IoT: Internet of Things, or Internet of Threats

Garrick Ng

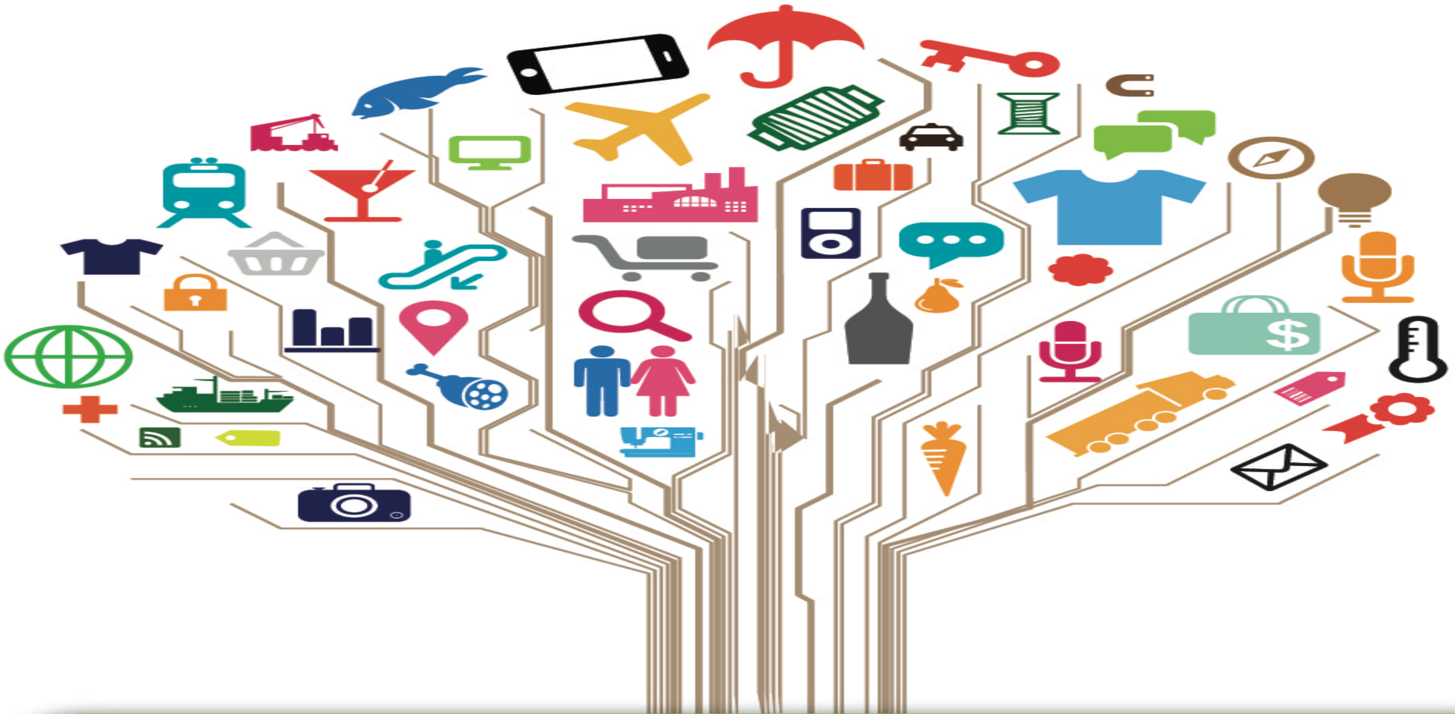
Cyber Security Professionals Awards – Gold Winner

SCC Security SIG Chairman

Chief Technology Officer

Cisco Hong Kong, Macau, Taiwan

April 2017



Internet of Things (IoT)

GS1

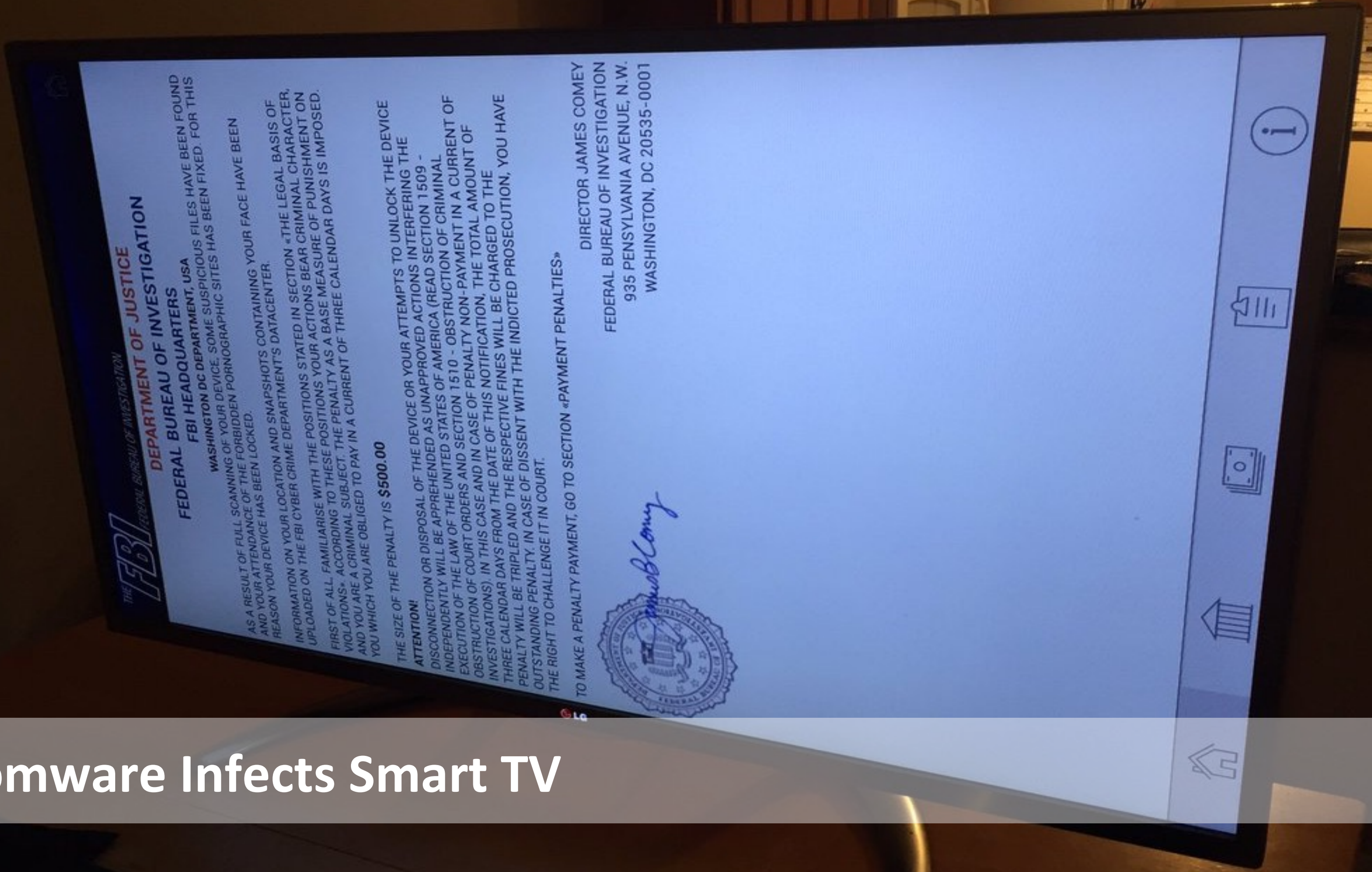
Consumer IoT

Enterprise IoT

Industrial IoT

Consumer IoT

- These devices are highly constrained in terms of
  - Physical size, Inexpensive
  - CPU power, Memory, Bandwidth
  - Autonomous operation in the field
- Power consumption is critical
  - If it is battery powered then energy efficiency is paramount, batteries might have to last for years
- Some level of remote management is required
- Value often linked to a Cloud platform or Service



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS». ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.

THE SIZE OF THE PENALTY IS **$500.00**

ATTENTION!
DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

TO MAKE A PENALTY PAYMENT, GO TO SECTION «PAYMENT PENALTIES»

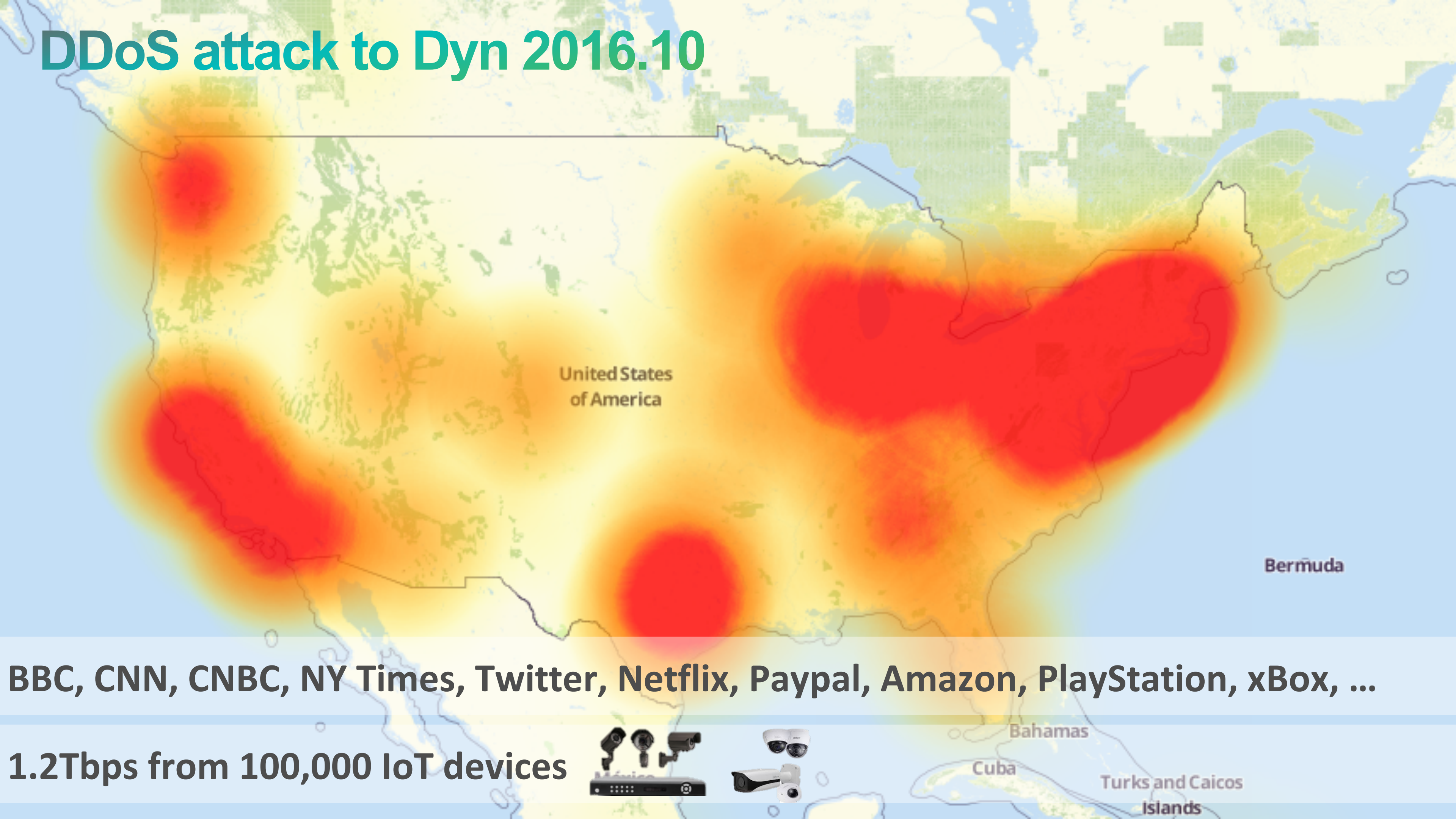
DIRECTOR JAMES COMEY
FEDERAL BUREAU OF INVESTIGATION
935 PENSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20535-0001

Ransomware Infects Smart TV

Nov 2016

A target can become a weapon

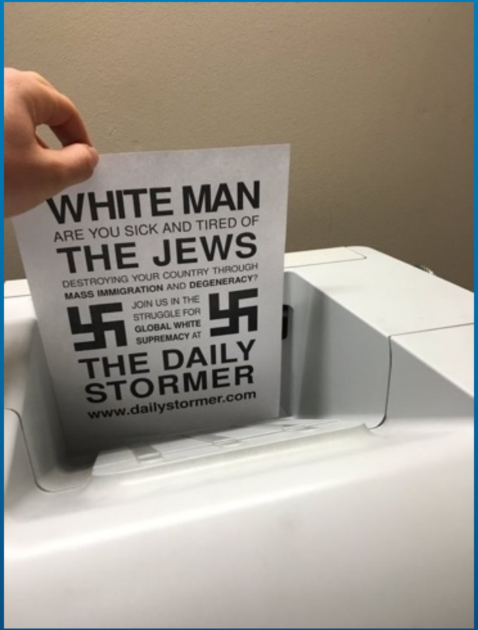
DDoS attack to Dyn 2016.10



BBC, CNN, CNBC, NY Times, Twitter, Netflix, Paypal, Amazon, PlayStation, xBox, …

1.2Tbps from 100,000 IoT devices

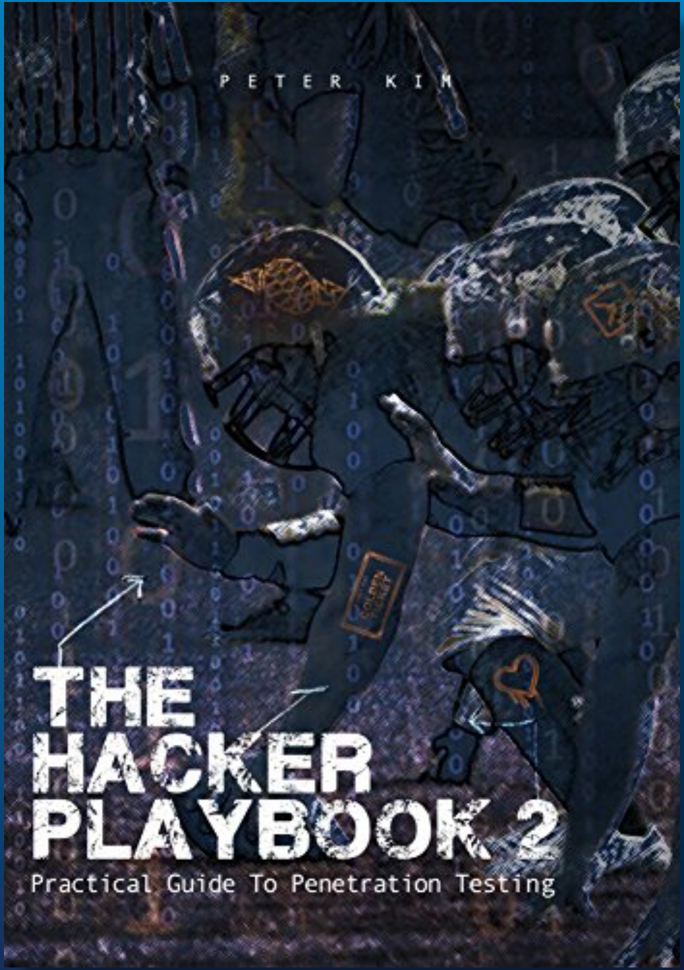
Enterprise IoT



WHITE MAN
ARE YOU SICK AND TIRED OF
THE JEWS
DESTROYING YOUR COUNTRY THROUGH
MASS IMMIGRATION AND DEGENERACY?
JOIN US IN THE
STRUGGLE FOR
GLOBAL WHITE
SUPREMACY AT
THE DAILY
STORMER
www.dailystormer.com

29,000 printers in dozens of college campuses across US

Mar 2016



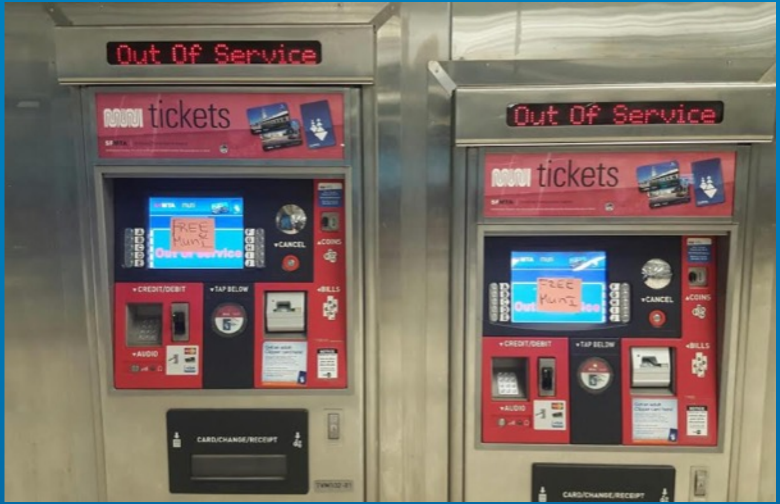
“I probe around for a multifunction printer and see that it is configured with default passwords. Great I am in”

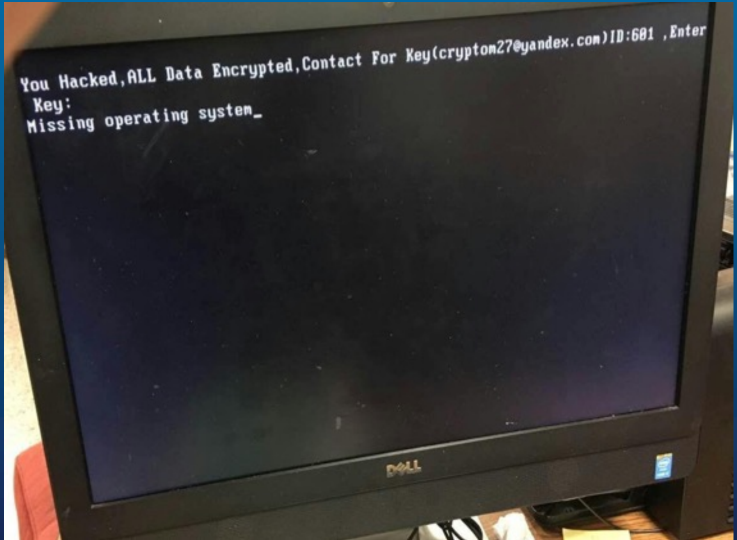
“YES! We've compromised a number of companies using printers as our initial foothold......................”

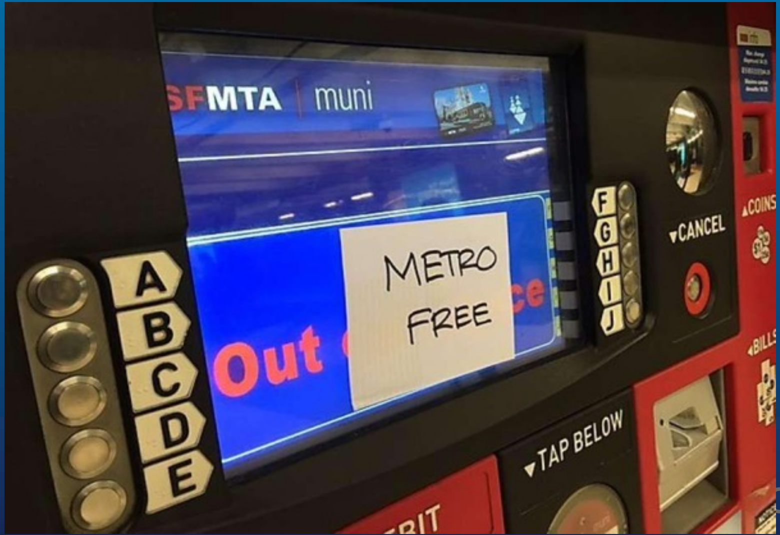
...........Hackers Playbook by Peter Kim.

San Francisco MUNI Railway, 900 computer encrypted, demand for $73,000

Nov 2016




```
You Hacked,ALL Data Encrypted,Contact For Key(cryptom27@yandex.com)ID:601 ,Enter
 Key:
Missing operating system_
```



ov 2016

Information Theft

Physical Damage

Insulin Pump (Human SCADA System)

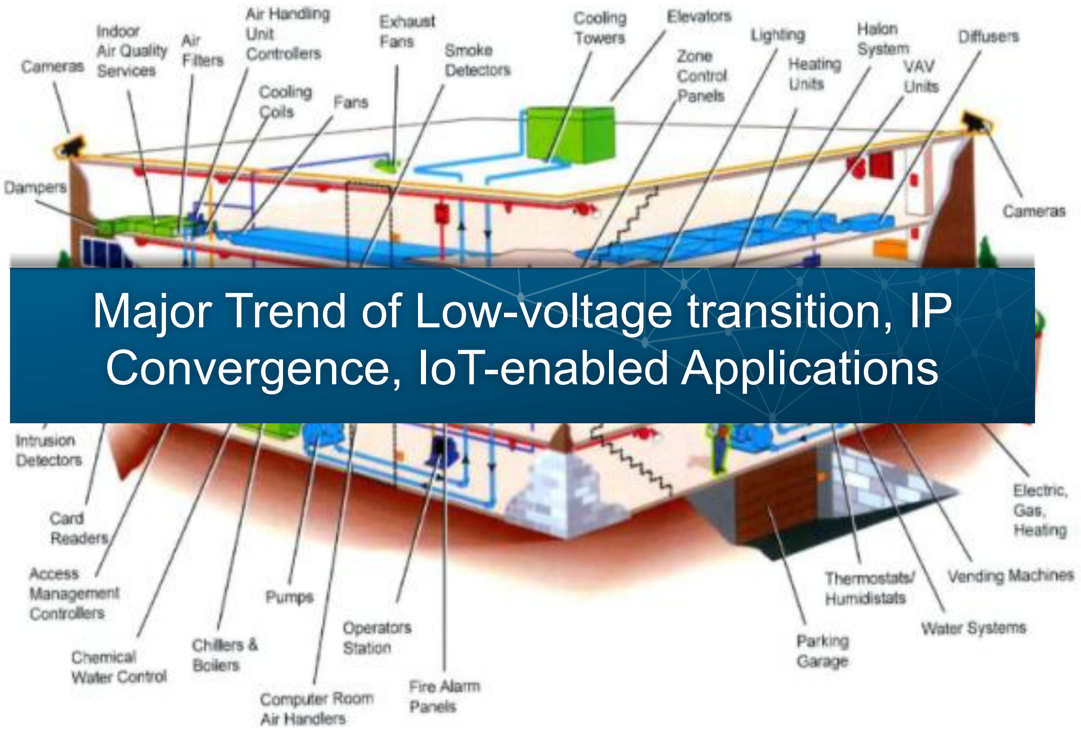
Barnaby Jack

Hacked Jeep

Commercial Buildings Digitization

Enterprise IoT (EIoT)

- Lighting
- HVAC
- Energy/Metering
- Physical Security
- Inventory
- Sensors
- Appliances



Major Trend of Low-voltage transition, IP Convergence, IoT-enabled Applications

Cisco Smart & Connected Real Estate

DDoS attack to BAS takes down heating system to 2 buildings (Lappeenranta, Finland)

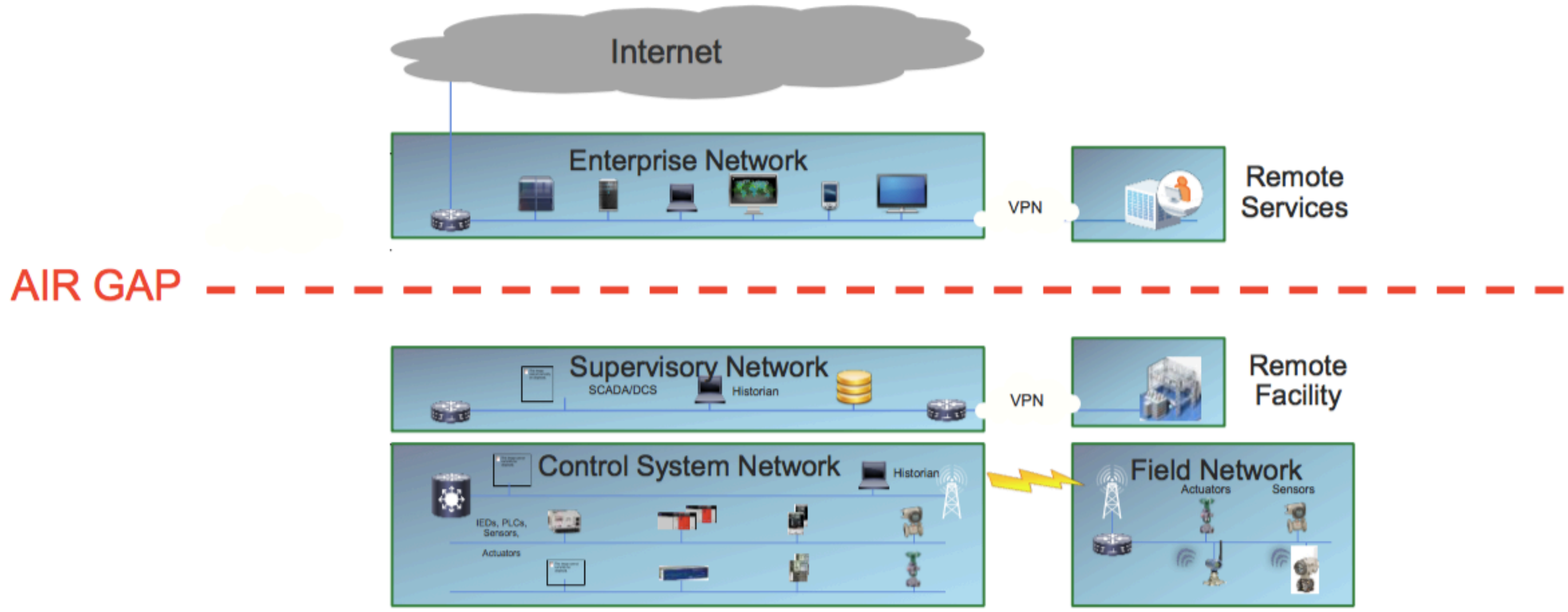
Nov 2016

Industrial IoT
Industrial Control Systems

Assets We need to Protect

Asset	Description	Examples and Notes
IEDs	Intelligent Electronic Device – Commonly used within a control system, and is equipped with a small microprocessor to communicate digitally.	Sensor, actuator, motor, transformer, circuit breaker, pump
RTUs	Remote Terminal Unit – Typically used in a substation or remote location. It monitors field parameters and transmit data back to central station.	Overlap with PLC in terms of capability and functionality
PLCs	Programmable Logic Controller – A specialized computer used to automate control functions within industrial network.	Most PLCs do not use commercial OS, and use “ladder logic” for control functions
HMIs	Human Machine Interfaces – Operator’s dashboard or control panel to monitor and control PLCs, RTUs, and IEDs.	HMIs are typically modern control software running on modern operating systems (e.g. Windows).
Supervisory Workstations	Collect information from industrial assets and present the information for supervisory purposes.	Unlike HMI, a supervisory workstation is primarily read-only.
Data Historians	Software system that collects point values and other information from industrial devices and store them in specialized database.	Typically with built-in high availability and replicated across the industrial network.
Other Assets	Many other devices may be connected to an industrial network.	For example, printers can be connected directly to a control loop.

OT Network Security



Airgap Security Quotes

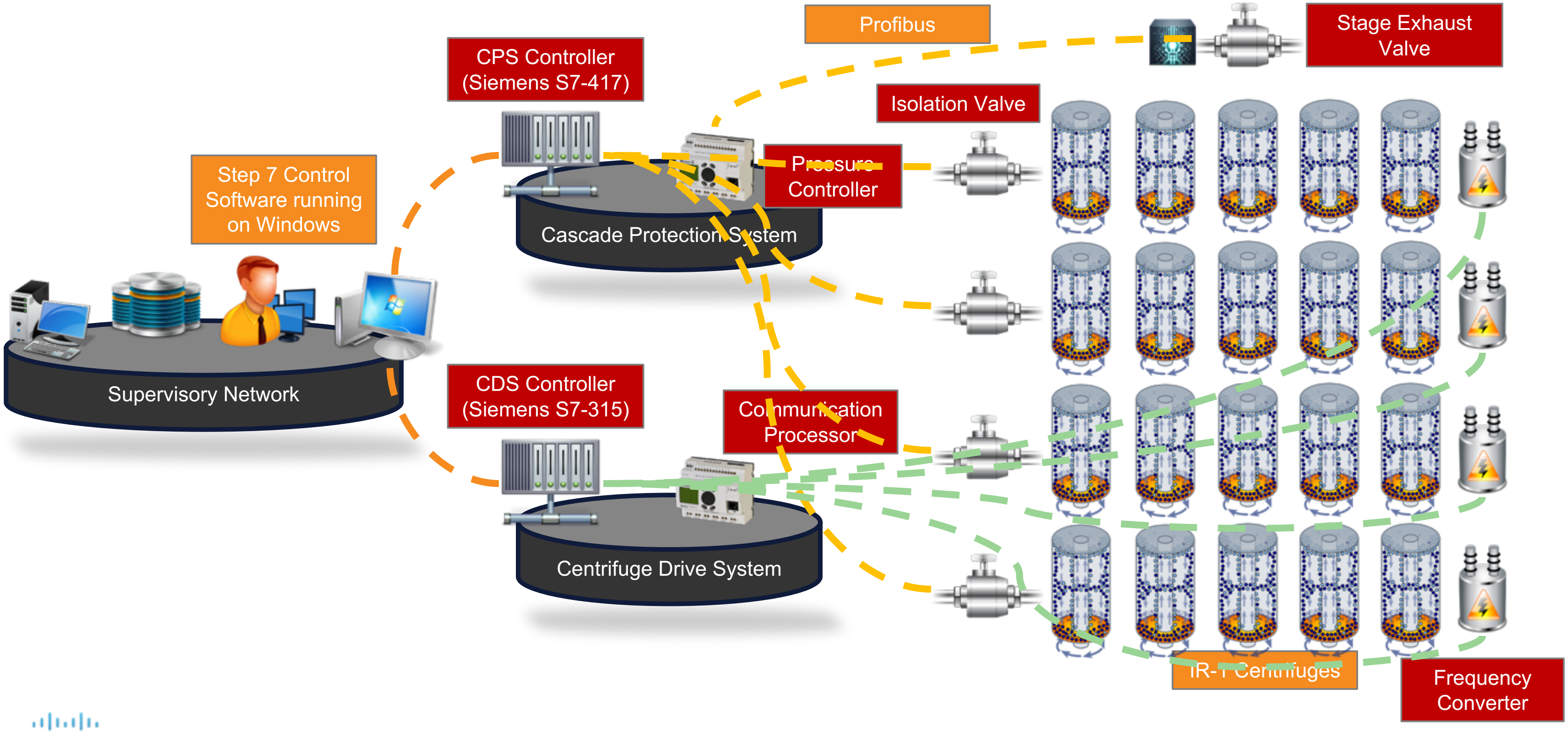
"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, **we see 11 direct connections** between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

Source: The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing

BTC Oil Pipeline

Iran Natanz Nuclear Facility … Stuxnet

Target ICS Infrastructure – Iran’s Natanz Nuclear Facilities



Physical attack mechanism

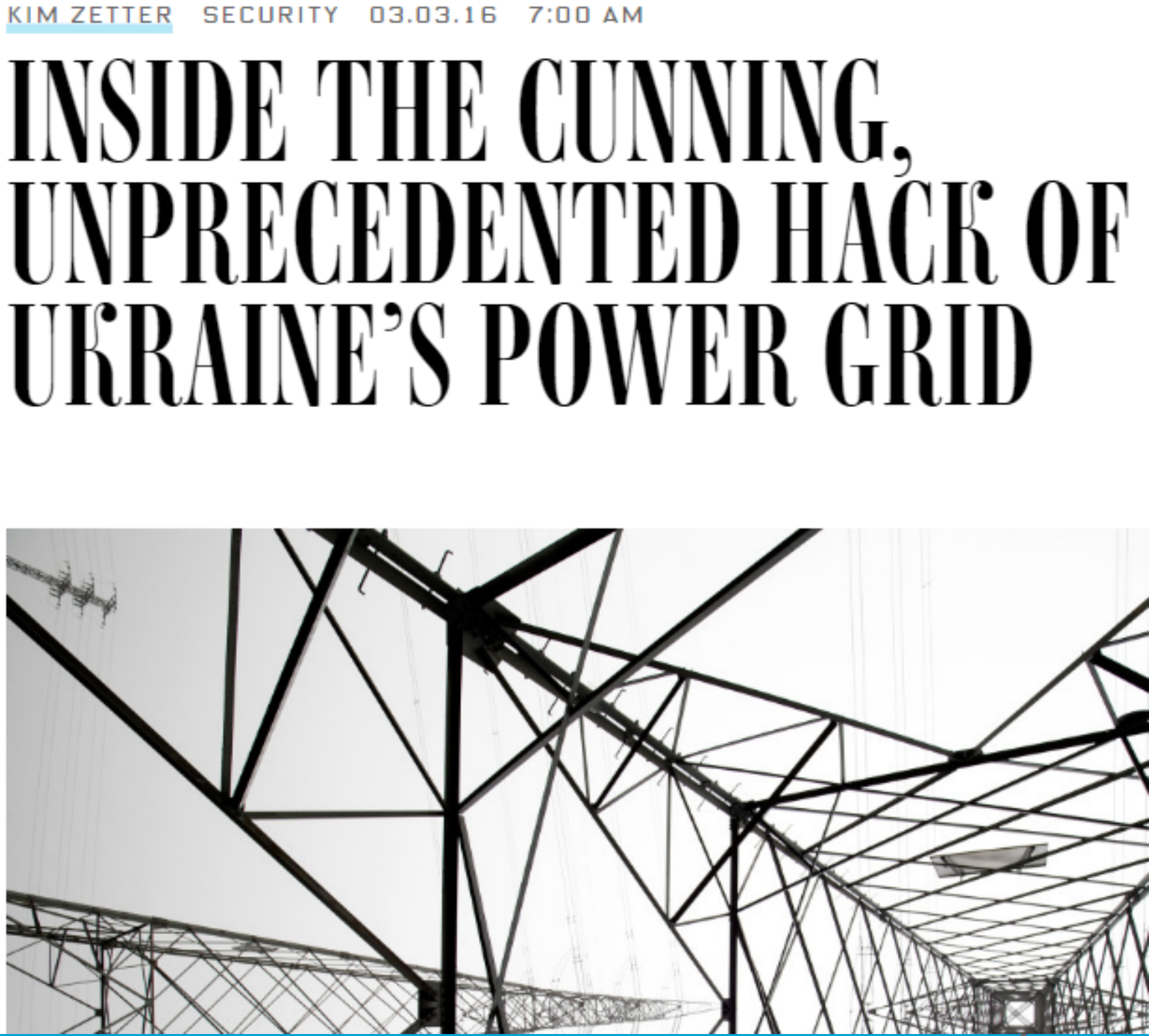
1. Measures and records rotation frequency for 13 days
   - Expected range : 800hz to 1000hz
2. Accelerate rotation frequency to 1400hz for 15 minutes
3. Sleep for 27 days
4. Slow rotation frequency to 2Hz for 50 minutes
5. Sleep for 27 days
6. Go to 2

International Space Station ISS

Impact in Ukraine:

Power lose to 225K people for 1-6 hours

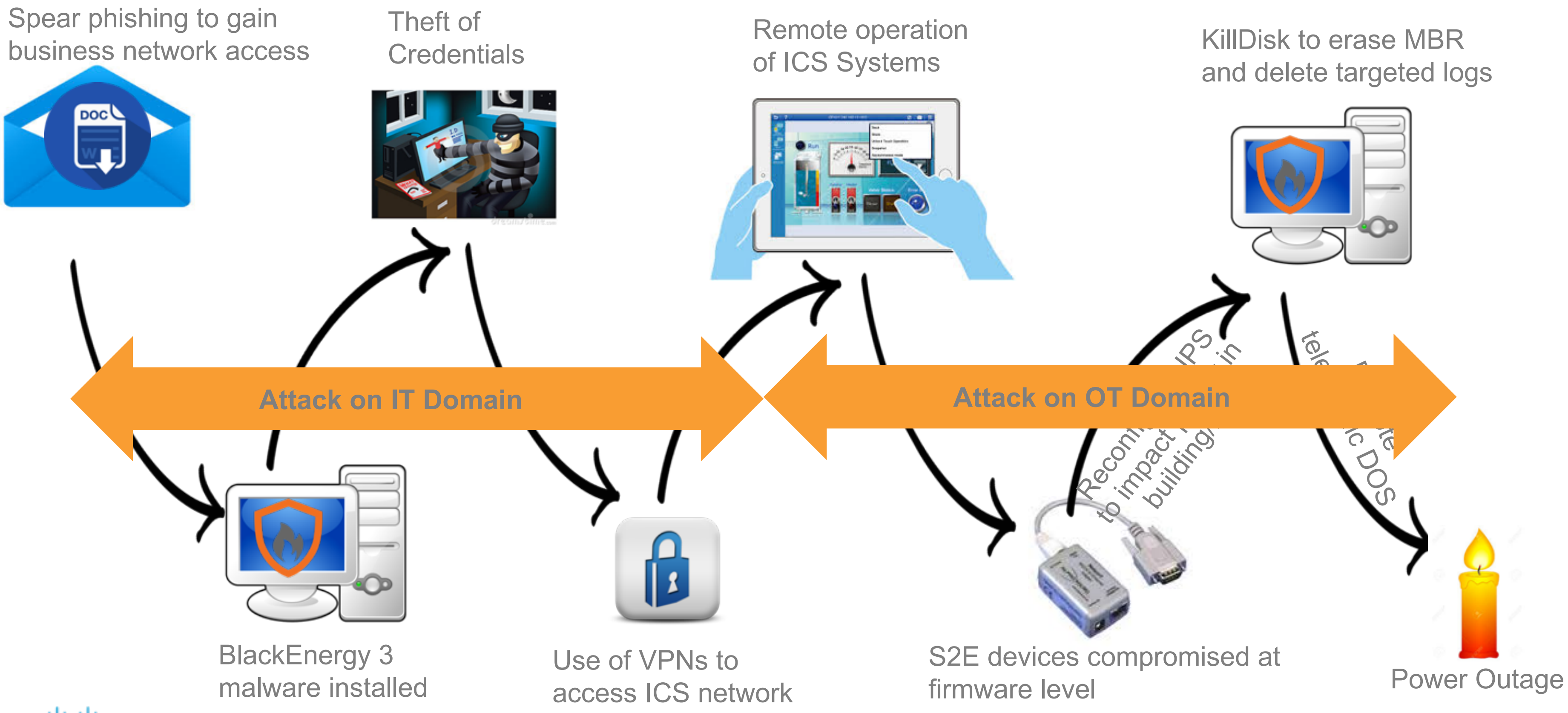
30 sub-stations disconnected



KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

Ukraine Grid Attack – Chronology of Events



Spear phishing to gain business network access

Theft of Credentials

Remote operation of ICS Systems

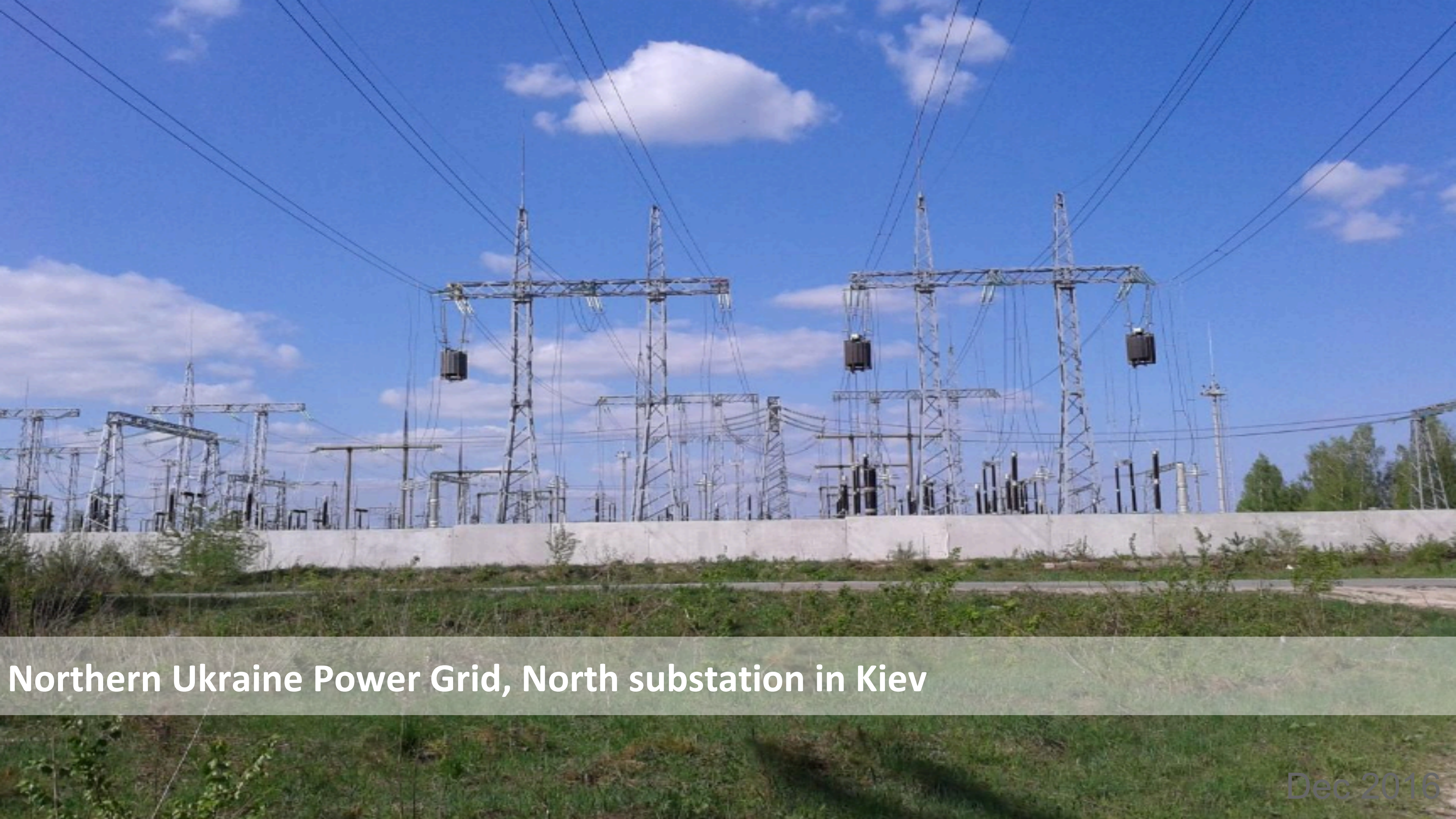
KillDisk to erase MBR and delete targeted logs

BlackEnergy 3 malware installed

Use of VPNs to access ICS network

S2E devices compromised at firmware level

Power Outage



Northern Ukraine Power Grid, North substation in Kiev

IT and OT Technologies Convergence

Illustrative

IT – Info Tech | OT Oper Tech

Purdue Model

- **Level 5** Enterprise Network
- **Level 4** Site Business Planning
- **Level 3.5** DMZ Demilitarized Zone
- **Level 3** Plant Zone Site Operations & Control
- **Level 2** Cell/Area Zone Area Control
- **Level 1** Cell/Area Zone Basic Control
- **Level 0** Cell/Area Zone Process

Digital Healthcare	Connected Retail	Connected City	Connected Service Provider	Connected Car	Connected Transportation	Digital Manufacturing	Connected Utilities
100% IT	90% IT	90% IT	70% IT	60% IT	60% IT	30% IT	30% IT
E.g. Virtual Patient, IP Video, Wi-Fi, RFID, Medical Inventory Trackers, Patient Media Experience	E.g. Store-in-a-box, Digital Experience, Electronic Shelf-Edge Labels, Product Tracking Tags	E.g. City Wi-Fi, Location, Traffic, Safety/ Security, Smart Trash Bins,& Smart Building	E.g. Fleet, asset Management	E.g. Collaborative to Navigation Applications	E.g. 60% IT Stations, Wi-Fi, Automated Kiosks/Console Traffic & Parking Sensor	E.g. ERP, Finance, & A/P	E.g. Backend Offices
	10% OT	10% OT	30% OT	40% OT	40% OT	70% OT	70% OT
	E.g. Asset Tracking	E.g. Asset Tracking	E.g. Remote Cell Towers	E.g. Automotive Subsystems Interior to Safety Sensors	E.g. Roadways, Trackside, Onboard, & Mobile Signature Device	E.g. SCADA, ICS,EMS,AGC, Automation, Robots, Assets Tracking, & RFID Tag Reader	E.g. Smart Gas Meter, Power Room, Distribution & Substation, Oilfield, Refinery, & Smart Grid Devices

Note: IT & OT As Defined by IOT BU
*OT Baseline Features

IT (Information Technology) Vs OT (Operation Technology)

Security Policies	IT Network	OT Network
Focus	Protecting Intellectual Property and Company Assets	24/7 Operations, High OEE, Safety, and Ease of Use
Priorities	1. Confidentiality 2. Integrity 3. Availability	1. Availability 2. Integrity 3. Confidentiality
Types of Data Traffic	Converged Network of Data, Voice and Video (Hierarchical)	Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical)
Implications of a Device Failure	Continues to Operate	Could Stop Processes, Impact Markets, Physical Harm
Threat Protection	Shut Down Access to Detected Threat and Remediate	Potentially Keep Operating with a Detected Threat
Upgrades and Patch Mgmt	ASAP During Uptime	Scheduled During Downtime
Infrastructure Life Cycle	Equipment upgrades and refresh <5yr	Avoid Equipment upgrades (lifespan 15+ yrs)
Deployment conditions	Controlled physical environments	Harsh environments (temp, vibration, etc)

IT/OT Converged Security Model

Cloud Internet	OT Partners & Services	Cloud-based Threat Protection Network-wide Policy Enforcement Security Information & Event Management (SIEM)
IT	Enterprise Network	Enterprise Edge (VPN, IPS, NGFW) Anti-Virus Corporate Directory
DMZ	Demilitarized Zone	Plant Edge (VPN, IPS & Remote Access) Stateful Firewall Access Control
OT	Process, Supervisory	SIEM, Remote Services Platform OT Policy Mgmt, SW, Config, AV & Asset Mgmt. Cyber & Physical Access Control Systems
	Control, Automation	Ruggedized Firewall Ruggedized IDS / IPS Segmentation: VLANs, VRFs, ACLs

Availability
Integrity
Confidentiality

Identity Mgmt & Access Control
Threat Detection & Mitigation

IoT Enabler - Cisco Connectivity Fabric

Cisco IoT System

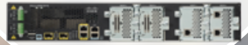
Industrial Switching

IE 1K, 2K,3K,4K,5K, CGS

Industrial Routing

IR 809/829,IR 509

CGR 1000



CGR 2000

LoRa GW

IR809 GW

IR829 3-sector GW

Network Management

FND, IND,IOT-DM, IOK, IOX/Fog Director

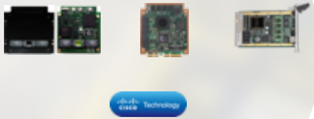
Industrial Wireless

IW 3700, 1552H

Industrial Security

ISA 3000

Embedded Networks



ESS, 5900 ESR 5921 SW ESR

Cisco IoT System Network Connectivity

IoT Network as a Sensor and Enforcer

IE Switches, IR Routers, ISE

High performance, H/W accelerated VPN – IR 809, 829

Portfolio wide consistent policy enforcement

Attack and abnormal traffic detection mitigation

Misconfiguration prevention

MAC Bypass for legacy device identification

DDOS attack mitigation

Industrial Switching

IE 2000, 3000
CGS2000

IP67

IE 4000

IE 5000

Industrial Routing

IR 829

IR 809

Simplified Compliance | Risk Mitigation | Consistent Policy Enforcement | Increased System Availabilty

Industrial Security - ISA 3000

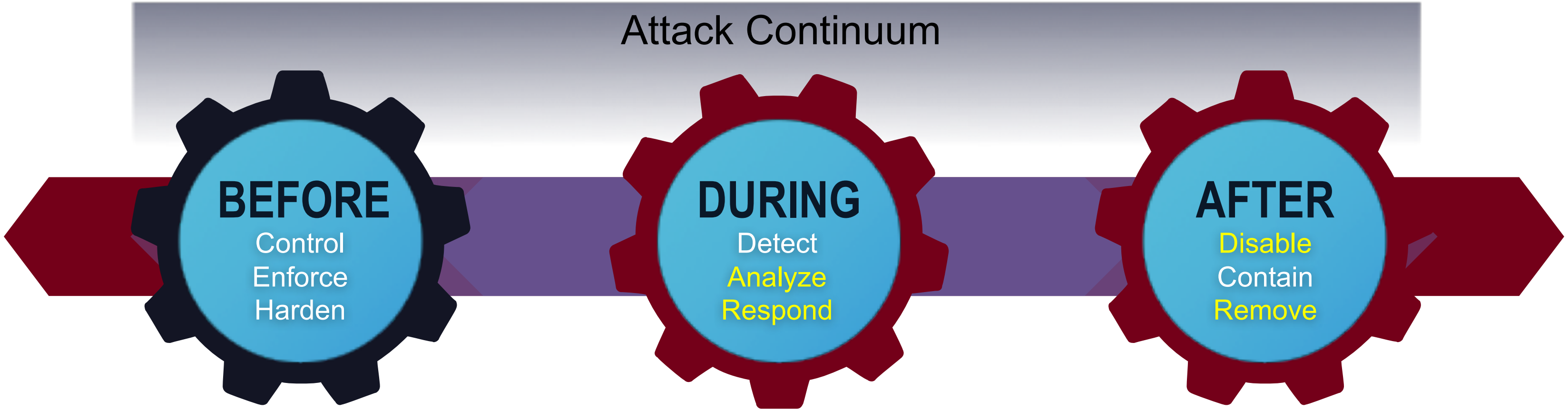
ISA 3000 Fibre

ISA 3000 Copper

- Industrial, Energy, Marine, Railway Compliance
- Services include Firewall, VPN and SourceFire IPS, DHCP, and NAT
- Two Configurations
  - Copper: 4x10/100/1000BaseT; 2x10/100/1000BaseT
  - Fibre: 2x1GbE (SFP)
  - LED scheme is OT Ready

- DIN Rail mounting with optional Rack Mounting
- Connectors: Management Interface (RJ45 and USB); Power supports 24-12 AWG; Factory Reset
- Thermals: -40C to 60C no airflow; -40C to 70C with 40LFM; -34C to 74C with 200LFM

Cisco Threat Centric Security Model



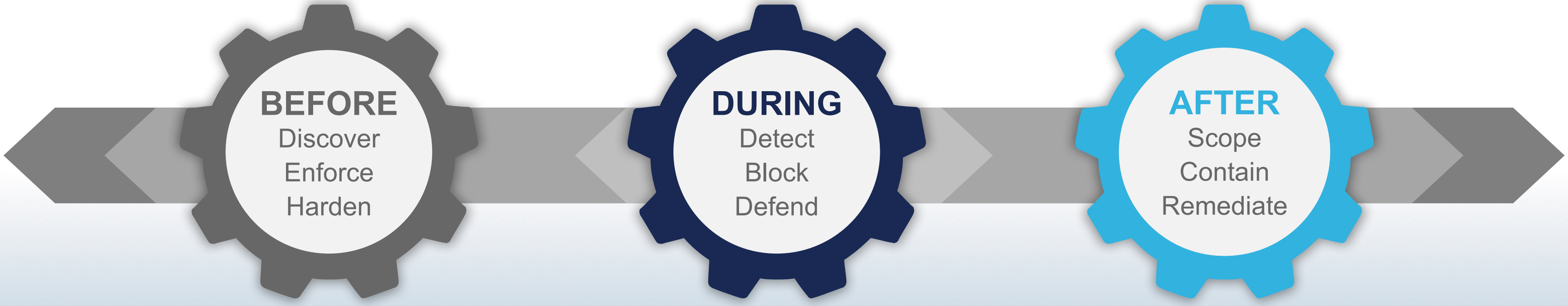
Access Control, Policy and Identity management

Dynamic Network Segmentation

Industrial NGFW, IPS

Network Behavior and Anomaly Detection

Threat Centric model to cover the Entire Attack Continuum



BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

DNS Layer Protection & CASB

Firewall	VPN	NGIPS	Cognitive Threat Analytics (CTA)
NGFW	UTM	Email & Web Security	Network Behavior Analysis

Secure Access + Identity Services

Advanced Malware Protection (AMP) & Threat Grid (Sandbox)

Visibility, Context, Segmentation & Threat Intelligence

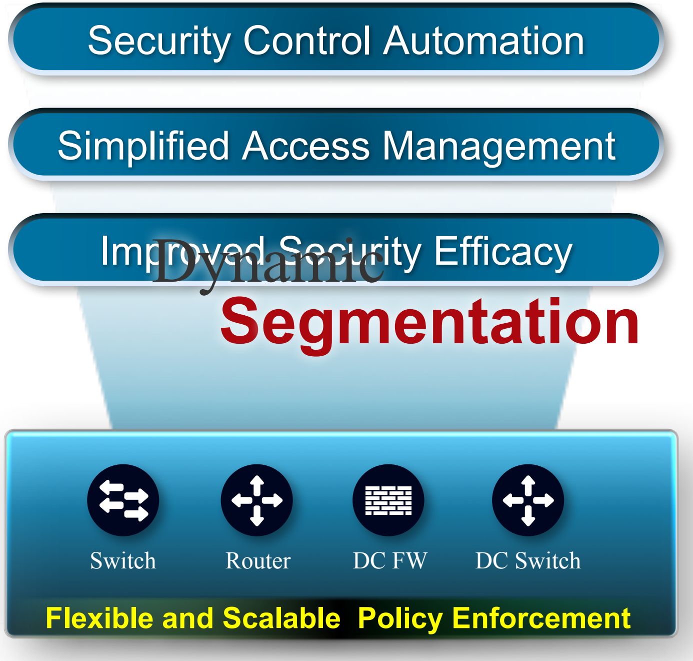
Automatic remediation with ISE and TrustSec

Traditional Security Policy (ACL)

Business Policy (ISE)

Protected Assets

Source	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT



Security Control Automation

Simplified Access Management

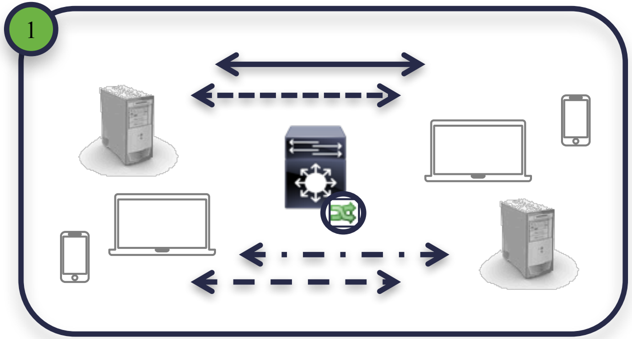
Improved Security Efficacy

Dynamic Segmentation

Flexible and Scalable Policy Enforcement

Network Traffic Visibility – Behavior & Anomaly Detection

- Comprised Credential, Insider Threat, Suspicious Activities through Netflow

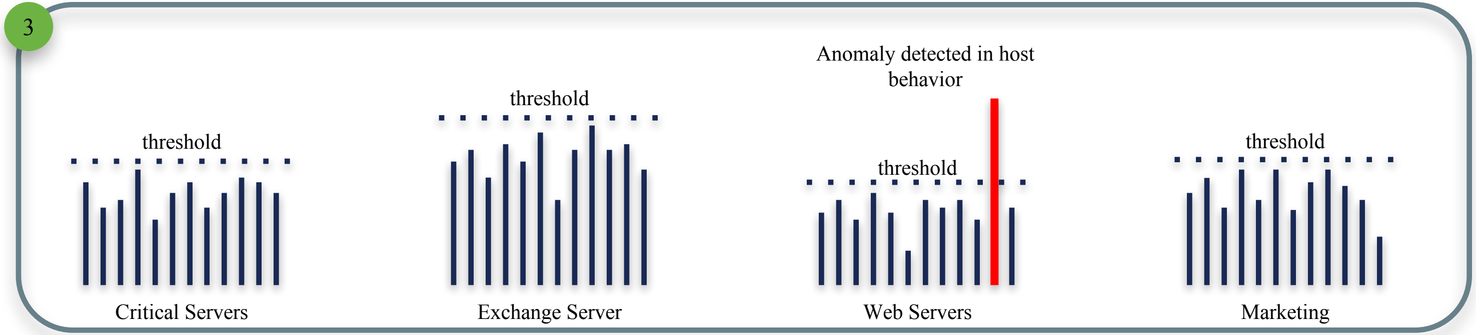


Collect & Analyze Flows

2

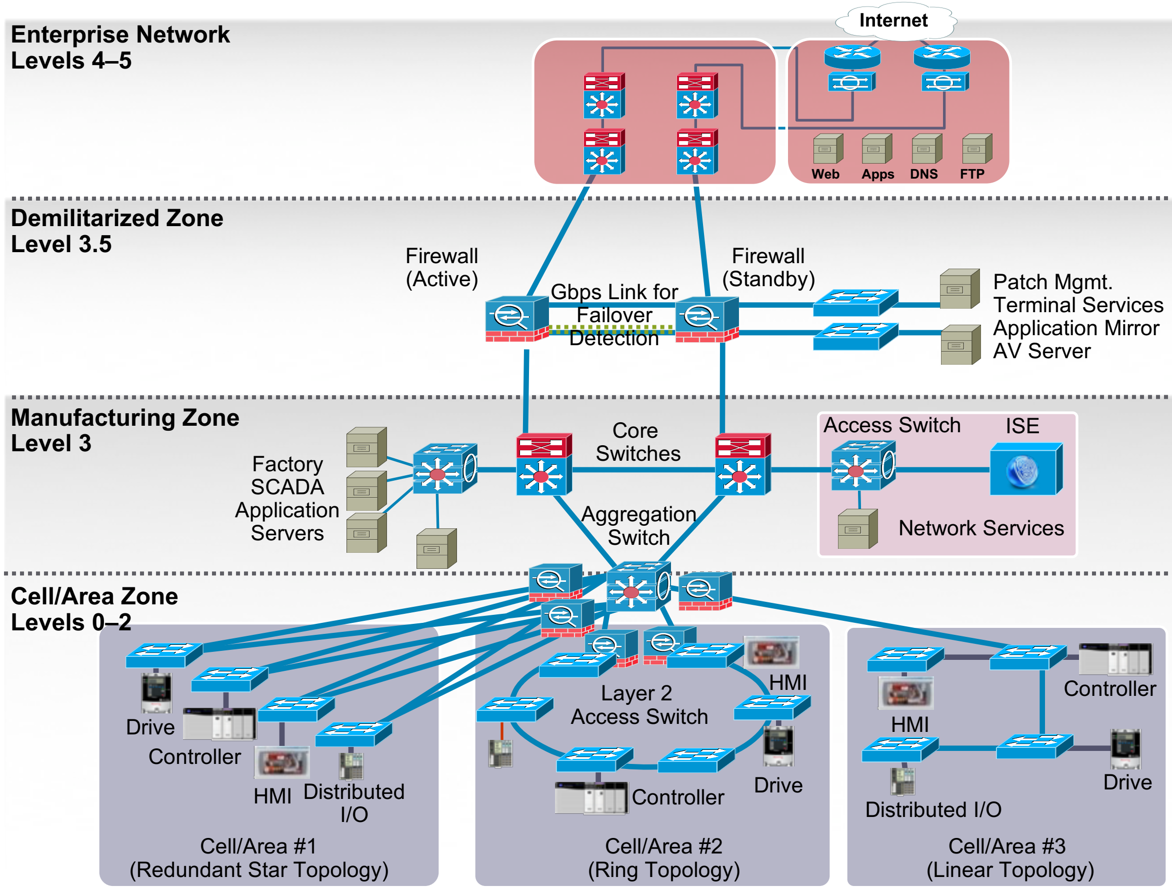
- # Concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of SYNs received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Establish Baseline of Behaviors



Alarm on Anomalies & Changes in Behavior

IT/OT Converged Security Model – Manufacturing



Cloud-based Threat Protection

Network-wide Policy Enforcement

Access Control (application-level)

VPN & Remote Access Services

Next-Generation Firewall

Intrusion Prevention (IPS)

Stateful Firewall

Intrusion Protection/Detection (IPS/IDS)

Physical Access Control Systems

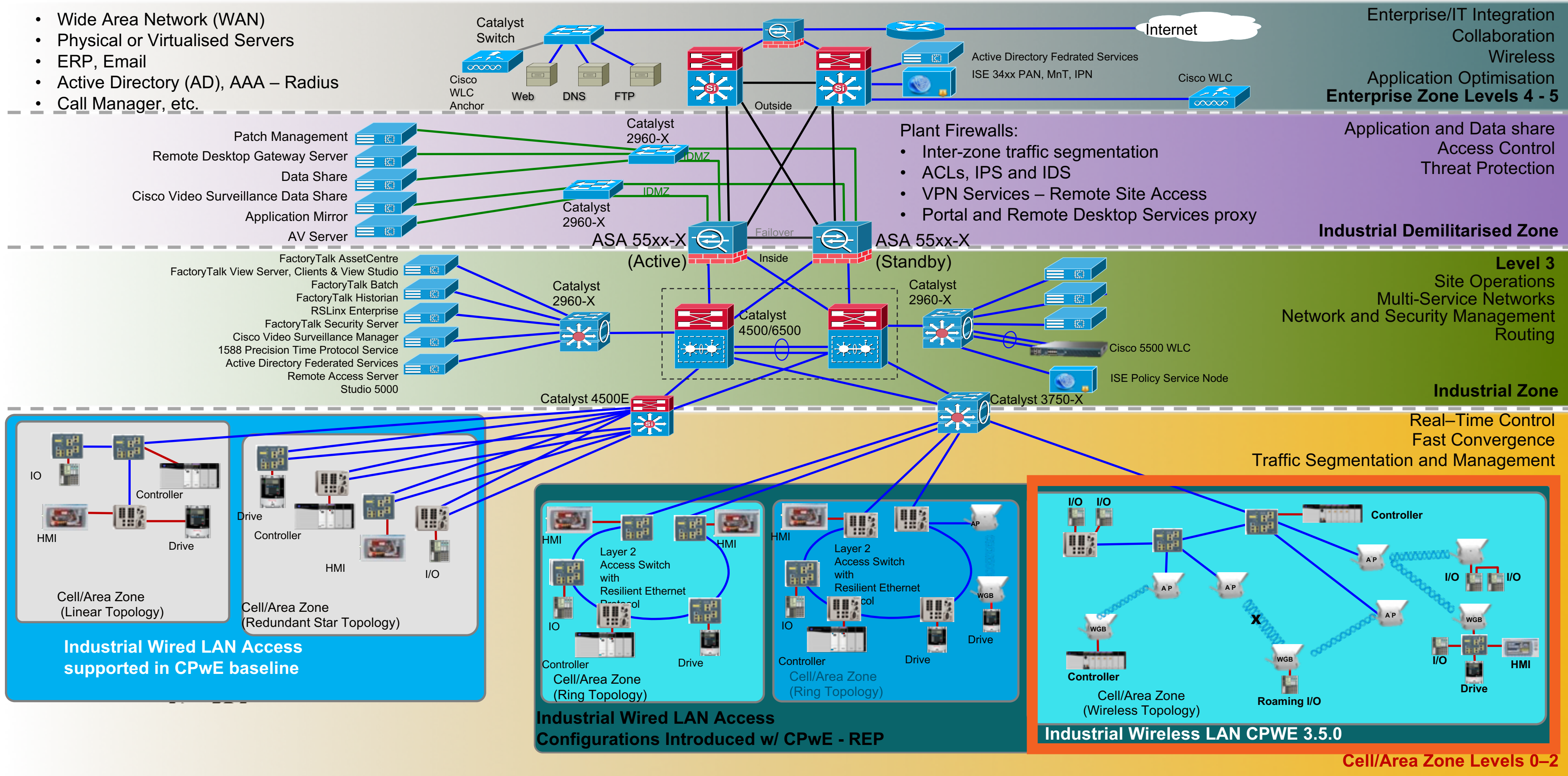
Ruggedized Firewall

Ruggedized Intrusion Protection (IDS)

Remote Monitoring / Surveillance

SW, Config & Asset Mgmt

CPwE 3.5 Overall Architecture with Wireless



- Wide Area Network (WAN)
- Physical or Virtualised Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager, etc.

Enterprise/IT Integration
Collaboration
Wireless
Application Optimisation
Enterprise Zone Levels 4 - 5

Plant Firewalls:

- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services – Remote Site Access
- Portal and Remote Desktop Services proxy

Application and Data share
Access Control
Threat Protection
Industrial Demilitarised Zone

Level 3
Site Operations
Multi-Service Networks
Network and Security Management
Routing
Industrial Zone

Real–Time Control
Fast Convergence
Traffic Segmentation and Management

Industrial Wired LAN Access supported in CPwE baseline

Industrial Wired LAN Access Configurations Introduced w/ CPwE - REP

Industrial Wireless LAN CPWE 3.5.0

Cell/Area Zone Levels 0–2

In Summary

- Threat on IoT is real
- Industrial Networking
  - Convergence, IP everywhere, Focus on security
- Cyber Security
  - Beyond Air Gap
  - Before - During – After Security Model
  - Wired and Wireless Considerations
  - Follow Best Practices

Garrick Ng - CTO: garng@cisco.com
Raymond Poon – Solutions Architect: raypoon@cisco.com