03Mar2022

# Classification of Cyber Attack

**SHALEEN KHETARPAUL**
**Assistant Vice President - IT**
**BSES RAJDHANI POWER LTD.**

# Introduction



**BSES RAJDHANI POWER Ltd.**

- JV between BSES (RInfra) and Govt of Delhi
- Distributes power to an area spread over 750 sq. km of South & West Delhi
- Consumer density : ~3100 per sq km.
- Consumer base: Approx 2.7 million
- AT&C Losses: 7.8 % (FY 2021-22)
- Peak Load: 3211 MW (FY 2021-22)

# Why Cyber Security



## Importance of Information & Cyber Security:

**TECHNOLOGY**

- Digital upgrade to new technologies like cloud, AI
- Mobile Applications for consumer and field operations


**SMART GRID**

- 2 way / Bilateral communication
- Big data with correlation


**INTEGRATION (IT & OT)**

- IT – Create, process, store, retrieve & send information
- OT – Monitor & control the performance of physical device


**DEMAND RESPONSE - HOME AUTOMATION PRODUCTS**

- Home utility products
- Electric vehicles, charging stations

# CYBER ATTACK



Cyber attack in Critical Sector are carried with malicious intent:

- **Supply Continuity -** Compromise the Power Supply System
- **Grid Security –**
  - ✓ Render the grid operation in-secure
  - ✓ Gaining Sensitive operational Data
- **Health & Safety -** Equipment damages or even in a cascading grid brownout/blackout
- **Data Protection -** Access to consumer Personal Identity data

Cyber Attack is Classified under 2 categories:

1. **WEB BASED –** Occur on website or Web Application
2. **SYSTEM BASED –** Compromise Network

# Web Based Attacks - I



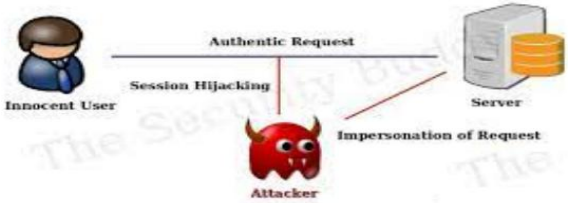
## 1. Injection attacks

- ✓ Malicious input is injected into a web application to manipulate its operation and fetch the required information.
- ✓ Lead to data theft \ loss, loss of data integrity, denial of service
- ✓ **Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

## 2. DNS Spoofing (cache Poisoning)

- ✓ Malicious input is introduced into a DNS resolver's cache, causing re-direct traffic to an incorrect IP address \ website.
- ✓ Lead to access personal information, steal money, spread malware.

## 3.Session Hijacking (Cooking Hijacking)




- ✓ Exploitation of valid user session, to gain unauthorized access to information.
- ✓ Application layer (http) hijacking and Transport layer (TCP & UDP) hijacking

## 4. Phishing

- ✓ Social engineering attack, where malicious actors send messages pretending
- ✓ to be trusted person or entity.

## 5. Brute force

- ✓ Uses a trial and error method, to obtain actual data like user password and personal identification number.
- ✓ Used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

# Web Based Attacks - II



**6. Denial of Service –**

- ✓ Make a server or network resource unavailable to the users.
- ✓ Flooding the target with traffic or sending it information that triggers a crash.
- ✓ It uses the single system and single internet connection to attack a server. It can be classified into the following-

**a. Volume-based attacks –** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

**b. Protocol attacks-** It consumes actual server resources, and is measured in a packet.

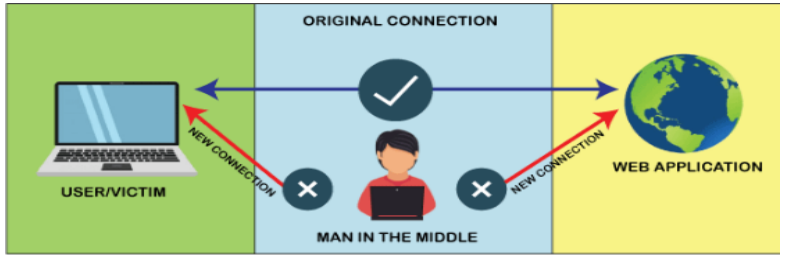
**c. Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

**7. URL Interpretation –**

- ✓ Change certain parts of a URL, to access pages, which he is not authorized to browse..

**8. Man in the middle attacks**

- ✓ Wiretapping, where attacker intercepts the connection between client and server
- ✓ and selectively modifies data.
- ✓ Prevention by using encryption, VPN, etc



# System Based Attacks - I



**1. VIRUS**

- ✓ malicious software program that spread throughout the computer files. Triggered by activation of host or executable file.
- ✓ It is a replicating malicious computer program and can also execute instructions that cause harm to the system.

**2.WORM**

- ✓ Type of malware whose primary function is to self-replicate itself to spread to uninfected computers. Executed via system vulnerability.
- ✓ Worms often originate from attachments that appear to be from trusted senders.

**3.TROJAN HORSE**

- ✓ Designed to collect valuable information from host computer and network.
- ✓ Not self replicating and interprets as application of utility use.

**4.BACKDOORS**

- ✓ Bypasses the normal authentication process, creates an alternative entry point or backdoor to access Dbase and fileserver.

**5. BOTS**

- ✓ A bot (short for "robot") is an automated process to manipulate or disrupt website, application or API.
- ✓ Common examples of bots program are the crawler, chatroom bots, and malicious bots.

# RECOMMENDATION – RISK ASSESMENT



**IDENTIFY ASSETS**

- Prepare an Asset Register
- Categorize assets w.r.t criticality = confidentiality, Availability, Integrity
- Calculate Asset Criticality Value

**IDENTIFY THREATS & VULNERABILITIES**

- Security violation, Incident, Likelihood & Magnitude of Impact,
- Design, Development, Dependency, Testing, VA-PT,
- Existence & effectiveness of existing controls

**ANALYZE & MEASURE**

- Current Controls, New Controls (Cost & Time),
- Increase CIA, Safety, Reliability, Meets Legal & Regulation
- Risk = Asset Criticality * Threat * Likelihood

**MITIGATE & REVIEW**

- Avoid, Transfer, Mitigate, Review
- Implement Controls – Management, Operation, Technical, Policy
- Calculate Residual Risk = Revised Threat * Revised Likelihood

# VULNERABILITY ASSESSMENT & PENETRATION TESTING



**IDENTIFY ASSETS**

- **Scope Selection (IT & OT) –** Risk Sheet, Critical function, Incident etc
- **Identify Vendor –** choose CERT emplaned vendor

**PLAN**

- **Test Strategy -** Discuss test strategy with vendor
- **Test Environment -** Gather data, access, schedule, test bed etc.

**TEST**

- Web Application - Use OWSAP guidelines
- OT (RTU, IED)
- Perform configuration test, Perform penetration test.

**ANALYZE**

- Categorize vulnerabilities w.r.t criticality
- Analyze threat vs vulnerability, discuss with team

**CONCLUDE**

- Close vulnerabilities
- Update Risk Register

# CYBER SECURITY – MITIGATION TECHNIQUES



## GOVERNANCE

1. Framework
2. Internal Audit
3. 3rd party Audit
4. Cyber Insurance

## SERVER

1. Hardening
2. Patching
3. Backup & Restore
4. Redundancy
5. Authentication
6. Anti-Virus
7. Malware Protection

## NETWORK

1. Web Security (Internet)
2. Secured Zoning
3. Device Mapping @ Firewall
4. Intrusion Prevention / Detection
5. Block Open Ports

## APPLICATION

1. Strong authentication
2. Secure Session timeout
3. Encryption & Data Validation
4. Patch Mgmt

## PHYSICAL

1. Isolate
2. Perimeter
3. Fencing
4. Controlled Access

# Thank You

*For discussions/suggestions/queries email: www.indiasmartgrid.org*
*www.isgw.in*
*Links/References (If any)*

**India Smart Grid Forum**
CBIP Building, Malcha Marg,
Chanakyapuri,
Delhi-110021
Website: www.indiasmartgrid.org