GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

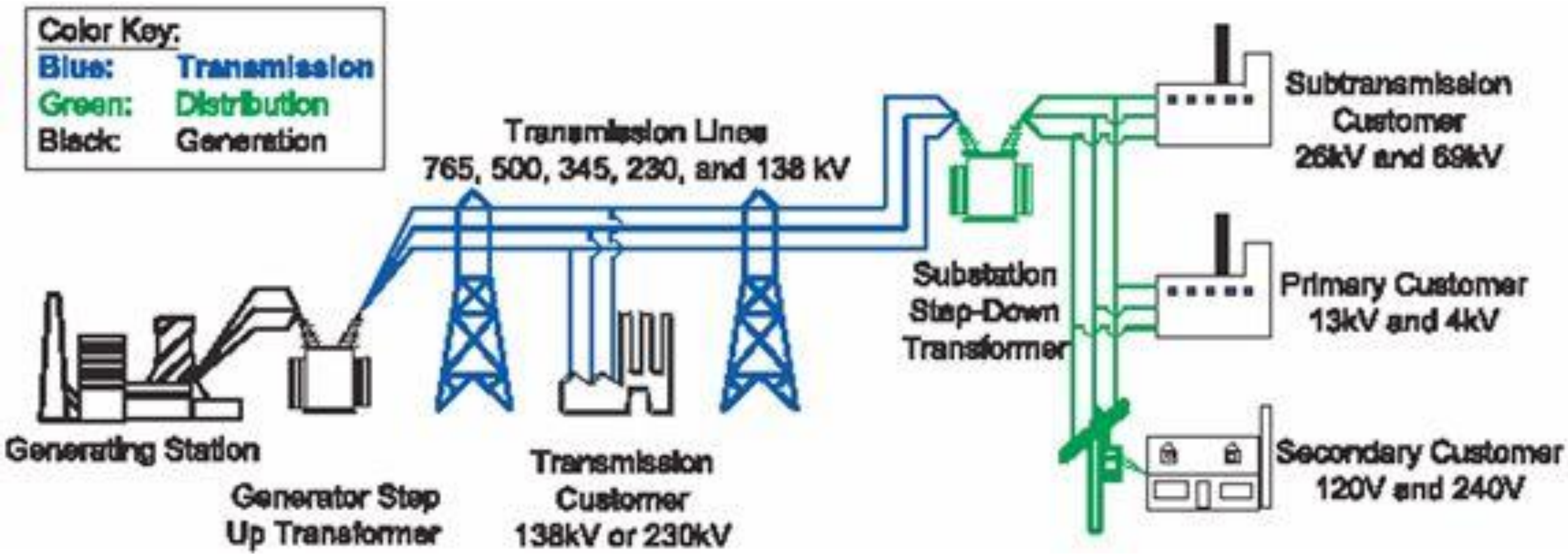
Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

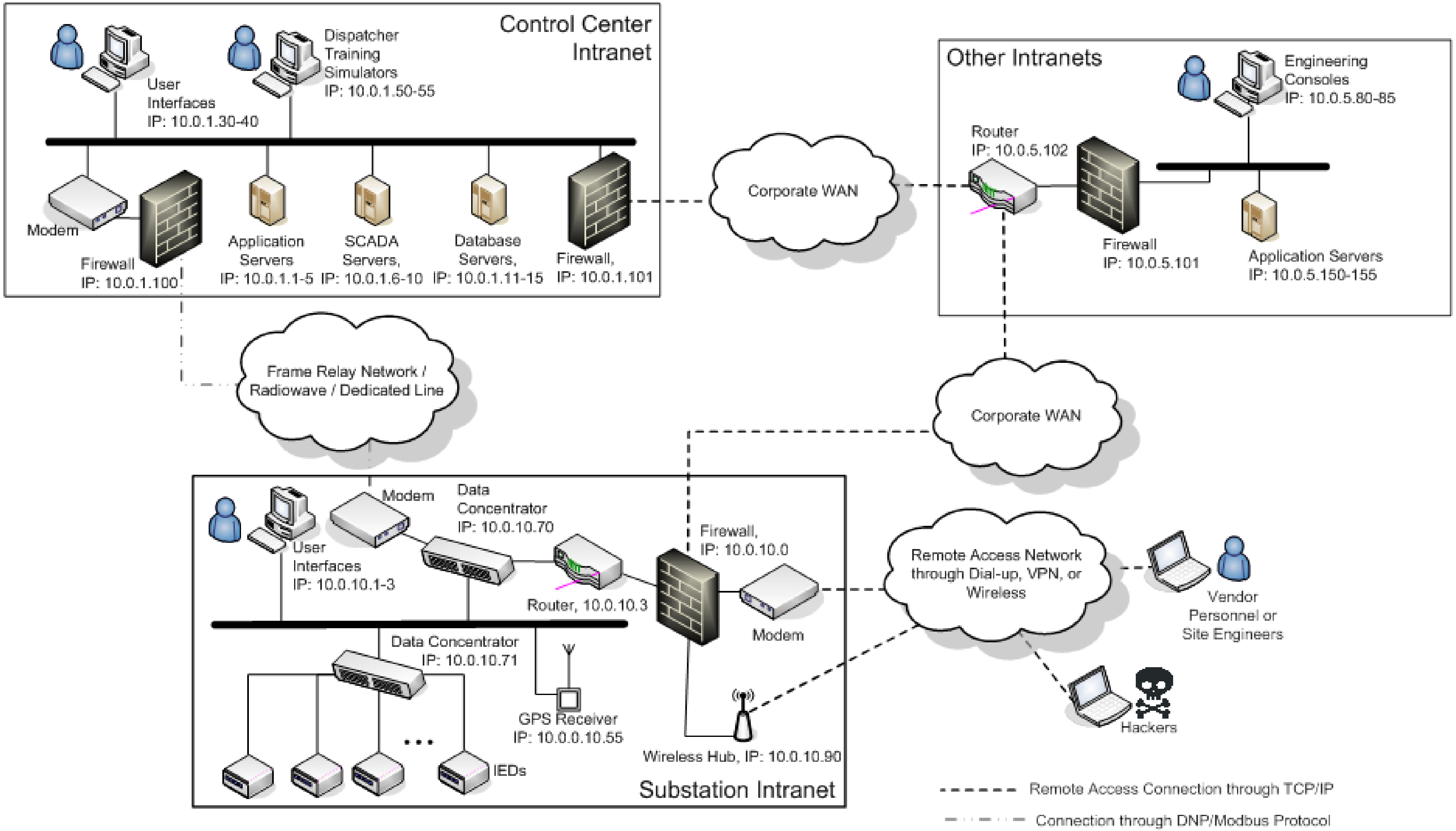
March 5-16, 2018

The Electric Power Grid

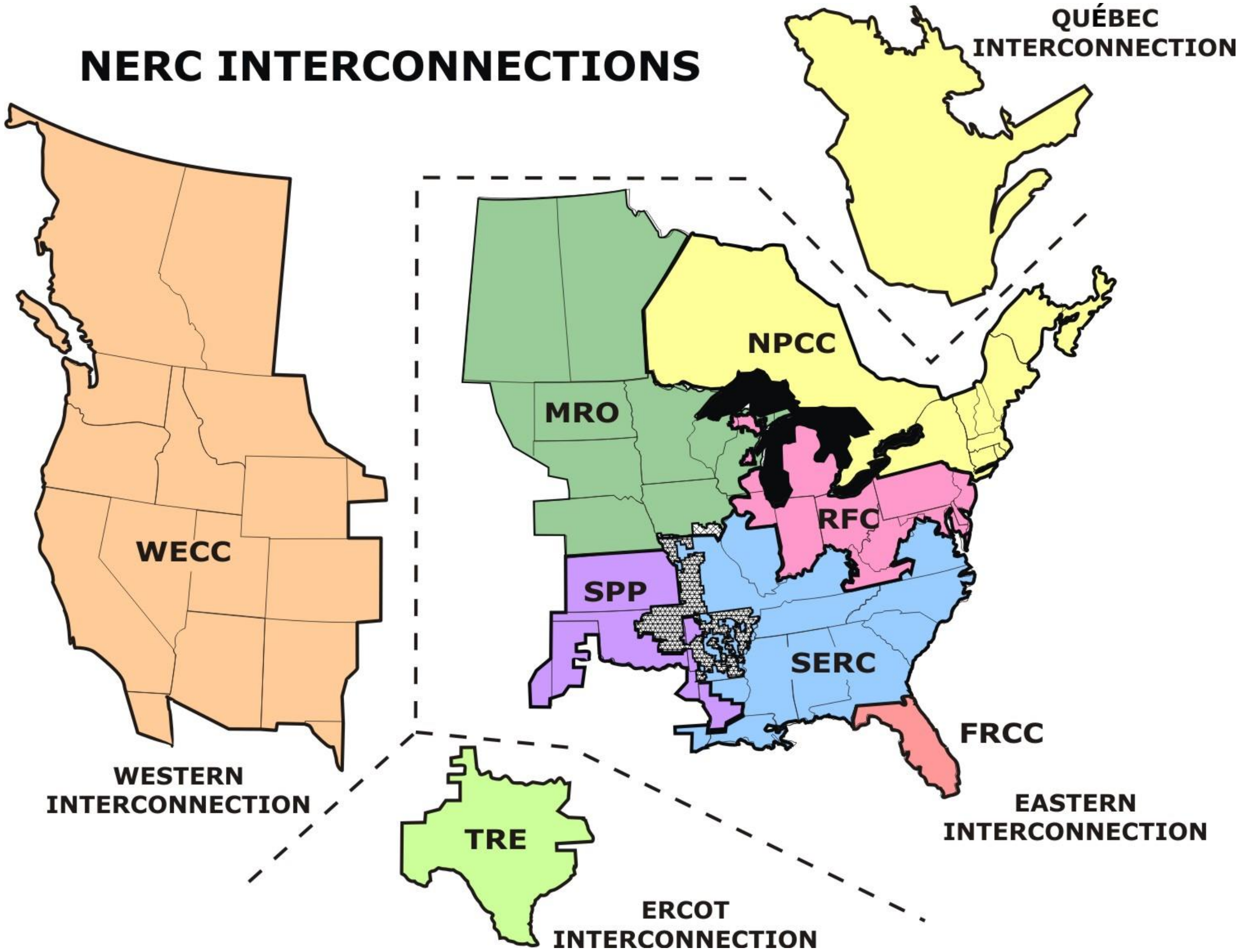


Credit: *U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability*

SCADA Control Network – A schematic

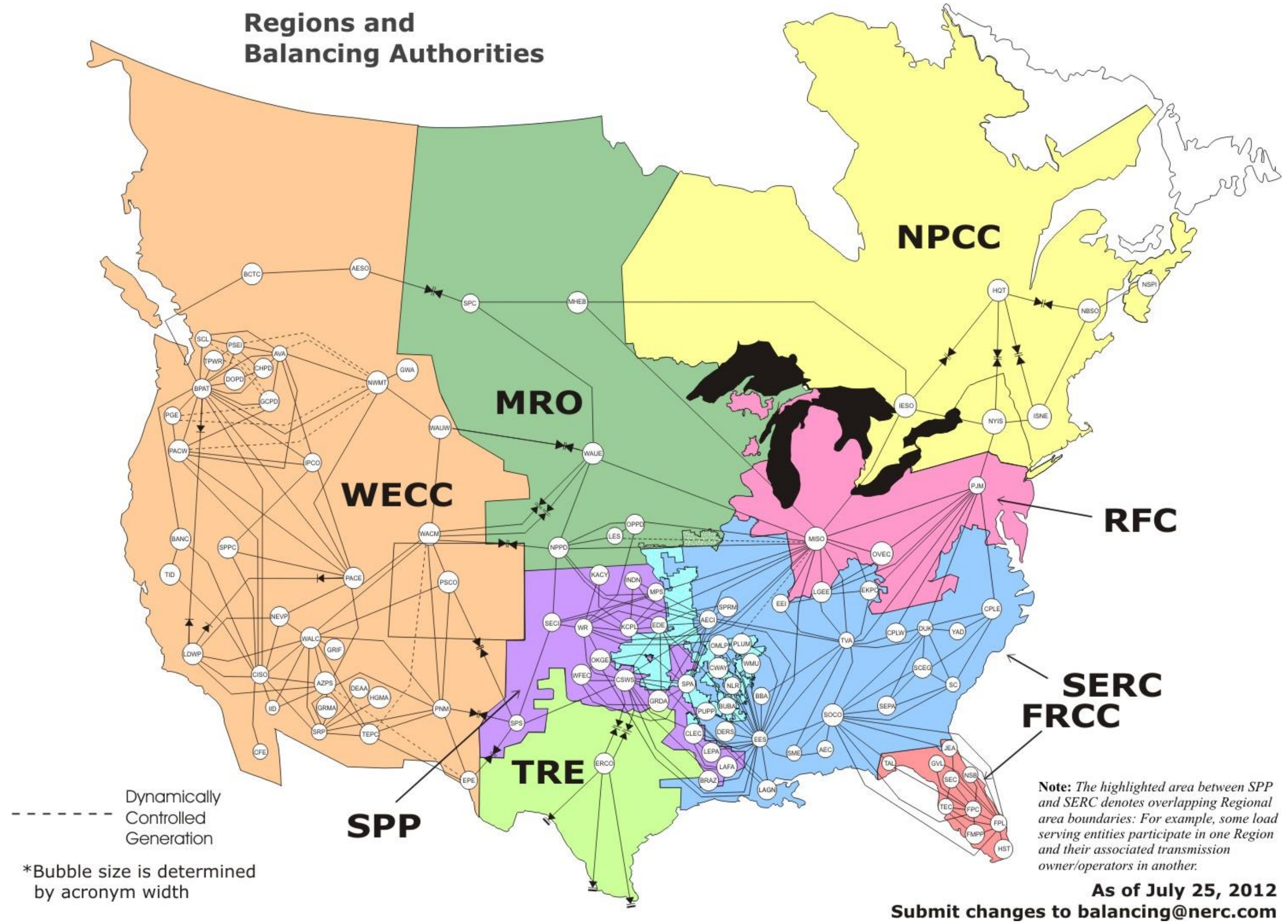


US Power Grid: NERC Interconnections



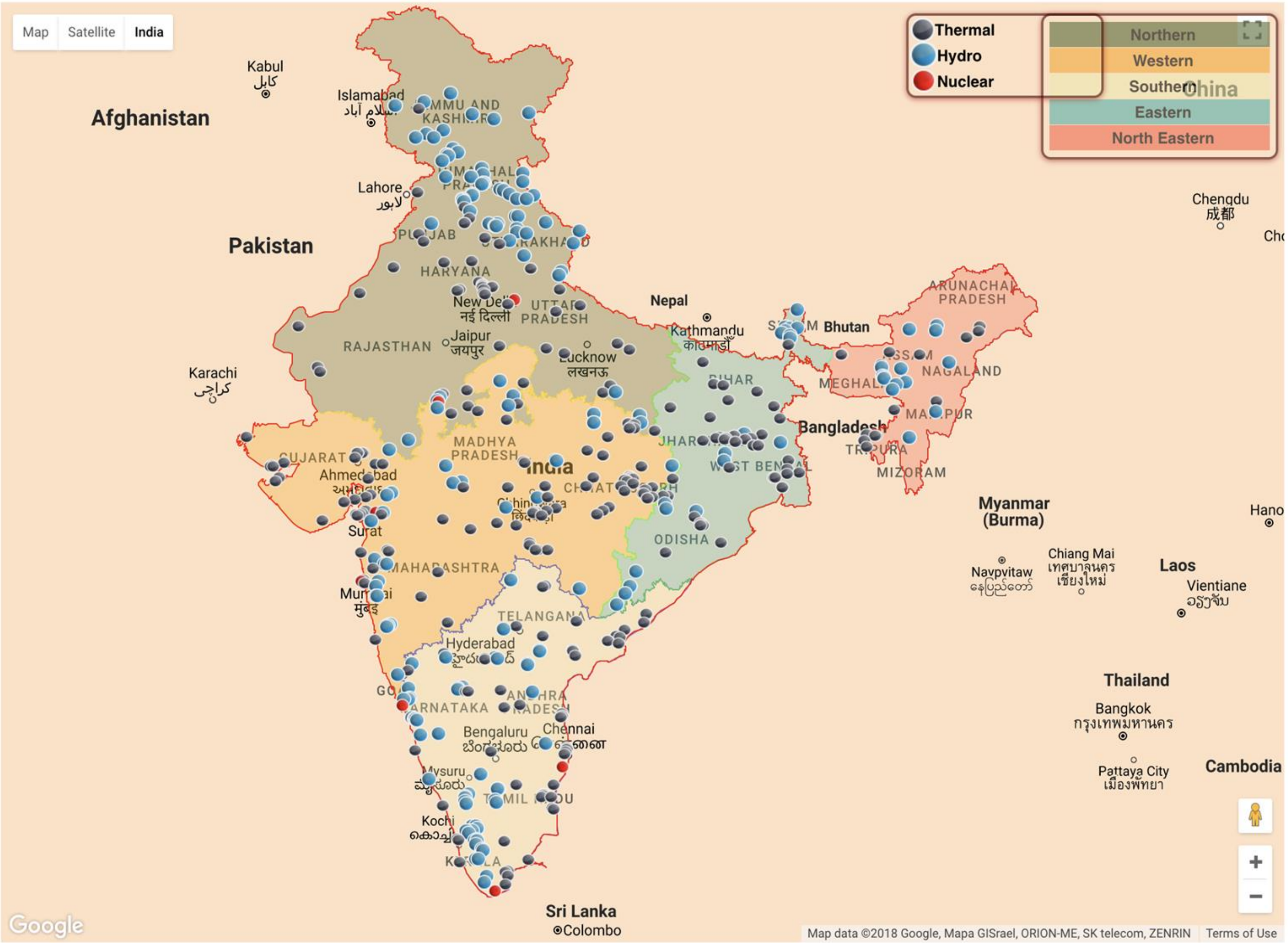
Credit: [North Amercian Electric Reliability Corporation (NERC)]

US Power Grid: NERC Regions



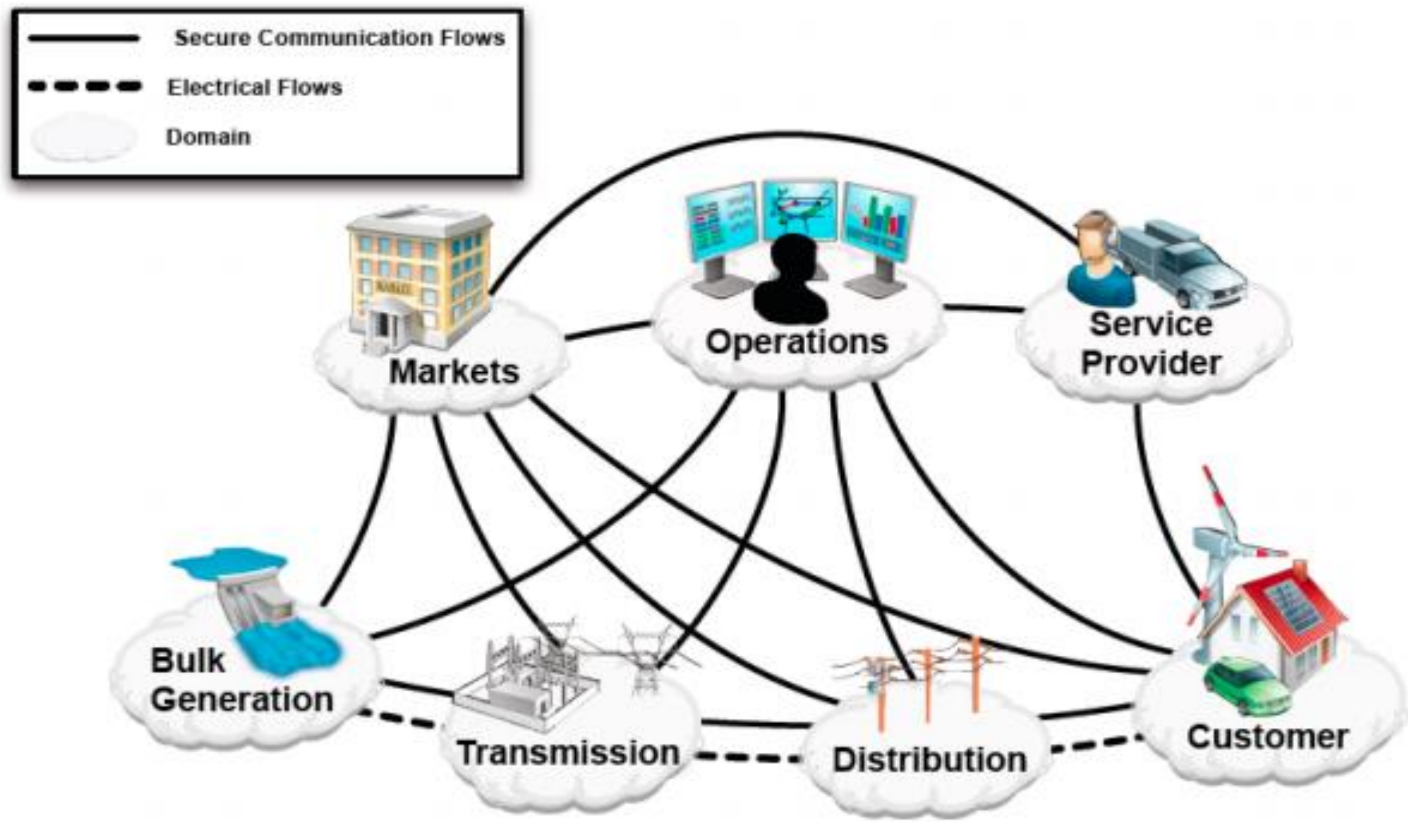
Credit: [*North Amercian Electric Reliability Corporation (NERC)*]

Indian Power Grid: Interconnections [Generation source - wise]



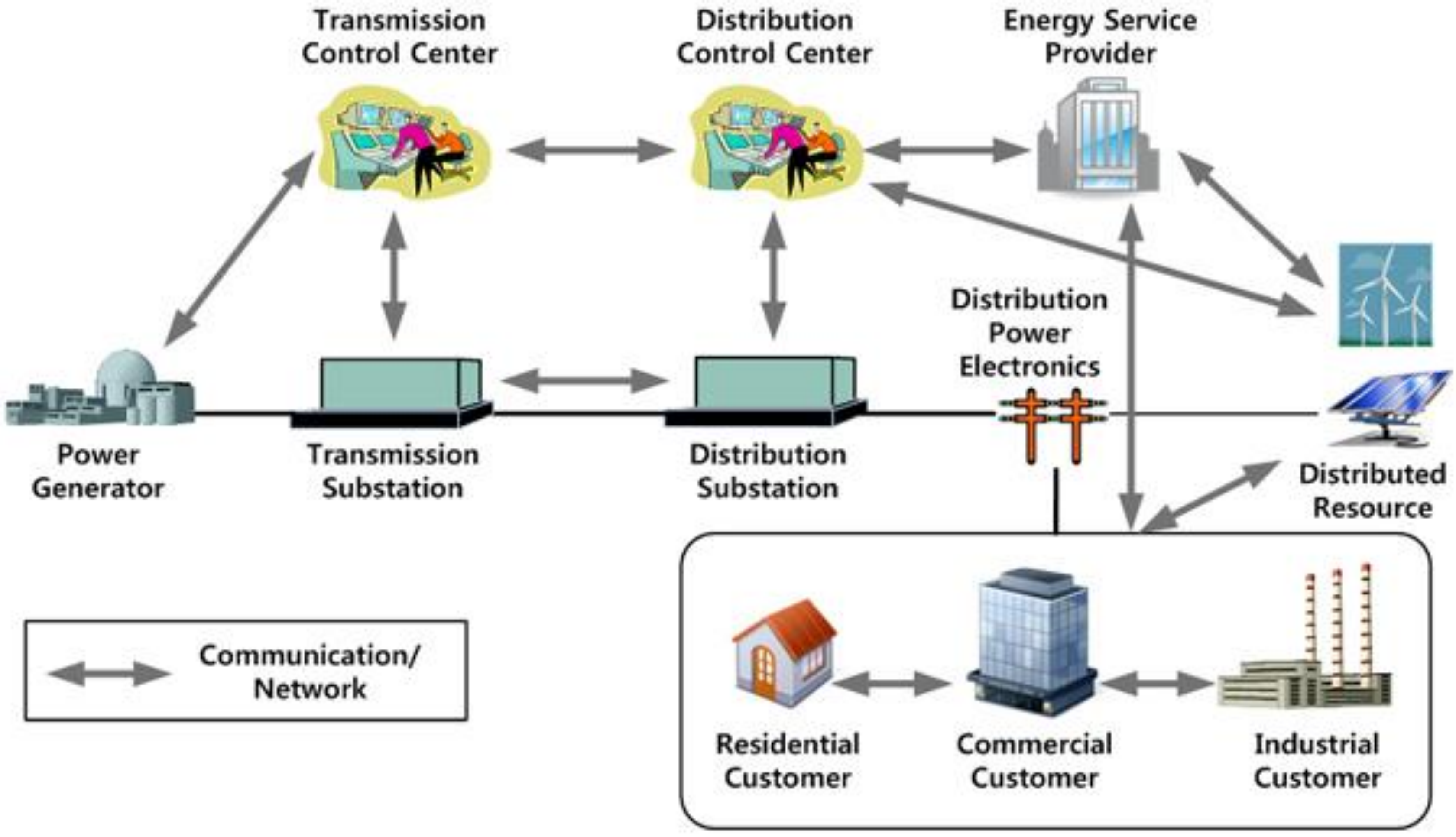
Source: http://npp.gov.in/

Smart Grid: A Cyber-Physical System



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, February 2012

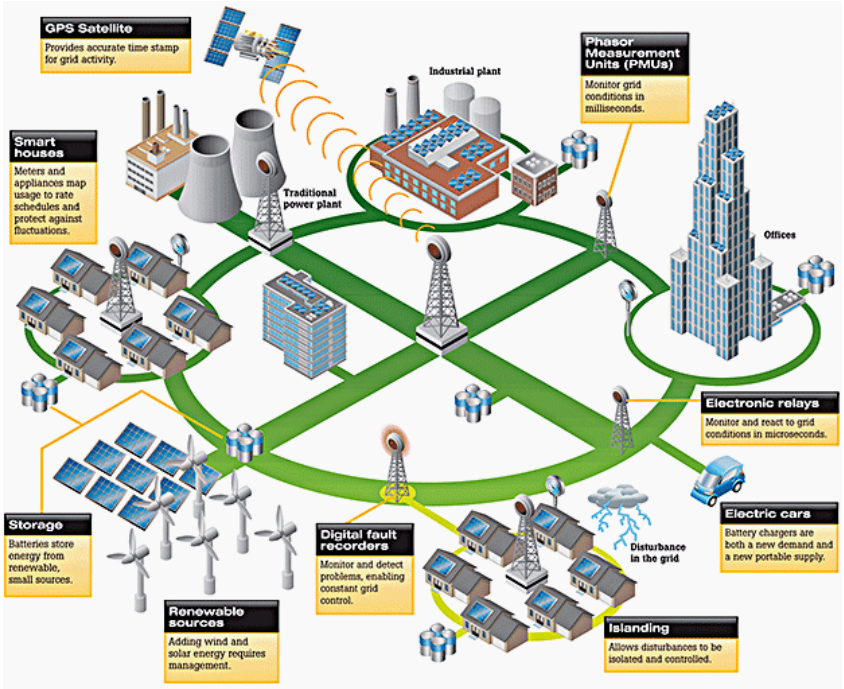
Smart grid – A cyber-physical system



Modern Smart Grid

A backbone system augmented with “***accessories***”, such as

- Distributed Energy Resources (DERs)
- Microgrids
- PMU/micro-PMUs
- Storage
- Smart appliances
- Demand response
- Electric vehicles, ….



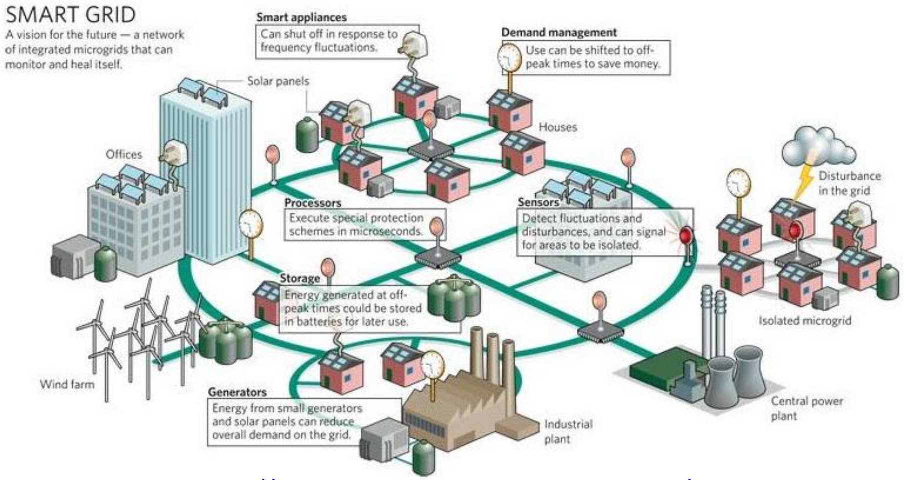


Figure source: http://engineering.electrical-equipment.org/energy-efficiency-building/smart-grids-infrastructure-technology-and-solutions.html
https://www.ennomotive.com/what-are-and-why-of-smart-grids/

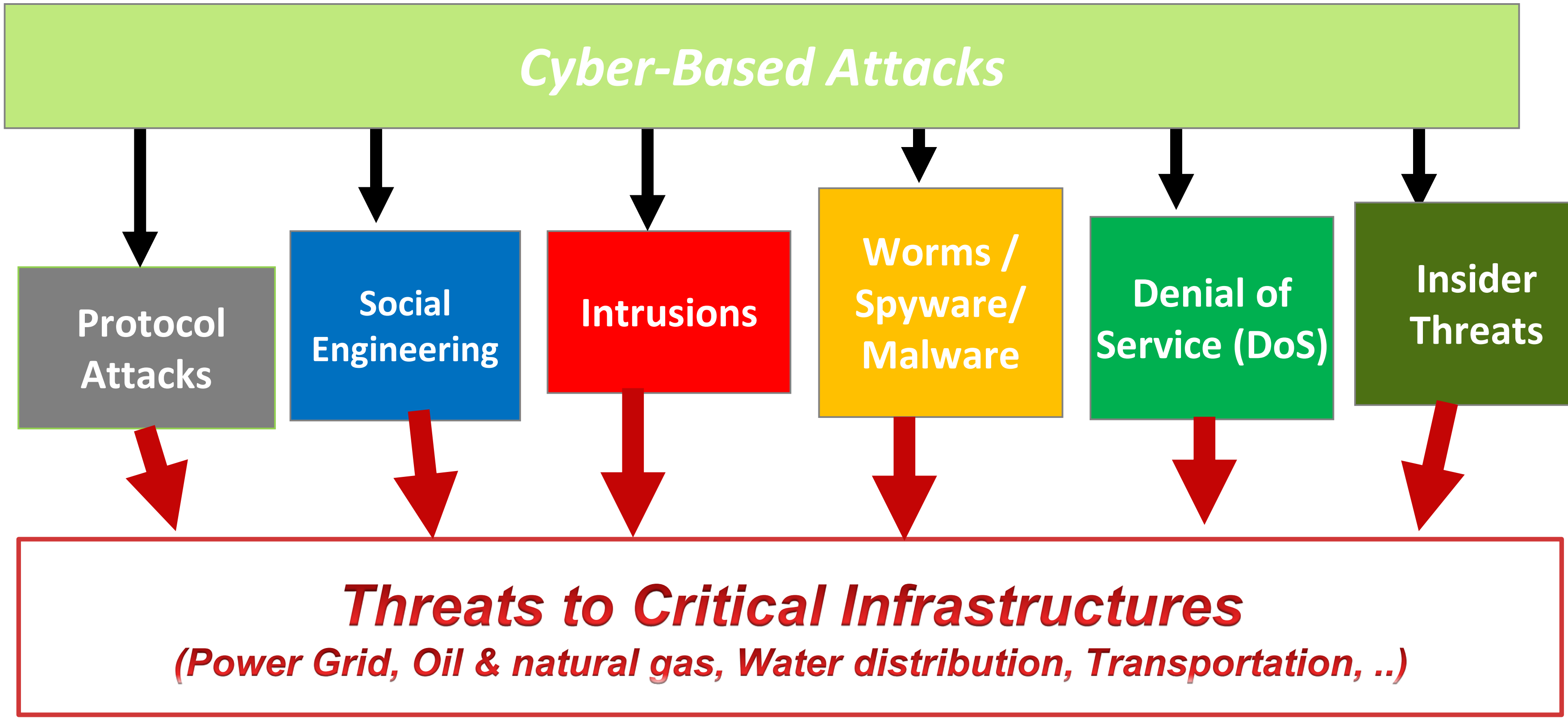
Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Outline of **Module 1**

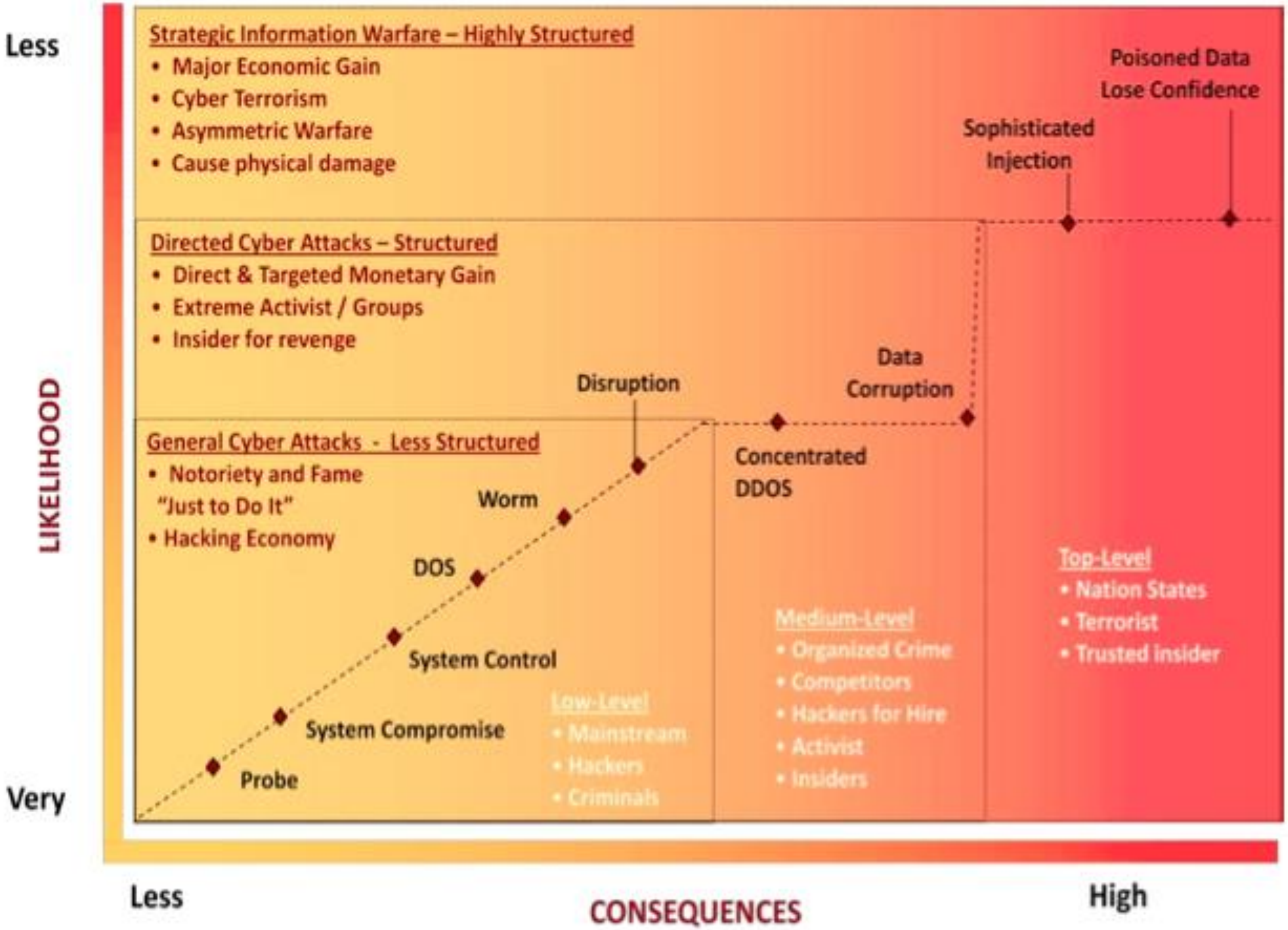
- SCADA and automation concepts
- Cyber Threats, Attacks, Consequences
- System Security concepts
- Information & Network security concepts

Cyber Threats to Critical Infrastructures



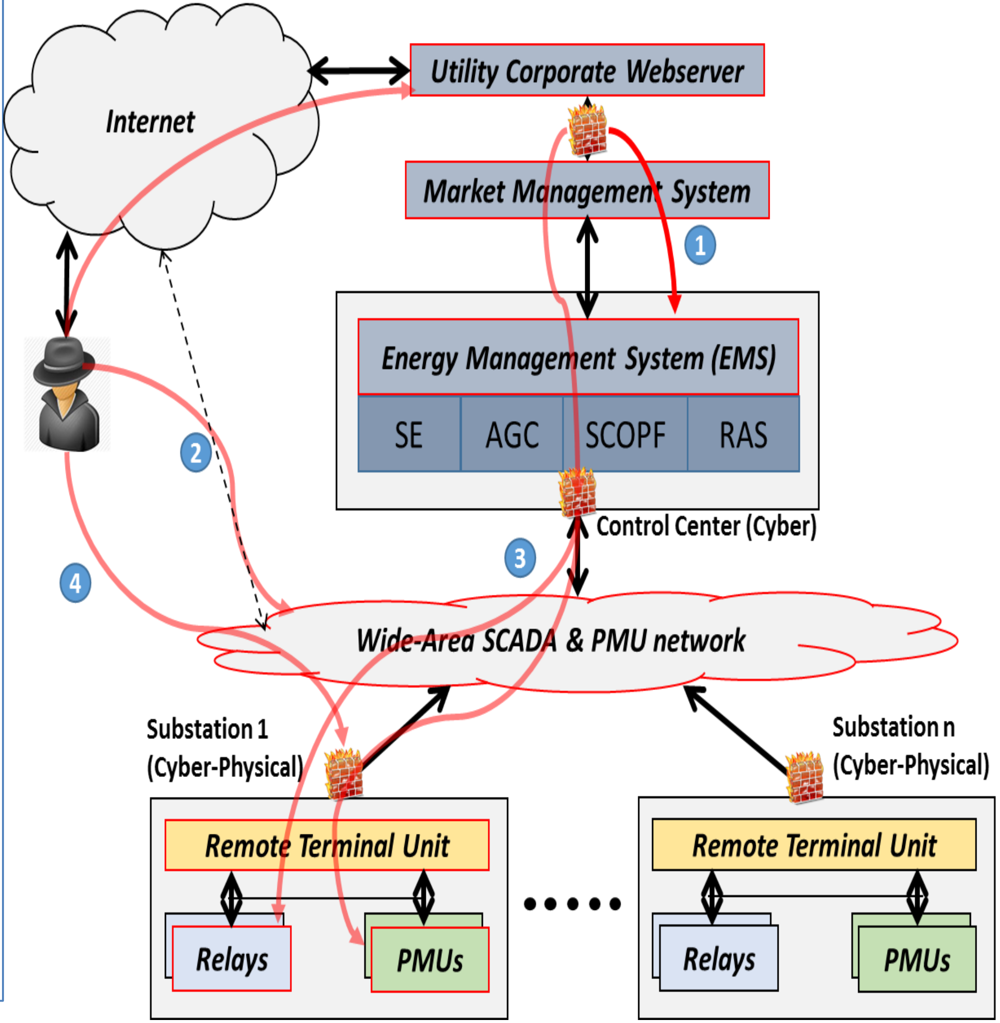
[Government Accounting Office, CIP Reports, 2004 to 2010 and beyond]; [NSA "Perfect Citizen", 2010]:
Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

Cyber Threats Landscape is dynamic !!! (DOE/NERC HILF Report)

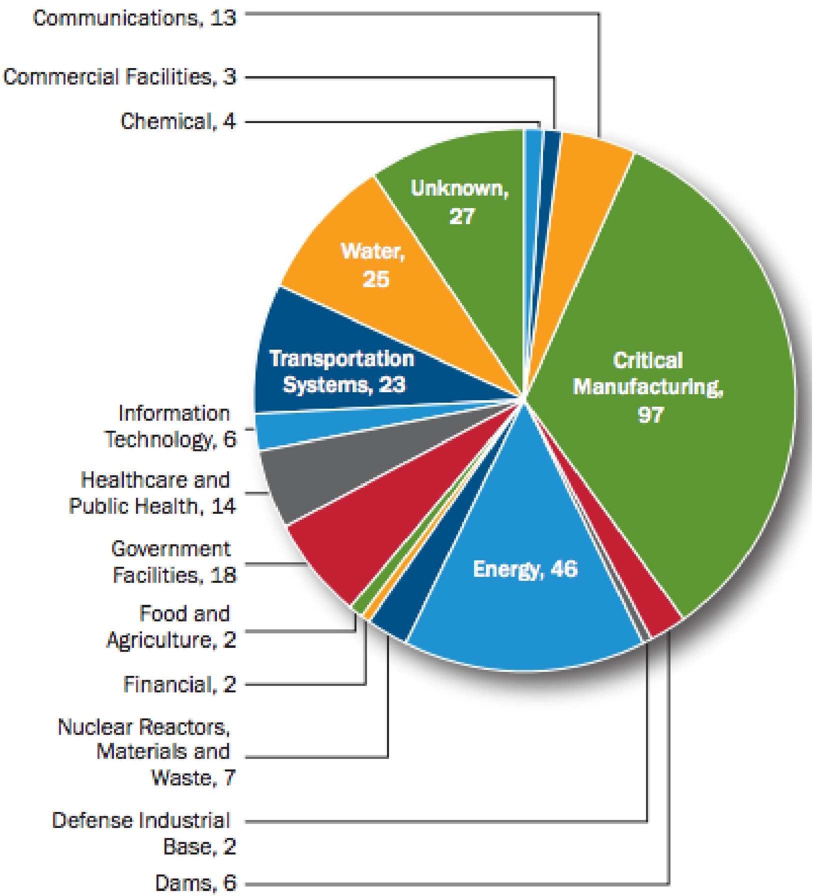


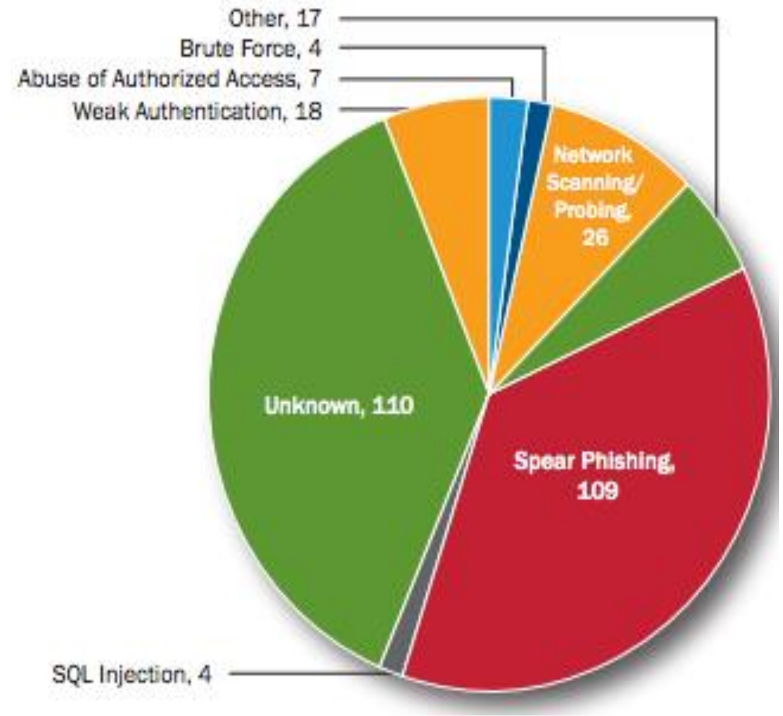
Attack Surface is increasing …

- Multiple attack paths and large attack surface
- Static configurations and network traffic → easy for reconnaisance
- Lack of clear metrics and tools to assess attack surface and reduce it
- Convergence of IT and OT lacking …
- Emergence of Internet of Things (IoT) in the grid context
- Distribution assets, smart meters, and DERs (wind, solar) are being increasingly deployed and are potentially vulnerable!



Cyber attack is growing - ICS-CERT 2015 Report





- 295 total intrusions in FY 2015
- 46 incidents in Energy Systems

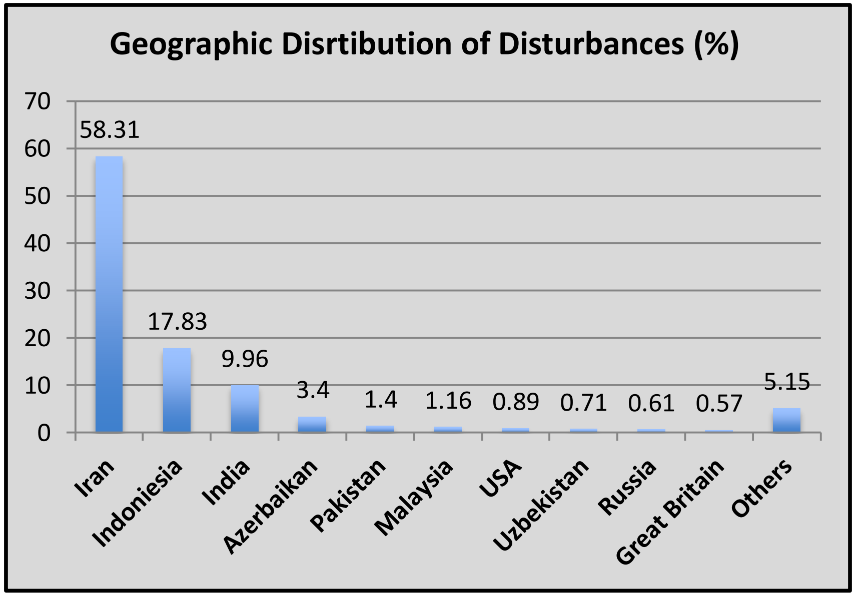
Source: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

Malware – Stuxnet (July 2010)

- Target – Industrial control systems
- Modifies code on PLCs in Uranium enrichment facilities
- Alters the speed of centrifuges used for Uranium enrichment

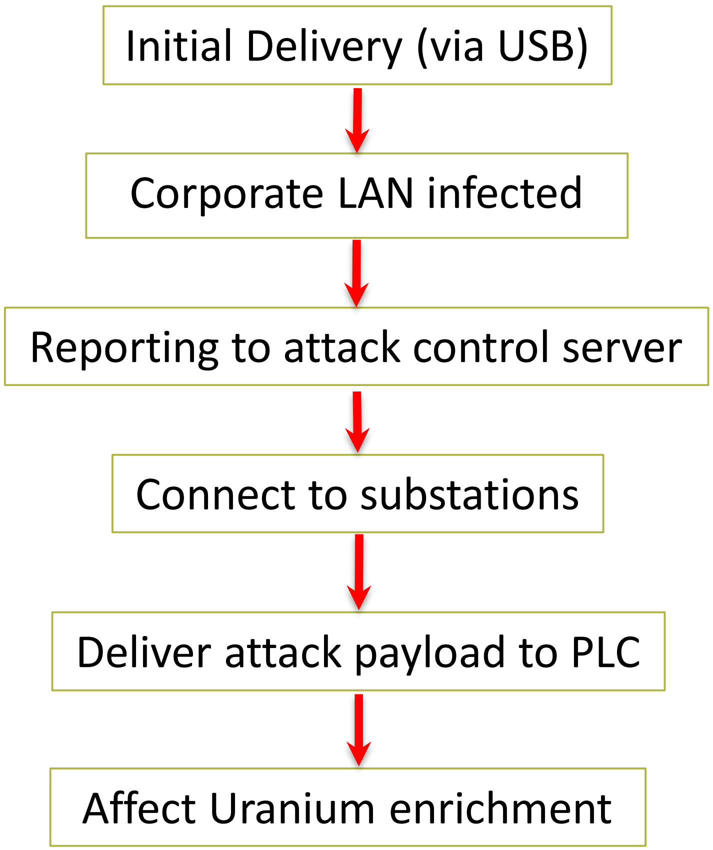
Features

- 7 methods of propagation
- **4 zero-day exploits**
- 3 rootkits
- 1 known exploit
- 2 unauthorized stolen certificates
- 2 Siemens security issues



Stuxnet – July 2010

Possible Attack Path



Lessons Learned

- Took 1 year to discover
- > 100,000 machines infected
- Professionally written code
- Infected PLCs appear to function normally

Future Requirements

- Active network monitoring
- Behavior and reputation based access control lists
- Anomaly detection
- Insider threat mitigation

What happened in Ukraine in Dec. 2015?

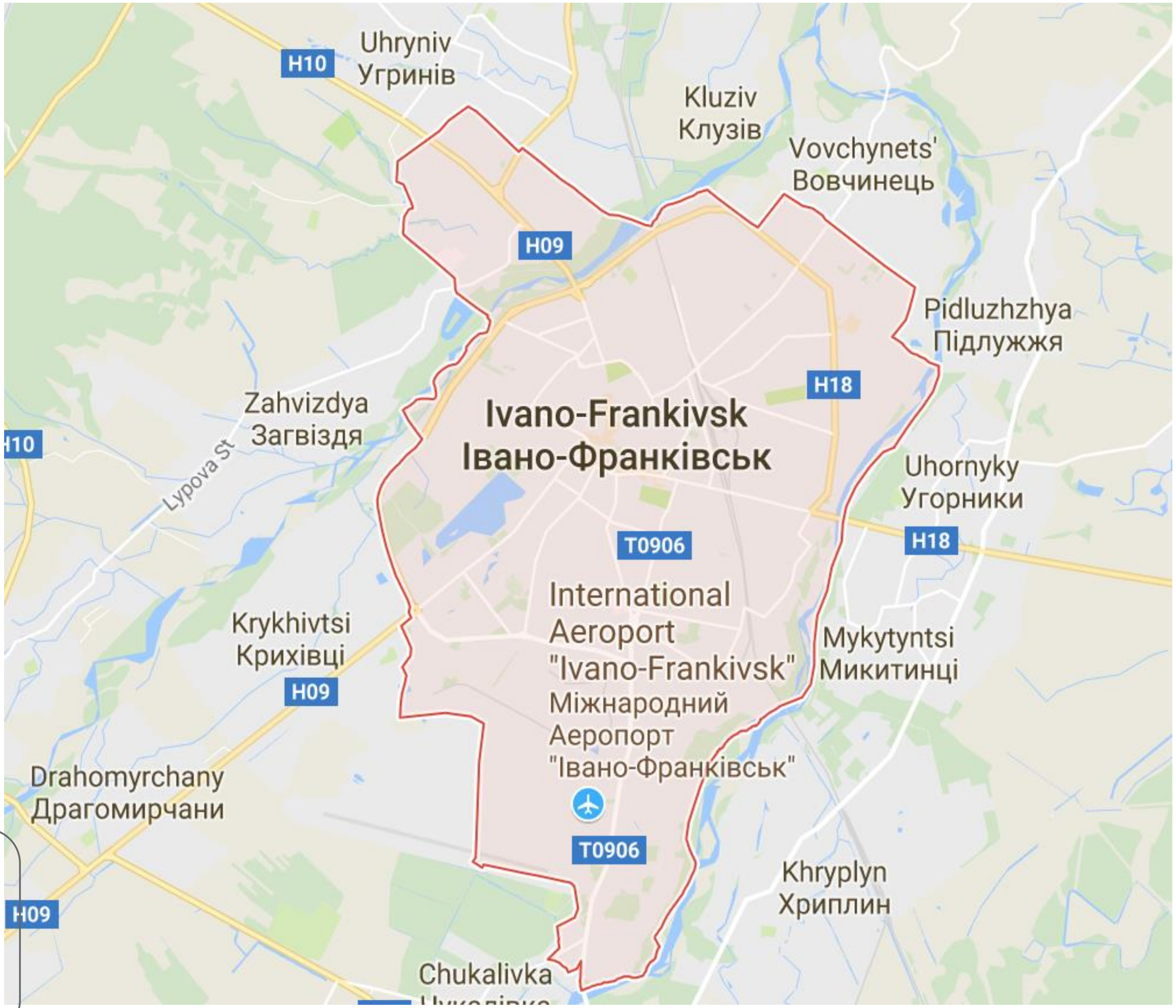
Attack-Impacts

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

Attack path

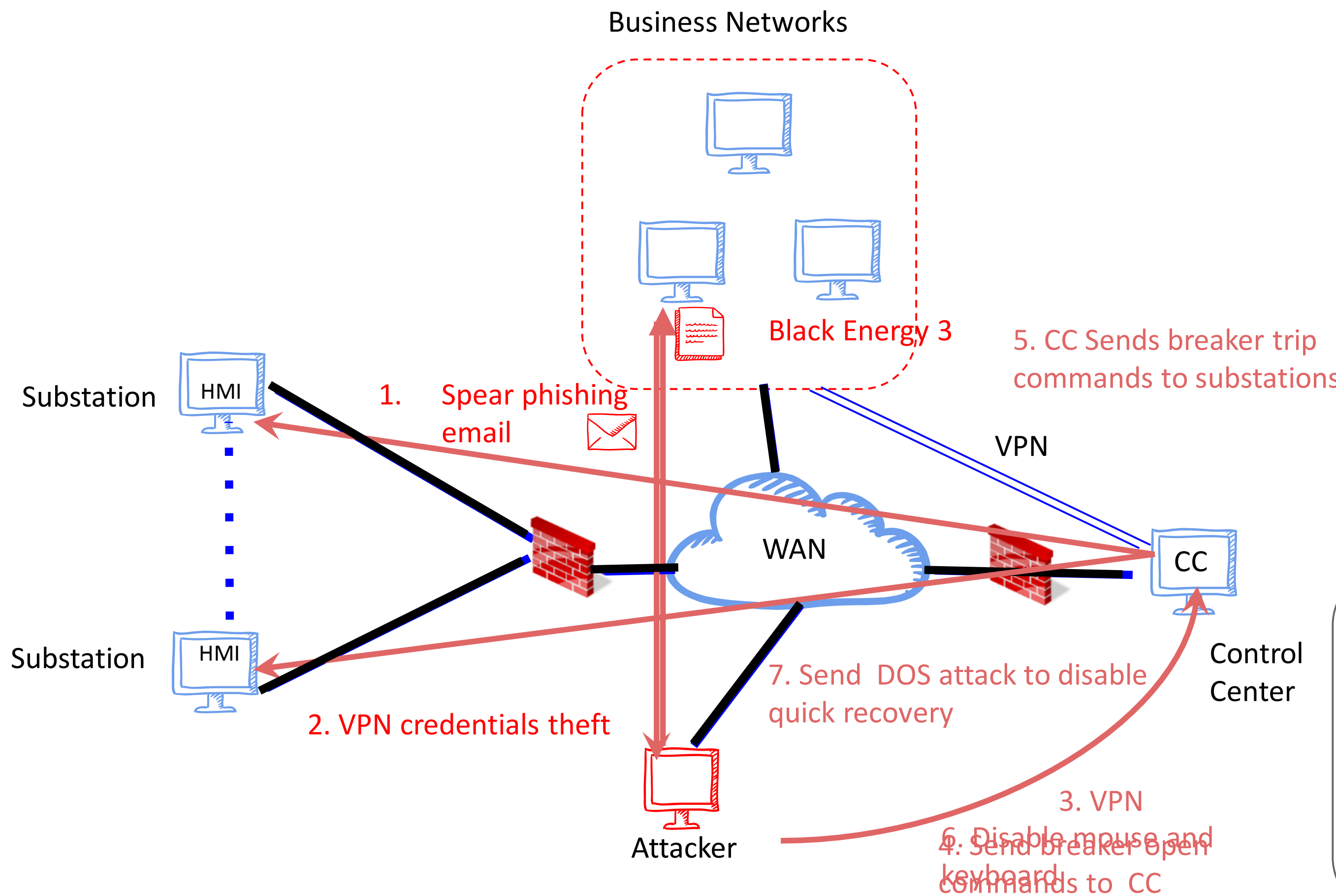
1. Spear phishing
2. Steal VPN credentials
3. VPN login
4. Open the breakers

Blackout Region: More than half of **Ivano-Frankivsk** region, some parts of **Chernivisti** region, some areas of **Kyiv** region.



Source: NERC Report on Ukraine attack

What happened in Ukraine in Dec. 2015?



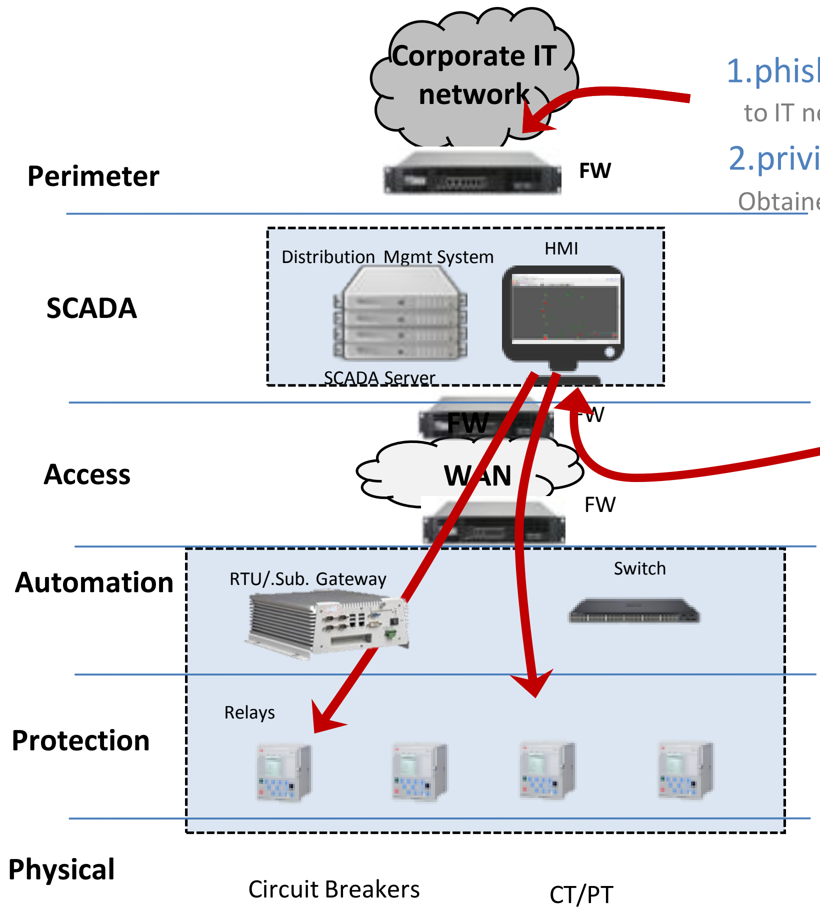
Attack-Impacts

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

Attack path

1. Spear phishing
2. Steal VPN credentials
3. VPN login
4. Open the breakers

Ukraine grid's attack in Dec. 2015 ?



IT

1.phishing email
to IT network

2.privilege escalation
Obtained admin on DC

OT Pre-Impact

3.ot vpn login
Stolen credential from DC used to remotely login to vpn

4.install malware
BlackEnergy malware installed on control systems

5.remote hmi session
Created remote operators session to SCADA server

6.trip breakers
Operate key circuit breakers, 225,000 customers offline

OT Post-Impact

7.disable systems
Wipe SCADA servers, brick serial-ethernet converts and control center ups

8.telephone ddos
Telephone DDoS prevents communication about grid state

225K customers without power

Ack: Dr. Adam Hahn, Washington State University

Can such an attack happen elsewhere?

- Yes, it did happen again in Ukraine in Dec. 2016
  (at a much lower scale)

- Can it happen in a developed country?
  It depends???

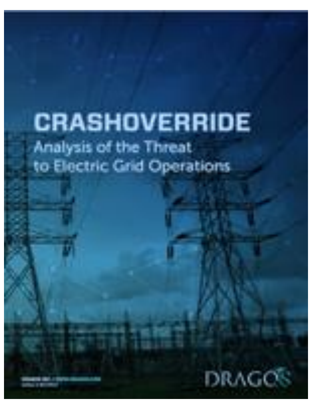
- Which country? Who are adversaries?

- Grid is heterogeneous, varying levels of automation, varying level of cyber security preparedness

- Distribution grid is a low hanging fruit!

2016 Malware

Anton Cherepanov. WIN32/INDUSTROYER: A new threat for industrial control systems, ESET. June 12, 2017.



CRASHOVERRRIDE: Analysis of the Threat to Electric Grid Operations. Dragos. Version: 2.20170613.

First malware to specifically target grid devices???

Modules

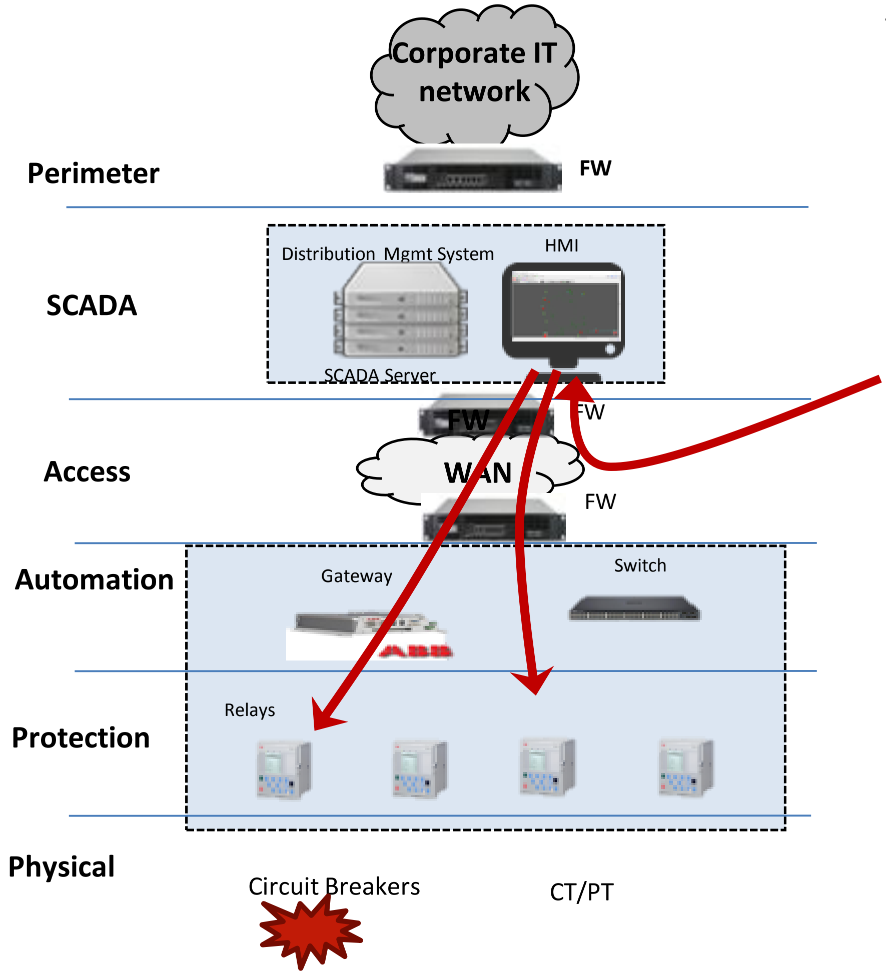
Power Systems:
- IEC 60870-5-101
- IEC 60870-5-104
- IEC 61850 (MMS)
- OPC

General:
- Backdoor/C2
- Port scanning
- DoS exploits

Modules referenced config file for target info
- attempted to enumerate IOAs

61850
- Searched for config file
- Enumerate all devices in subnet
- Identify switching/CB points (CSW)
- Operate switches:
  - (i) Continually open
  - (ii) Toggle between open/close
  - (iii) Other…

Ukraine 2016 Attack



IT	OT Pre-Impact	OT Post-Impact
????	1. remote access 2. install malware Crashoverride malware installed on control systems 3. activate modules 4. trip breakers	????

Ack: Dr. Adam Hahn, Washington State University

Comparison of Ukraine Attacks

Differences

	2015	**2016**
Target:	Control Center/HMI	Substation
Malware:	Remote Access Tool	Custom Protocol Modules
Anomalies:	1) Remote session 2) SCADA commands	1) Communication session 2) Network Enumeration

Similarities

1) No new vulnerabilities
2) Focus on actuation
3) Similar access methods?

What can R&D community do about it?

Conduct research that has BOTH intellectual merit and broader impacts

Promising areas include:

- IT Security & Beyond → CPS Security
- Holistic Security Framework & Defense in Depth approach
- Attack prevention, detection, mitigation, and resiliency
- Sound analytical foundation
- Realist Testbeds, models, data sets, and experimentation
- Highly skilled workforce development
- Partnership & Collaboration: Industry-University, International

Cyber attack classification

Timing attacks

- **Denial of Service attacks**
  - e.g. flood communication network and affect command information flow

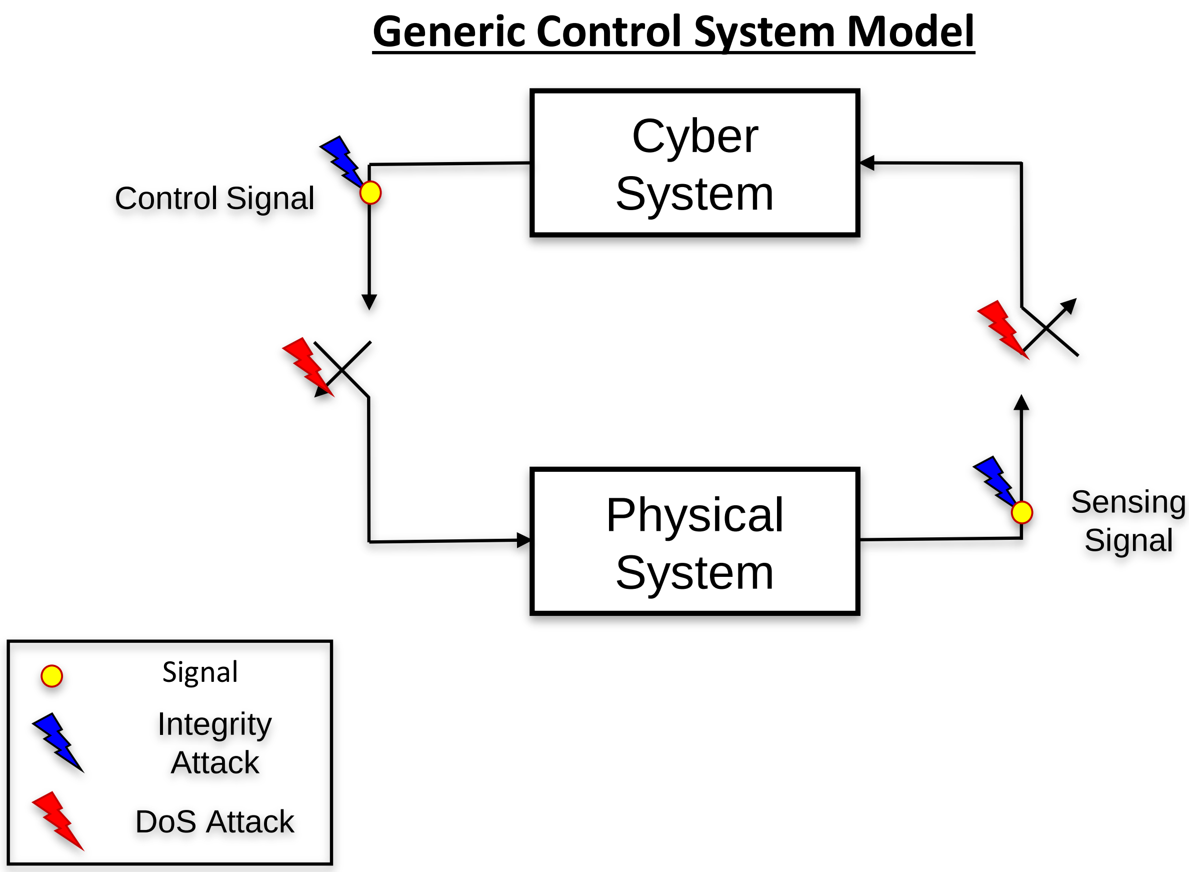
Data integrity attacks

- **Attacks on measurements or controls**
  - e.g., block instead of trip, VAR increase instead of decrease.

Coordinated attacks

- **Attacks coordinated in space, and/or time**
  - e.g. attack on SPS of major transmission line followed by attack on sub-transmission and distribution feeders

Control Systems Attack Model



Types of Attacks

- Data integrity
- Replay
- Denial of service
- De-synchronization and timing-based

Yu-Hu. Huang, Alvaro A. Cardenas, S. Amin, S-Z. Lin, H-Y. Tsai, and S. Sastry, "*Understanding the Physical and Economic Consequences of Attacks on Control Systems,*" International Journal of Critical Infrastructure Protection, 2(3):72-83, October 2009.

Attacks-Cyber-Control-Physical view

Attacks → **Cyber** → **Control** → **Physical**

Attacks

- Denial of Service
- Malware
- Spear Phishing
- Data integrity attacks
- Timing attacks
- Man-In-The-Middle attacks
- .....

Cyber

Devices
- EMS/DMS server
- HMIs
- PMUs
- Relays
- IEDs …

Networks
- Gateways
- Routers
- Protocols
- Data …

Control

Generation
- Governor control
- AGC, SCOPF
- Economic Dispatch

Transmission
- State Estimation
- Contingency analysis
- VAR compensation
- FACTS

Distribution
- Demand response
- Load shedding
- Storage control
- ….

Physical

- Blackout
- Stability violation
- Load rejection
- Equipment damage
- Economic impact
- .....

Cyber Intrusion Process

Footprinting

- **Identification of organization's security posture**
  - locations of the substations, control centers, or generating units
  - IP addresses and email address of the utility company

Scanning

- **Exhaustively identify the possibilities access points**
  - Access points: Wireless connection, LAN, VLAN, VPN, and
  - Tools: War dialing or Traffic sniffer

Enumerating

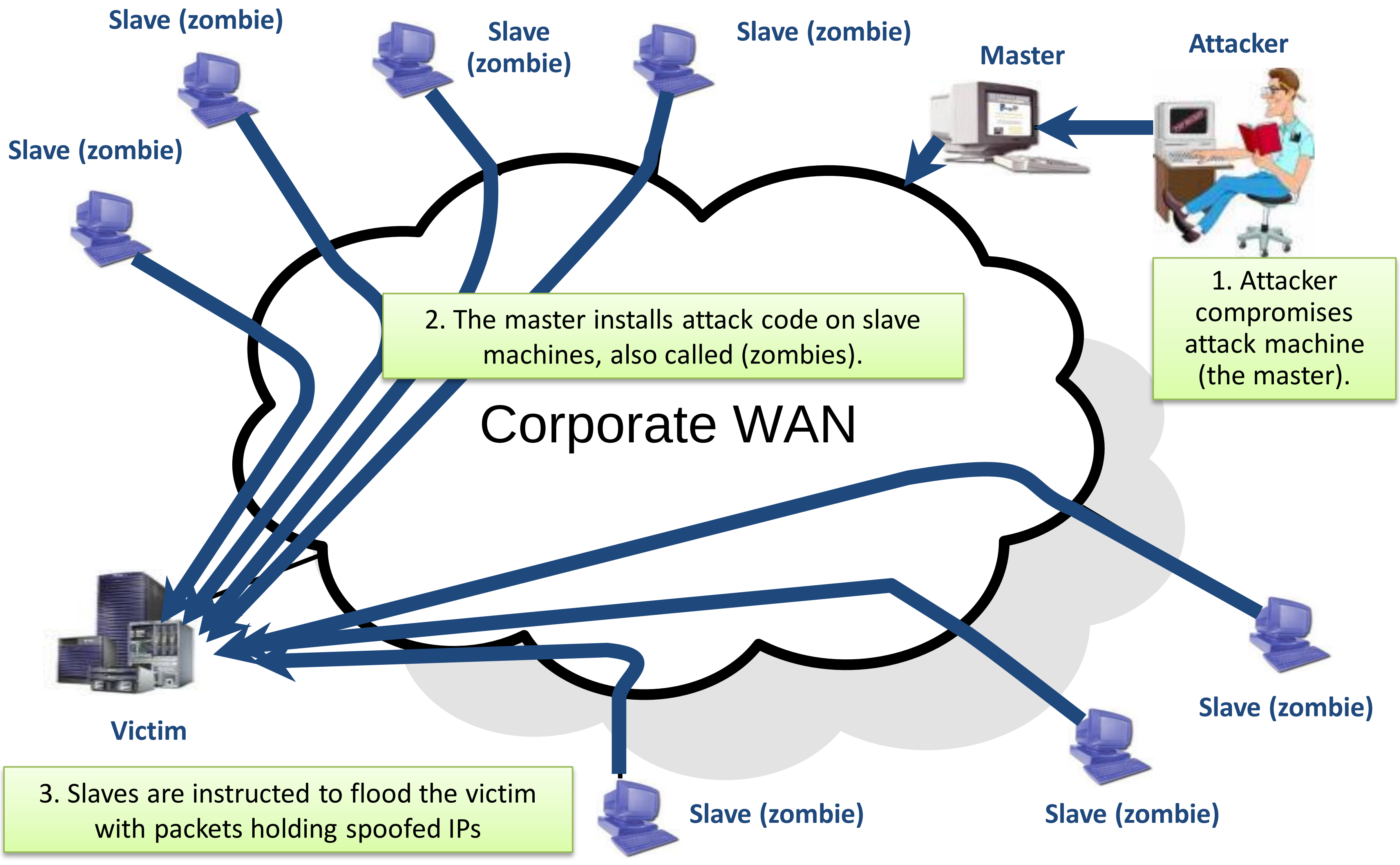
- **Listing all active ports available** on a target IP address
  - *Password guessing*: Dictionary, brute-force, or social engineering

Exploit!

- This is where an attacker **got lucky**!

But we do not want them to be lucky…

Denial of Service (DoS) Attacks



Power Grid Cyber Security Roadblocks

- Legacy systems
- Geographically disperse
- Insecure remote connections
- Long system deployments
- Limited physical protections

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- No “fail-closed” security mechanisms
- Widespread availability of technical info

Securing system is chalenging …

- **Open and interoperable protocols**
- **Security vs. performance tradeoff**
- **Security vs. usability tradeoff**
- **Security is expensive**
- **Attackers enjoy breaking into a system**
- **Security had been not a design criteria**

- **Attack surface is expanding!**
- **Cyber Threat Landscape is dynamic!**
- **Securing legacy infrastructure is a challenge!**

- **Cybersecurity Life-cycle model**
- **End-to-end Security**
- **Cybersecurity architectural concepts**

A Cybersecurity Lifecycle Model

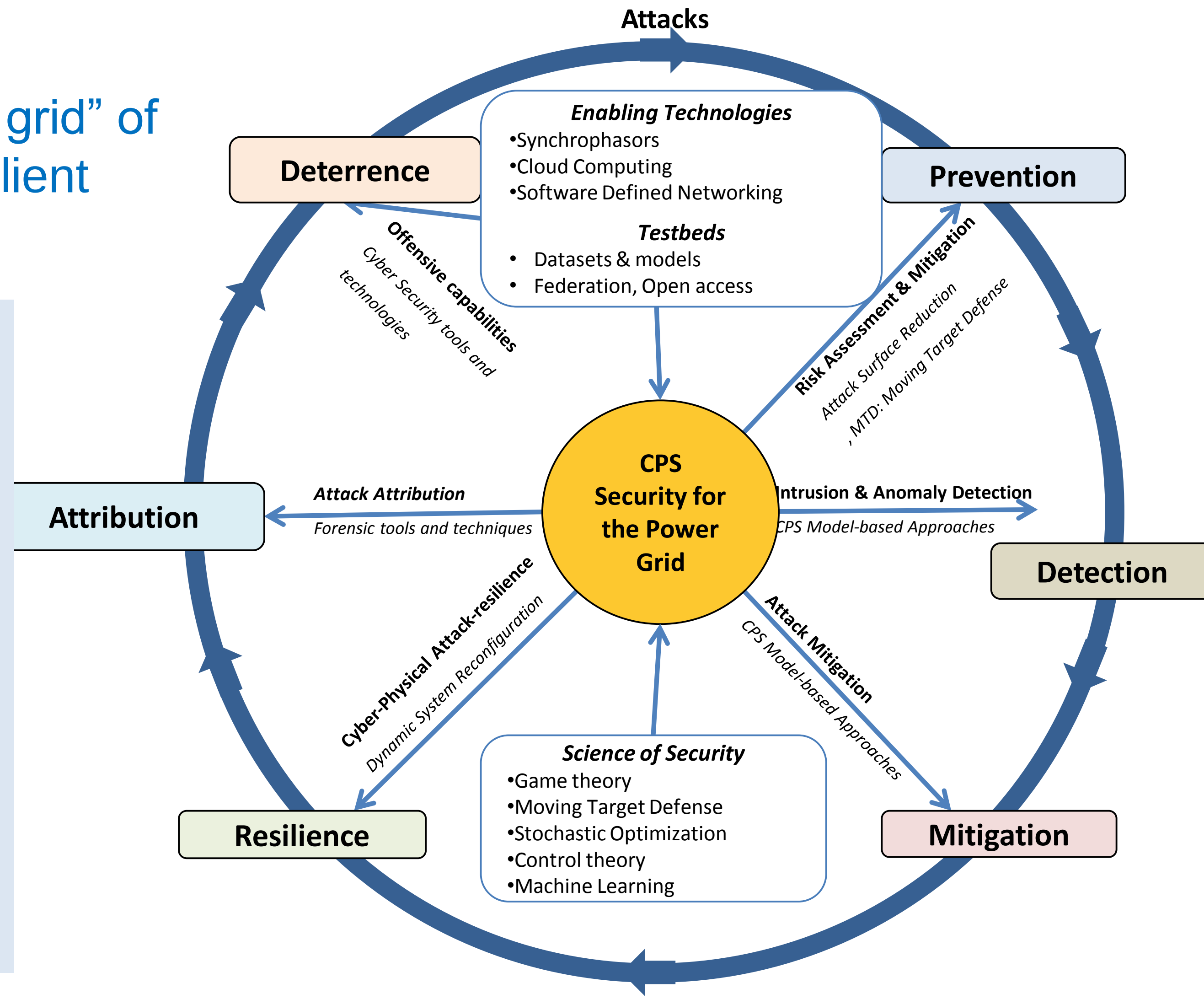
Vision:

Transform “fault-resilient grid” of today into an “attack-resilient grid” of the future

- Technology
- Process
- People
- Regulation

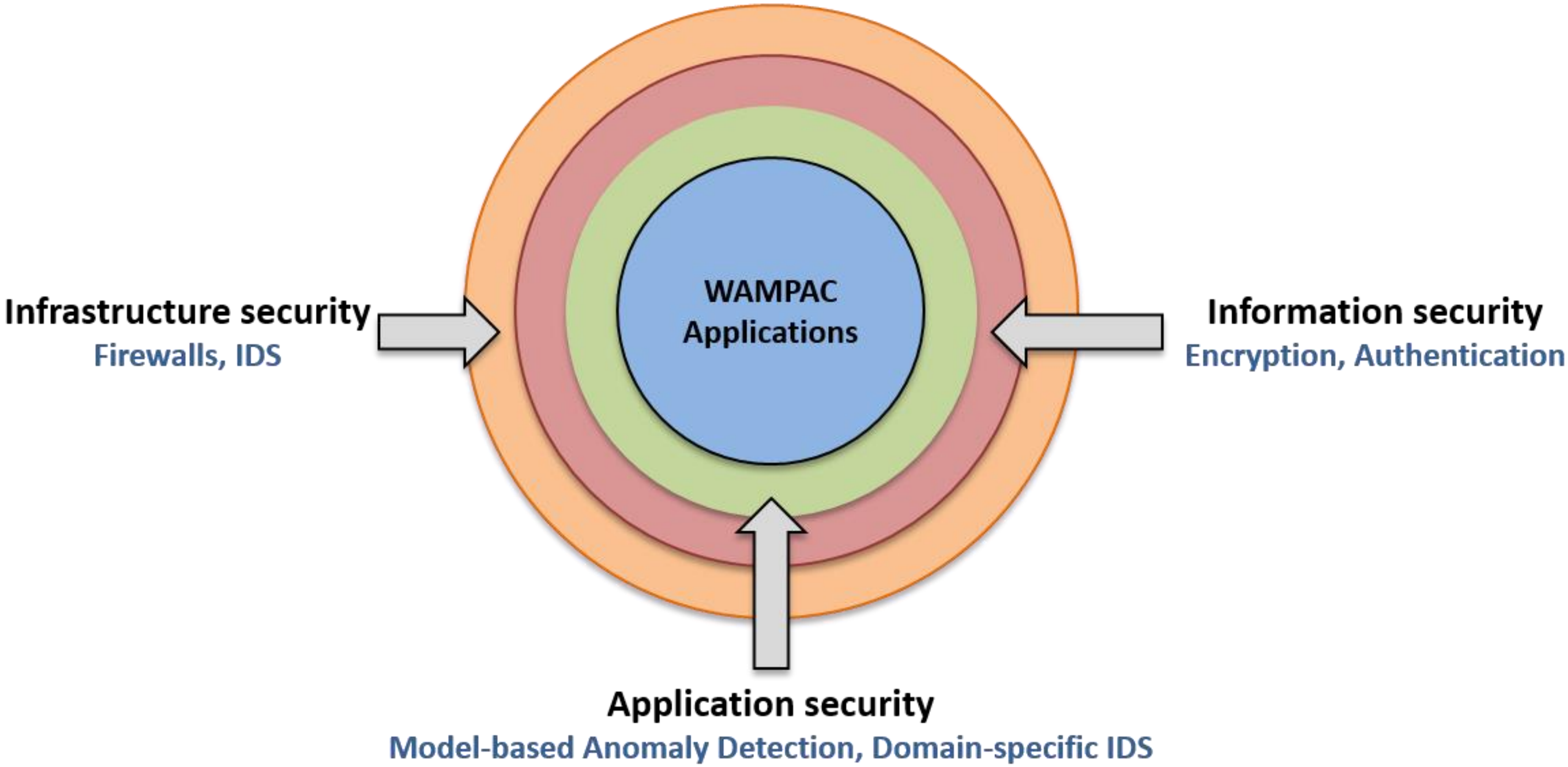
Industry Collab.

- Problem formulation
- Testbed Experiments
- Tech Transfer
- Education & Training
- Workforce Develop.

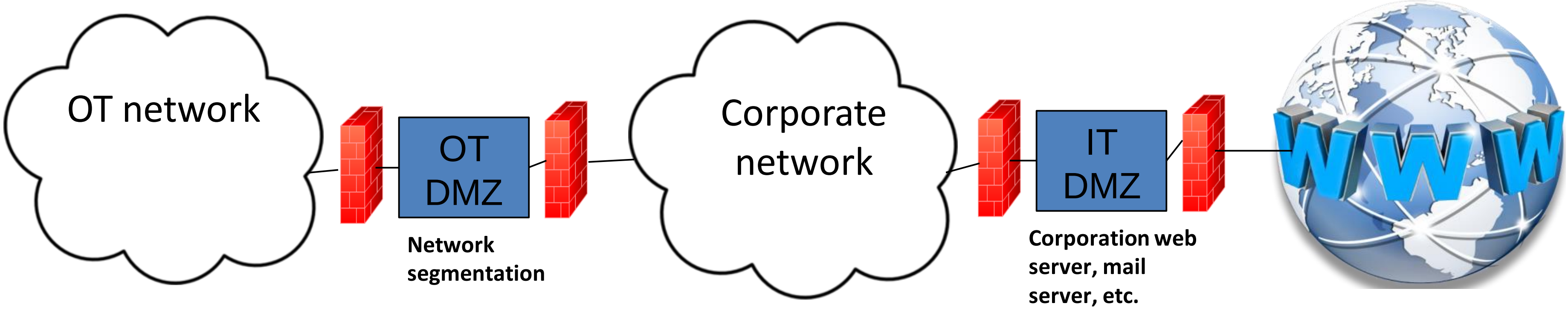


A. Ashok, M. Govindarasu, and J. Wang, “CPS Security for WAMPAC”, Proc. of the IEEE, May 2017

Cybersecurity Architecture: **Defense-in-Depth**

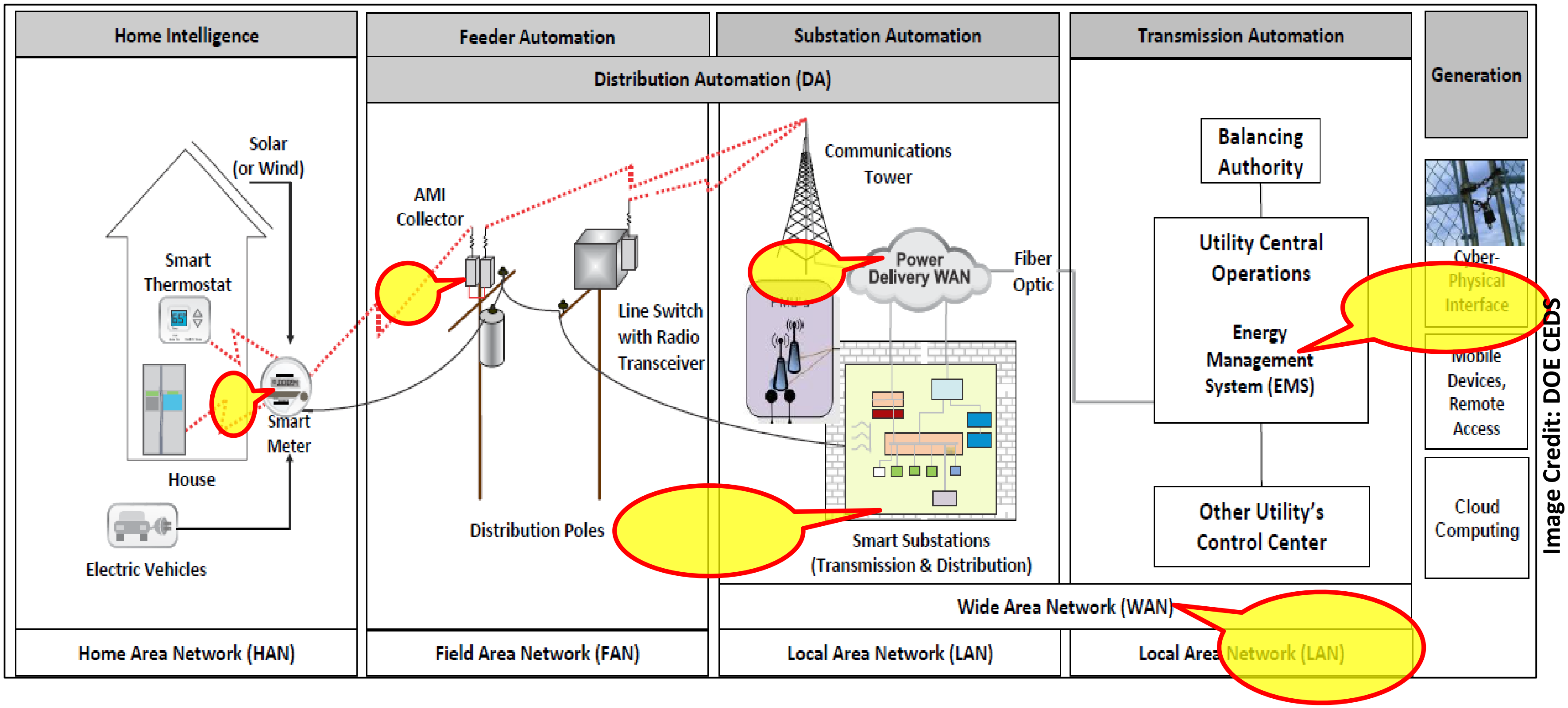


Cybersecurity Architecture: **Network Segmentation**



- OT network must segmented from IT / Corporate network
- Use De-Militarized Zone (DMZ) for data sharing

End-to-End Security in the Energy Delivery System



Assess Risk	Develop and Implement New Protective Measures	Manage Incidents

Three key steps in US DOE Cybersecurity Roadmap

Beyond IT Security – Why?

Legacy Infrastructure

- Limited encryption capabilities
- Poor patch management
- Software bugs
- Security not design criteria

Encrypted comm. can also be tampered

- Replay attacks
- DoS attacks
- Timing attacks
- Advanced Persistent Threats (APTs)
- Insider Threats including user mistakes

Evolving Vulnerability and Threat landscape

- Secure system today could be a vulnerable system tomorrow
- Information/Infrastructure security secure only the entry points
- Application security identifies anomalies in data when IT and infrastructure security fails

Smart Security = Info + Infra + System

	Information Security	Infrastructure Security	Control Systems Security
NEEDS	❑ Information Protection ▪ Message Confidentiality ▪ Message Integrity ▪ Message Authenticity	❑ Infrastructure protection ▪ Routers ▪ DNS servers ▪ Links ▪ Internet protocols ❑ Service availability	❑ Generation control apps. ❑ Transmission control apps. ❑ Distribution control apps. ❑ Real-Time Energy Markets
MEANS	❑ Encryption/Decryption ❑ Digital signature ❑ Message Auth.Codes ❑ Public Key Infrastructure	❑ Traffic Monitoring ❑ Statistical analysis ❑ Authentication Protocols ❑ Secure Protocols ❑ Secure Servers	❑ Attack-Resilient Control Algos ❑ Model-based Algorithms - Anomaly detection - Intrusion Tolerance - Bad data elimination ❑ Risk modeling and mitigation

Cyber Attacks: Deter, Prevent, Detect, Mitigate, be Resilient, Attribution

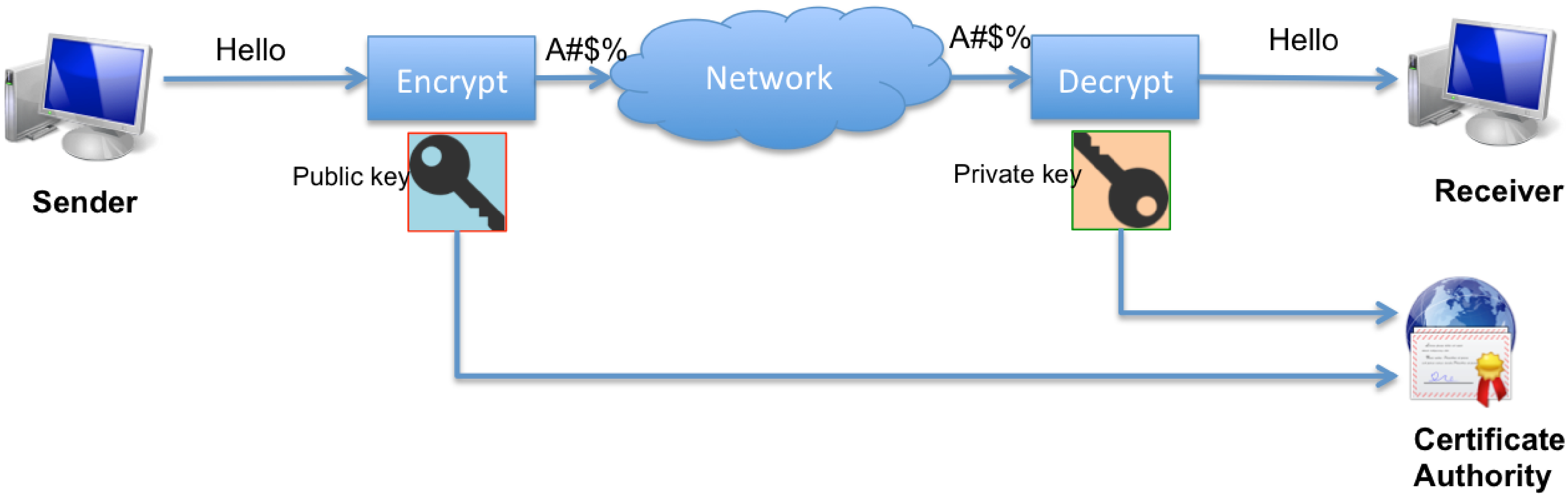
Information & Network Security concepts

Security Properties

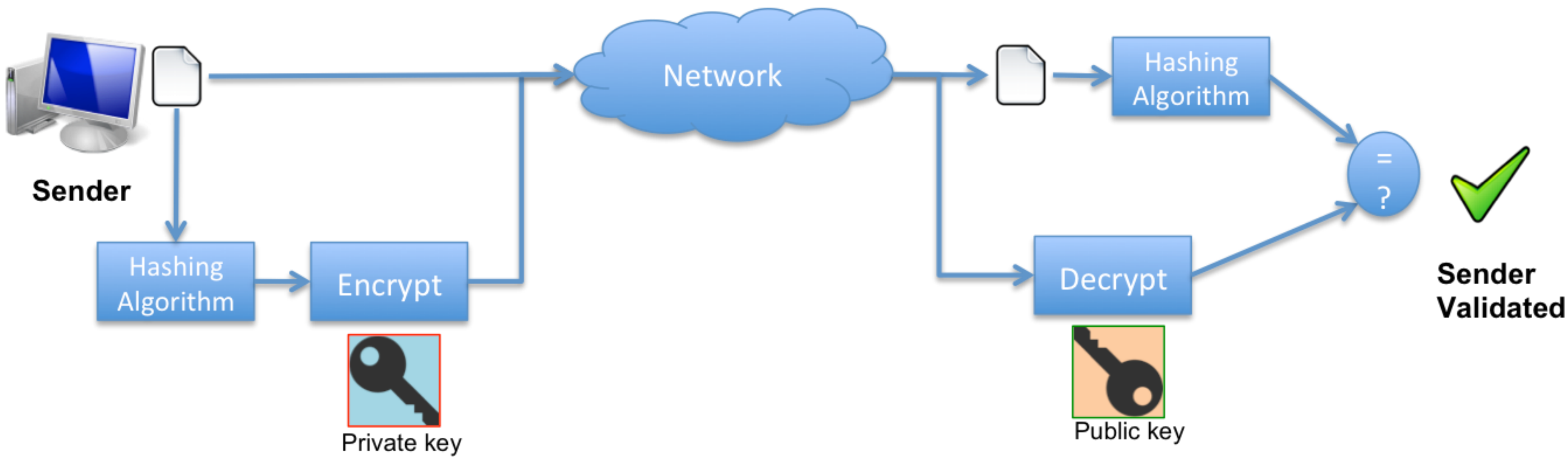
- Confidentiality:
  - Message content should be accessed by authorized users only
  - Achieved by using encryption
- Integrity:
  - Making sure that message was not altered (in transit, or later) without detection
  - Achieved by using hashing
- Availability:
  - services must be accessible and available to authorized users
- Authentication:
  - Sender, receiver want to confirm identity of each other
  - Achieved by using digital signatures
- Non-Repudiation:
  - The actual sender can not claim that he did not send the message
  - Achieved by using digital signature

Symmetric Key Encryption

Asymmetric Key Encryption



Authentication – Digital Signatures



Security Properties

IT – OT Priorities mismatch

Traditional IT Systems	Industrial Control Systems
Confidentiality	Availability/Integrity
Integrity	Integrity/Availability
Availability	Confidentiality

Power Grid Applications – Sample Cyber Security Requirements

Power Grid Applications	Information & Infrastructure Security	Application Security
AMI	I, AT, C	I, N
DMS	I, A, AT	I, AT
EMS	I, A, AT	I, AT
WAMPAC	I, A, AT, C	I, A
Power Markets	I, A, AT, C	I, N

Confidentiality (C), Integrity (I), Availability (A), Authentication (AT), Non-repudiation (N)

Additional Requirements in SCADA/OT

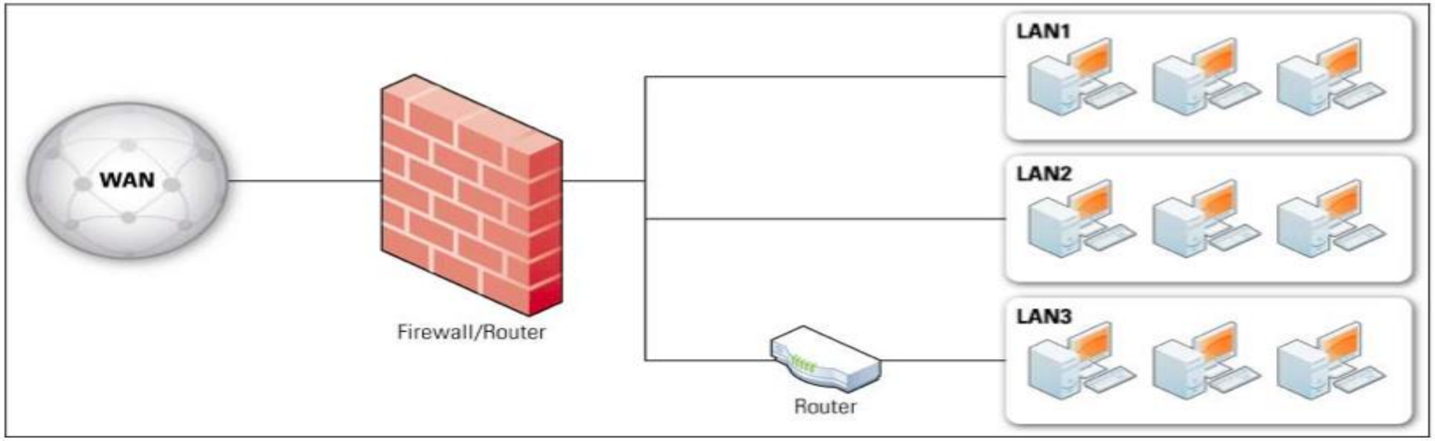
- Real-Time Requirements – e.g., Protection and Control Apps
- Stability requirements (to avoid cascading failure)
- Safety considerations
- Legacy platforms and Devices
- Limited processing and communication capabilities
- Patch management is not easy, needs to be carefully planned
- Security solutions must be tailored to make sure <u>it doesn't have adverse effect</u> on system operation

Network Security – Firewalls

Firewalls control flows of network traffic between networks or hosts based on security policies.

Recommendations for improving effectiveness and security of firewalls

- Create firewall policies that specifies **how firewalls should handle inbound and outbound network traffic.**
- Identify all requirements that should be considered when determining which firewall to implement.
- Create rule sets that implement the organization’s firewall policy while supporting firewall performance.
- Manage firewall architecture, policies, software, and other components throughout the life of the firewall solutions.



Source: Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, September 2009.

Network Security – Firewalls

Firewall Technologies

- Packet Filtering
- Stateful Inspection
- Application Firewalls
- Application-Proxy Gateways
- Dedicated Proxy Servers
- Virtual Private Networking
- Network Access Control
- Unified Threat Management
- Web Application Firewalls
- Firewalls for Virtual Infrastructures

Firewall Policies

- Policies based on IP Addresses and Protocols
    - IP addresses and IP characteristics
    - IPv6
    - TCP and UDP
    - ICMP
    - IPsec protocols
- Policies based on Applications
- Policies based on User Identity
- Policies based on Network Activity

Source: Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, September 2009.

Network Security – IDS

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

Intrusion prevention is the process for performing intrusion detection and attempting to stop detected possible incidents.

Types of Intrusion Detection and Prevention Systems

- **Network-Based** – monitors network traffic for suspicious activity
- **Wireless** – monitors wireless network traffic for suspicious activity
- **Network Behavior Analysis** – examines traffic to identify threats that generate unusual traffic flows, e.g. DDoS attacks, malware, policy violations
- **Host-Based** – monitors characteristic of a single host and events occurring for suspicious activity

Detection Methodologies

- Signature-Based Detection
- Anomaly-Based Detection
- Stateful Protocol Analysis

Source: Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, February 2007.

Network Security – IDS

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

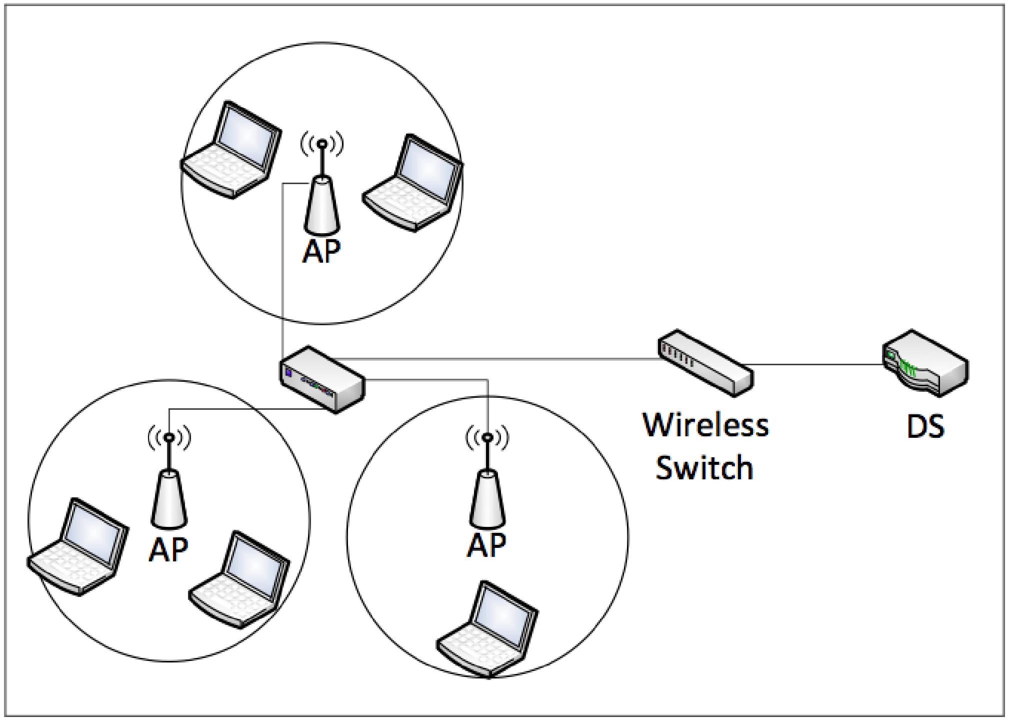
A robust IDPS solution can be achieved using a combination of these 4 IDPS technologies.

Source: Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, February 2007.

Network Security – WLAN Security

WLAN's are extensions to wired LAN's based on IEEE 802.11 standard.

Fundamental architecture of WLAN consists of Access Points (AP), client devices, and Distribution Systems (DS) that connect to wired LAN's.



Steps to minimize risk:

1. Password Policies & management

1. Encrypt data using standards like WPA2

1. Restrict access using security controls

    1. Mac address filtering
    2. Disable appropriate network interfaces, bridging traffic

1. Configure host-based network security tools like firewalls, IDS

Source: Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153, February 2012.

Network Security – WLAN Security

Passive attacks

- Eavesdropping
- Traffic analysis

Active attacks

- Masquerading
- Replay
- Message modification
- Denial of Service
- Misappropriation
- Deploying rogue WLAN devices

WLAN security

- Attack Monitoring
- Vulnerability Monitoring
- Monitoring tools
    - Wireless IDS & IPS
- Periodic Assessment

Source: Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153, February 2012.

Summary

- SCADA and automation concepts
- Cyber Threat landscape, attacks, impacts
- Security architecture concepts
- Information security concepts – Symmetric and asymmetric key cryptography, digital signatures
- Network security concepts – Firewalls, IDS, WLAN Security

Conclusions

- Threat landscape is dynamic, attacks are increasing …
- Human is often the weakest link in the security chain
- Smart Grid Security = Info Sec + Infra Sec + App Sec + Physical Sec
- FROM Fault-Resiliency TO Attack-Resiliency
- Defense-in-Depth & End-to-End Security
- Cybersecurity Life-cycle model & CPS Security solutions
- Cybersecurity of DERs, Microgrids & Supply Chain
- CPS Security Testbeds & Experimentations
- Industry Collaboration & Tech Transfer & Standard Devleopment
- Education and workforce development & Industry Training are critical
- Synergistic collaboration: Industry-University-National Labs

THANK YOU …

- Acknowledgements:
  - Iowa State University, USA
  - U.S. National Science Foundation (NSF)
  - U.S. Depart of Energy (DOE)
  - U.S. Department of Homeland Security (DHS)
  - U.S. NSF IU/CRC Power Engr. Research Center (PSERC)
  - Iowa State Univ., Electric Power Research Center (EPRC)
  - University of Minnesota

  - **Collaborators**:

    Prof. Chen-Ching Liu, Washington State University (WSU)
    Prof. Venkat Ajjarapu, Iowa State University (ISU)
    Dr. Adam Hahn, Washington State University
    Dr. Aditya Ashok (ISU)
    Dr. Siddharth Sridhar (PNNL)
    Dr. C. W. Ten, Michigan Tech.

- **Professional**:
  - IEEE PES - PSACE CAMS Cyber Security Task Force