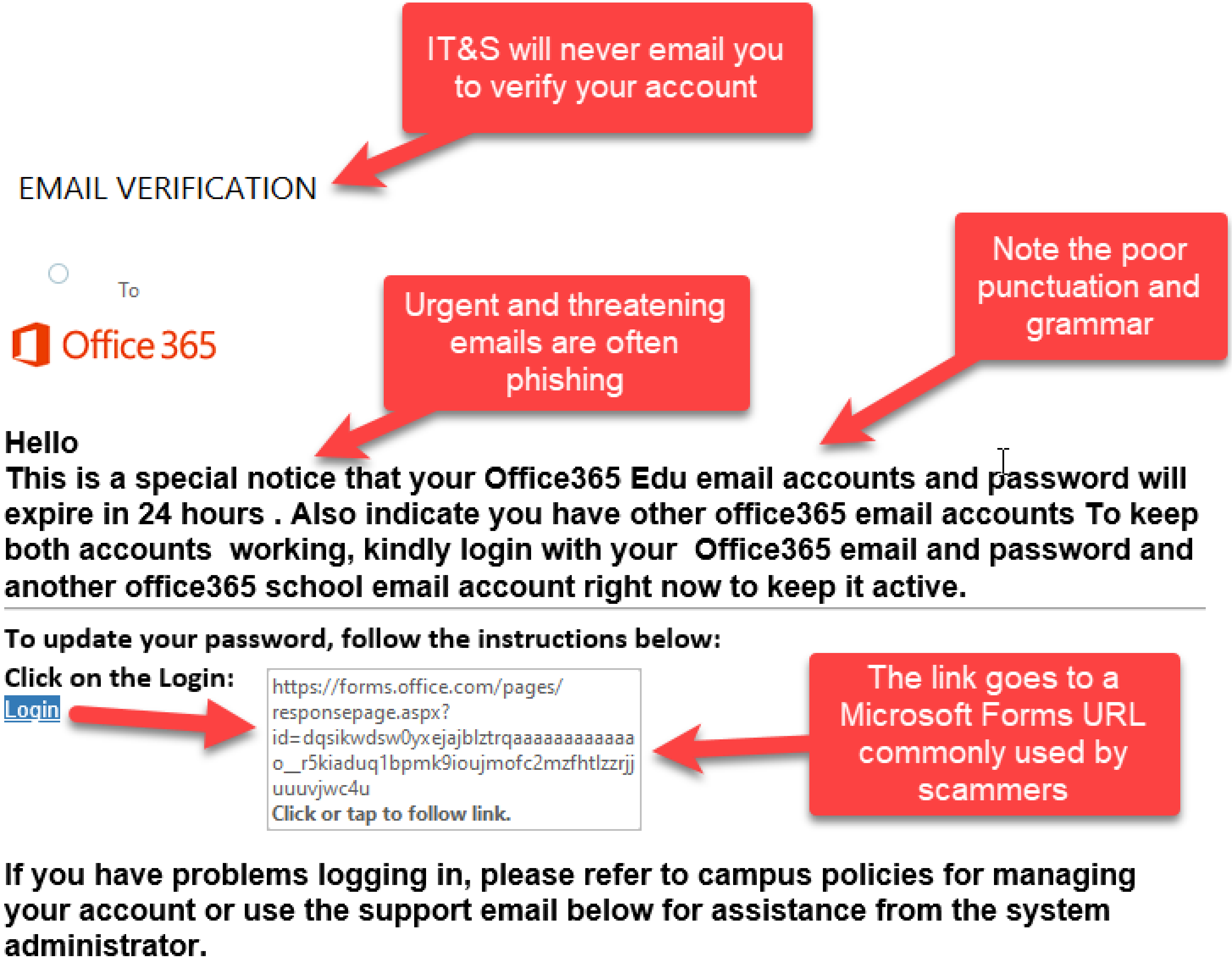
Service Disruption

- Supply chain attack
- Generative AI attacks
- Deepfake scams

Emerging Threats

© Prof. Weiyin Hong 2024

Phishing Emails



IT&S will never email you to verify your account

EMAIL VERIFICATION

○ To

Office 365

Urgent and threatening emails are often phishing

Note the poor punctuation and grammar

Hello
This is a special notice that your Office365 Edu email accounts and password will expire in 24 hours . Also indicate you have other office365 email accounts To keep both accounts working, kindly login with your Office365 email and password and another office365 school email account right now to keep it active.

To update your password, follow the instructions below:

Click on the Login:
Login

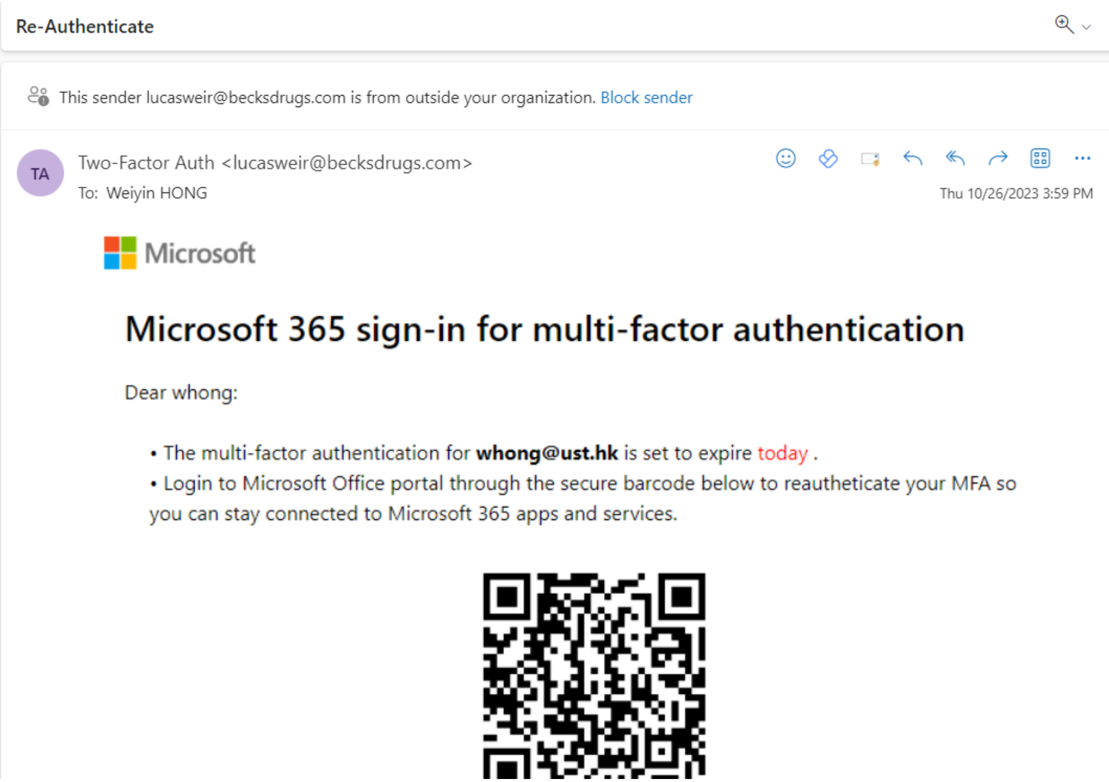
https://forms.office.com/pages/responsepage.aspx?id=dqsikwdsw0yxejajblztrqaaaaaaaaaaaao__r5kiaduq1bpmk9ioujmofc2mzfhtlzzrjjuuuvjwc4u
Click or tap to follow link.

The link goes to a Microsoft Forms URL commonly used by scammers

If you have problems logging in, please refer to campus policies for managing your account or use the support email below for assistance from the system administrator.

© Prof. Weiyin Hong 2024

Information Technology Services Center



This sender lucasweir@becksdrugs.com is from outside your organization. Block sender

Two-Factor Auth <lucasweir@becksdrugs.com>
To: Weiyin HONG
Thu 10/26/2023 3:59 PM

Microsoft

Microsoft 365 sign-in for multi-factor authentication

Dear whong:

- The multi-factor authentication for **whong@ust.hk** is set to expire today .
- Login to Microsoft Office portal through the secure barcode below to reautheticate your MFA so you can stay connected to Microsoft 365 apps and services.

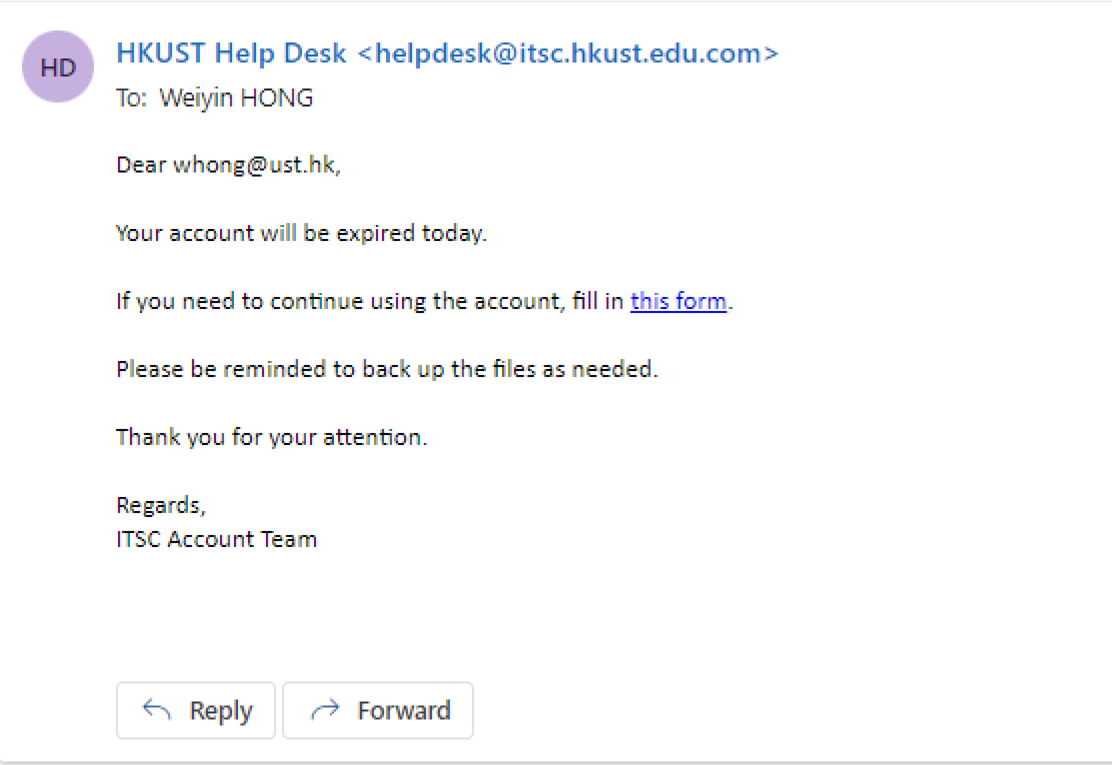
/hich is co
ıus link to

ng email.
tinuous e

ning oppo
e their un

ttachment
/ have fina
fection, as

ture. Thes
ı this topi


HKUST Help Desk <helpdesk@itsc.hkust.edu.com>
To: Weiyin HONG

Dear whong@ust.hk,

Your account will be expired today.

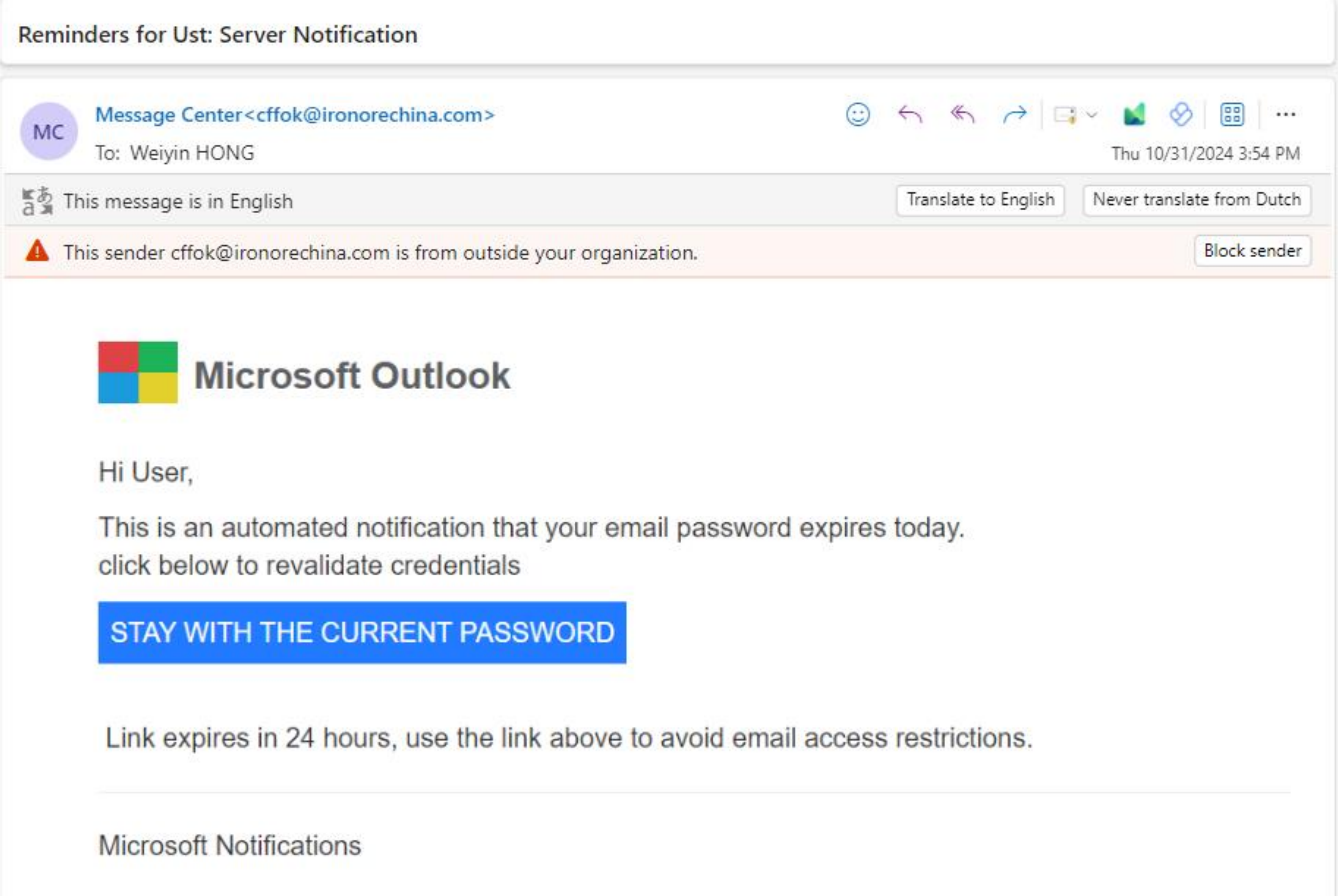
If you need to continue using the account, fill in this form.

Please be reminded to back up the files as needed.

Thank you for your attention.

Regards,
ITSC Account Team

Best Regards,
Bill Fung
IT Security Officer and Head (Cybersecurity Operations)



Reminders for Ust: Server Notification

Message Center<cffok@ironorechina.com>

To: Weiyin HONG

Thu 10/31/2024 3:54 PM

This message is in English

This sender cffok@ironorechina.com is from outside your organization.

Microsoft Outlook

Hi User,

This is an automated notification that your email password expires today.
click below to revalidate credentials

Link expires in 24 hours, use the link above to avoid email access restrictions.

Microsoft Notifications

Social Engineering

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

- "People are the weakest link!" – By Kevin Mitnick, the infamous hacker
  - Lack or improper training
  - Inexperience
  - Mistakes
  - Lack of awareness

- Kevin Mitnick. Talks at google. https://www.youtube.com/watch?v=aUqes9QdLQ4

Social Engineering

it could install malicious software, did you know this?

https://www.youtube.com/watch?v=aP8yrkkLWlM

Countermeasures?

- Conduct regular phishing awareness programs and simulation for all staff
- Maintain a principle of least privilege for each user group and account.
- Remove or disable commonly abused and non-essential services, if appropriate.

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

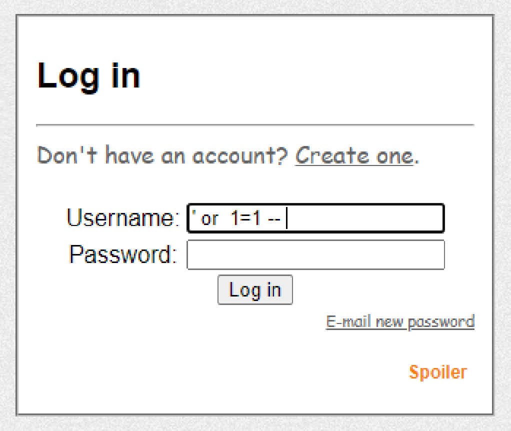
Emerging Threats

SQL Injection

- When developers fail to properly validate user input before using it to query a relational database, one may gain access to unauthorized information.

```
SELECT * FROM customers WHERE username = ‘Joe’ AND password = ‘xyz123$’
```

```
SELECT * FROM customers WHERE username = ‘ or 1=1 --  AND password = ‘ ’
```



Log in

Don't have an account? Create one.

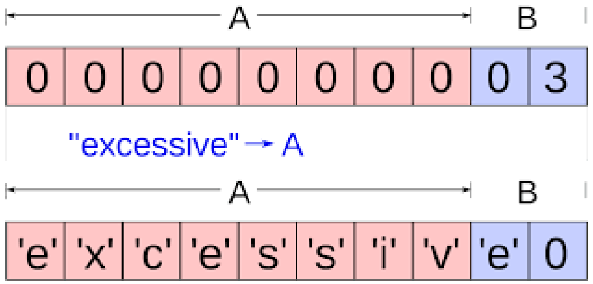
Username: ' or 1=1 --

Password:

```
SELECT * FROM customers WHERE username = '' or
1=1 -- ' AND password = '';
```

Buffer Overflow

- A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space.
- This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.



- Assembly and C/C++ are popular programming languages that are vulnerable to buffer overflow, in part because they allow direct access to memory.
- Python, JAVA, COBOL, are less vulnerable.

Countermeasures?

- Hire better IT team
- Increase IT budget

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

Emerging Threats

© Prof. Weiyin Hong 2024

Do you think that the hackers want you to know that they are in?

© Prof. Weiyin Hong 2024

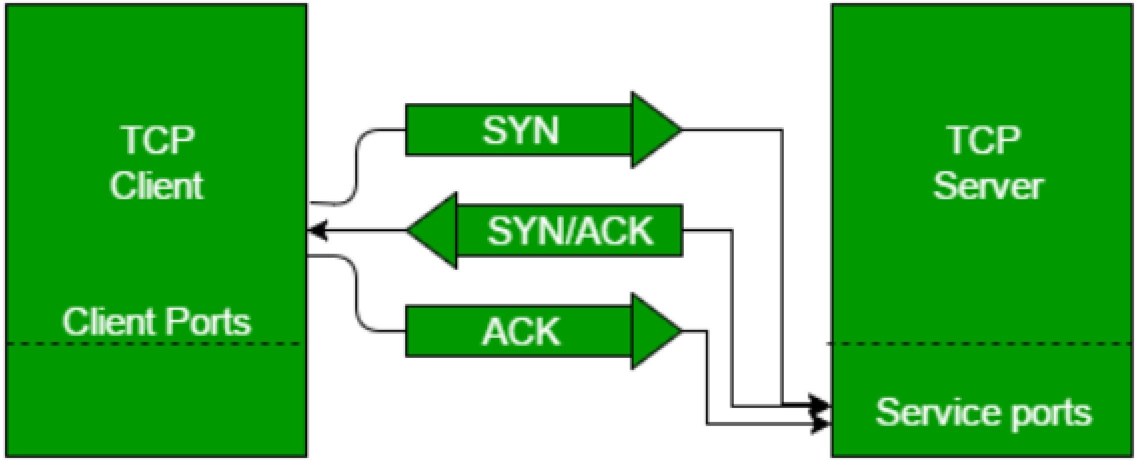
Common Denial of Service (DoS)

– Purpose: disrupts service provision and so business continuity by making a server “busy”

– Method: hackers send thousands of false requests to “flood” a server so that it cannot respond to other legitimate users

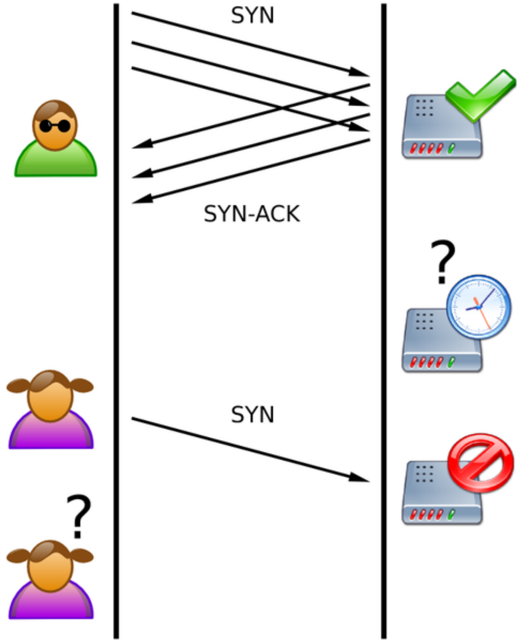
Common DoS

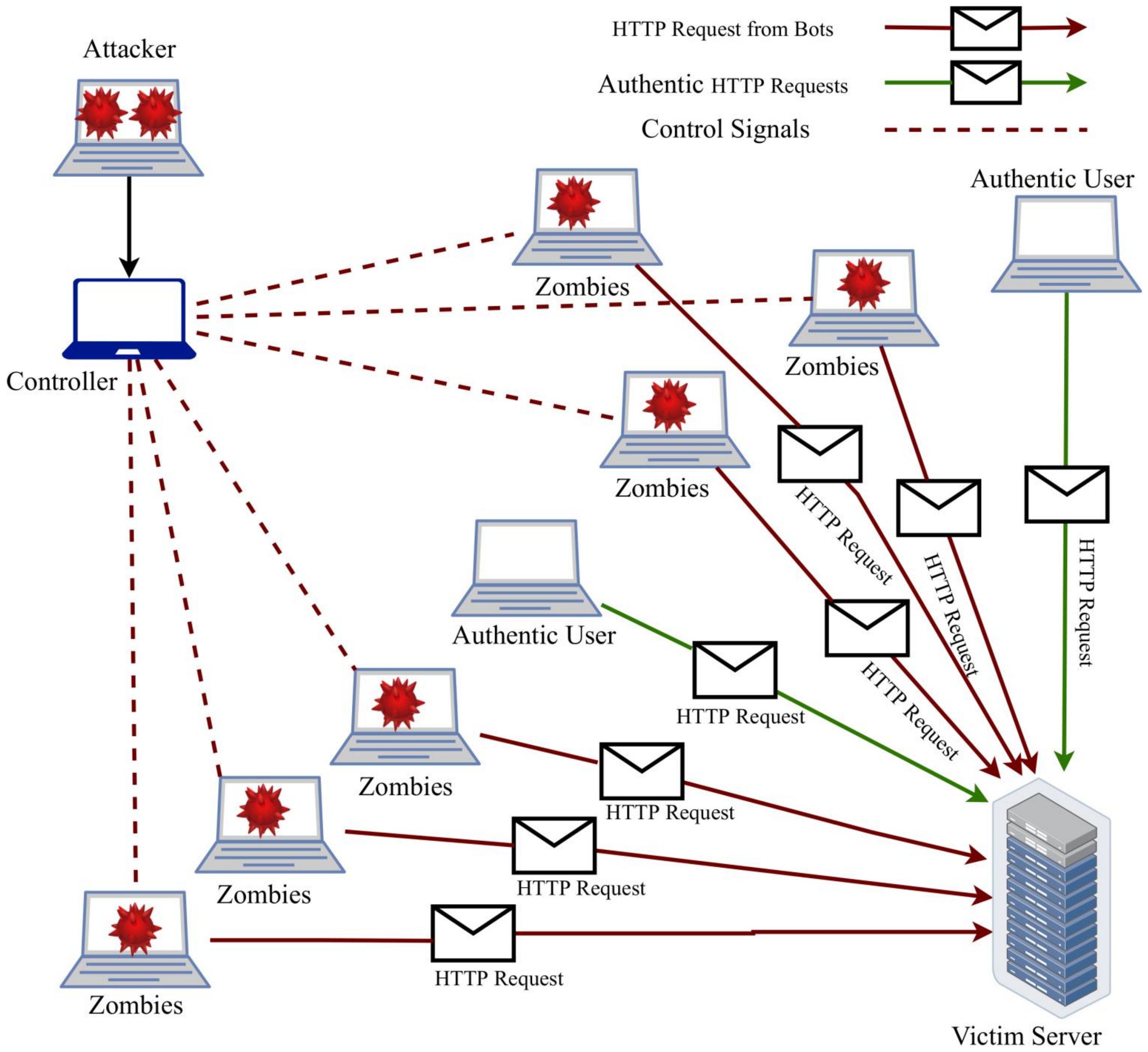
- SYN flooding: exploits TCP three-way handshake feature to establish connections



Common DoS

- Two typical ways
  - Malicious client not sending ACK back to server
  - SYN request started by a spoofed IP address





Distributed DoS (DDoS)

- Often sent from "zombies".
- More sophisticated attacks involve distributed zombies, hence the name DDoS.

Botnet Arithmetic

Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	Starts to fill typical ISP backbone
100,000	1.0 Mbps	100 Gbps	
1,000,000	1.0 Mbps	1000 Gbps	

The average botnet size is now about 20,000 computers (*Wikipedia)*

- **ZeuS (13 million+)**
- **Storm (about 2 million)**
- **Mariposa (23 million)**
- **ZeroAccess (9 million)**

TRUE STORY

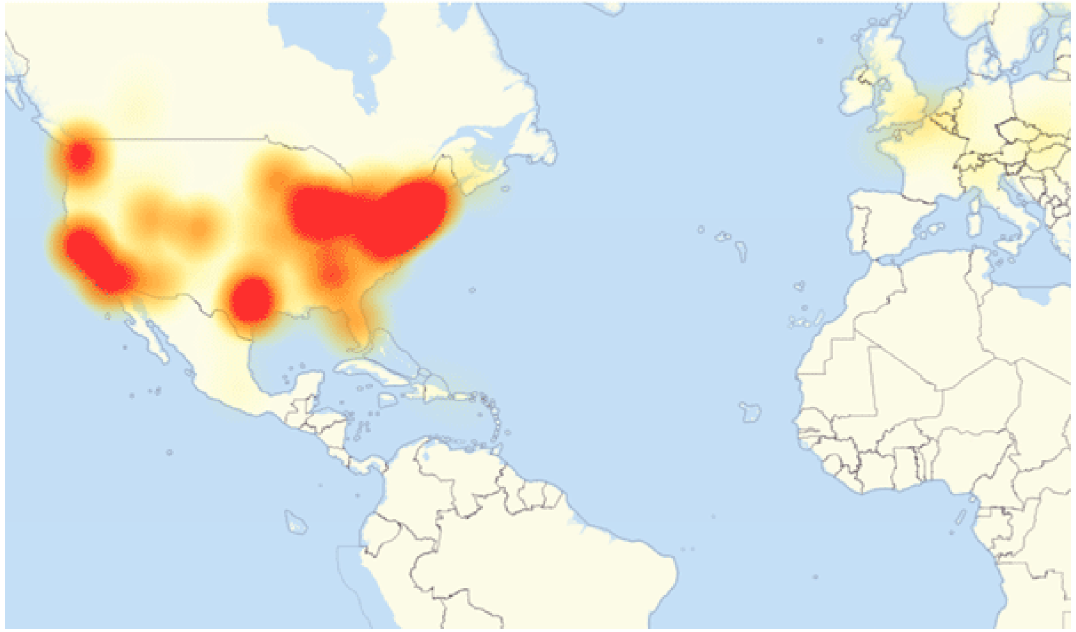
AWS, Google, and Cloudflare 2023

Google 2020

AWS 2020

Mirai DYN 2016

Github 2018



Countermeasures?

- Largely technical
- Work with reliable cloud service providers, ISP, and police

edgenext
How Does AI Help Detect and Prevent DDoS Attacks in Modern Networks
www.edgenext.com
</>

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

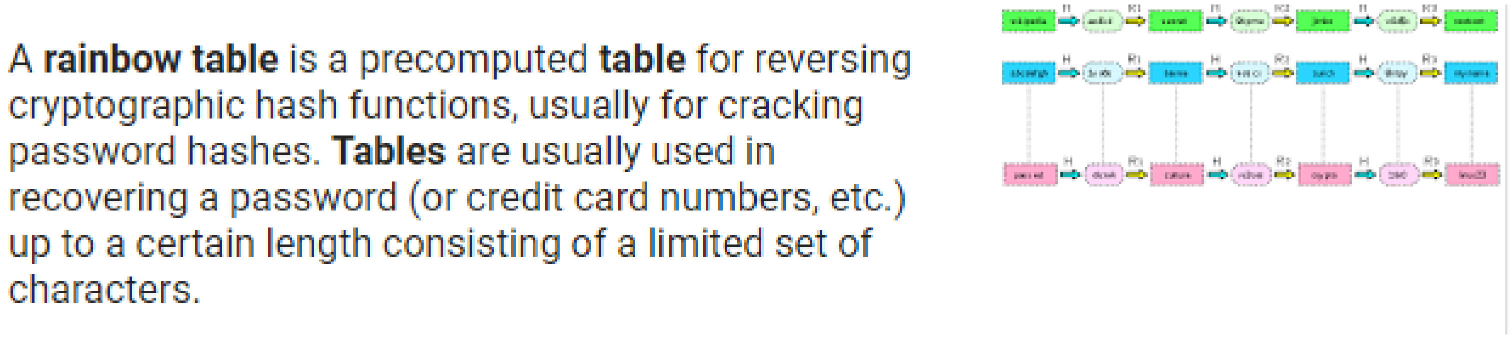
- Supply chain attack
- Generative AI attacks
- Deepfake scams

Emerging Threats

© Prof. Weiyin Hong 2024

(1) Password Cracking

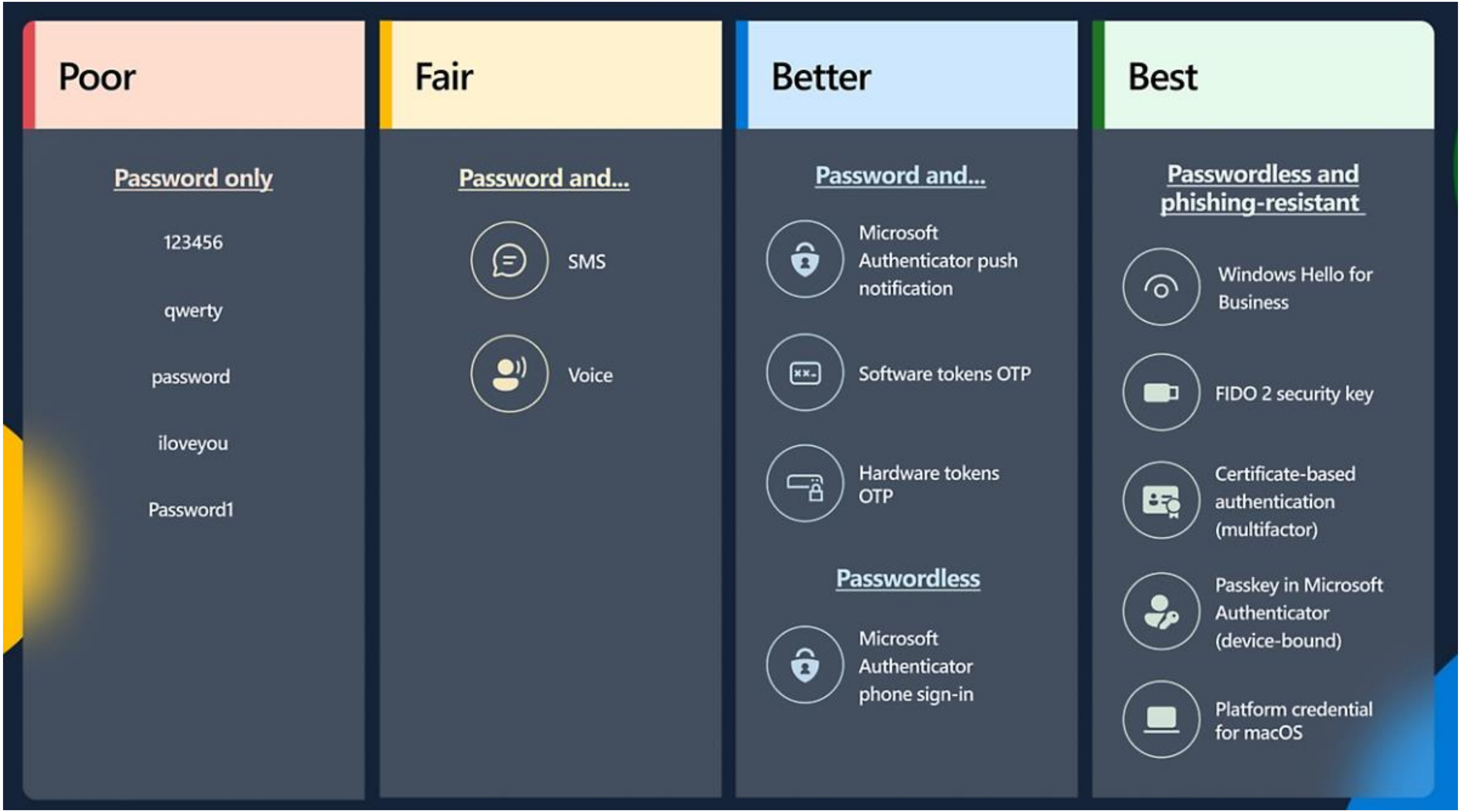
- Guessing – birthday, ID, name, etc.
- Dictionary attack – repeatedly try dictionary words until access is granted
- Brute-force attack – exhaustively try all combinations of characters
  - – *Success primarily depends on ???*
- Rainbow table



A **rainbow table** is a precomputed **table** for reversing cryptographic hash functions, usually for cracking password hashes. **Tables** are usually used in recovering a password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters.

Countermeasures?

How do you manage your passwords to ensure their safety?



Poor

Password only

- 123456
- qwerty
- password
- iloveyou
- Password1

Fair

Password and...

- SMS
- Voice

Better

Password and...

- Microsoft Authenticator push notification
- Software tokens OTP
- Hardware tokens OTP

Passwordless

- Microsoft Authenticator phone sign-in

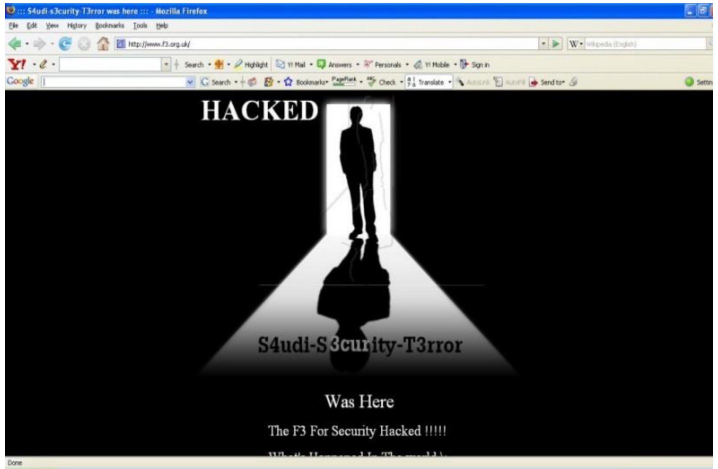
Best

Passwordless and phishing-resistant

- Windows Hello for Business
- FIDO 2 security key
- Certificate-based authentication (multifactor)
- Passkey in Microsoft Authenticator (device-bound)
- Platform credential for macOS

(2) Sabotage or Vandalism

- Involve deliberate sabotage of a computer system or acts of vandalism to destroy an asset or damage the image of an organization.


::: S4udi-s3curity-T3rror was here ::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.f3.org.uk/
Done

HACKED

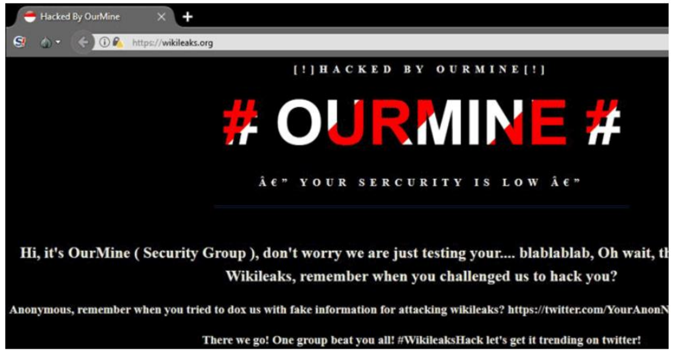
S4udi-S3curity-T3rror

Was Here

The F3 For Security Hacked !!!!!

Oops! WikiLeaks Website Defaced By OurMine

August 30, 2017 Wang Wei



[!]HACKED BY OURMINE[!]

OURMINE

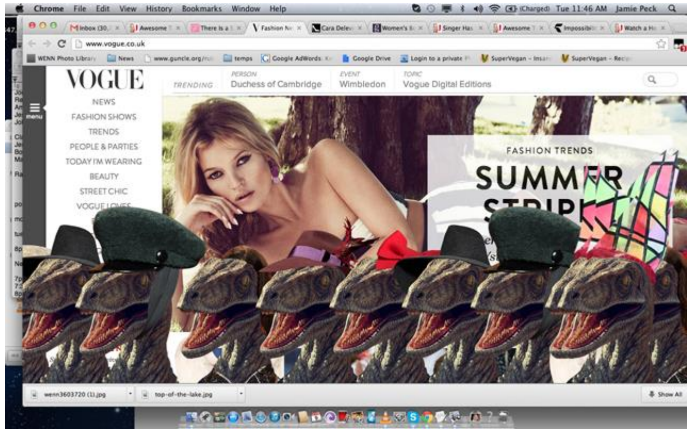
Â€" YOUR SERCURITY IS LOW Â€"

Hi, it's OurMine (Security Group), don't worry we are just testing your.... blablablab, Oh wait, th
Wikileaks, remember when you challenged us to hack you?

Anonymous, remember when you tried to dox us with fake information for attacking wikileaks? https://twitter.com/YourAnonN

There we go! One group beat you all! #WikileaksHack let's get it trending on twitter!

OurMine is in headlines once again—this time for defacing WikiLeaks website.



(3) IoT and IIoT

- IoT, Internet of Things, is often referred to a "smart" object. Everything from cars, home appliances to shoes and light switches that connect to the internet, passing and receiving data and connecting the physical world to the digital world are considered as smart object.

Hack All The Things: 20 Devices in 45 Minutes

1,308,318 views • Oct 2, 2014

https://www.youtube.com/watch?v=h5PRvBpLuJs

- ✓ Car!!
- ✓ CCTV Camera
- ✓ Smart bulbs
- ✓ Smart refrigerator
- ✓ Network printer
- ✓ Smart TV
- ✓ Home cloud storage
- ✓ Blue-Ray Player
- ✓ …
- ✓ …
- ✓ …

(3) IoT and IIoT

- IIoT, **Industrial** Internet of Things, are used for industrial purpose such as manufacturing, supply chain monitor and management system.
- IIoT connects critical machines and sensors in high-stakes industries such as aerospace, defense, healthcare and energy.
- These are the systems in which failure often results in life-threatening or other emergency situations.

(4) Cryptojacking

- Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.

© Prof. Weiyin Hong 2024

Threats and Attacks

- Virus/Worms/Trojan horse
- Extortion/Ransomware

Malware

- Packet sniffer
- Spoofing
- Pharming
- Man-in-the-middle

Communication Interception

- Phishing
- Vishing

Social Engineering

- SQL Injection
- Buffer overflow

Software Flaw

- DoS or DDoS

Service Disruption

- Password cracking
- Sabotage/Vandalism
- IOT and IIOT
- Crypojacking

Others

- Supply chain attack
- Generative AI attacks
- Deepfake scams

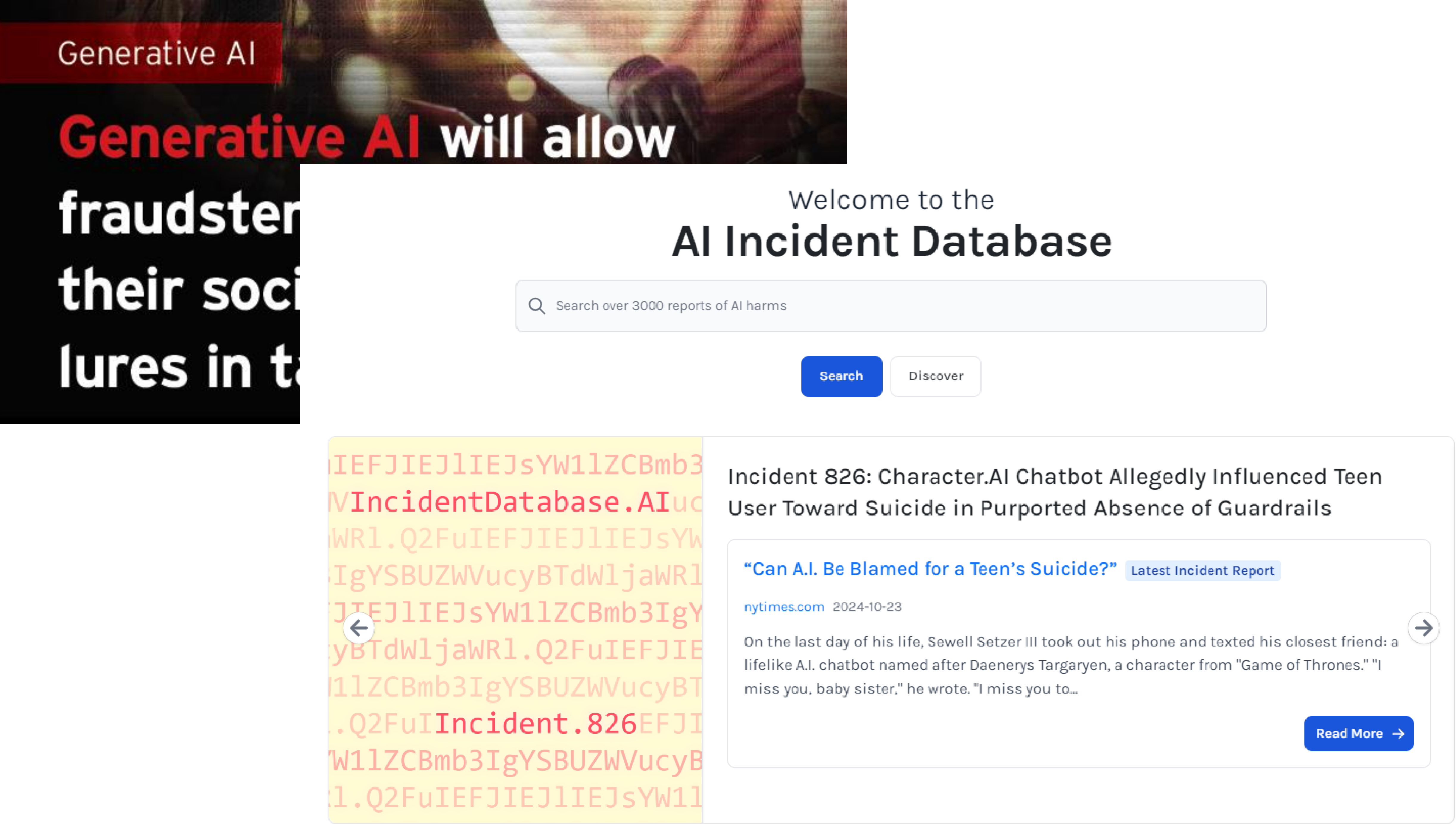
Emerging Threats

Supply Chain Attack

TRUE STORY

The SolarWinds attack is the most astonishing breach of 2020. The cybercriminal's creativity, persistence, and resources were rather remarkable.

https://www.youtube.com/watch?v=DWe2Fk0m7zo



Generative AI

Generative AI will allow
fraudster
their soci
lures in t

Welcome to the

AI Incident Database

Incident 826: Character.AI Chatbot Allegedly Influenced Teen User Toward Suicide in Purported Absence of Guardrails

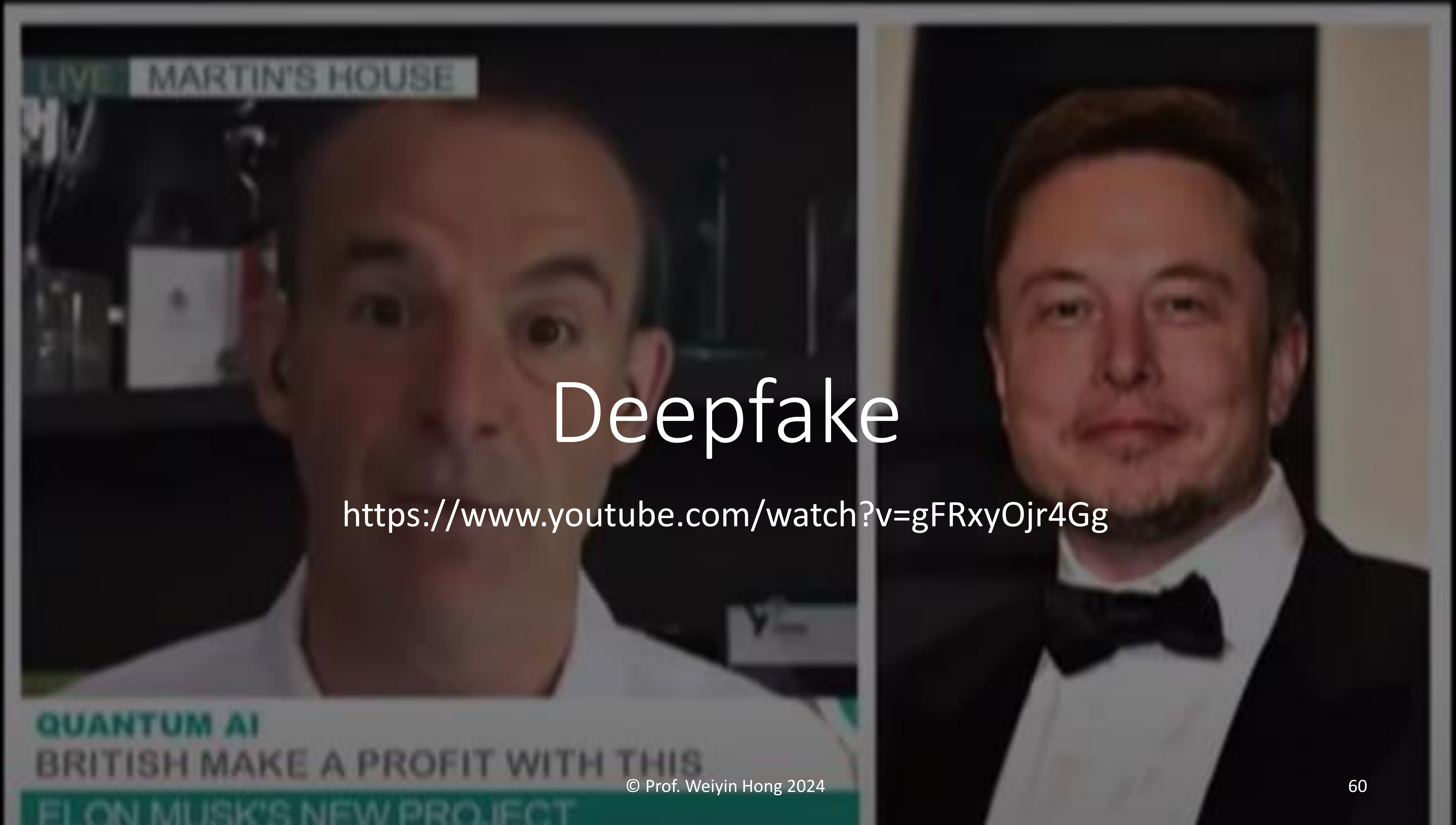
"Can A.I. Be Blamed for a Teen's Suicide?" Latest Incident Report

nytimes.com 2024-10-23

On the last day of his life, Sewell Setzer III took out his phone and texted his closest friend: a lifelike A.I. chatbot named after Daenerys Targaryen, a character from "Game of Thrones." "I miss you, baby sister," he wrote. "I miss you to...

Deepfake

https://www.youtube.com/watch?v=gFRxyOjr4Gg



Countermeasures?

Take-home Exercise:

- Mapping various types of attacks to the CIA Triad.

	Confidentiality	Integrity	Availability
Malware			
Ransomware			
DDoS			
…			
…			
..			