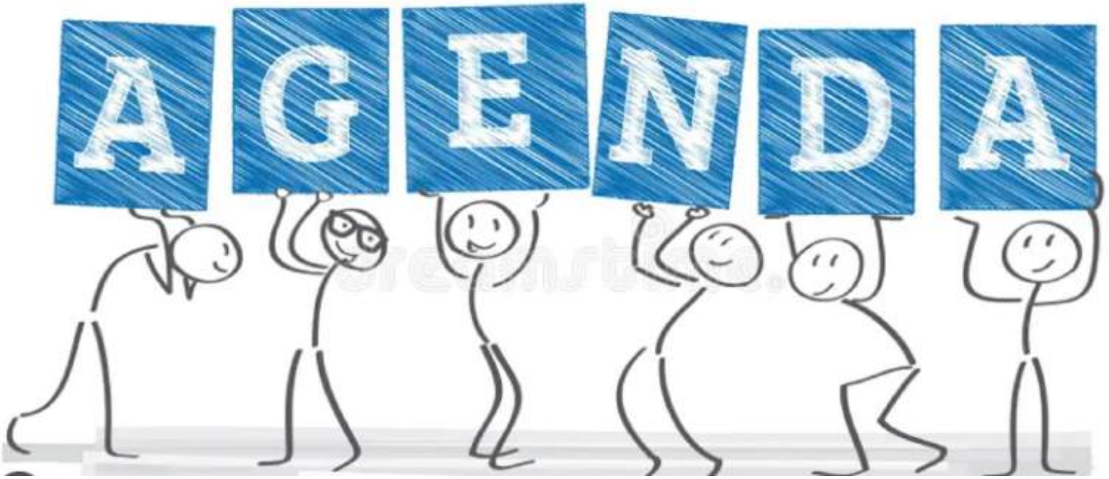
Cyber Security

Lecture 1.1

Overview of the Course

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Lecture Agenda



- Course Information and Protocol
- Cyber Security: A Bigger Picture
- Categories of Cyber Security
- History of Cyber Attacks
- Prerequisites of the Course
- A discussion on Course Modules

Course Info & Protocols

About the Instructor

Dr. Muhammad Arif Butt

Asst. Prof. at Department of Data Science
University of Punjab, Lahore
arif@pucit.edu.pk
https://www.linkedin.com/in/dr-arif-butt/
https://arif.phd
https://arifbutt.me

Education:

- Graduation from Pakistan Military Academy Kakul
- MPhil CS from University of Punjab, Lahore
- PhD CS from University of Punjab, Lahore

Experience:

- Served in field/staff/instructional posts in Pakistan Army
- Assistant Professor, Department of Data Science

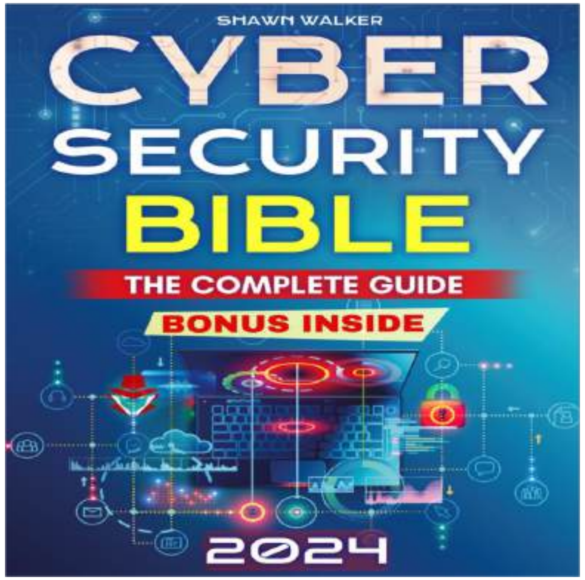
Research Interests:

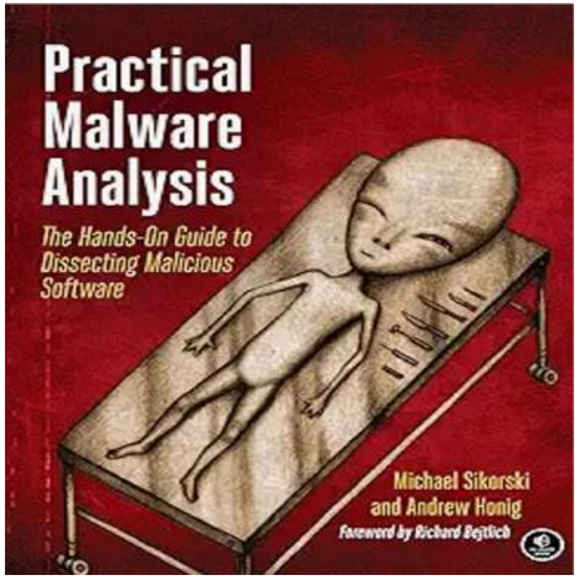
- Embedded and real time operating systems
- Vulnerability research and exploit development
- Cyber Security
- AI/LLM Security

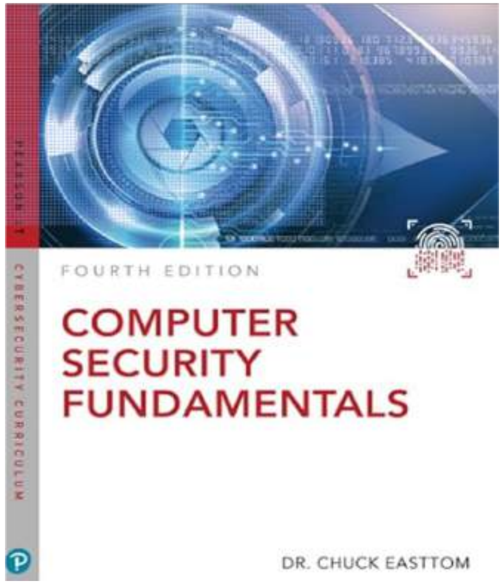
Course Information

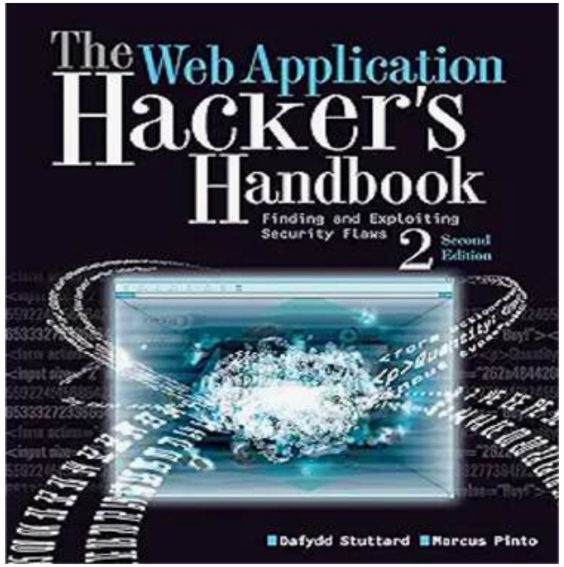
- Lectures Slides/Handouts Available at: https://arifbutt.me
- Video Lectures Available at: https://youtube.com/learnwitharif
- Codes Hosted at: https://github.com/arifpucit
- Grades Website: https://online.pucit.edu.pk
- Prerequisites:
  - OS and Internetworking with Linux
  - Basic programming skills in Python, C, and Assembly
- Office: Building-C, FCIT (NC)
- Students Counseling hours:
  - Mon: 0900 hrs – 1000 hrs
  - Tues: 1130 hrs – 1230 hrs
- 24 hour turnaround for email: arif@pucit.edu.pk

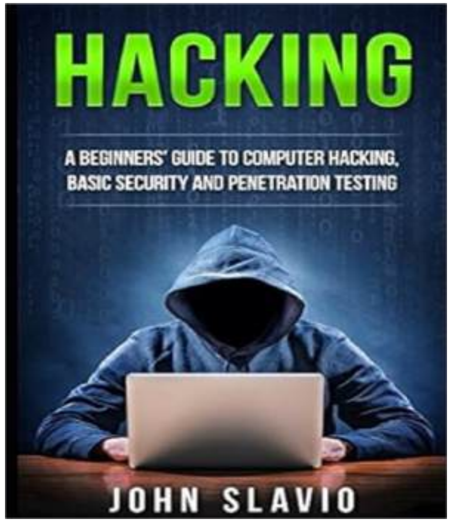
Text and Reference Books

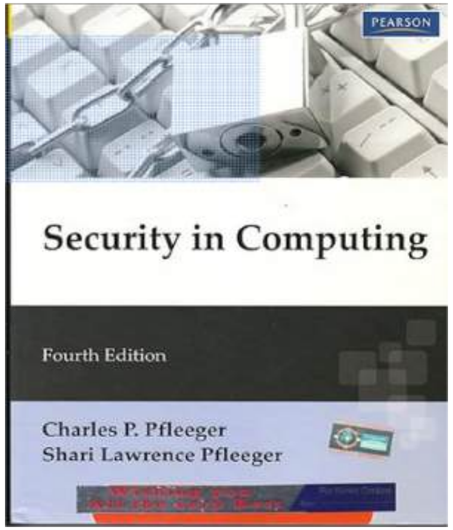


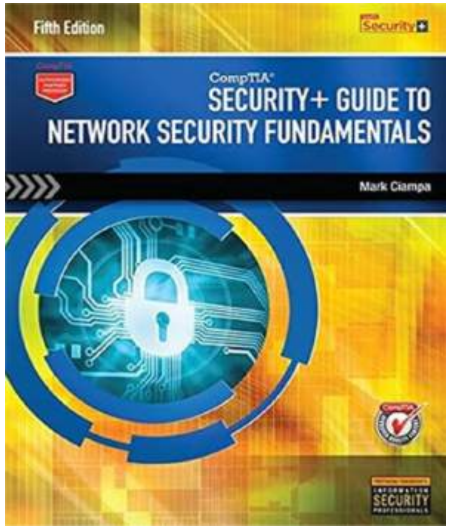

Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich


PEARSON IT CYBERSECURITY CURRICULUM
FOURTH EDITION
COMPUTER SECURITY FUNDAMENTALS
DR. CHUCK EASTTOM


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard Marcus Pinto


HACKING
A BEGINNERS' GUIDE TO COMPUTER HACKING, BASIC SECURITY AND PENETRATION TESTING
JOHN SLAVIO





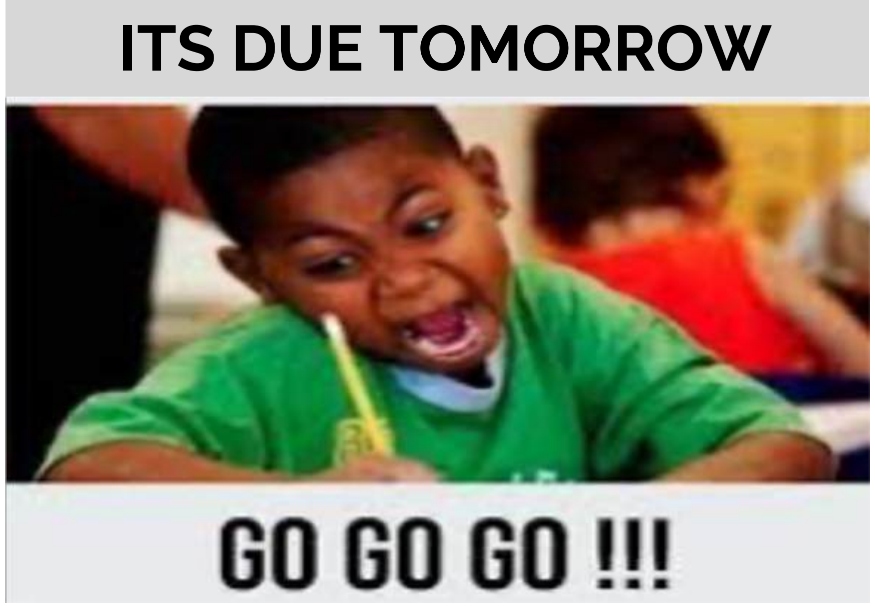
Who cares to get an A

- Final-Term Exam: 40
- Mid-Term Exam: 35
- Sessional Activities: 25
  - Assignments: 30%
  - Quizzes: 40%
  - Class Activities: 30%

Lecture Format

Late submission guidelines protocol

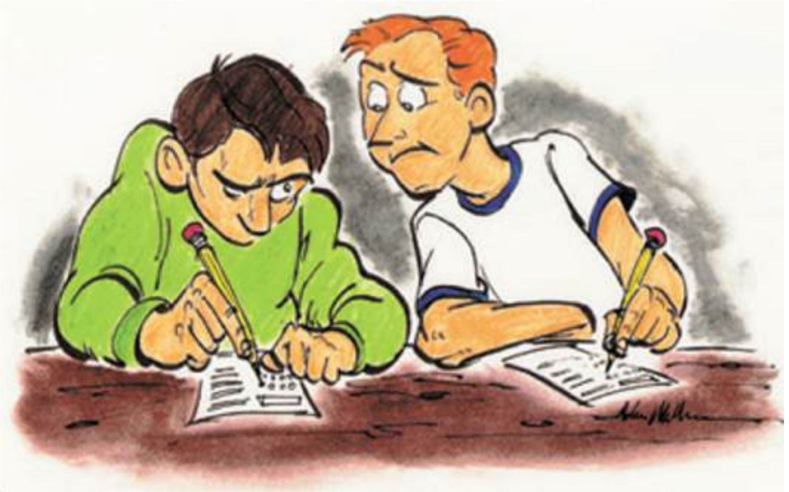
- Late Assignment submissions will not be accepted!
- There will be no retake on exams and quizzes!



Start working on your tasks early and submit well before time.

Cheating Policy

- Academic integrity
- Both the cheater and the student who aided the cheater will be held responsible for the cheating
- The instructor may take actions such as:
  - require repetition of the subject work,
  - assign 'zero' or may be ‘negative’ marks for the subject work,
  - for serious offenses, assign an F grade for the course



Cyber Security

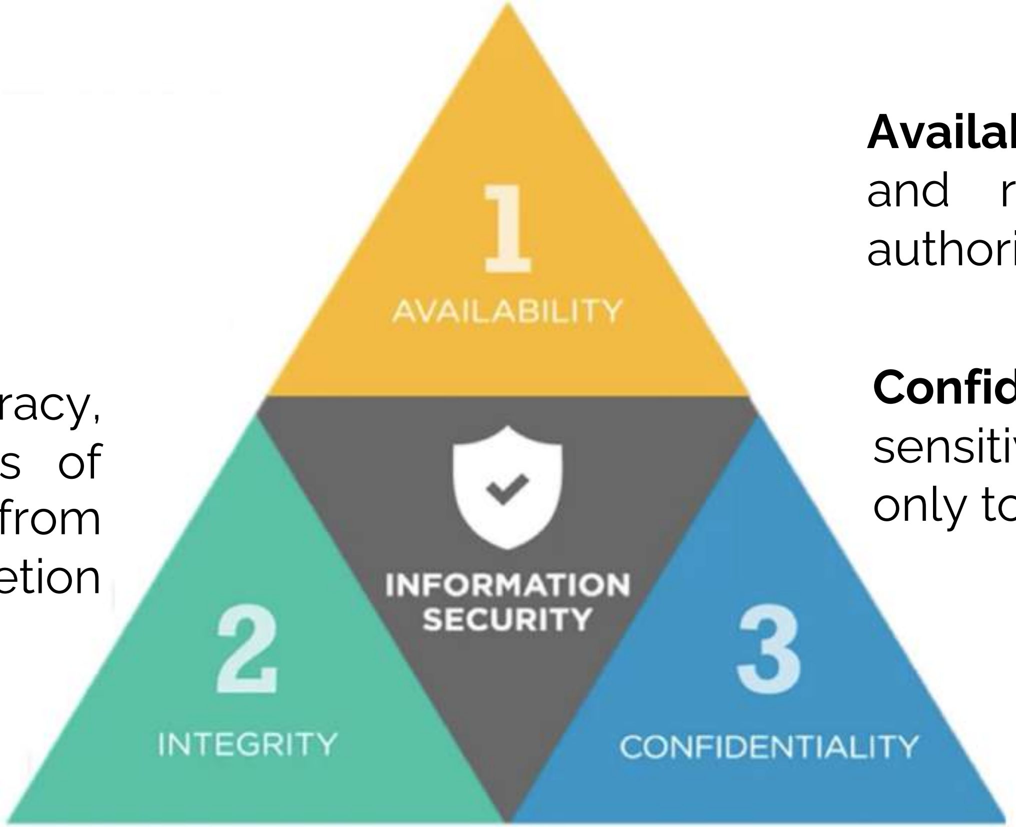
The Big Picture

What is Cyber Security?

- **Cybersecurity** is the practice of protecting systems, networks, devices and data from from cyber threats such as malware, ransomware, phishing, data breaches and so on to safeguard both individual and organizational digital assets.
- It encompasses a wide range of domains, including information security, network security, application security, and incident response.
- It involves the application of technologies, processes, and practices to ensure the confidentiality, integrity, and availability of information

CIA Triad

CIA Triad is the foundational model in IS, representing three core principles that ensure the protection of information



Availability ensures that information and resources are accessible to authorized users when needed

Confidentiality ensures that sensitive information is accessible only to authorized users.

Integrity ensures the accuracy, consistency and trustworthiness of information by protecting it from unauthorized modification, deletion or corruption

Opposite of CIA is DAD

- **Disclosure** means someone not authorized is getting access to the system.
- **Alteration** means your data has been altered.
- **Destruction** means your data or system have been destroyed.

100$ Question: Finding the right mix

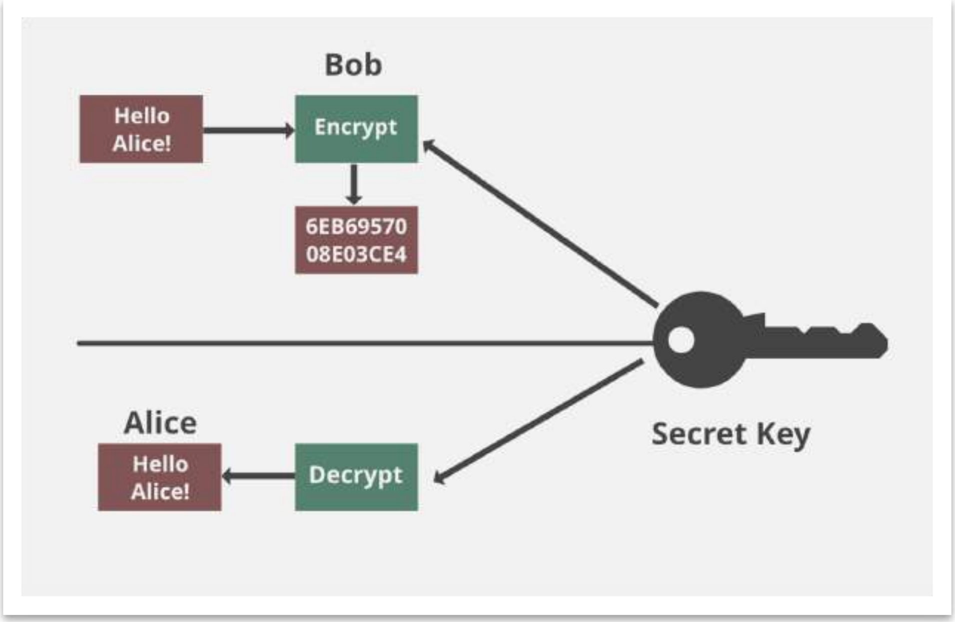
- Ensuring too much **C**, **A** will suffer.
- Ensuring too much **I**, **A** will suffer.
- Ensuring too much **A**, both **C** & **I** will suffer

CIA Triad: Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized users.

Measures to achieve Confidentiality:

- **Encryption:** (3DES, Blowfish, AES, RSA, DSS, PGP)
- **Secure Transport Protocols:** (SSL, TLS, IPSec)
- **Access Control:** (DAC, MAC, RBAC)
- **Authentication Mechanisms:** (MFA, Biometrics)
- **NW Security Controls:** (Fire Walls, VPNs, IDS/IPS)
- **Least Privilege Principle:**
- **Physical Security:**
- **End-user Training:**

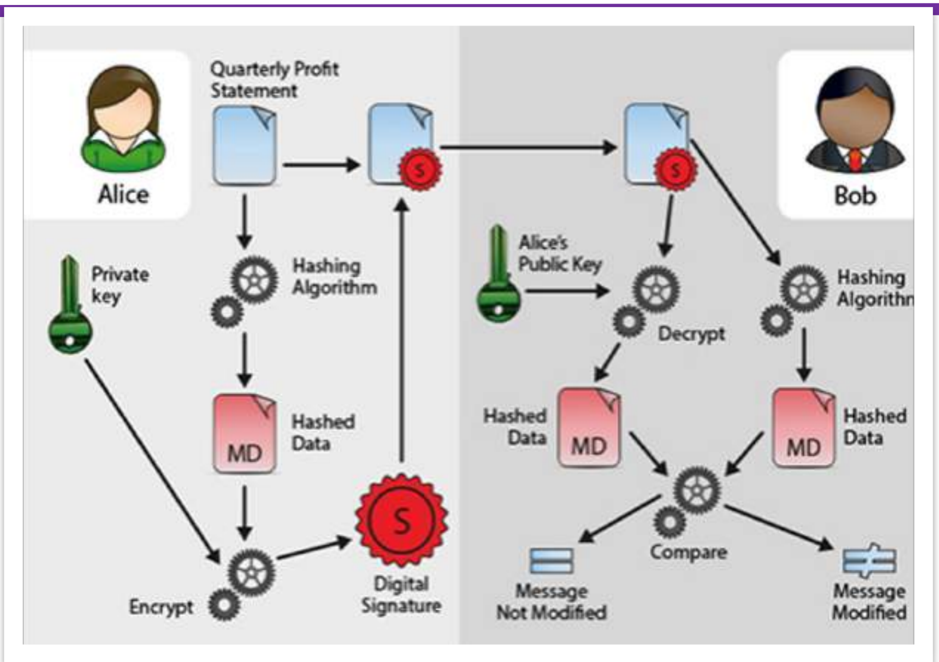


Threats:

- Social engineering/Phishing.
- Unauthorized NW access & Port scanning.
- Eavesdropping and MitM attacks.
- Password dump stealing and attack on your encryption (cryptoanalysis).
- Authorized users may abuse their access to retrieve sensitive data.

CIA Triad: Integrity

Integrity: ensures the accuracy, consistency and trustworthiness of information by protecting it from unauthorized modification, deletion or corruption



Measures to achieve Integrity:

- **Hashing,** generating a fixed size hash value for data , so that any alteration is easily detectable. (MD5, SHA-256, SHA-512)
- **Checksums,** using checksums to detect errors in data communication or storage. (CRC-32, Adler32)
- **Digital Signature,** is used to verify the authenticity and integrity of a message or document. (RSA, PGP)
- **Version Control,** is used to track changes to document or code, allowing roll back if unauthorized changes are detected. (Git, SVN)
- **Active Logging,** maintaining logs that track data changes, system access and transactions (Splunk, Elastic Stack)

Threats:

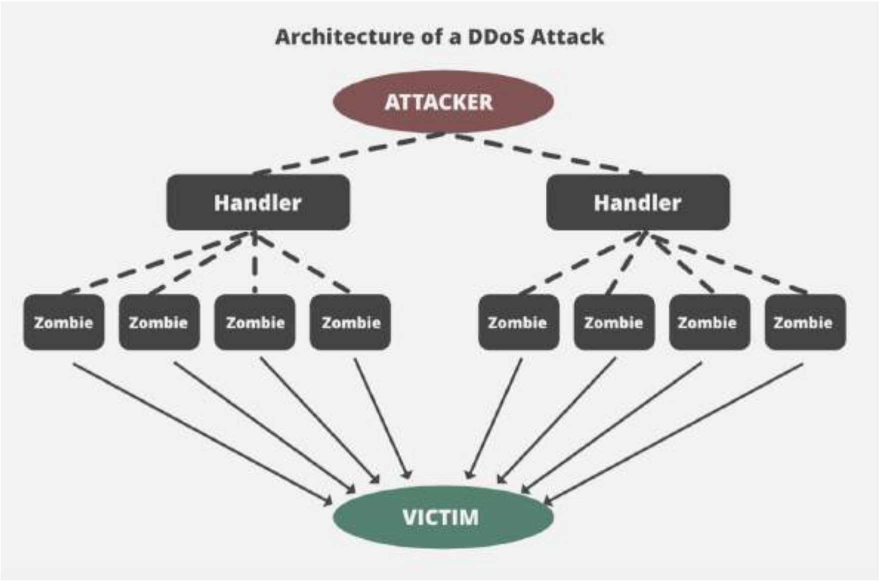
- MitM for tempering
- Data corruption by malware
- Malicious code injection
- Ransomware
- Deleting/altering DB records by SQLi
- DNS Spoofing / Cache Poisoning
- Replay attacks

CIA Triad: Availability

Availability: Achieving Availability ensures that information and resources are accessible to authorized users when needed.

Measures to achieve Availability:

- **Redundancy and Failover**, Implementing redundant systems and automatic failover mechanisms (RAID, Load balancers, Data Center Failover)
- **DDoS Protection**, using security measures to ensure continuous availability of services. (Cloudflare, Akamai)
- **Backup and Recovery**, Regularly backing up data and maintaining recovery procedures to restore systems in case of a disaster. (Veeam, Acronis, AWS Backup)
- **High Availability Architecture**, Using HA designs in systems avoiding single points of failure. (Clustering, Virtualization, Container Orchestration (Kubernetes, Docker).
- **Patch Management**, Keeping systems and applications updated to prevent downtime caused by security vulnerabilities or bugs.



Threats:

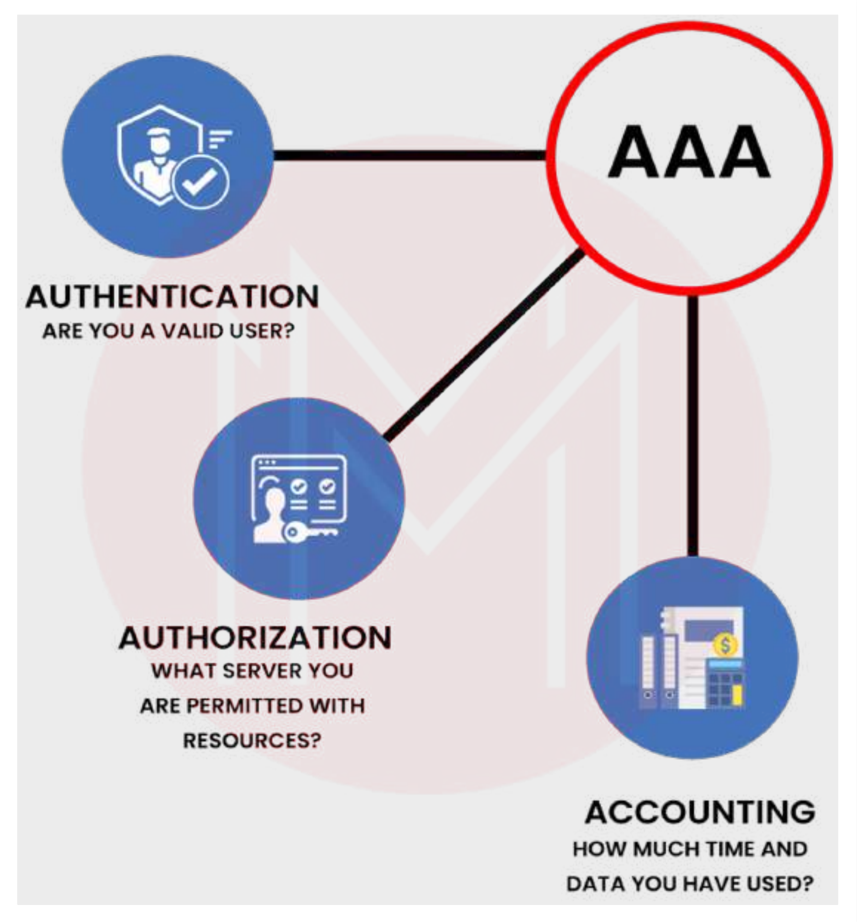
- DDoS
- Ransomware (for availability).
- H/W or S/W Failure.
- Natural disasters.
- Sabotage / Insider attacks.
- Resource exhaustion attacks.
- Logic bombs.

AAA Architecture

- **Authentication** is the process of verifying the identity of a user or system trying to access a resource.
  - Something you know (password, passphrase, PIN)
  - Something you have (NIC, ATM, Passport)
  - Something you are (Biometrics)
  - Somewhere you are (Geographic location, IP, MAC address)
  - Something you do (signatures, pattern unlock)

- **Authorization** determines what an authenticated user or system is allowed to do, specifying access levels or permissions based on the user role or identity. (DAC, MAC, RBAC)

- **Accountability**, also known as auditing, involves tracking and recording user activities and resource usage. This information is used for monitoring, analysis, and compliance purposes.



Cyber Security

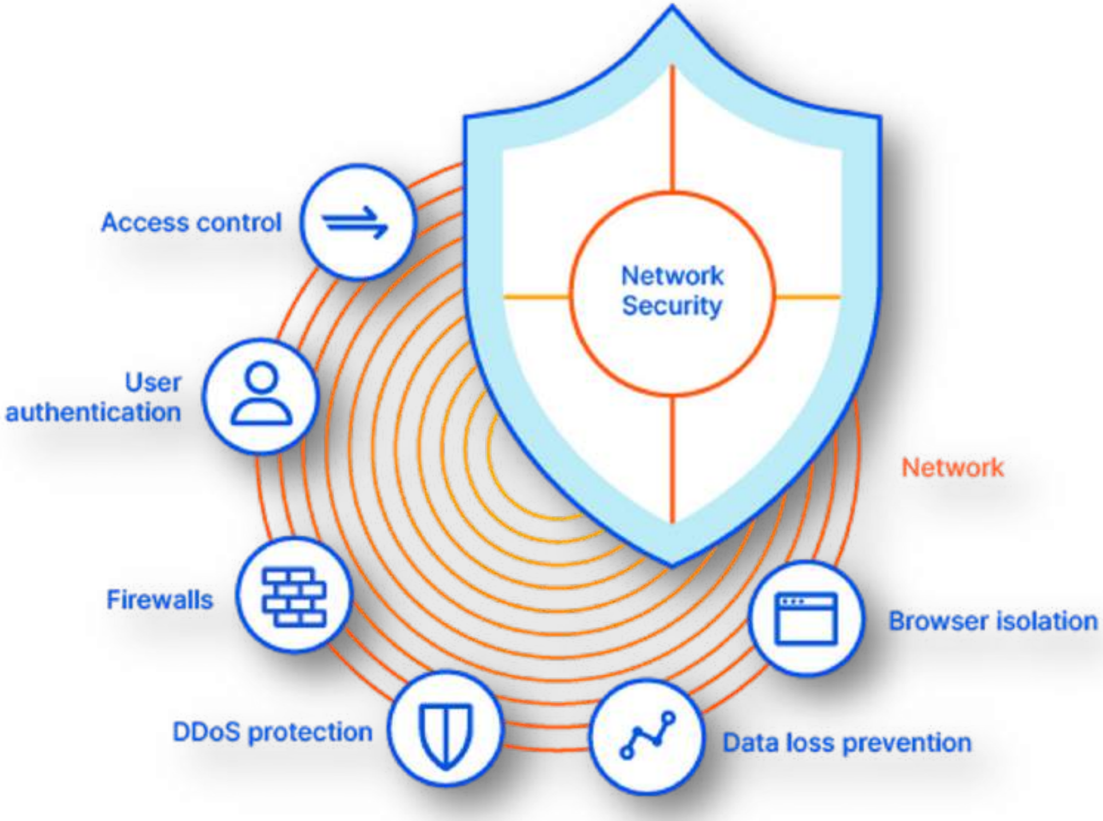
Major Categories

Information Security

- **Information Security (InfoSec)** is the practice of protecting information from unauthorized access, disclosure, disruption, modification, or destruction.
- It aims to ensure the confidentiality, integrity, and availability (CIA Triad) of data, whether it's in storage, processing, or transit, through the use of policies, procedures, and technologies.
- Information security encompasses a wide range of security practices, including risk management, cryptography, access controls, and incident response, to protect both digital and physical information assets.

Network Security

- **Network Security** is the practice of protecting the confidentiality, integrity, and availability of data and resources as they are transmitted or accessed across a network.
- It involves a combination of policies, procedures and technologies to prevent unauthorized access, misuse, modification, or disruption of network infrastructure.
- Network security includes measures such as encryption, security protocols, firewalls, IDS/IPS, and access controls to safeguard communication between devices and protect networks from threats like cyberattacks, malware, and data breaches.

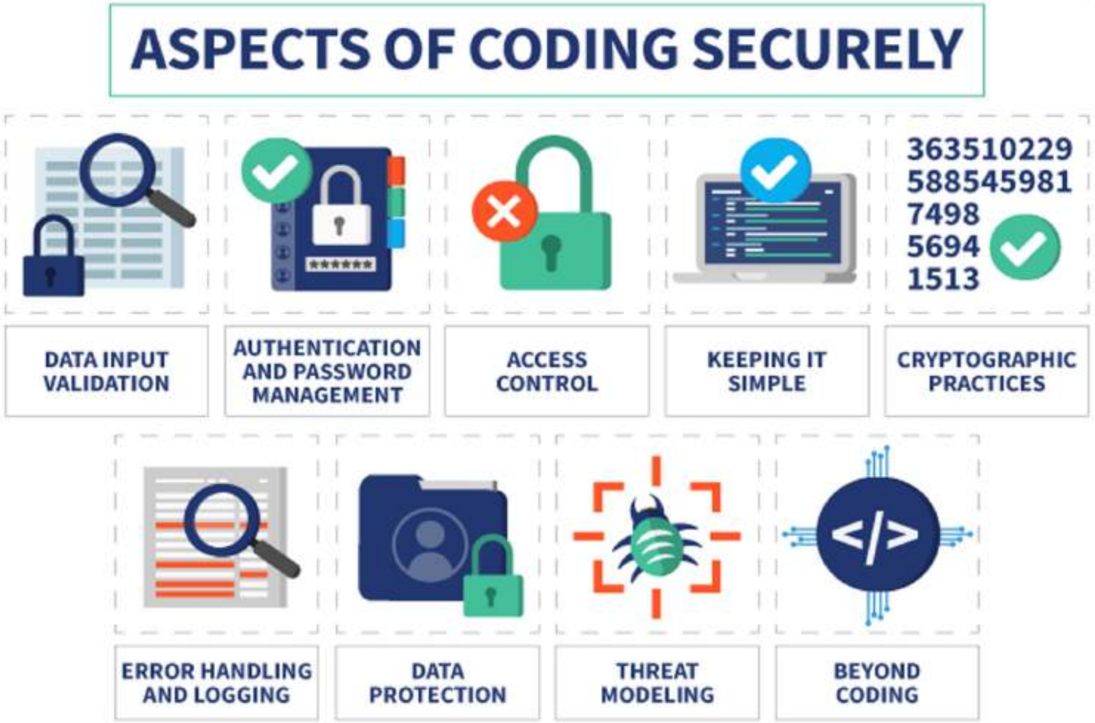


Operating System Security

- **OS security** focuses on protecting the operating system from vulnerabilities and threats, ensuring that the system operates securely and is resistant to attacks.
- It is achieved through following steps:
  - Regularly applying updates and patches to address vulnerabilities and improve security.
  - Configuring the OS to reduce its attack surface by disabling unnecessary services and features
  - Access Control
  - User Authentication
  - File System Security

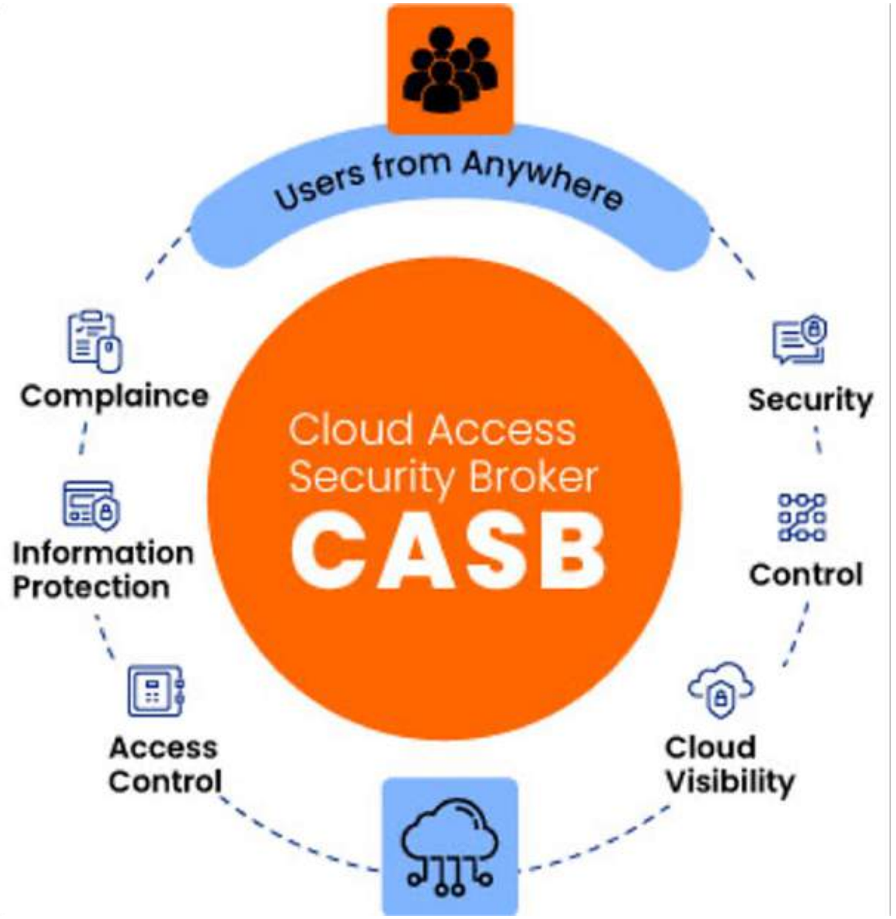
Application Security

- **Application security** focuses on protecting software applications from threats and vulnerabilities that could lead to unauthorized access, data breaches, or other forms of exploitation.
- This includes techniques like secure coding, input validation, authentication, authorization, encryption, and regular security testing (such as vulnerability scanning and penetration testing).
- Application security aims to identify and fix vulnerabilities, such as SQL injection or cross-site scripting (XSS), to prevent malicious attacks.



Cloud Security

- **Cloud security** is the practice of safeguarding data, applications, and services hosted in cloud environments from unauthorized access, data breaches, and other cyber threats.
- Cloud security measures include encryption, Identity and Access Management (IAM), network security, Data Loss Prevention (DLP), and regular security monitoring.
- It addresses both the responsibilities of cloud providers (infrastructure security) and customers (secure configuration and data protection) to prevent threats like data leaks, account hijacking, and misconfigurations.



IoT Security

- **IoT security** is the practice of protecting Internet of Things (IoT) devices and the networks they connect to from cyber threats, unauthorized access, and vulnerabilities.
- Key IoT security practices include device authentication, encryption, secure firmware updates, network segmentation, and monitoring for unusual activity.
- IoT security is critical because these devices often have limited processing power, making them more susceptible to attacks, and they can serve as entry points for threats like malware or unauthorized control in broader network environments.

Collection of interconnected devices that communicate and transfer data through the Internet

The Future: Security of Gen-AI Models

LLM Security Threats

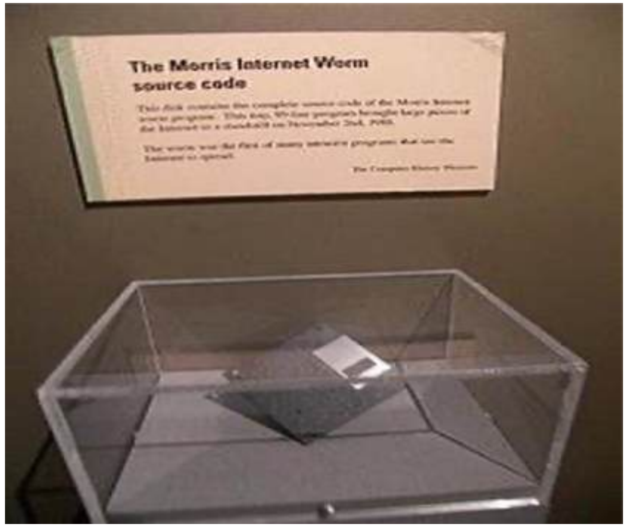
- Prompt injection
- Jail breaking
- Backdoor and data poisoning
- Adversarial inputs
- Insecure output handling
- Data extraction & privacy
- Data reconstruction
- Denial of service
- Privilege escalation
- Water marking and evasion
- Model theft

DALL-E: "Automation"

History of Cyber Attacks

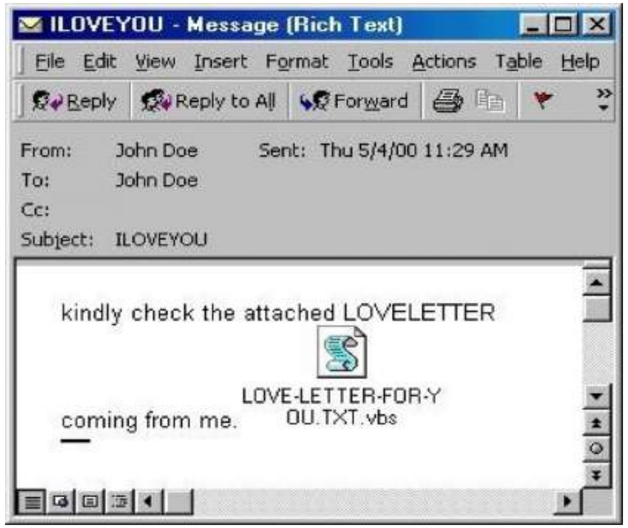
Famous Cyber Attacks

Morris Worm (1988): Often considered one of the first major worms, created by Robert Tappan Morris. It was designed to exploit vulnerabilities in Unix systems and spread across the internet. It infected around 6,000 computers, causing significant disruption by slowing down systems and making them unusable.



Melissa Virus (1999): The Melissa virus was a computer virus that spread quickly through email attachments in 1999. It targeted Microsoft Word and Outlook users, and was one of the first viruses to raise awareness of the risks of opening unsolicited emails

ILOVEYOU Worm (2000): The ILOVEYOU Worm, also known as the Love Bug, spread through email with a subject line that read "I Love You." It used a social engineering trick to lure recipients into opening an infected attachment. It caused widespread damage, affecting 10 million computers globally, and led to billions of dollars in damages.


ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Reply Reply to All Forward

From: John Doe Sent: Thu 5/4/00 11:29 AM
To: John Doe
Cc:
Subject: ILOVEYOU

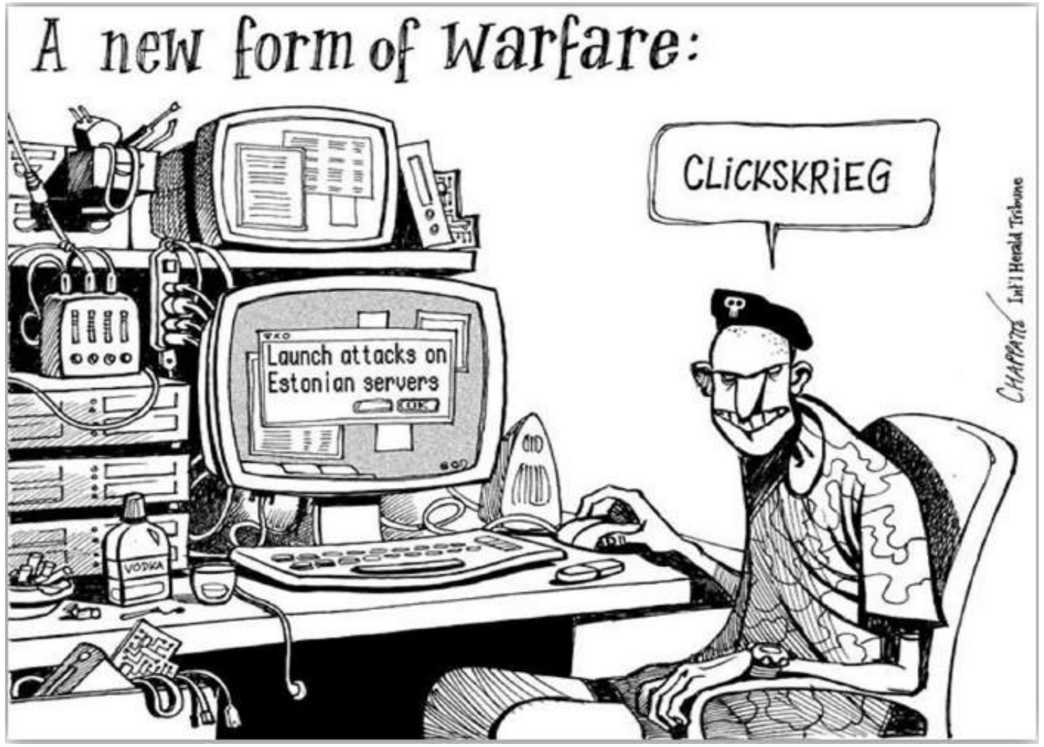
kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Famous Cyber Attacks

Cyber Attacks against Estonia (2007): In 2007, Estonia experienced a series of major cyber attacks, widely regarded as one of the first large-scale, politically motivated, state-sponsored cyber warfare campaigns.

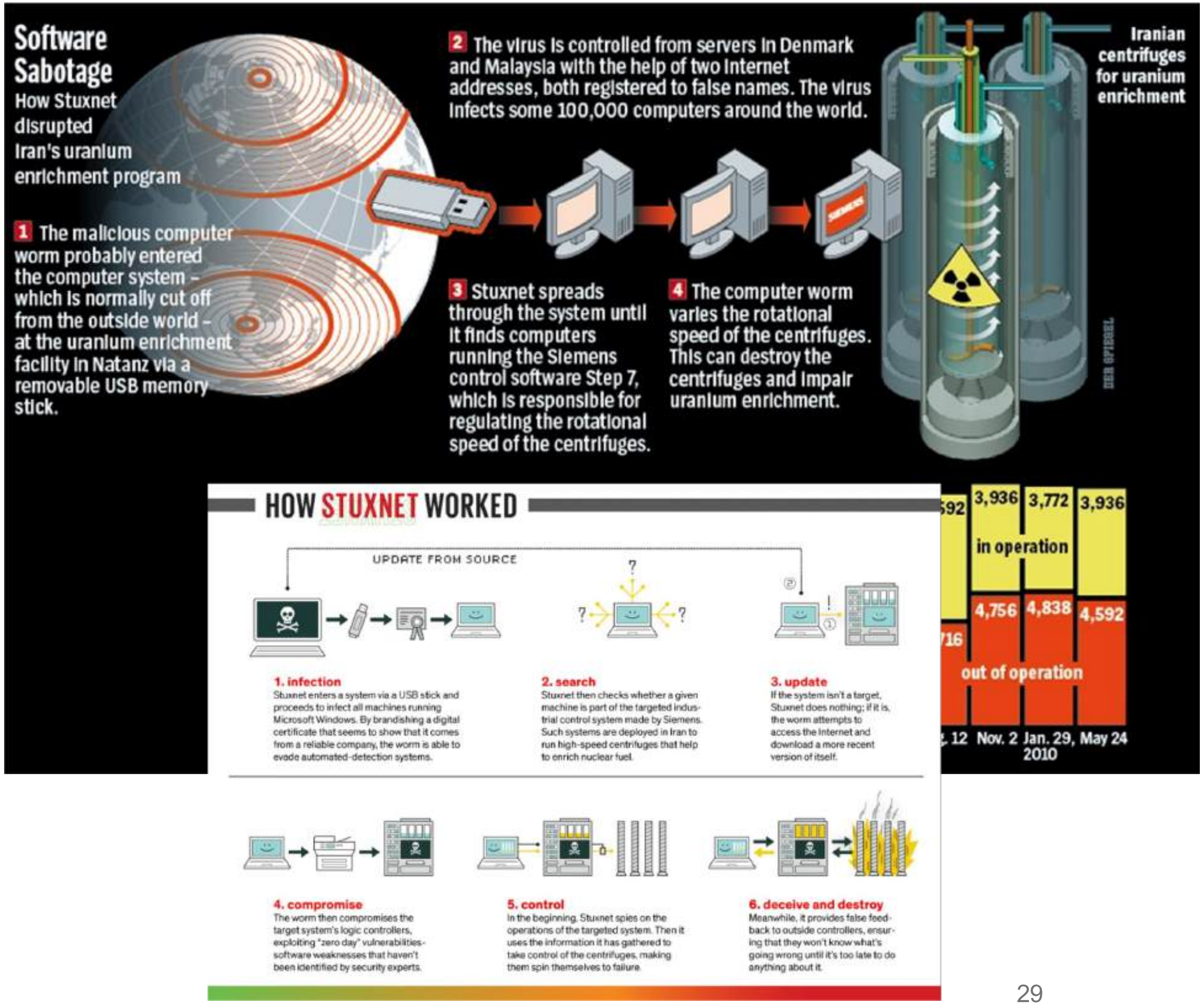
- These attacks targeted government institutions, banks, media outlets, and other critical infrastructure, effectively disrupting the nation's online services for several weeks.
- It involved DDoS (Distributed Denial of Service) attacks, overwhelming servers with traffic to shut down websites and services.
- Russia was widely suspected of being behind the attacks.



Famous Cyber Attacks

Stuxnet (2010):

- Stuxnet was a sophisticated worm believed to be created by the U.S. and Israeli governments to target Iran's nuclear facilities. Worm spread through Windows computers, but its primary function was to cause physical damage to the centrifuges by altering their speeds without detection, while simultaneously sending normal operating signals to monitoring systems.
- It is considered one of the first known cyber weapons and demonstrated the potential for cyber-attacks to cause physical damage.



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Famous Cyber Attacks

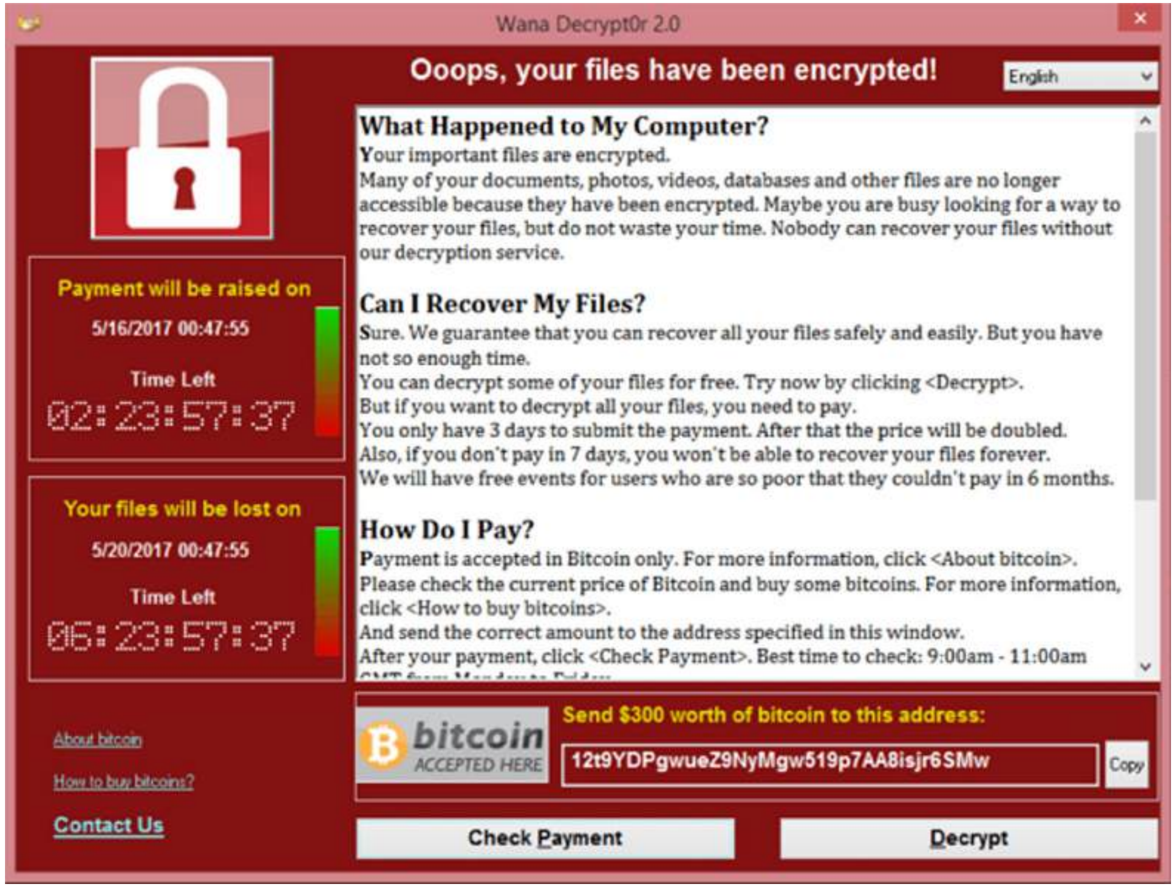
Sony PlayStation Network Hack (2011):

- Attackers compromised Sony's PlayStation Network (***PSN Hack***), gaining access to personal information of around 77 million users.
- They used a combination of phishing techniques and SQL injection to gain unauthorized access to Sony's servers. Data Breach forced Sony to shut down the PSN for nearly a month.
- Sony faced financial loss of $171 million approx., making it one of the largest security breaches of its time.
- The breach led to the suspension of the network, significant financial losses, and a major hit to Sony's reputation.

Famous Cyber Attacks

WannaCry Ransomware Attack (2017):

- WannaCry attacked computers worldwide by exploiting a vulnerability in Microsoft’s Server Message Block protocol.
- Vulnerability ID: CVE-2017-0144
- Exploit used: EternalBlue, developed by NSA, leaked by shadow brokers hacking group.
- It encrypted users’ files and demanded ransom payments in Bitcoin.
- The attack affected more than 300,000 computers across 150 countries, with total damage ranging from hundreds of millions to billions of dollars
- Attack caused significant financial losses, halted critical services, and highlighted the dangers of outdated software and unpatched security vulnerabilities



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

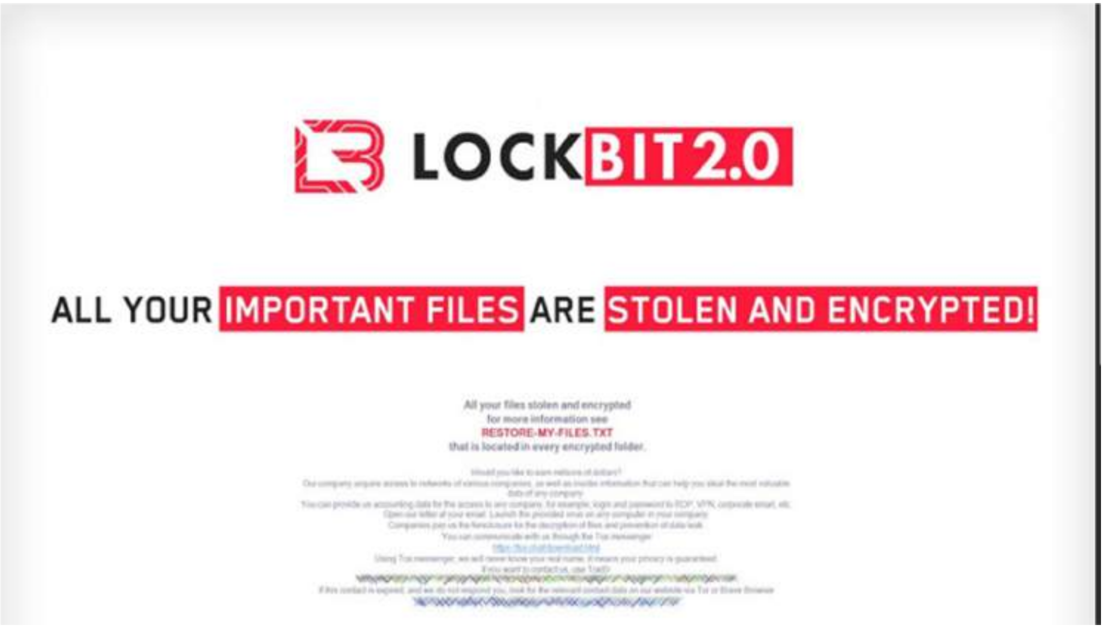
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Famous Cyber Attacks

LockBit (2019):

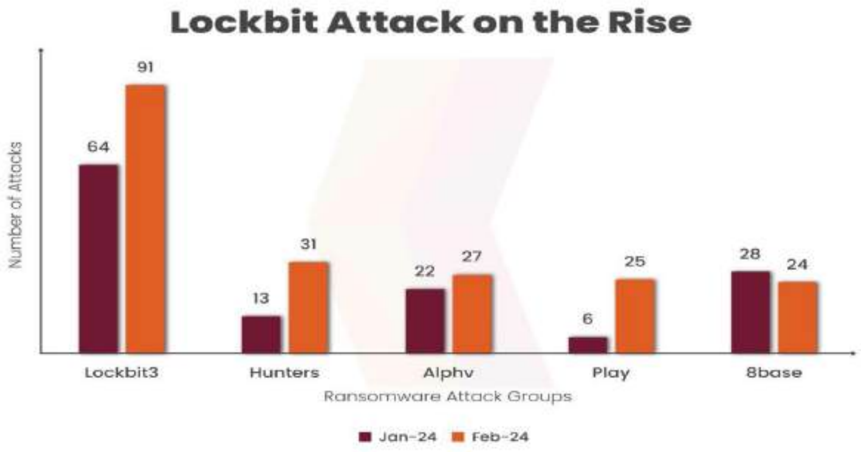
- A notorious ransomware group known for its multiple versions of ransomware, including LockBit 1.0, 2.0, and the latest, LockBit 3.0. Each version has become more sophisticated, with enhanced encryption and better evasion tactics. The group operates under a ransomware-as-a-service (RaaS) model, allowing other cybercriminals to use their software for a fee.
- Attacked financial services, healthcare and transportation sectors.
- Used in approximately 1,700 ransomware attacks in US between January 2020 to and May 2023, with US$91 million paid as ransom.
- Also declared as the world's most prolific ransomware in 2022.


LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

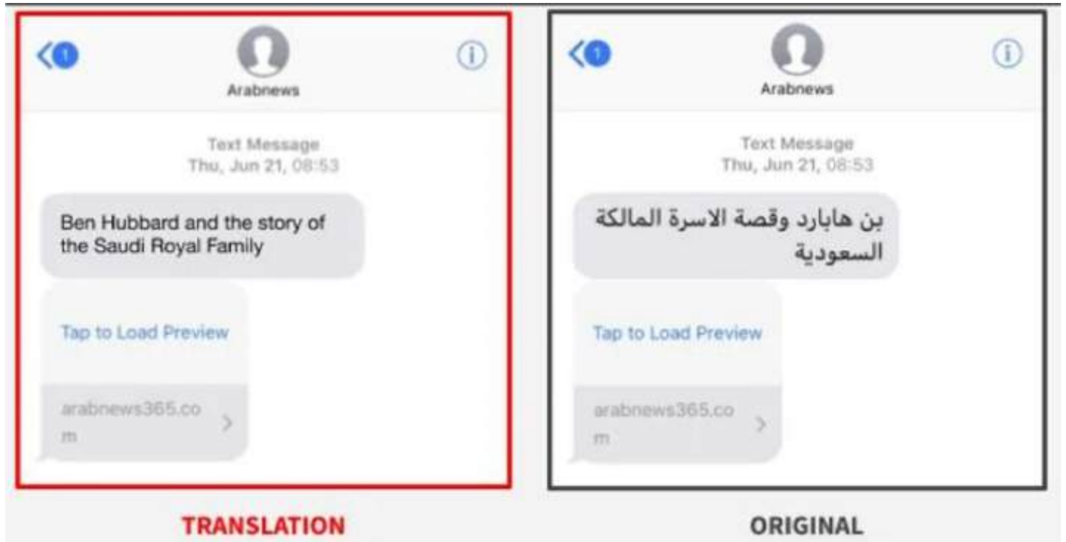
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[illegible]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[illegible]



Famous Cyber Attacks

Pegasus (Forced Entry) (2021): Pegasus (Forced Entry) refers to a specific exploit of the Pegasus spyware, developed by Israeli company NSO group. It explored a zero-day in Apple's iMessage, allowing the spyware to be installed on a device without any interaction from the victim. This attack didn’t require the victim to click on a malicious link or open a compromised file; it could be silently triggered just by receiving a specially crafted message. Once installed, Pegasus could monitor calls, messages, emails, and even activate microphones and camera

Operation Triangulation (2023): This operation utilized Pegasus spyware to silently compromise mobile devices and gain access to sensitive data. Operation Triangulation is a targeted cyberattack on iOS devices conducted using a chain of four zero-day vulnerabilities.



Arabnews

Text Message
Thu, Jun 21, 08:53

Ben Hubbard and the story of the Saudi Royal Family

Tap to Load Preview

arabnews365.com

TRANSLATION

Arabnews

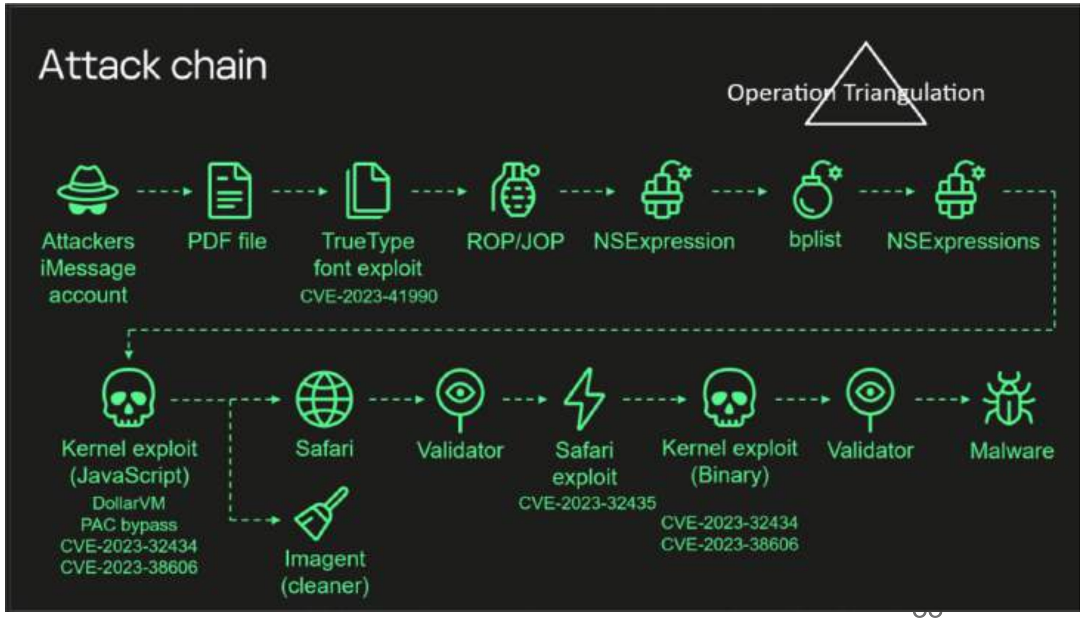
Text Message
Thu, Jun 21, 08:53

بن هابارد وقصة الاسرة المالكة السعودية

Tap to Load Preview

arabnews365.com

ORIGINAL


Attack chain
Operation Triangulation
Attackers iMessage account
PDF file
TrueType font exploit CVE-2023-41990
ROP/JOP
NSExpression
bplist
NSExpressions
Kernel exploit (JavaScript) DollarVM PAC bypass CVE-2023-32434 CVE-2023-38606
Safari
Imagent (cleaner)
Validator
Safari exploit CVE-2023-32435
Kernel exploit (Binary) CVE-2023-32434 CVE-2023-38606
Validator
Malware

Famous Cyber Attacks (Cont..)

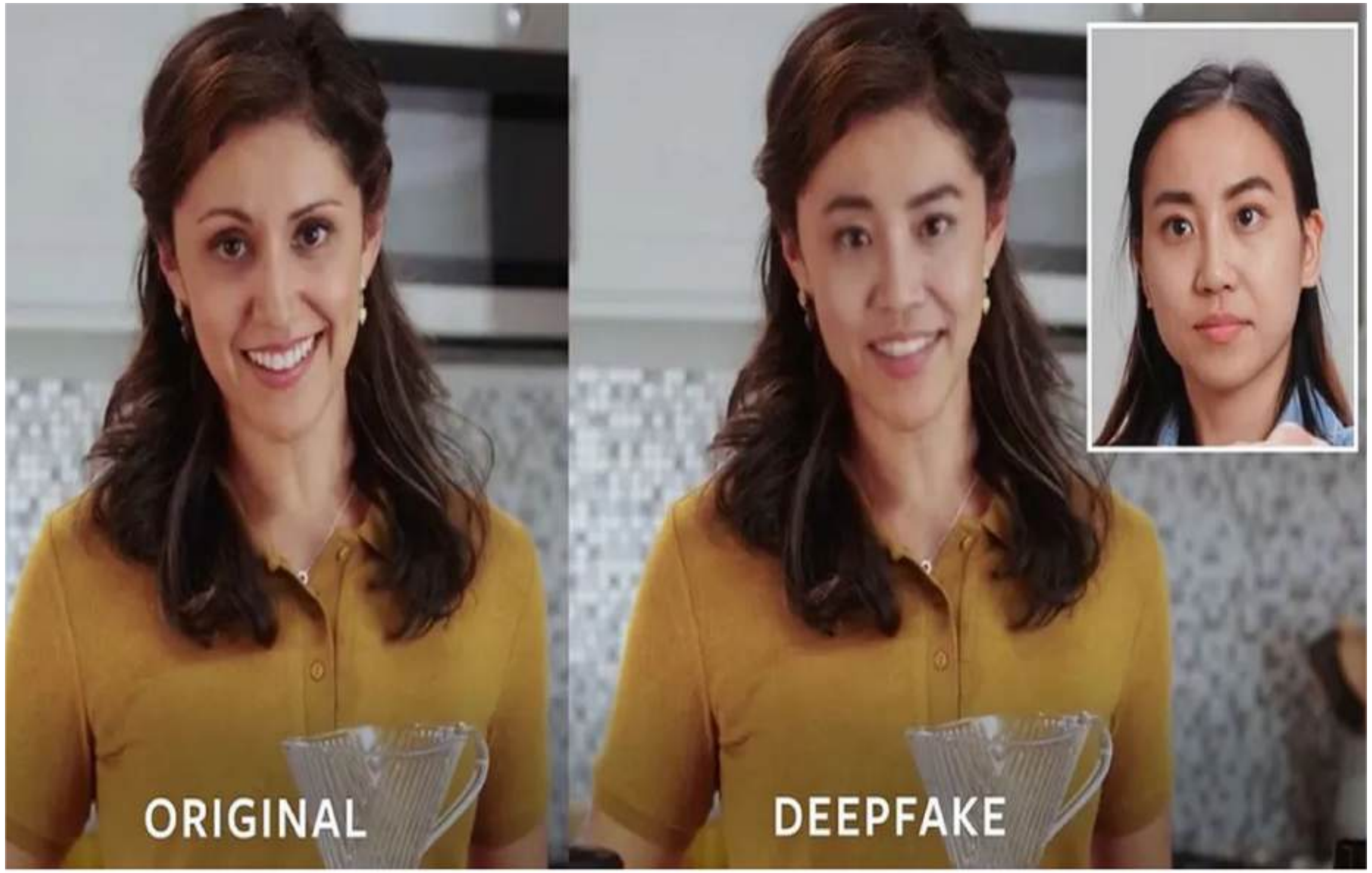
IoT (Internet of Things) Attacks

- **Mirai Botnet (2021)**: The Mirai botnet, which was initially used for DDoS attacks, continues to exploit vulnerabilities in IoT devices to launch large-scale attacks.
- IoT device vulnerabilities can lead to widespread disruptions and can be used to launch attacks on various services. It stresses the importance of securing connected devices and updating their software regularly.

Famous Cyber Attacks (Cont..)

Deepfake AI: Deepfake AI poses significant challenges to cybersecurity, as it can be used to create highly convincing fake audio, video, and text content that can deceive individuals and manipulate public opinion

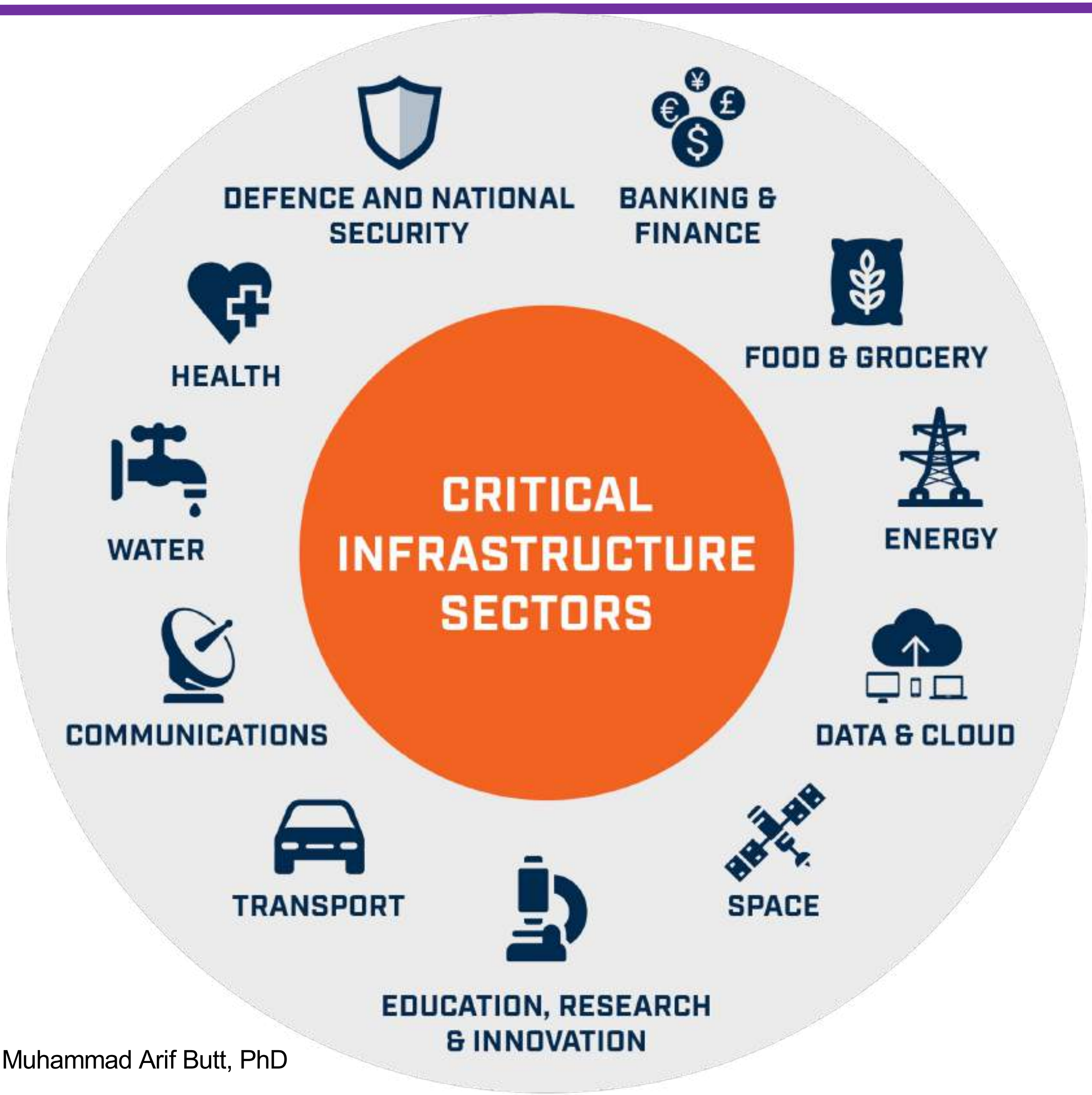
- Social Engineering Attacks
- Phishing and Fraud
- Reputation Damage
- Misinformation and Disinformation Campaigns
- Authentication and Trust Issues



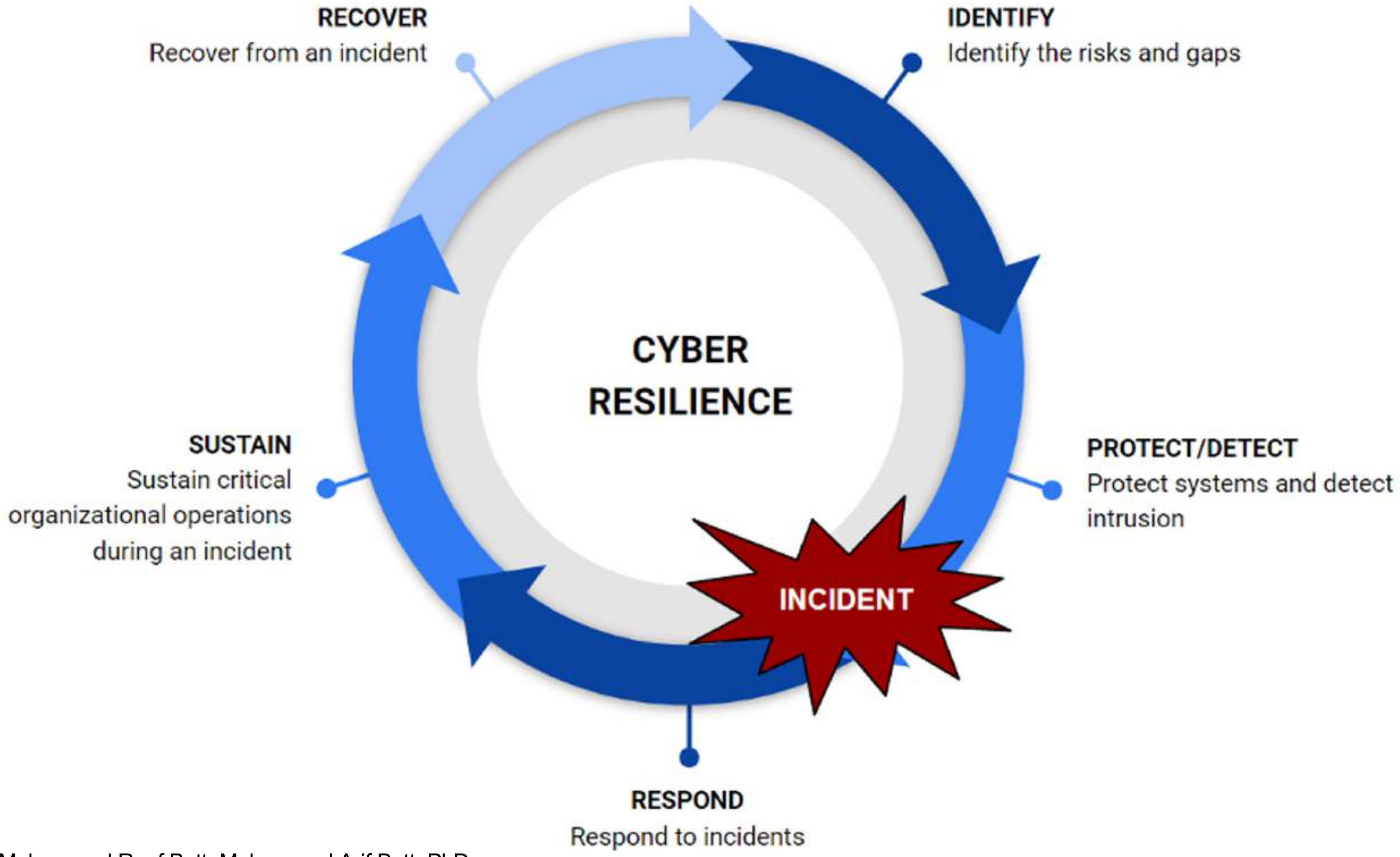
Impacts of Cyber Attacks

- **Financial Losses**: Direct financial losses due to theft, ransom payments, and fraud, as well as indirect costs from downtime, recovery efforts, and legal fees.
- **Operational Disruption**: Interruption of business operations, affecting productivity and service delivery. Critical infrastructure attacks can lead to widespread disruptions in essential services.
- **Reputational Damage**: Loss of customer trust and damage to the organization's reputation, which can affect future business prospects and customer relationships.
- **Data Privacy Concerns**: Exposure of personal and sensitive data, leading to increased risks of identity theft, phishing, and privacy violations.
- **Regulatory and Legal Consequences**: Increased scrutiny from regulators and potential legal actions, resulting in fines and compliance costs.
- **National Security Risks**: Espionage and attacks on critical infrastructure can have implications for national security and geopolitical stability.

National Critical Infrastructure


CRITICAL INFRASTRUCTURE SECTORS
DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
FOOD & GROCERY
ENERGY
DATA & CLOUD
SPACE
EDUCATION, RESEARCH & INNOVATION
TRANSPORT
COMMUNICATIONS
WATER
HEALTH

Cyber Resilience

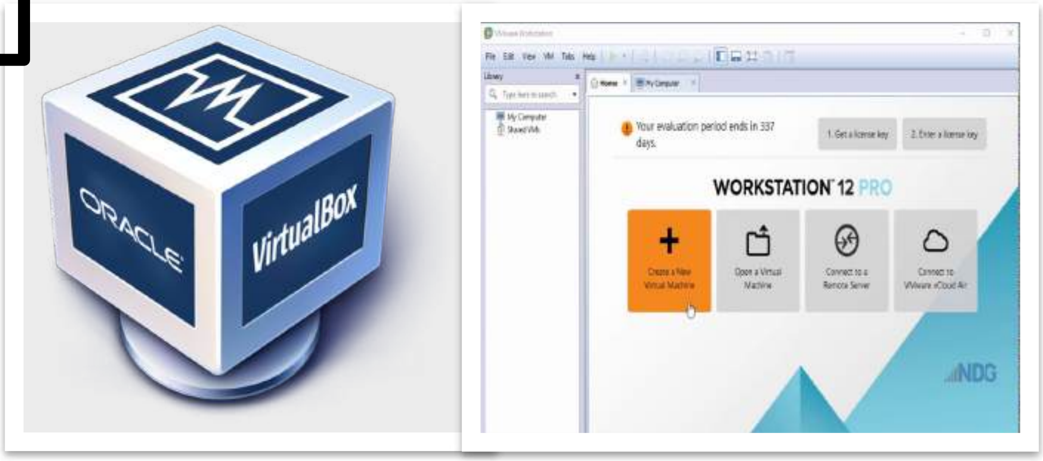

RECOVER
Recover from an incident
IDENTIFY
Identify the risks and gaps
CYBER
RESILIENCE
PROTECT/DETECT
Protect systems and detect intrusion
SUSTAIN
Sustain critical organizational operations during an incident
INCIDENT
RESPOND
Respond to incidents

Course Contents

Overview of the Course

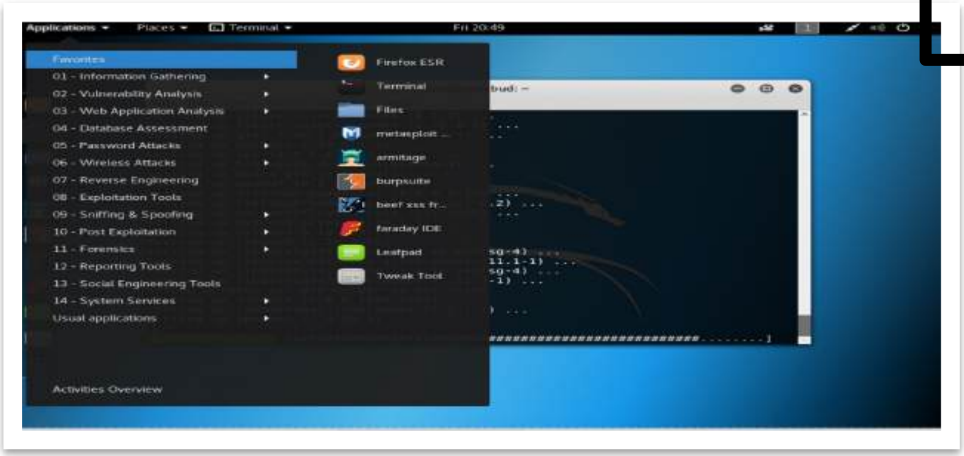
M1

Overview and pre-requisites


ORACLE
VirtualBox
Your evaluation period ends in 337 days.
1. Get a license key
2. Enter a license key
WORKSTATION 12 PRO
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
Connect to VMware vCloud Air
NDG

NW Attacks and Penetration Testing

M2



M3

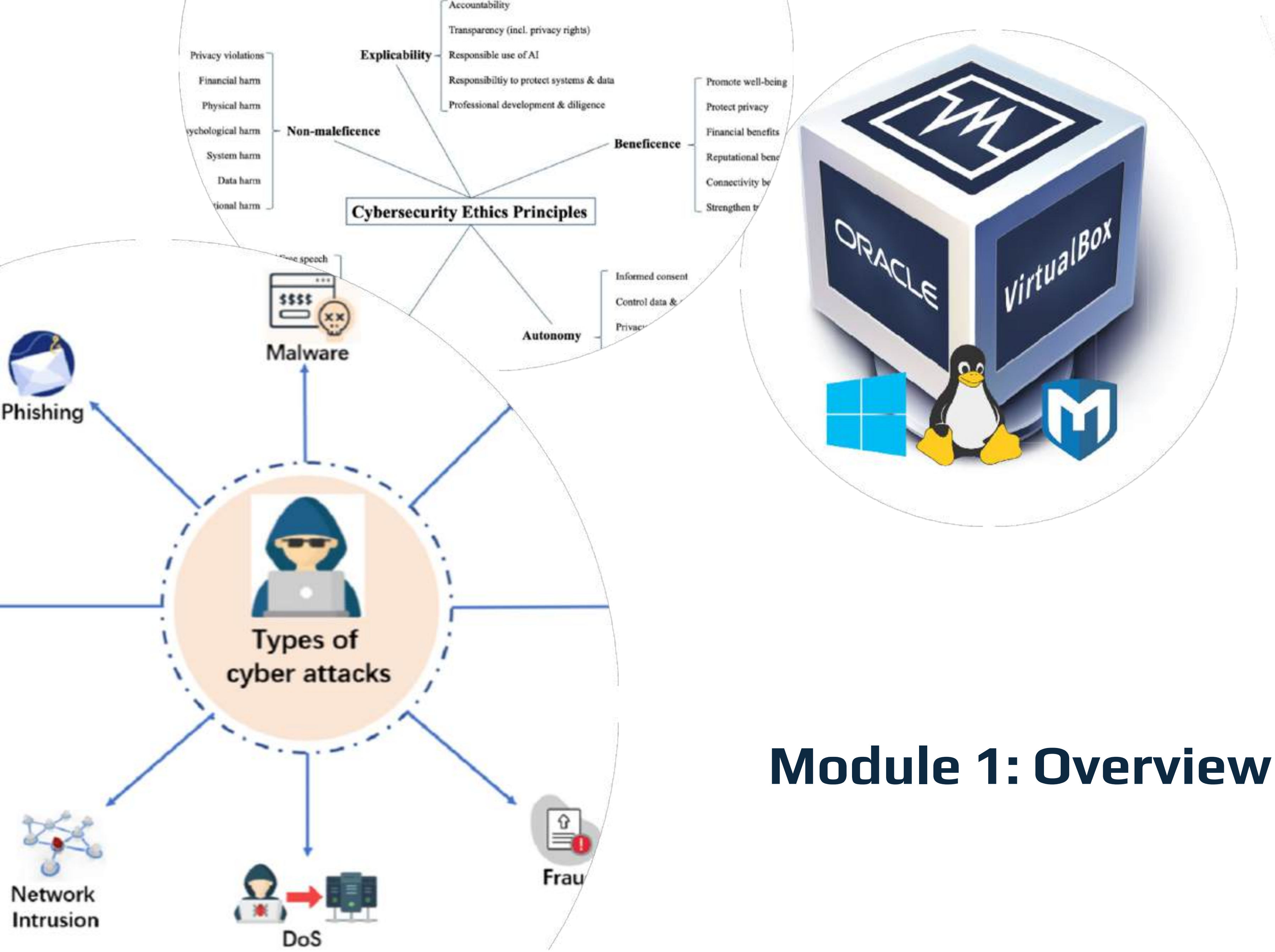
Reverse Engineering & Binary Exploitation

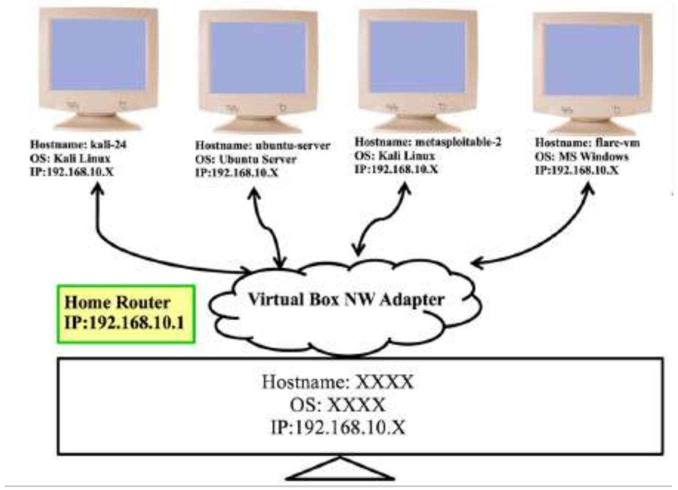
Malware Development and Analysis

M4

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Module 01: Overview and Prerequisites

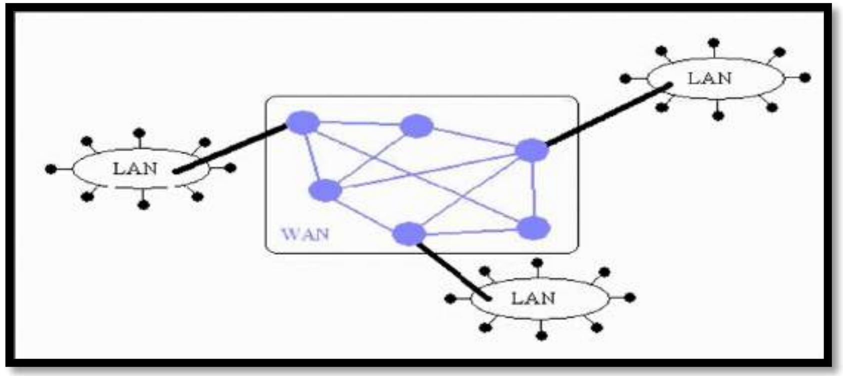


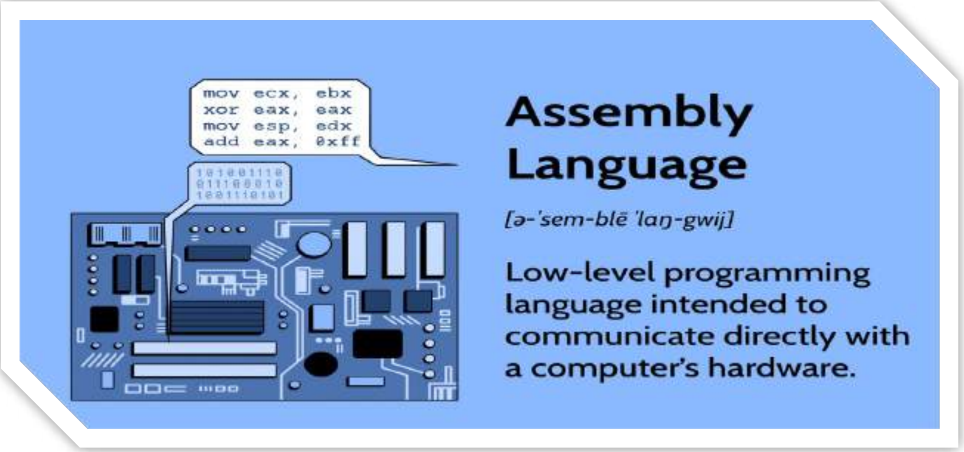


Module 1: Overview and Prerequisites

Prerequisites of the Course

Operating System
Linux
Windows
macOS
Android





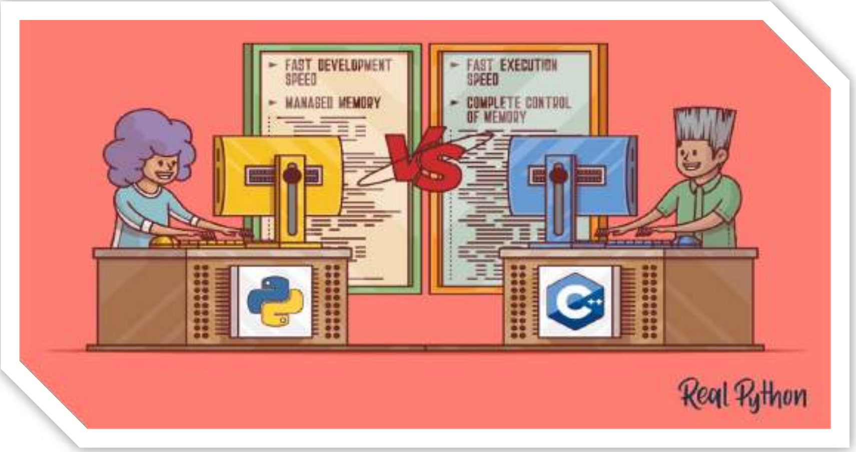
```
mov ecx, ebx
xor eax, eax
mov esp, edx
add eax, 0xff
```

```
1010011101
0111000010
1001110101
```

Assembly Language

[ə-'sem-blē 'laŋ-gwij]

Low-level programming language intended to communicate directly with a computer's hardware.



Module2:
NW Attacks &
Penetration Testing

Module 2: NW Attacks & PT

Penetration testing (pen testing) is a systematic process used to identify and exploit vulnerabilities in a system, network, or application to understand the security risks.

1. Reconnaissance and Information Gathering
2. Scanning and Vulnerability Analysis
3. Exploitation and Gaining Access
4. Privilege Escalation
5. Maintaining Access and Persistent Mechanisms
6. Covering Tracks

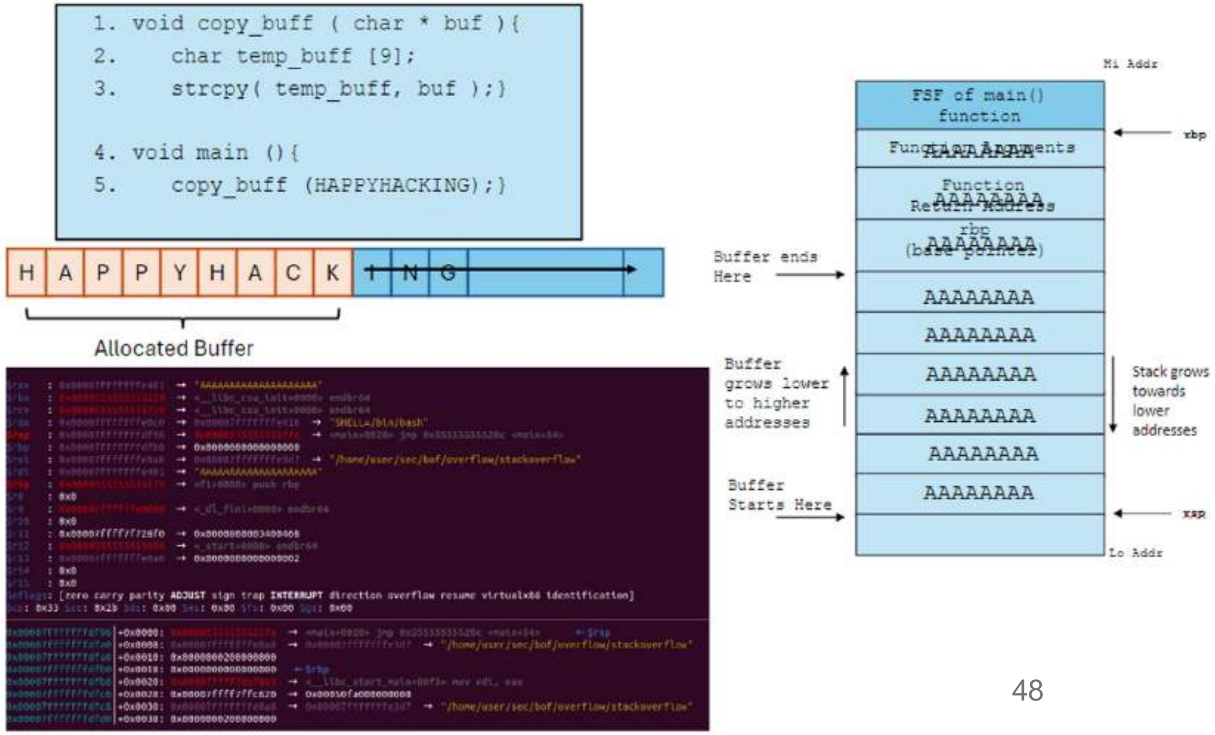
Module3: Reverse Engineering and Binary Exploitation

- **Reverse engineering** in cybersecurity refers to the process of analyzing and disassemblying software, hardware, or protocols to understand their inner workings, often with the goal of extracting valuable information, identifying vulnerabilities, malicious behavior or weaknesses.
- Key purposes of reverse engineering are:
  - Software cracking or protection
  - Vulnerability research
  - Malware analysis
  - Digital forensics
- Tools used in reverse engineering are:
  - GNU GDB
  - IDA Pro
  - Radare2
  - X64dbg
  - Wireshark
  - Burp Suite

Module 3: Reverse Engineering & Binary Exploitation

- **Binary exploitation** is a category of cyber attack where an attacker abuses vulnerabilities in compiled binary programs (executable files, libraries, etc.) to gain unauthorized access, escalate privileges, or execute arbitrary code. This often involves leveraging flaws in the way a program handles input, memory, or system resources.

- Common vulnerabilities that lead to binary exploitation include:
  - Buffer overflow
  - Integer overflow
  - Use after free
  - Race condition
  - Return oriented programming
  - Format string vulnerability
  - Shellshock vulnerability
  - SUDO vulnerability
  - COW vulnerability



```
void copy_buff ( char * buf ){
    char temp_buff [9];
    strcpy( temp_buff, buf );}

void main (){
    copy_buff (HAPPYHACKING);}
```

```
$rax   : [illegible] → "AAAAAAAAAAAAAAAAAA"
$rdi   : [illegible] → "AAAAAAAAAAAAAAAAAA"
$r9    : 0x0
$r10   : 0x0
$r11   : 0x00007ffff7f728f0 → 0x0000000003409468
$r13   : [illegible] → 0x0000000000000002
$r14   : 0x0
$r15   : 0x0
$eflags: [zero carry parity ADJUST sign trap INTERRUPT direction overflow resume virtualx86 identification]
$cs: 0x33 $ss: 0x2b $ds: 0x00 $es: 0x00 $fs: 0x00 $gs: 0x00
[illegible] +0x0000: [illegible]
[illegible] +0x0008: [illegible] → "/home/user/sec/bof/overflow/stackoverflow"
[illegible] +0x0010: 0x0000000200000000
[illegible] +0x0018: 0x0000000000000000  ← $rbp
[illegible] +0x0020: [illegible]
[illegible] +0x0028: 0x00007ffff7ffc620 → 0x000050fa00000000
[illegible] +0x0030: [illegible] → "/home/user/sec/bof/overflow/stackoverflow"
[illegible] +0x0038: 0x0000000200000000
```

Module4: Malware Development & Analysis

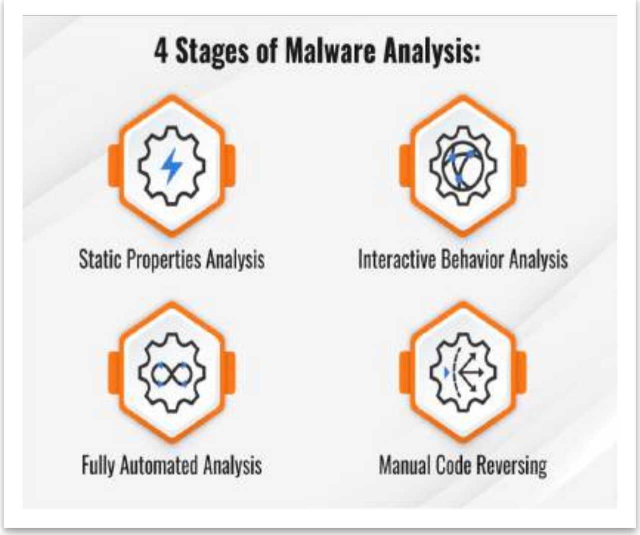
Module 4: Malware Development & Analysis

Malware development refers to the process of creating malicious software designed to infiltrate, damage or steal data from, or disrupt the operation of computers, NW or devices

- Ransomware: WannaCry, Ryuk
- Spyware: Pegasus, WebWatcher
- Trojan Horse: RAT, ZBot
- Adware: Superfish, Crossrider
- Worms: SQLSlammer, MyDoom
- Rootkits: SonyBMG, ZeroAccess
- Virus: ILoveYou, Melissa
- Botnets: Gameover Zeus, Exobot
- Fileless Malware: LOTL, PowerGhost

Module 4: Malware Development & Analysis

- Understanding Malwares and its types
- Building closed environment to perform analysis
- Understanding the procedure to perform the analysis
- Understanding the art of writing detection rules



4 Stages of Malware Analysis:

- **YARA**: Yet Another Ridiculous Acronym is a versatile and powerful tool for malware detection, classification and hunting. It help writing custom rules to detect threads that might bypass traditional security solutions.
- **ClamAV**: An open-source antivirus engine used for detecting and removing malware, including viruses, trojans, and worms.
- **Snort**: An open-source IDS/IPS that helps in monitoring network traffic in real time to detect suspicious activities and potential security threats.

Happy Hacking 😎

To Do:

Go through Handout # 1.2 at your own and set-up your own Virtual Hacking Lab for all the class activities and assignments using either Virtual Machines or Docker Containers or both ☺