Cybersecurity Fundamentals

PRESENTED BY
ABK Bhuiyan
Guest Lecturer
Daffodil International University

Do Your Part. #BeCyberSmart

Part I : The Discussion

PRESENTED BY
ABK Bhuiyan
Guest Lecturer
Daffodil International University

Do Your Part. #BeCyberSmart

Scope & Coverage

1. Introduction to Cybersecurity
2. Overview of cybercrime
3. Awareness, Acts & Punishment
4. Cybersecurity Basics
5. Cryptography Basics

What is Cybersecurity?

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

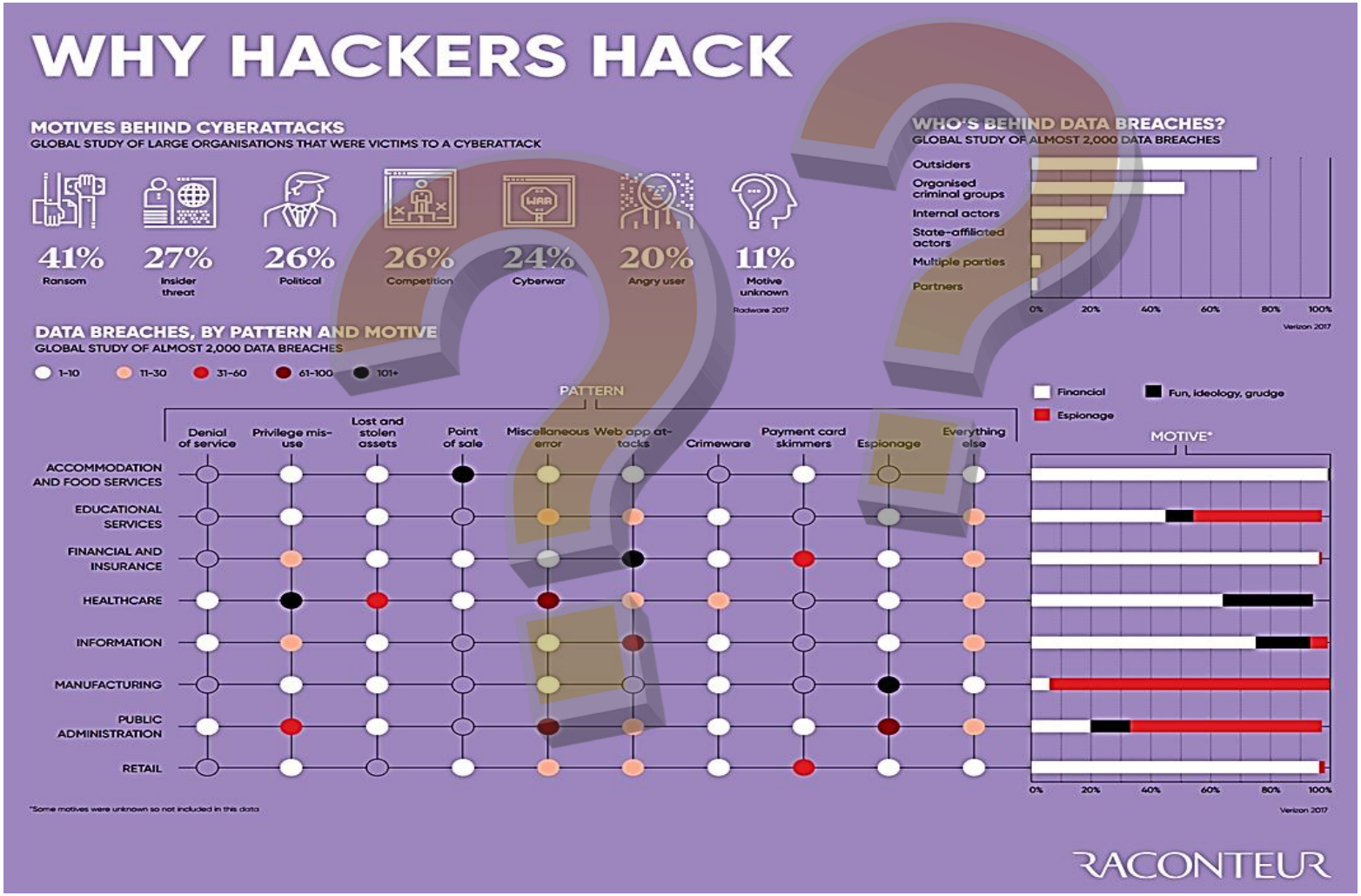
Cybercrime

- **What is it?**
  - Cybercrime is any crime which is committed electronically.
  - This can include…
    - Theft
    - Fraud
    - Sometimes even murder

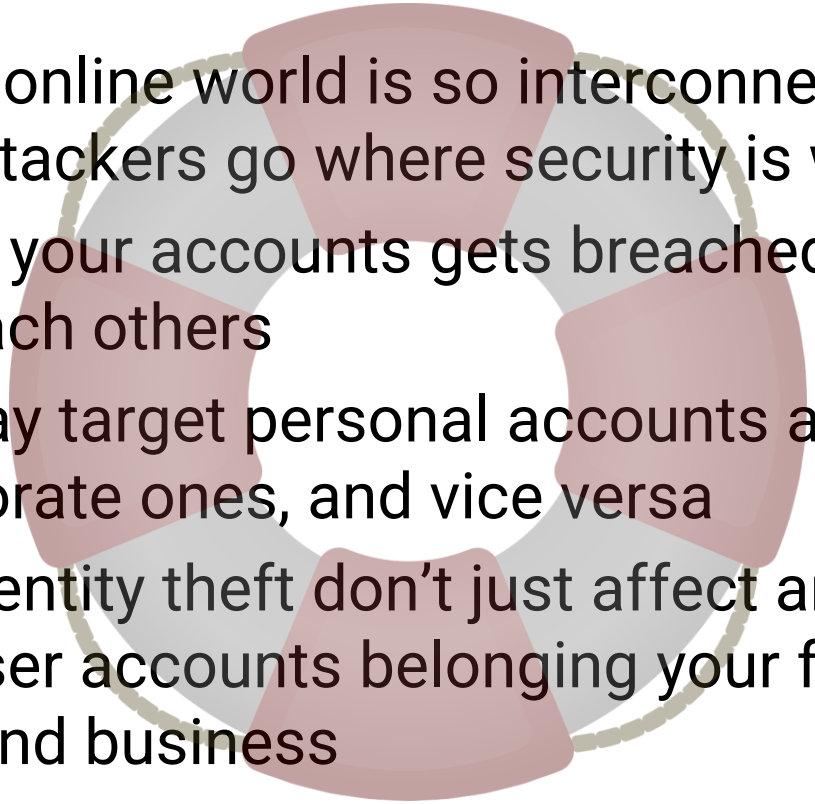
Examples

- ✓ Identity theft
- ✓ Child sexual abuse materials
- ✓ Financial theft
- ✓ Intellectual property violations
- ✓ Malware
- ✓ Malicious social engineering

Motive Behind Cybercrimes



Why Should User Care?



- Because the online world is so interconnected, everyone is a target Attackers go where security is weakest
- If just one of your accounts gets breached, criminals can use it to breach others
- Criminals may target personal accounts and data to breach corporate ones, and vice versa
- Fraud and identity theft don’t just affect an individual; it can affect user accounts belonging your family, friends, coworkers, and business

Cybersecurity is Safety

- **Security-** We must protect our computers and data in the same way that we secure the doors to our homes.
- **Safety-** We must behave in ways that protect us against risks and threats that come with technology.

Impact of Cybercrime

- A study by Deloitte's reveals that, "Various organizations lost 5% of their total business impact due to cybercrime.
- According to IBM different companies faces 60% of their reputation failure within 6-12 months of a successful cyber attack.
- According to the IBM and Ponemon Institute average cost of security breach in 2021 is $4.2M which is a 10% raise from 2020.

Statistics to Imagine the Severity of the Attacks

- Only this year total number of major cyber-attacks held 1,291 worldwide which causes more than $6 trillion in 2021 [Source, McAfee]
- And per day more than 2,200 cyber-attacks per day. That equates to about one cyber-attack every 39 seconds.
- Globally, 30,000 websites are hacked daily. 64% of companies worldwide have experienced at least one form of a cyber-attack
- Globally, 1,097 organizations were hit by ransomware attacks in the first half of 2021 which causes more than $75 billion in 2021

Statistics to Imagine the Severity of the Attacks

- According to the Kaspersky Security Bulletin, Bangladesh is in the second position in the level of infection among all the countries.
- 69.55% unique users are in the highest risk of local virus infection in Bangladesh.
- 80% users are the victim of spam attack.

User Awareness

Cyber-Criminals

System Administrators
Some scripts appear useful to manage networks…

Cracker:
Computer-savvy programmer creates attack software

Posts to

Hacker Bulletin Board
SQL Injection
Buffer overflow
Password Crackers
Password Dictionaries

Script Kiddies:
Unsophisticated computer users who know how to execute programs

Downloads

Reports

Successful attacks!
Crazyman broke into …
CoolCat penetrated…

Posts to

Criminals: Create & sell bots -> generate spam
Sell credit card numbers, etc…

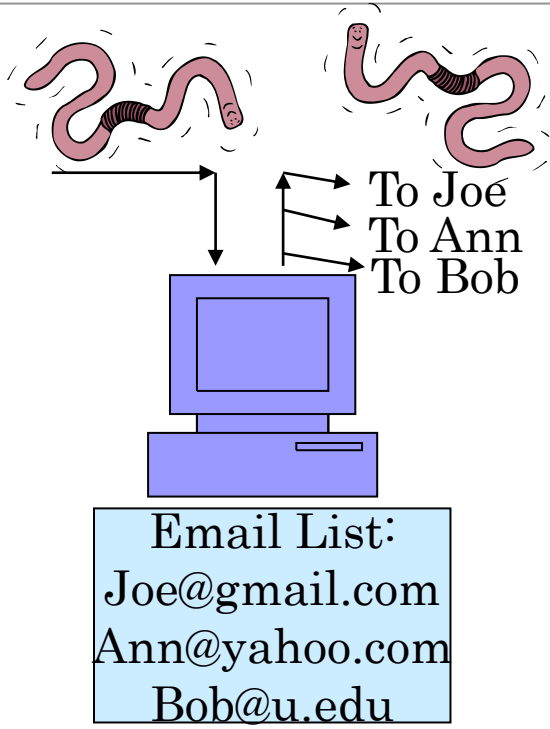
Malware package earns $1K-2K
1 M Email addresses earn $8
10,000 PCs earn $1000

Leading Threats in Cyber World

- Malware
- Ransomware
- Bots & Rootkits
- Viruses & Trojan Horses
- Social Engineering
- Phishing
- Public Wi-Fi

- Financial (theft, fraud, blackmail)
- Political /state (state level/ military)
- Fame/ kudos (fun/ status)
- Hacktivism (cause)
- Pen testers (legal hacking)
- Police
- Insider
- Business

Malware



What is Malware?

Any software intended to…

- Damage
- Disable

- Or give someone unauthorized access to your computer or other internet-connected device

Ransomware

- **What is Ransomware?**
- Malware that is designed to make data or hardware inaccessible to the victim until a ransom is paid
- Wannacry attack 2017 - One of the biggest cyber attacks to occur.
- Is said to have hit 300,000 computers in 150 countries.
- Companies affected include; NHS, Renault, FedEx, Spanish telecoms and gas companies, German railways.

Examples

- Cryptolocker
- Winlock
- Cryptowall
- Reveton
- Bad rabbit
- Crysis
- Wannacry

Social Engineering

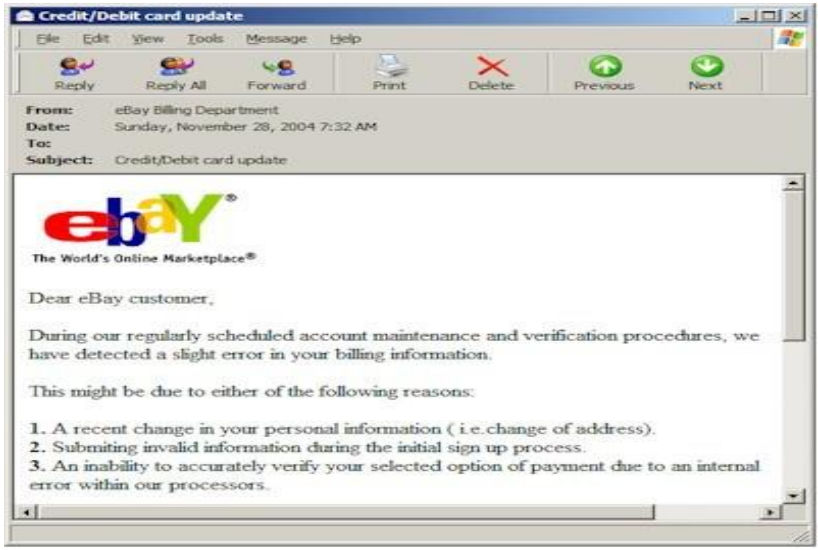
- Criminals Can take advantage of you by using information commonly available through-
  - Social media platforms
  - Location sharing
  - In-person convers

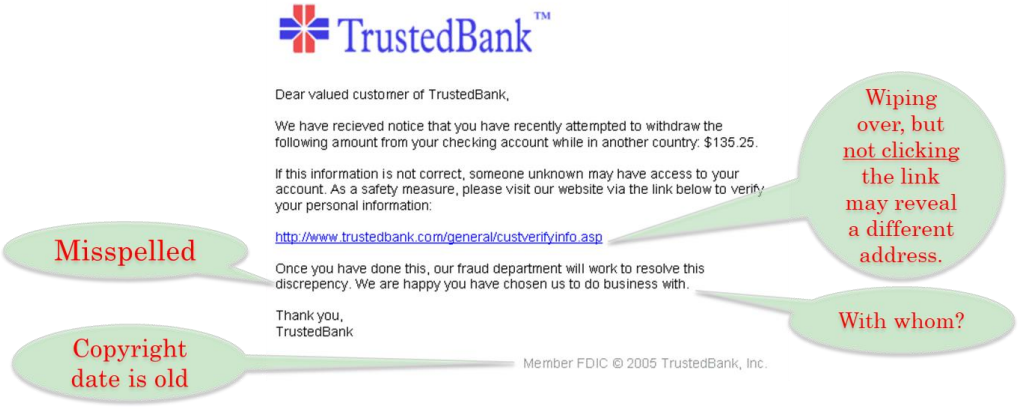
Examples

- Phishing
- Pretexting
- Baiting
- Quid pro quo
- Tailgating
- Inside job
- Swatting

Phishing

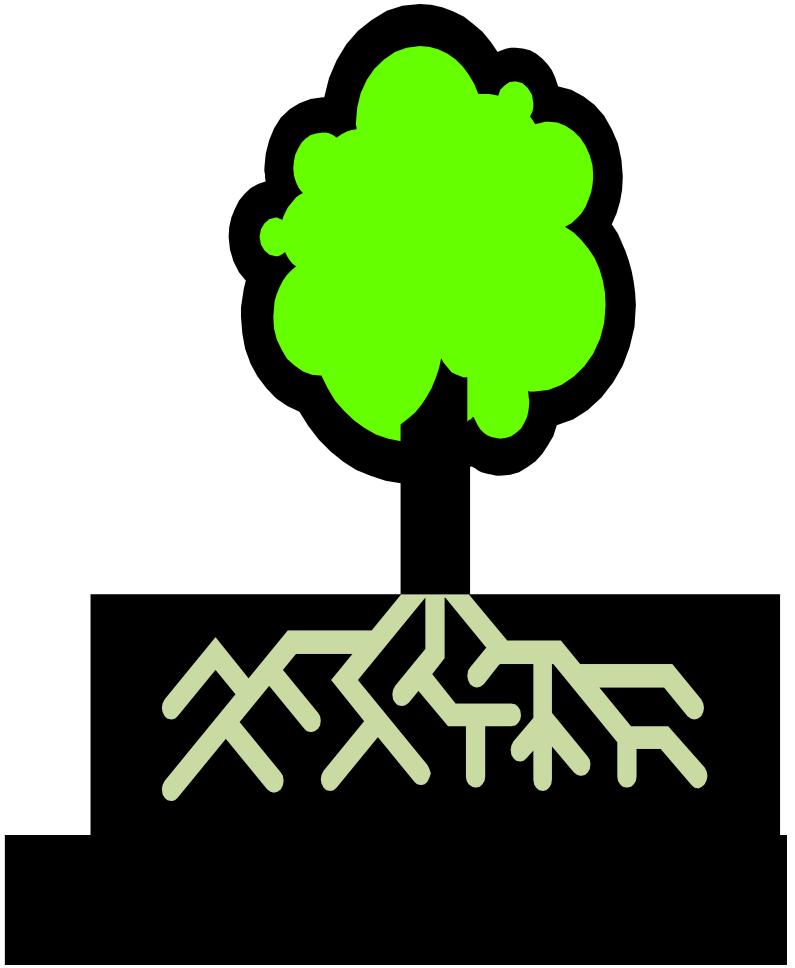
- Phishing: A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.





Rootkit

- Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.
- May enable:
  - Easy access for the hacker (and others)into the enterprise
  - Keystroke logger
- Eliminates evidence of break-in.
- Modifies the operating system.



How to Handle Cyber threats?

You are the best defence!

- Technology is only a small part of Cyber Defence
- **You** are the most important person – protect yourself
- For businesses the most important and best defence is Cyber Security Aware employees – train your staff

Always be aware!

Always be on your guard!

How to Handle Cyber threats?

Proactive Measures

- Building Cyber Security Awareness Among the Employees
- Develop Standard Security Policy for the company
- Staff Training
- Develop Resilience Network
- Security Audit
- Ensure Proper Implementation of Company Security policy

Reactive Measures

- **Incident Response Team**
- **Vulnerability assessment and analysis**
- **Disaster Recovery plan**
- **Reinstallation procedures**



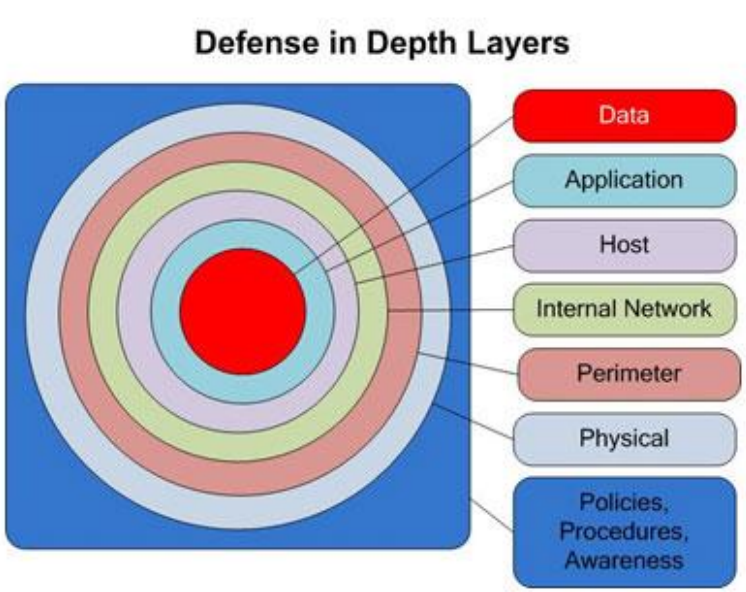


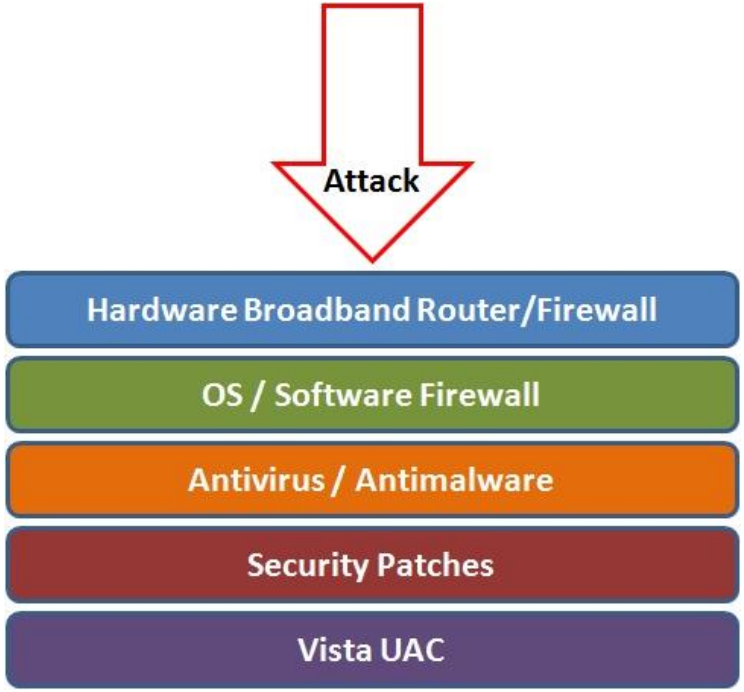

Required Security Awareness Fields

- Password Security
- Email Security
- Safe Browsing
- Ransomware
- Privacy
- Data Security and Encryption
- Mobile Device Security
- Duo Account Security
- Securing The Human Training
- Reporting an incident
- Reminders
- Other Security Resources

Best Practices to avoid these threats

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.





Digital Security Act Bangladesh

Key Provisions of Digital Security Act 20218, Bangladesh:

- ✓ The act includes provisions for punishment for offenses such as hacking, spreading propaganda, and cyber terrorism.
- ✓ It also includes provisions for the protection of personal data and privacy.
- ✓ The act allows law enforcement agencies to seize digital devices for investigation purposes.

Reporting Cybercrime

- Report to
  - https://www.facebook.com/cpccidbdpolice/
- Hotline
  - +8801730336431
- National Incident Reporting portal
  - https://www.cirt.gov.bd/incident-reporting/
- Police Cyber Support for Woman
  - https://www.police.gov.bd/en/police_cyber_support_for_women

Open Discussion

THANK YOU

Part II : The Basics of Cybersecurity

PRESENTED BY
ABK Bhuiyan
Guest Lecturer
Daffodil International University

Do Your Part. #BeCyberSmart

Cybersecurity Divisions

1

Computer Security

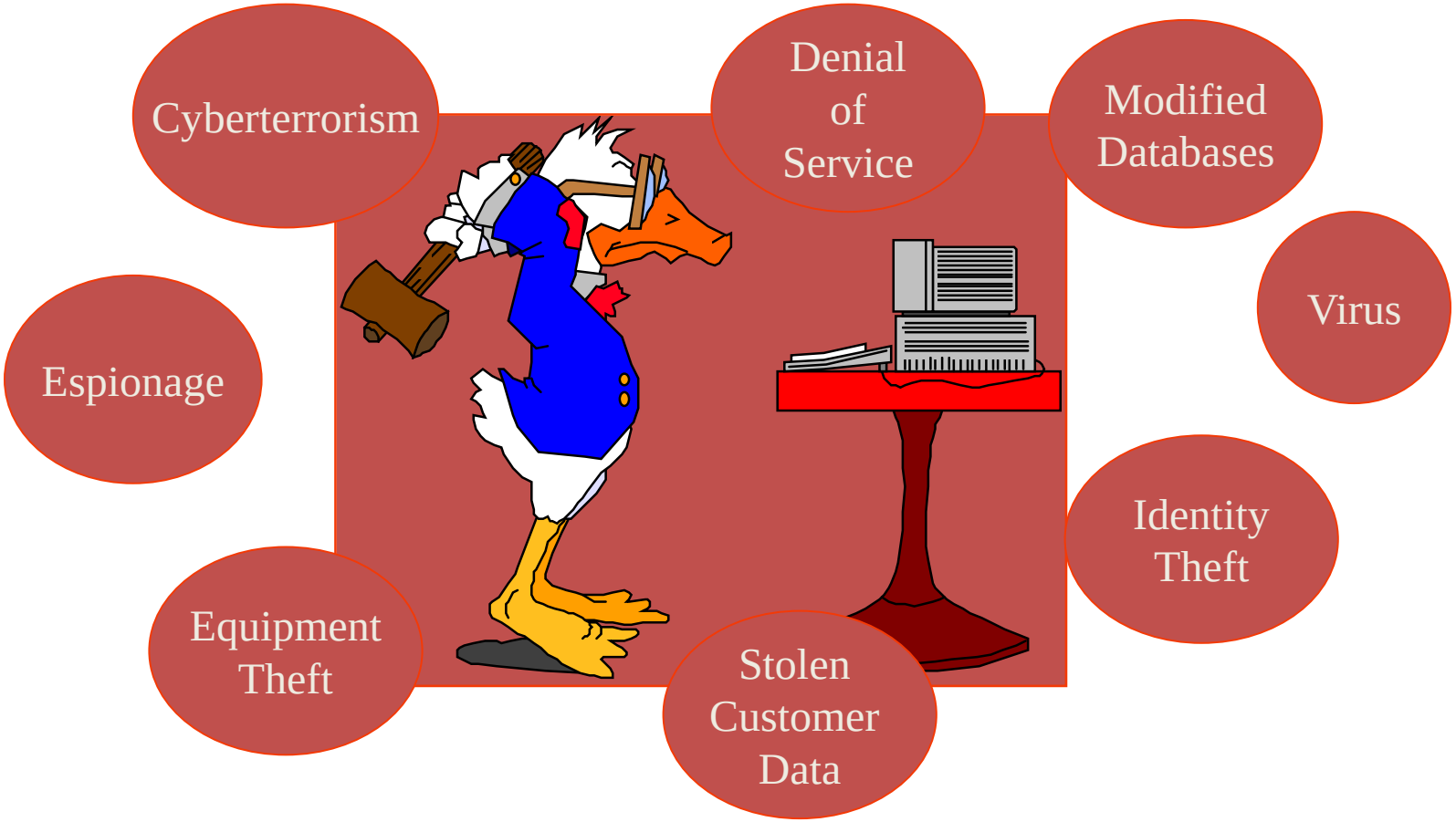
"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)."

2

Cryptography

"The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification."

“Secure” Computer System



Security Objectives

Confidentiality: Who is authorized?

Integrity: Is data „good?"

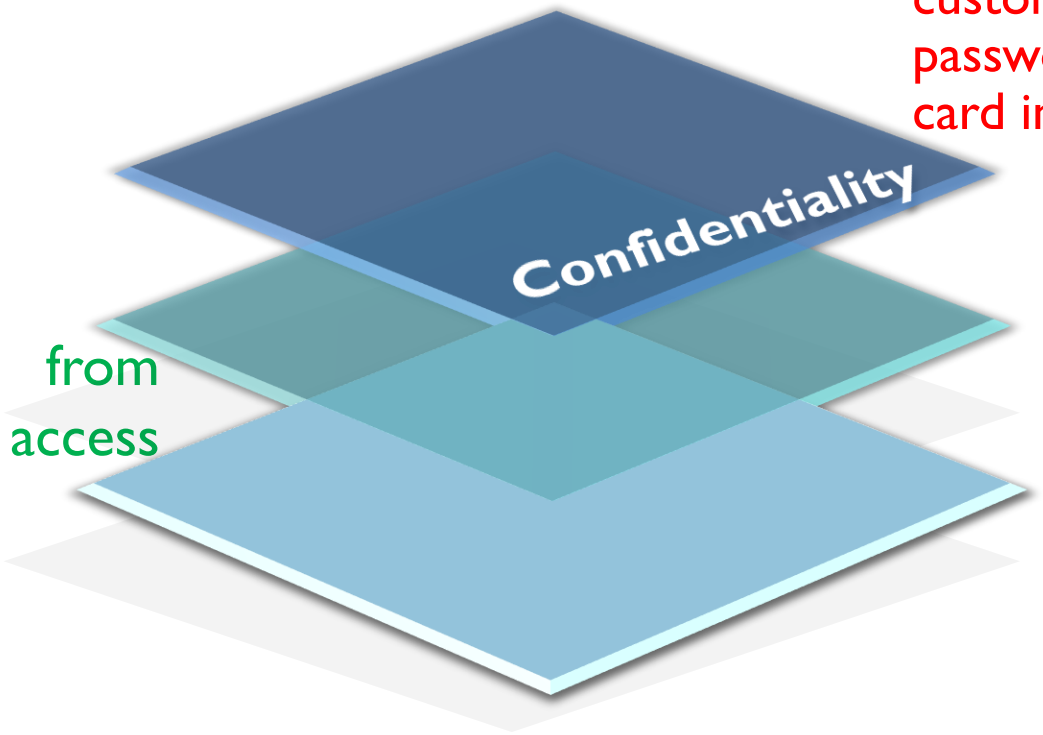
Availability: Can one access data whenever needed?

More
NIST Special Publication 800-12, revision 1 *An Introduction to Information Security* section 1.4

Confidentiality

Example:

Criminal steals customers' usernames, passwords, or credit card information

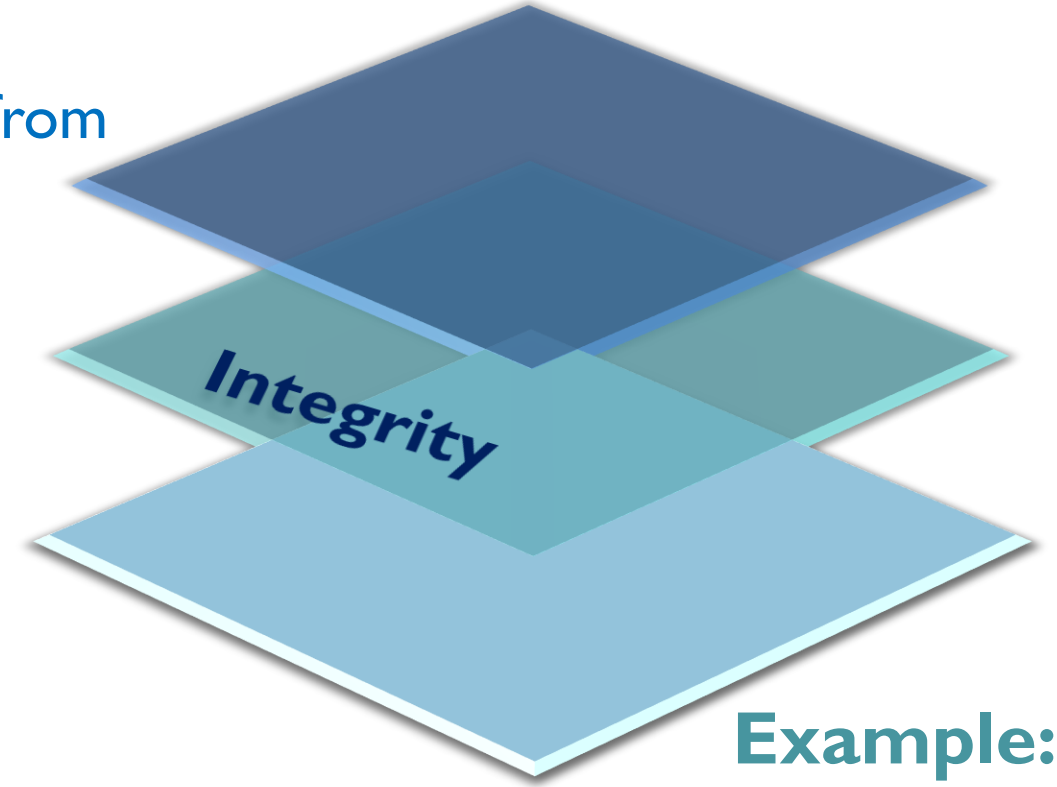


Protecting

information from unauthorized access and disclosure

Integrity

Protecting information from unauthorized modification



Example:

Someone alters payroll information or a proposed product design

Availability

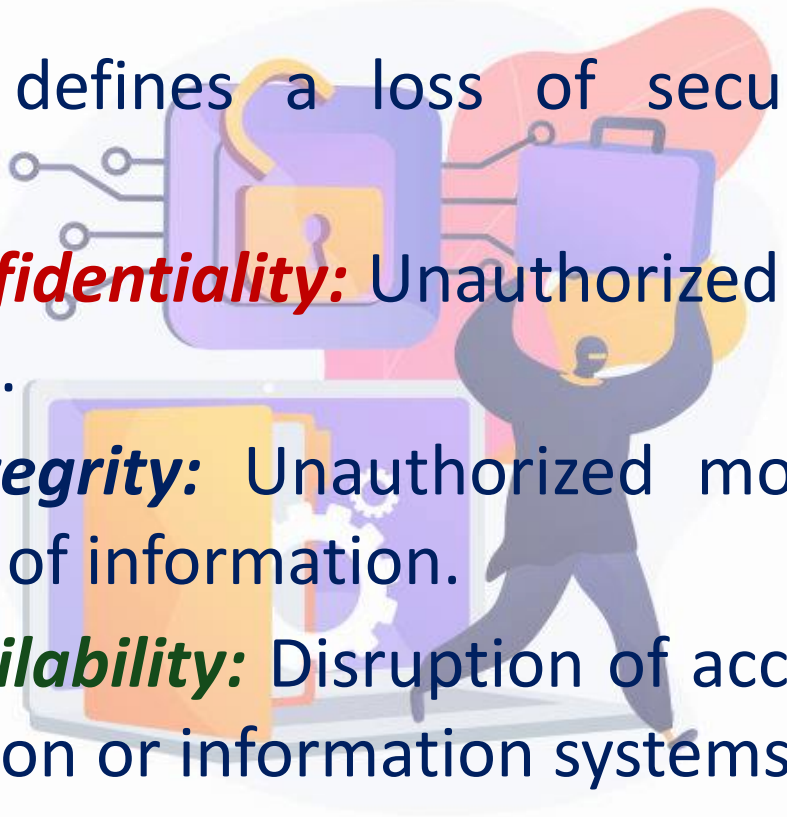
Example:

Your customers are unable to access your online services

Preventing

disruption in how information is accessed

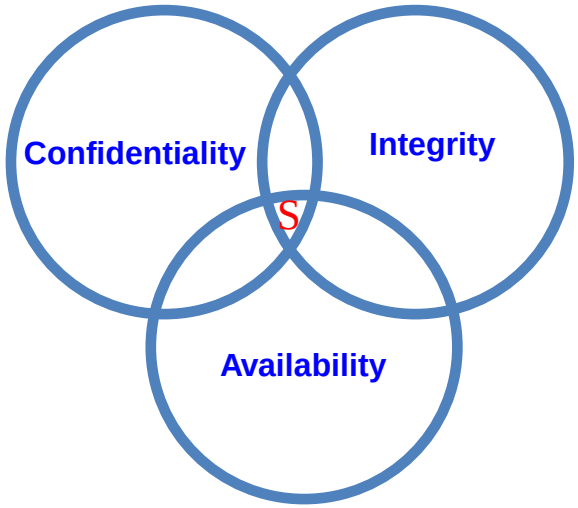
Loss of Security

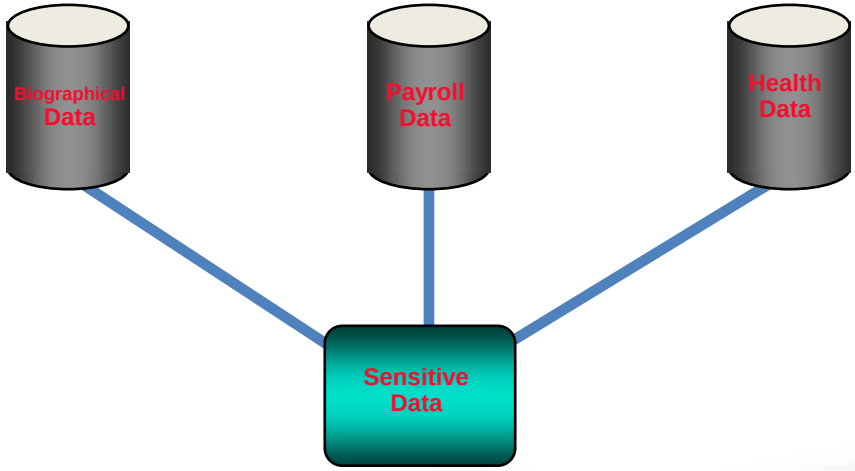


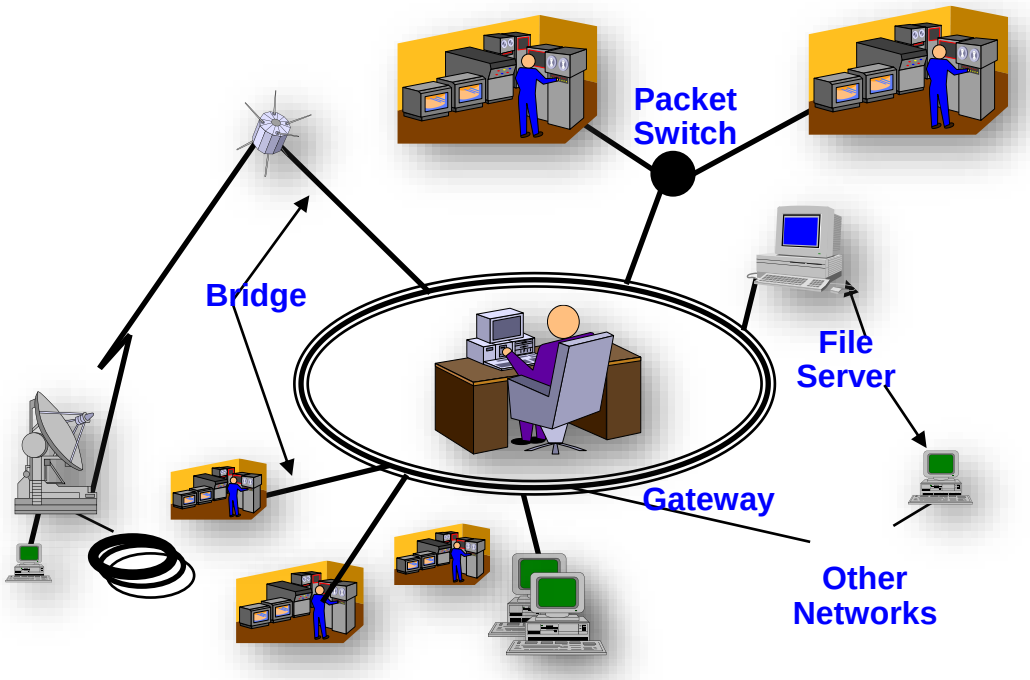
The following defines a loss of security in each objective:

- ***Loss of Confidentiality:*** Unauthorized disclosure of information.
- ***Loss of Integrity:*** Unauthorized modification or destruction of information.
- ***Loss of Availability:*** Disruption of access to or use of information or information systems.

Balancing CIA







Need to balance CIA

Ex: Disconnect computer from Internet to increase confidentiality (availability suffers, integrity suffers due to lost updates)

Ex: Have extensive data checks by different people/systems to increase integrity (confidentiality suffers as more people see data, availability suffers due to locks on data under verification)

Security Attacks

Attack

= exploitation of one or more vulnerabilities by a threat; tries to defeat controls

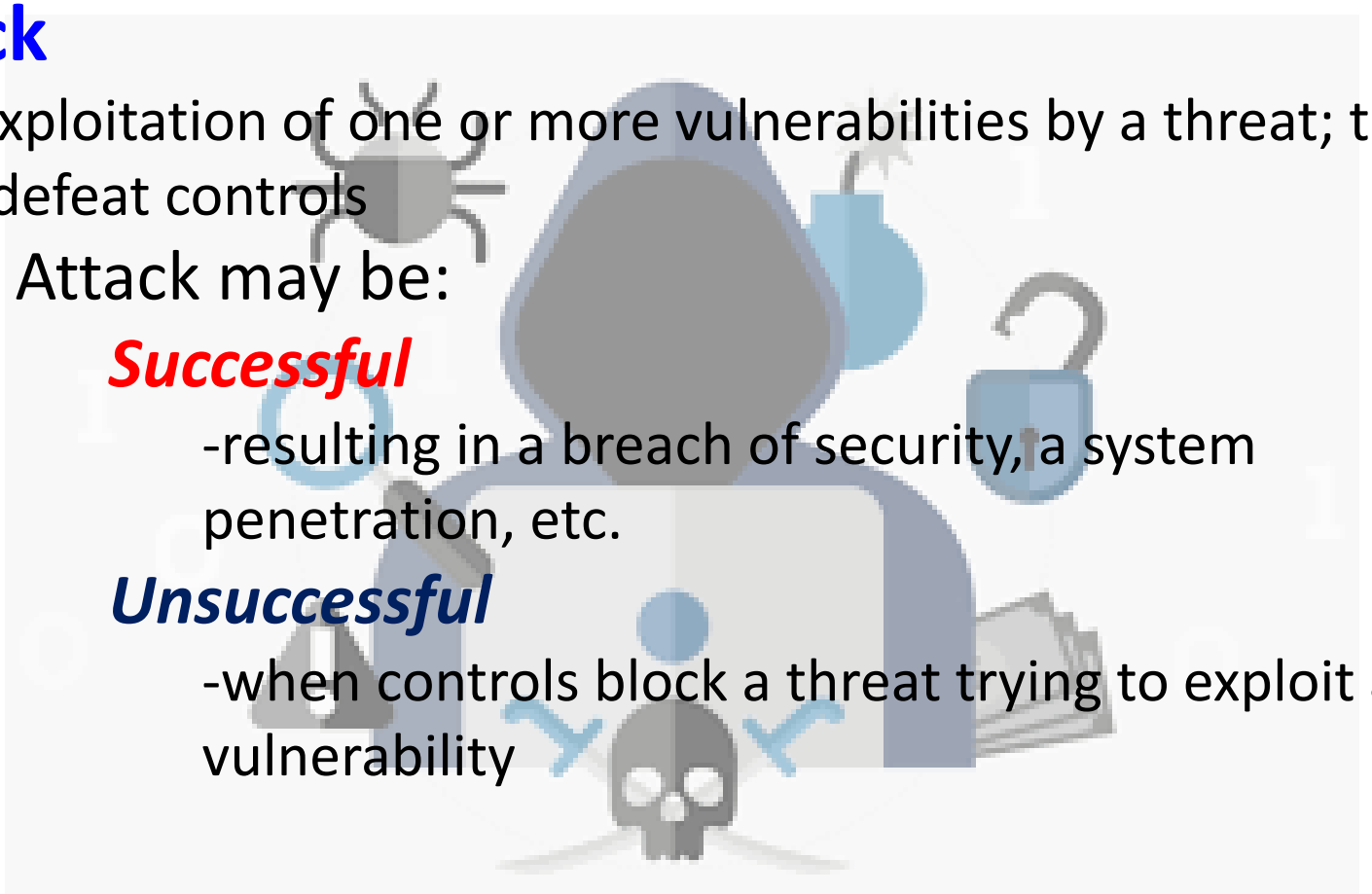
Attack may be:

Successful

-resulting in a breach of security, a system penetration, etc.

Unsuccessful

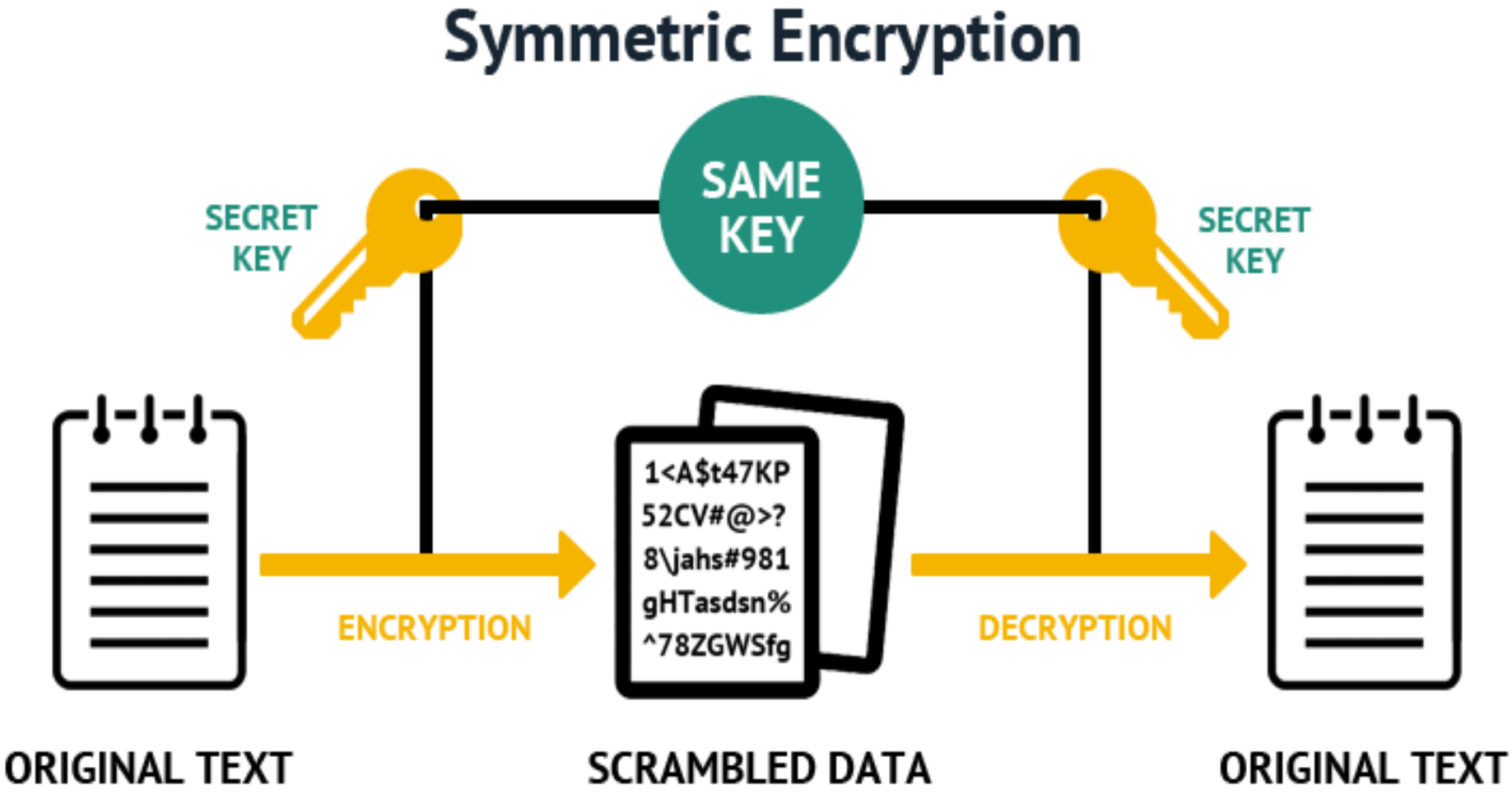
-when controls block a threat trying to exploit a vulnerability



Cryptography

- A collection of mathematical techniques for protecting information
- Most important technique is ***encryption/decryption***
  - ✓ ***Symmetric encryption*** (symmetric key encryption):
    - encrypt/decrypt a message using the same key
    - ***Key***: a piece of information or sequence of bits
  - ✓ ***Asymmetric encryption*** (asymmetric key encryption):
    - one key used for encryption (public key), another key used for decryption (private key)

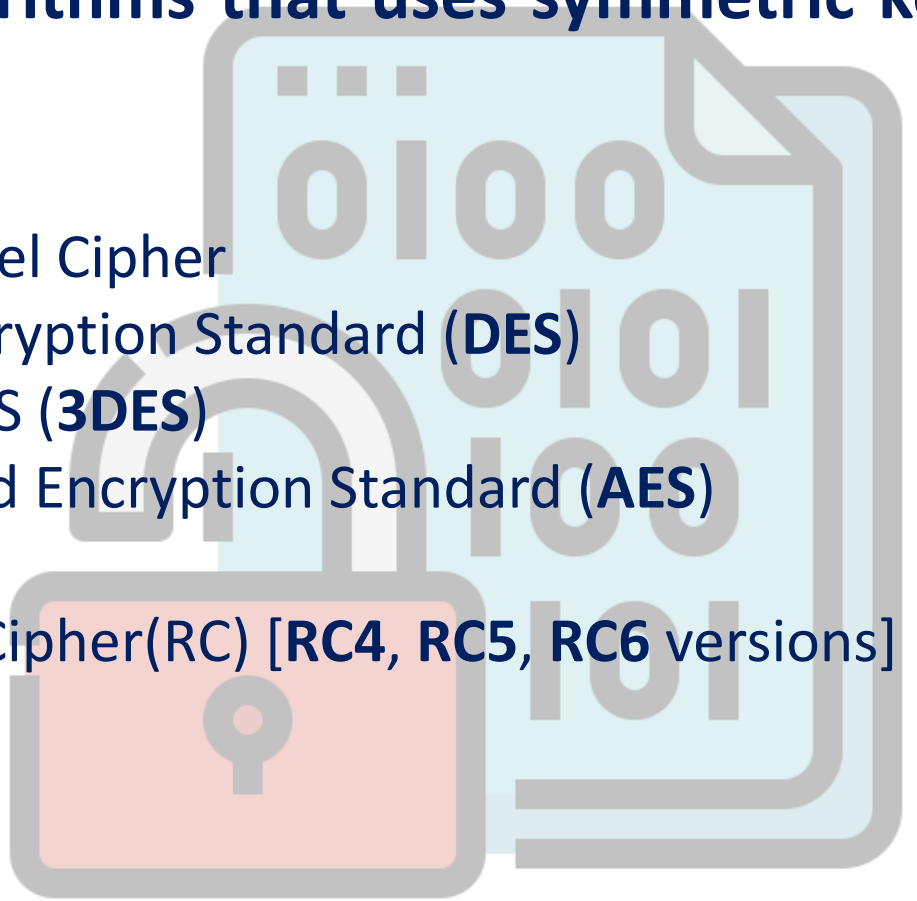
How Symmetric Key Encryption Works



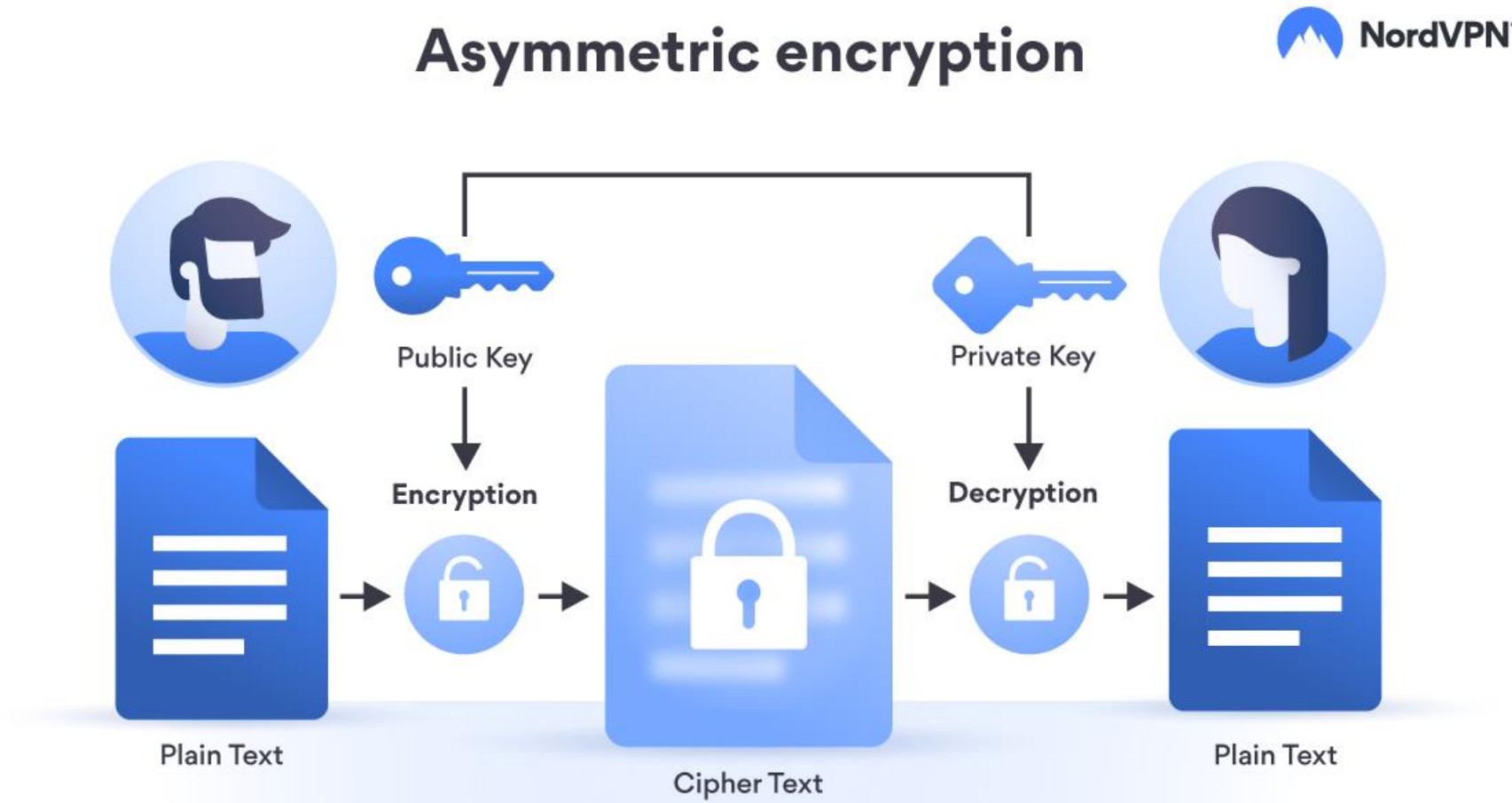
Symmetric Encryption

- **Some algorithms that uses symmetric key encryption method:**

  - ✓ The Feistel Cipher
  - ✓ Data Encryption Standard (**DES**)
  - ✓ Triple DES (**3DES**)
  - ✓ Advanced Encryption Standard (**AES**)
  - ✓ **Blowfish**
  - ✓ Rivest's Cipher(RC) [**RC4**, **RC5**, **RC6** versions]



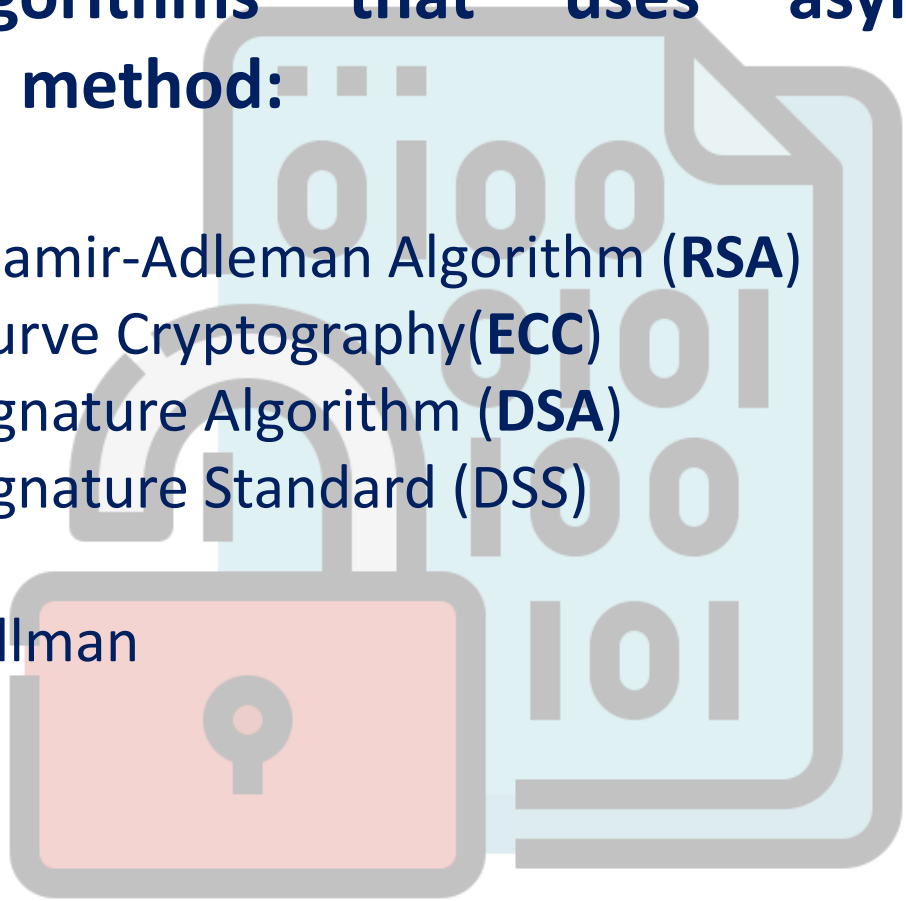
Asymmetric Encryption: How Works



Asymmetric Encryption

- **Some algorithms that uses asymmetric key encryption method:**

  - ✓ Rivest-Shamir-Adleman Algorithm (**RSA**)
  - ✓ Elliptic Curve Cryptography(**ECC**)
  - ✓ Digital Signature Algorithm (**DSA**)
  - ✓ Digital Signature Standard (DSS)
  - ✓ **El Gamal**
  - ✓ Diffie-Hellman



Open Discussion

contact me

- +880 1831 661534
- +880 1775 168357
- abkbhuiyanjehad@gmail.com
- abdullah.bin@contessabd.com
- abdullah.cis@diu.edu.bd
- www.linkedin.com/in/abdullah-bin-kasem-bhuiyan

THANK YOU