How to prevent a Stuxnet like attack on India's soil (Power Infrastructure)

Adarsh Palaskar Indian Institute of Technology, Jodhpur.

Current State of Cyber Security in India

Population 1,295.2 million

Area (km²) 3.3 million

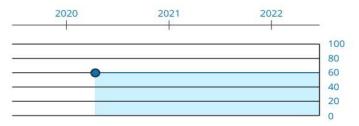
GDP per capita (\$) 7.8 thousand

46th National Cyber Security Index

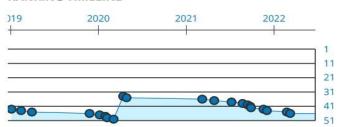
10th Global Cybersecurity Index 134th ICT Development Index

67th Networked Readiness Index

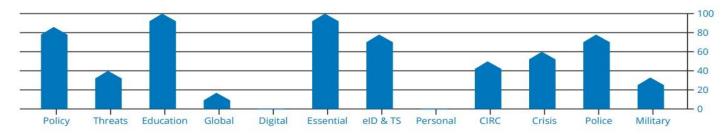
NCSI DEVELOPMENT TIMELINE



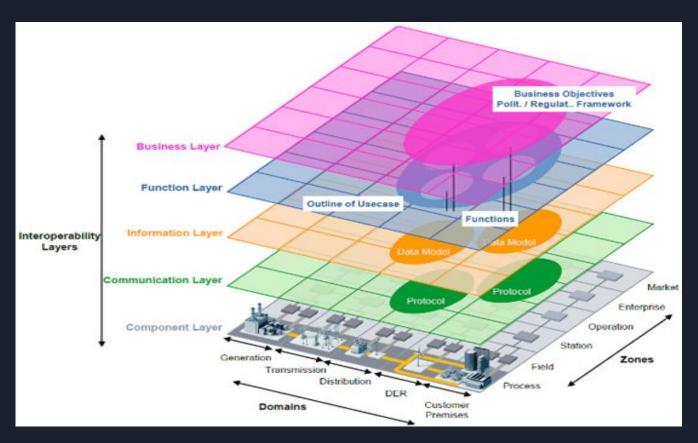
RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE

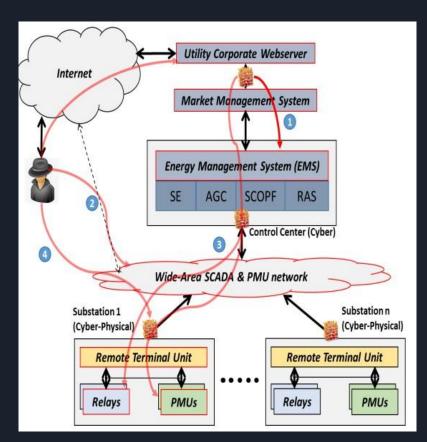


Smart Grid Architecture



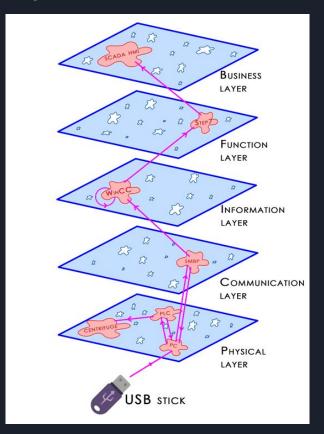
Increasing Attack Surface

- Multiple Attack paths and large attack surface
- Static configuration and network traffic makes it easy for reconnaissance attacks
- Emergence of Internet of Things (IoT)
 in the grid context
- Lack of clear metrics and tools to assess attack surface and to reduce it
- Distribution assets, smart meters, and DERs (wind, solar) are being increasingly deployed and are potentially vulnerable!



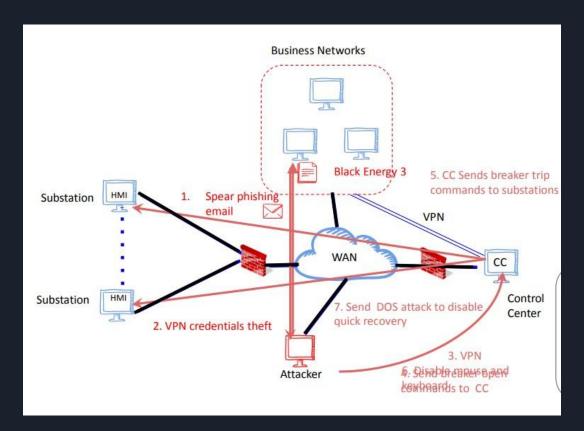
Stuxnet(2010)

- Targeted industrial control systems and compromised code on PLCs
- 7 methods of propagation
- 4 zero-day exploits
- 3 rootkits
- 1 known exploit
- 2 unauthorized stolen certificates
- 2 Siemens security issues
- Took 1 year to discover and
 >100,000 machines infected

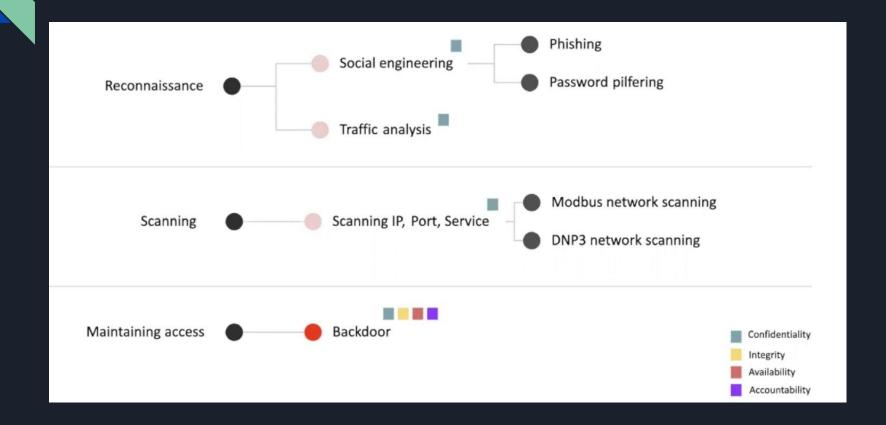


Ukraine's grid attack(2015)

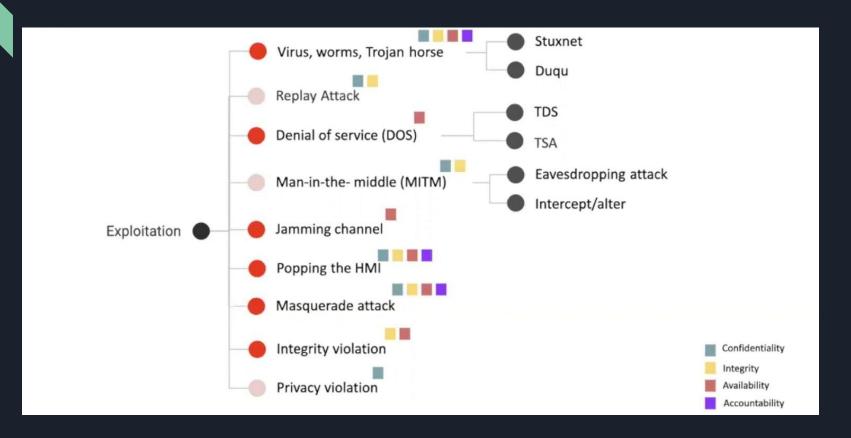
- Coordinated cyber attack
- 3 distribution
 companies ~30
 substations targeted
- 225k customers experienced outage



Smart Grid Attacks



Smart Grid Attacks



Security Strategy

After Attack

Objectives:

Forensics
Deploying an offensive

- Forensic Analysis
- IDS signature, database, and security policies updated.
- Launching an offensive post a successful forensic report

Pre-Attack

Objectives:

Data Security
Device Security
Network Security

- Modern Encryption Techniques
- IDS, SIEM
- Using Firewalls
- Device protection
- Design flaws

During Attack

Objectives:

Attack Detection Attack Mitigation

- Rule based IDS
- Pushback and reconfiguration methods
- FHSS, DSSS
- IDS with smart context

Thank you!