Cyber Security What Why Where?

Let us build some basic understanding!

August 2023

CAZE LABS
ignite innovations, harness open source!

www.cazelabs.com

Module Scope

- Concepts, Terms (Privacy, Confidentiality, Integrity, Threats)
- Criticality and impact of security (Vulnerability)
- Typical Domains and use cases
- Application scenarios

What is Cyber Security?

Cyber

Security

~ Digital, Computer, Information Technology, internet, digital communication, computer-based systems, virtual reality

cybernetics
the science of communications and automatic control systems in both machines and living things.

~ free from danger, threat, harm, damage, loss

physical / not

XYZ Security – Information, Financial, Social, National.....!

Reduce vulnerability, risk, damage...

Make it secure – protect from ...

Protecting computer systems from attacks

Prevention & Recovery

Prevention & Recovery

Cyber Security

What all to protect / types?

Computers | Software/Programs | Networks | Data

Applications (Web, Mobile and More!)

Network

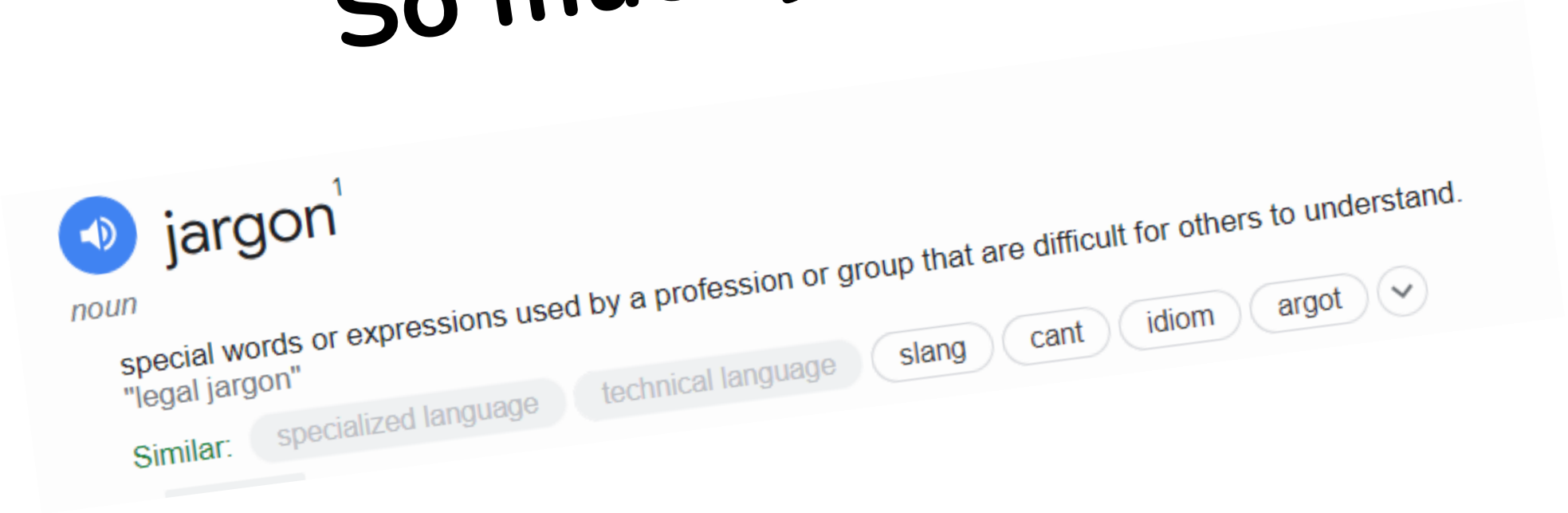
Cloud

Infrastructure

Information (~leak)

Data (~ loss/damage)

So much jargon..!



Cyber Security

Protect C/P/N/D..

Privacy

Assurance of confidentiality/access to info of the entity

Confidentiality

Authorized restriction on access/disclosure of X

Integrity

Complete, correct, unaltered, not tampered, not changed...

Malware

Malicious software designed to harm or exploit

Phishing

Method to gain info with misleading links/websites/emails

Threat

Potential action that can cause harm

Vulnerability

Weakness in the system (threat targets this!)

Risk

Potential situation of loss / damage

Attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access

Encryption

converting information into a code to prevent unauthorized access

VPN

Virtual Private Network – Secure network

2FA

2 Factor Authentication: two steps identification

IDS

Intrusion Detection System – monitors suspicious activities

Authentication

Verify the identity of a person or a device

Hack

Unauthorized intrusion, with malicious intent

Penetration Testing

Simulated/authorized attack to assess/ensure security

Exploit

Malicious code/method to take advantage of a vulnerability (install malware, do DoS…)

CVE

Common Vulnerabilities & Exposures

CVSS

Common Vulnerability Scoring System – standard to assess the severity of vulnerabilities

Access Control

Control the access (authorized)

IAM

Identity and access management

Incident

Instance/occurrence of an attack (cyber attack/security breach)

Incident Response

Process of handling incident

SSL

Secure Sockets Layer – secure link between server and client

SSF

Software Security Framework: evaluating the security of vendors and payment software

PA-DSS

Payment Application Data Security Standard (SSF created by PCI SSC for PA-DSS)

PCI SSC

Payment Card Industry Security Standards Council formed in 2006 by major credit cards companies

Secure SLC

Secure Software Lifecycle validates the security controls and practices (process)

Secure Software Standard

Reviews the overall security of software

?

?

Homework ☺

?

?

?

Criticality & Impact of Security


POP CORN
IT'S MOVIE TIME!


5 Key Cybersecurity Threat Trends in 2023

Cyber attacks increased > 125% through 2021

Internet Users Experienced Cyber Attacks in 2022:
68% India | 49% USA | 40% Australia | 39% Global Average

Data Breach Cost average $4.35 million

236.1 million ransomware attacks occurred globally in the first half of 2022.

Financial

Reputation

Hard to Recover

Additional Reads : Industry Reports

- One Cyber Security Stats
- Report from Akamai
- Report from Crowdstrike

Typical Domains, Use cases and Application Scenarios

Domains

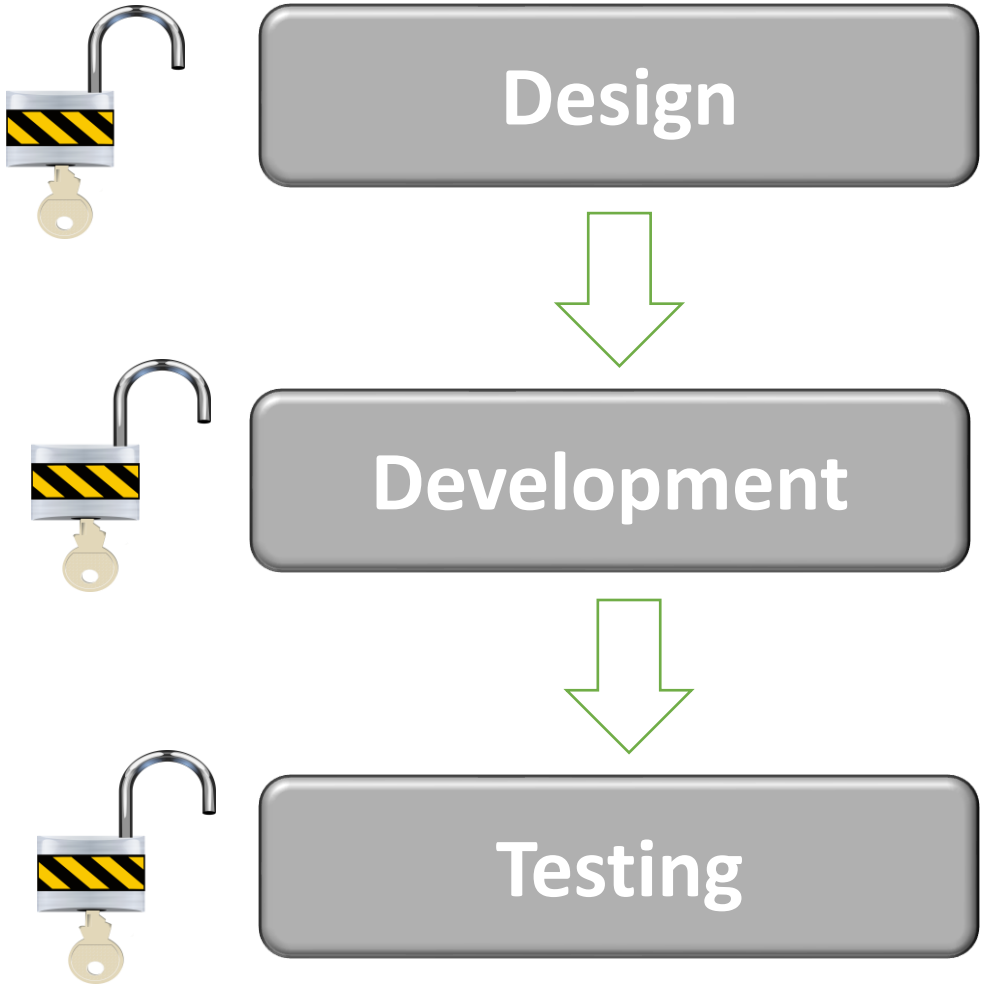
- Application (Web, Mobile…)
- Network
- Cloud
- Information
- Device
- IoT
- Data
- …

Unlimited threats...!

- Malware
- Ransomware
- DoS / DDoS
- Phishing
- Social Engineering
- Exploitation of Exploits (Zero Day Attack)
- MitM Attack
- Drive by Download
- APT (Advanced Persistent Threat)
- Internal Threats (Weak Security Assets)
- ....

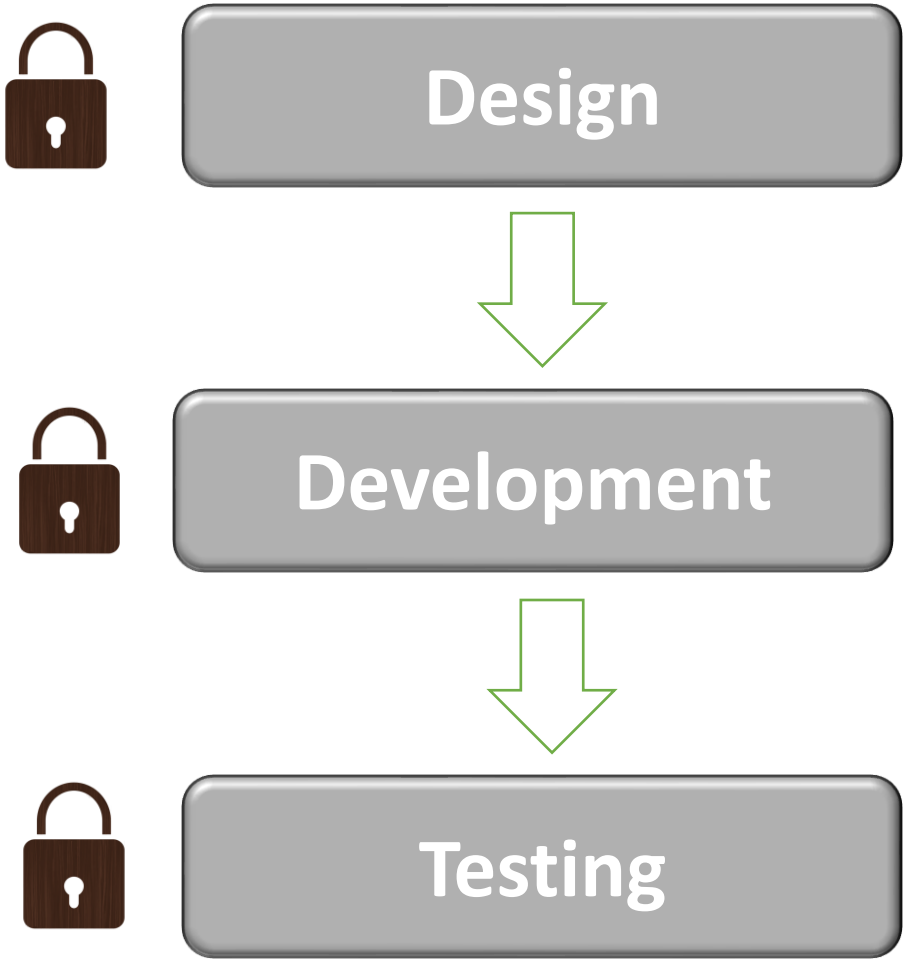
Typical Vulnerabilities

- Lack of DFX for Security
- Unsecured APIs / Communications
- Lack of Auth
- Old software/tech
- Lack of encryption/data protection
- Poor coding practices (unsecured)
- Lack of security testing
- Lack of awareness/security insights
- Unsecured deployments and configs
- Lack of updates
- Open Secrets!
- ....



Explore ways to protect…

- Secure Design & Architecture
- Secure Coding
- Penetration Testing



Encryption | Secure Communication or API | Secure IAM | IDS | Security Standards | Secure Coding Guidelines | Pen Test Methods, Practices | Least Privilege | Fail Safe | Param Validation | Audit trails & logging | Safe Error exception handling | Secure Config | Threat Modeling | Imbibe CVE assessments | risk assessment & mitigation ….

Thank You!

CAZE LABS

ignite innovations, harness open source!

www.cazelabs.com

Disclaimer: The information and content in these slides are intended for general educational purposes only. There can be information from the public domain and no claim on copyrights or usage licensing. Hence, you are not supposed to use it for any other purpose other than for informational & learning purposes. No representations or warranties of any kind are provided. We disclaim any liability for any loss or damage, including indirect or consequential loss or damage, or any loss or damage arising from the use of these educational slides. By using these educational slides, you agree to this disclaimer