Take down: Hackers looking to get paid

By: Ernie P. Dalesio, The Associated Press

JUN 22, 2017 @ 05:00 AM 8,040

Cyber Attack At Honda Stops Strikes

Peter Lyon, CONTRIBUTOR

Opinions expressed by Forbes Contributors are their own.

Honda was forced to halt production at its Sayama plant after WannaCry worm spread

The WannaCry worm is still alive. Honda said that it was forced to halt production for one day at its Sayama plant near Tokyo after finding the WannaCry ransomware in its computer network.

This virus is the same one that infected over one million computers in 2017 and demanded a ransom for their repair.

Irish power grid compromised by foreign actor: report

BY: JOE DERMICHEL 10/30/7 10:57 PM EDT

Comey to teach ethical leadership course at William & Mary

ADMINISTRATION — WM 385 480

“Pentagon Papers”: Even at its best the press didn’t stop war

ADMINISTRATION — WM 385 480

White House: Trump will not go to Mar-a-Lago amid shutdown

Politi: Trump ends first year with lowest approval of any modern president

ADMINISTRATION — WM 385 480

Kelly has frequently threatened to quit if Trump didn’t listen to him: report

A foreign power compromised the cybersecurity of the state-owned Irish power grid company EirGrid, Ireland's independent newspaper reports.

The report, issued Monday in Ireland, says that the telecommunications company Vodafone discovered last month that hackers had compromised its systems more than two months prior.

The attackers then installed eavesdropping software on the routers used by EirGrid and were able to see encrypted communications sent by the
Securing the Internet of Things

Philippe Roggeband, Manager
GSSO EMEAR Business Development
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKIOT-2112
The IoT pillars

While these pillars represent disparate technology, purposes, and challenges, what they all share are the vulnerabilities that IoT devices introduce.
It’s not just about the “things”

IoT World Forum Reference Model

Levels

7. Collaboration & Processes
   (Involving People & Business Processes)

6. Application
   (Reporting, Analytics, Control)

5. Data Abstraction
   (Aggregation & Access)

4. Data Accumulation
   (Storage)

3. Edge Computing
   (Data Element Analysis & Transformation)

2. Connectivity
   (Communication & Processing Units)

1. Physical Devices & Controllers
   (The “Things” in IoT)
Agenda

• Challenges and Constraints
• Specific threats and Protection mechanisms
• Cisco best practices and solutions
• Q&A
• Conclusion
Agenda

- Challenges and Constraints
  - Specific threats and Protection mechanisms
  - Cisco best practices and solutions
- Q&A
- Conclusion
Consumer IoT Characteristics
Consumer objects Challenges and constraints

- 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
Connected objects complexity

- Single Bus is used to exchange information
- Example CAN messages:
  - A/C temperature
  - Radio Volume
  - Lights
  - Cruise Control
- Complex consumer objects may be part of a bigger picture
  - Smart City
  - Machine to Machine
Who is responsible?

- Manufacturer
- Owner
- Internet Service Provider
- Cloud solution provider
- User
Enterprise IoT
Enterprise IoT

- (Partially) controlled environment
- Security policies for objects (should) exist
- Cloud access security policies (should) exist
- **but...**
- Consumer objects may be connected by users
- Unsecure objects get hacked in devious ways
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
<table>
<thead>
<tr>
<th>End device OS support</th>
<th>EnergyWise</th>
<th>CoAP</th>
<th>MQTT</th>
<th>XMPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any, OpenRTOS</td>
<td>Contiki, RIOT, TinyOS, mbed, iOS, Android</td>
<td>Posix, windows</td>
<td>Linux, iOS, Android, windows, OSX, OpenWRT</td>
<td></td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>TCP/UDP</td>
<td>UDP</td>
<td>TCP</td>
<td>TCP</td>
</tr>
<tr>
<td>Standard</td>
<td>Proprietary &amp; Open</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
</tr>
<tr>
<td>Development community</td>
<td>Cisco &amp; Cisco Partners</td>
<td>Cisco, ARM, Eclipse, libcoap, Eclipse Mosquito/Paho</td>
<td>Allseen alliance</td>
<td></td>
</tr>
<tr>
<td>Implementation languages</td>
<td>C, Java</td>
<td>C, Java, Python, Go, C#, Ruby, Lua, C++</td>
<td>C, Java, Perl, Ruby, PHP, Lisp, Python, Haskell, TCL, JS</td>
<td></td>
</tr>
<tr>
<td>Standards body</td>
<td>Cisco / IETF</td>
<td>IETF</td>
<td>OASIS</td>
<td>IETF</td>
</tr>
<tr>
<td>Security</td>
<td>PSK, TLS</td>
<td>DTLS</td>
<td>TLS</td>
<td>TLS</td>
</tr>
<tr>
<td>Industry adoption trend</td>
<td>Cisco, Cisco partners</td>
<td>ARM, Cisco, Ericsson, Philips, Huawei, Alcatel-lucent</td>
<td>IBM, Elecsys, Eurotech</td>
<td>Qualcomm, Alseen, Cisco</td>
</tr>
</tbody>
</table>

- **IoT still evolving**
- **Multiple protocols emerging for IoT**
- **Open Source and open standards for widespread adoption**
- **CoAP gaining traction in the industry**
Security Threats

Service Disruption

• Vulnerabilities on Endpoints

• Vulnerabilities on Management Applications. (i.e Control/Monitoring)

Unauthorized Network Access

• Potential network entry point

• Unauthorized POE Devices

• End Points support only MAB – MAC spoofing risk

• Snooping of Control traffic

Traditional Threats

• IP/MAC spoofing

• MAC flooding

• DHCP related attacks

• DDoS

• DNS poisoning

• MITM
Industrial Control Systems
# Assets We need to Protect

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

The Rigid Silos between IT and OT

Cyber-Security IT/OT Convergence

**IT**
- Protect IT Assets
- Confidentiality, Integrity, Availability
- Data, Voice, Video
- Network Authentication
- Threat Detection

**OT**
- Operations uptime/Safety
- High Availability,
- Integrity, Confidentially
- Control
- Protocols/Motion
- Physical Access
- Process Anomalies

**Security Risk Assessment**
**Asset Visibility across IT/OT**
**Segmented Access Control**
**Evolving Security Regulations**
**Remote Access**
Industrial Networks: Manufacturing +

- **Fieldbus: 58%**
  - Annual growth: 7%
- **PROFIBUS: 17%**
- **Other fieldbuses: 15%**
- **AS-interface: 3%**
- **CAN/CANopen: 5%**
- **Devicenet: 5%**
- **CC-Link: 6%**
- **Modbus: 7%**
- **PROFINET: 8%**
- **EtherCAT: 6%**
- **Modbus-TCP: 4%**
- **Powerlink: 3%**
- **Other Ethernet: 6%**
- **WLAN: 2%**
  - Bluetooth: 1%
  - Other Wireless: 1%

**Industrial Ethernet: 38%**
- Annual growth: 20%

**Wireless 4%**
- Annual growth: 30%
Where are these Protocols Found?
CIP (Common Industrial Protocol) over Ethernet

- Developed in the late 90’s by Rockwell
- Now under the control of ODVA, known as EtherNet/IP
- Object-oriented approach
- Designed to be media-independent
- May now run over IP
Profibus and Profinet (Profibus over Ethernet)

Originally developed in late 1980s in Germany by the Central Association for the Electrical Industry.

Profibus is a Master/Slave protocol that supports multiple master nodes through the use of token sharing: when a master has control of the token, it can communicate with its slaves (each slave is configured to respond to a single master).

In Profibus DP-V2, slaves can initiate communications to master or to other slaves under certain conditions.

Typically, a master Profibus node is a PLC or RTU, and a slave is sensor, motor, or some other control system devices.
Profibus and Profinet (Profibus over Ethernet)

- Originally developed in late 1980s in Germany by the Central Association for the Electrical Industry.
- Profibus is a Master/Slave protocol that supports multiple master nodes through the use of token sharing: when a master has control of the token, it can communicate with its slaves (each slave is configured to respond to a single master).
- In Profinet DP-V2, slaves can initiate communications to master or to other slaves under certain conditions.
- Typically, a master Profibus node is a PLC or RTU, and a slave is a sensor, motor, or some other control system device.
• Modbus is the oldest and perhaps the most widely deployed industrial control protocol.

• Modbus is a request/response protocol using only three distinct PDUs: Request, Response, and Exception Response.

• **Modbus TCP** uses TCP/IP to transport Modbus commands and messages over Ethernet-based routable networks.

• Modbus is typically deployed between PLCs and HMIs, or between a Master PLC and slave devices such as PLCs, Drives, Sensors, and other I/O devices.
OPC (OLE for Process Control)

OPC is a suite of protocols that collectively enable Process Control Systems to communicate using Microsoft’s Object Linking and Embedding (OLE) architecture.

Originally OPC was DCOM-based, though recently has been updated to use OPC-UA (Unified Architecture) and OPC-XI (Express Interface). However, legacy OPC systems remain heavily deployed.

OPC is typically used as a gateway between fieldbus protocols and Windows-based computing networks.

OPC inherits security risks and vulnerabilities from Windows.
OPC (OLE for Process Control)

• OPC is a suite of protocols that collectively enable Process Control Systems to communicate using Microsoft’s Object Linking and Embedding (OLE) architecture.

• Originally OPC was DCOM-based, though recently has been updated to use OPC-UA (Unified Architecture) and OPC-XI (Express Interface). However, legacy OPC systems remain heavily used as a gateway between fieldbus protocols and Windows-based computing networks.

• OPC inherits security risks and vulnerabilities from Windows.

• OPC is typically used as a gateway between fieldbus protocols and Windows-based computing networks.
DNP3 is mainly used between master control stations and remote slave devices (e.g. RTUs).

DNP3 was a layer-2 protocol, and now works over TCP/IP (typically using TCP or UDP port 20000).

DNP3 is very reliable, while remaining efficient and well-suited for real-time data transfer.

DNP3 is bi-directional and support exception-based reporting.

Secure DNP3 is a DNP3 variant that adds authentication to the request/response process.

IEEE adopted DNP3 as IEEE Std 1815-2010 on the 23rd of July 2010 (Std 1815-2012 is the latest).
IEC 60870-5-104

- Standard for power system monitoring, control & associated communications for telecontrol, teleprotection, and associated telecommunications for electric power systems.

- IEC TS 60870-5-7 defines Security extensions, including authentication and end-to-end encryption, but rarely implemented due to increased complexity.
Common SCADA Security Issues

- Weak Access controls to HMI and other equipment
  - Separation of duty for operator, administrator, audit
  - Little or no Password management

- Physical segmentation of the SCADA network
  - Dual-homed servers or PLCs act as Firewall
  - Segmented network has only physical security

- Unauthenticated command execution

- Communication is un-encrypted

- Outdated operating systems left unpatched

- Rogue wireless access points without encryption

- Insufficient controls on contractors (i.e. access policy, laptops, etc…)

- Humans are writing the SCADA system software
Purdue Reference Model – Like OSI for Manufacturing

Enterprise Zone
- Enterprise Network Level 5
- Site Business Planning and Logistics Network Level 4

IDMZ
- Industrial Demilitarized Zone — Shared Access Level 3.5

Manufacturing Zone
- Site Manufacturing Operations and Control Level 3
- Area Control Level 2
- Basic Control Level 1
- Process Level 0

Cell/Area Zone
Kill Chain – ICS Variant

- Intrusion Phase
  - Reconnaissance
  - Targeting
  - Weaponization
    - Develop / Test
  - Delivery / Exploit / Persist
  - Install
  - Modify Systems
  - Command and Control
  - Attack
- Anti-Forensics
## OT Security Challenges

<table>
<thead>
<tr>
<th>Category</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>Lack of visibility into assets on network</td>
</tr>
<tr>
<td>Control</td>
<td>24x7 availability limits operational change</td>
</tr>
<tr>
<td>Compliance</td>
<td>Out of date OS &amp; firmware on PLC &amp; HMI etc.</td>
</tr>
<tr>
<td>Segmentation</td>
<td>Flatter networks – Bus &amp; Ring</td>
</tr>
<tr>
<td>Legacy Infra</td>
<td>Outdated systems prone to compromises and cyber challenges</td>
</tr>
<tr>
<td>Secure Access</td>
<td>Lack of security controls supporting vendor access.</td>
</tr>
</tbody>
</table>
Summary: Holistic View of Vertical Segments

Top Two: Manufacturing and Healthcare

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

- Challenges and Constraints
- **Specific threats and Protection mechanisms**
- Cisco best practices and solutions
- Q&A
- Conclusion
Connected objects: DNS DYN attack 2016
IOT Systems as Attack Surface

IOT devices and control systems are vulnerable
October 21st, 2016

Netflix, Twitter, Amazon, AirBnb, Spotify, NYT, Box, PayPal, …
Who is Dyn? (pronounced [ˈdaɪn])

• Company originally became known for providing DNS services for users with dynamic Internet Addresses (home users, small businesses)

• More recently, Dyn offers services to large enterprises that need a robust geographically diverse DNS infrastructure

• Dyn is one of the biggest, if not the biggest provider of such services. It maintains data centers around the globe and uses various techniques to provide redundancy
Authoritative & Recursive DNS

You, looking for Twitter.com

Your ISP
OpenDNS
Google DNS
...

Authoritative Server

DynDNS
...
Why Did Dyn Fail

- A large network of compromised devices (493,000 IoT devices (Cameras, DVRs, …) infected by Mirai was used to flood Dyn’s servers with traffic

- In particular servers used as part of Dyn’s enterprise offerings were targeted

- Dyn wasn’t able to handle the additional traffic, and its servers either stopped responding or responses were substantially delayed.
MIRAI Architecture overview

DDoS service sold to users who send attacks via C2 API

Attacker maintained a long lived connection to the report server via TOR

Susceptible victim IPs are sent to loaders

Successful scan results sent to report server

Loaders log in to victim devices and instruct them to download Mirai malware

Victims download and run Mirai malware to become bots

Bots communicate with a C2 server whose IP changes over time

Bots perform DDoS attacks and Telnet default credential scans

Bots

Loaders

D DoS Victims

Malware Distribution

C2 Server

Scanning Victims

Attacker

Service Users

Report Server
The MIRAI Botnet

• Reconnaissance phase
• Reporting of potential victims
• Malicious payload insertion
• Attack capabilities
Infection spreading mechanism

• Scanner.c looks for targets using random IP address generator

• Tries to access remote device using a list of hardcoded credentials

• Once access is successfully granted, sends back report

• Infects new remote device

• New remote device connects to C&C
Available attacks

• Straight up UDP flood
• Valve source engine query flood
• DNS water torture
• SYN flood with options
• ACK flood
• ACK flood to bypass mitigation devices
• GRE IP flood
• GRE Ethernet flood
• Plain UDP flood optimized for speed
• HTTP Layer 7 Flood
Securing the IoT

• On the device: firmware, admin password, physical access, …

• Between device and infrastructure: encryption, RF communication

• Infrastructure: Stealthwatch, Umbrella, Cloudlock, …
Smartcache in use during authoritative DNS DDoS attack against Dyn

1) Users requests access to twitter.com
2) OpenDNS try to reach tweeter’s authoritative DNS servers hosted by Dyn
3) Since Dyn is not available, OpenDNS use his smartcache feature and serves the cached IP 208.67.222.222
BrickerBot: Response to IoT-based DDoS attacks

- Author: “the Janitor”

- Vigilante worm that destroys insecure IoT devices, described as “Internet Chemotherapy.”

- Destroys low-security devices running a Linux package called BusyBox, which have telnet-based interfaces with default passwords.
Enterprise IoT
NOT an IoT attack after all...

Hotel ransomed by hackers as guests locked out of rooms

The Local
news.austria@thelocal.com

28 January 2017
10:42 CET+01:00
crime

Share this article

One of Europe's top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)
IoT: Medical

Hacking Insulin Pumps And Other Medical Devices From Black Hat

One of the briefings at Black Hat this year was a session on how vulnerable medical devices are to cyber attack, given by Jay Radcliff. This was part of our company's coverage of Black Hat and Defcon highlights sent via social media. Although the actual demonstration of an insulin pump being induced to given an insulin overdose as a

Bug can cause deadly failures when anesthesia device is connected to cell phones

No, it's not clear why anyone would ever connect a phone to a medical device.

by Dan Goodin - Apr 22, 2014 8:33 pm UTC

Federal safety officials have issued an urgent warning about software defects in an anesthesia delivery system that can cause life-threatening failures at unexpected times, including when a cellphone or other device is plugged into one of its USB ports.

The ARKON anesthesia delivery system is used in hospitals to deliver oxygen, anesthetic vapor, and nitrous oxide to patients during surgical procedures. It is manufactured by UK-based Spacelabs Healthcare Ltd., which issued a recall in March. A bug in Version 2.0 of the software running on the device is so serious that it could cause severe injury or death, the US Food and Drug Administration
Internet of Things (IoT) in the Enterprise

- does not introduce “new” security problems
- raises the stakes; medical devices, traffic control systems; IoT brings the need for security into daily life
Manufacturing: German Smelter 2014
December 2014 – Attack on German Smelter

Exploited Vulnerabilities by ICS Component
German Steel Mill Incident

- **Targeting**
  - People & Procedures
  - Spear phishing email to gain access to the corporate network

- **1st Stage Delivery**
  - Applications
  - Compromised host on corporate network

- **2nd Stage Delivery**
  - Network
  - Moved into the plant network (unknown technique)

- **Exploitation**
  - Unknown
  - Demonstrated knowledge of ICS and was able to cause multiple components of the system to fail
German Smelter Attack

- What is known:
  - Phishing Attack
  - Malware
  - Access to ICS System
  - Shutdown commands
  - Damaged smelter
Electric Utilities: Ukraine 2015
Ukraine Power Grid Incident

- 3 Ukrainian power distribution companies
- 30 sub-stations were disconnected
- 225K customers lost power for hours
- Attackers remotely controlled SCADA DMS

BlackEnergy & KillDisk

Researchers at security firm Trend Micro have found evidence suggesting that pieces of malware involved in the recent attacks against Ukraine’s energy sector have been used to target other types of organizations as well.

The Russia-linked BlackEnergy malware, known to target SCADA systems in Europe and the United States, and KillDisk, a plugin designed to destroy files and make systems inoperable, were spotted last year in attacks aimed at Ukraine’s energy sector. Ukrainian authorities accused Russia of being behind the attacks that resulted in significant power outages.

An analysis of the campaign revealed that while BlackEnergy and KillDisk had been found on the targeted systems, the malware was likely not directly responsible for the outages.

Trend Micro reported on Thursday that its researchers spotted BlackEnergy and KillDisk samples on the systems of a Ukrainian mining company and a major railway operator. Experts believe these attacks were conducted by the same threat actor that targeted the country’s power companies.

In the case of the infections at the Ukrainian mining company, experts uncovered several samples whose name and functionality was similar to the samples spotted in the power utility attacks. The malware, used in November and December 2015, communicated with some of the same command and control (C&C) servers observed in the energy attacks.

The security firm noticed that the systems of the same mining company were also infected with multiple variants of KillDisk. The samples don’t match the ones used in the energy attacks exactly, but they do exhibit the same functionality.

Trend Micro also spotted KillDisk infections on the systems of a Ukrainian railway company that is part of the country’s national railway system. The KillDisk sample found by researchers matched one used in the electric utility attacks.
Ukraine Grid Attack – Chronology of Events

Spear phishing to gain business network access

Thieves of Credentials

Remote operation of ICS Systems

KillDisk to erase MBR and delete targeted logs

Keylogger, screenshots

BlackEnergy 3 malware installed

Use of VPNs to access ICS network

S2E devices compromised at firmware level

Reconfigured UPS to impact power in building/DC

Remote telephonic DOS

Power Outage
All-time favorite : Stuxnet
How did Stuxnet work?

1. Infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. Search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. Update
If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. Compromise
The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. Control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. Deceive and Destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
The Target ICS Infrastructure – Iran’s Natanz Nuclear Facilities

Supervisory Network

- Step 7 Control
  Software running on Windows

CPS Controller (Siemens S7-417)

Cascade Protection System

- Pressure Controller

- Communication Processor

CDS Controller (Siemens S7-315)

Centrifuge Drive System

- Isolation Valve

- Stage Exhaust Valve

- IR-1 Centrifuges

- Frequency Converter

- PROFIBUS
What was so special about Stuxnet?

- The first rootkit targeting ICS
- Exploited four zero-day vulnerabilities in the dropper
- Compromised two digital certificates
- Ability to inject code into PLC
- Hide from control system operators
- Remotely controlled by CC or act autonomously
Agenda

• Challenges and Constraints
• Specific threats and Protection mechanisms
• **Cisco best practices and solutions**
• Q&A
• Conclusion
IoT “hygiene” – Trustworthy systems
Cisco IoT Threat Defense Components

- **Stealthwatch** - Visibility of connections and relationships
- **ISE** – Device / User identity
- **NGFW** – App Activity
- **AMP** – End Point Activity

- **AnyConnect** - Secure Connection in/out of OT network
- **ISE** – dynamic access control
- **FirePower** – Observe remote activities
- **DNS** – remote site risk protection

- **FP NGFW** - Segment IT and OT environments
- **TrustSec** - Segment OT devices in the IT network
- **ISE** – Align access with users / device
- **Switches** – Dynamic segmentation enforcement

- **Risk assessment** for baseline
- **Deployment and Migration**
- **Incident response Service** for breach situations
Access to the Manufacturing Floor – Cisco ISE

Consistent Secure Access Policy

Who
What
Where
When
How

Network

Partner Context Data

Cisco ISE
Profiling

- What ISE Profiling is:
  - Dynamic classification of every device that connects to network using the infrastructure.
  - Provides the context of “What” is connected independent of user identity for use in access policy decisions

- What Profiling is NOT:
  - An authentication mechanism.
  - An exact science for device classification
How we profile?

Collection

- NMAP
- AD
- NetFlow
- HTTP
- SNMP
- LLDP
- Radius
- DNS
- DHCP

Classification

Classifies based on Device fingerprint

- Process of collecting data to be used for identifying devices
- Uses Probes for collecting device attributes
Cisco IoT System Network Connectivity
IoT Network Network Visibility and Enforcement

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

Industrial Routing
IR 829
IR 809

Simplified Compliance
Risk Mitigation
Consistent Policy Enforcement
Increased System Availability
Visibility & Context in Industrial Networks

Security starts with Visibility

Discover Industrial Assets using CIP, PROFINET, Modbus, BACNet Protocols

Visualize connectivity between automation and networking assets

Context Enhances Security

Who
Bob

What
Rockwell PLC

When
11:00 AM EST on April 10th

Where
Extrusion, Zone-2, Cell-1

How
Wired Access

Compliance
Yes

Threat
None

Vulnerability
CVSS score of 6

IND shares industrial asset identity with ISE over pxGrid

… this Visibility combined with Context, becomes a force-multiplier for Security
Policy and Segmentation with TrustSec

Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers.
Visibility through NetFlow
Network as a Sensor

NetFlow provides
• Trace of every conversation in your network
• An ability to collect record everywhere in your network (switch, router, or firewall)
• Network usage measurement
• An ability to find north-south as well as east-west communication
• Light weight visibility compared to SPAN based traffic analysis
• Indications of Compromise (IOC)
• Security Group Information
Cisco Stealthwatch
System Overview

Non-NetFlow Capable Device

SPAN

Stealthwatch FlowSensor

Generate NetFlow

NetFlow / NBAR / NSEL

Network Devices

• Collect and analyze
• Up to 4,000 sources
• Up to 240,000 FPS sustained

StealthWatch FlowCollector

Stealthwatch Management Console

• Management and reporting
• Up to 25 FlowCollectors
• Up to 6 million FPS globally

NetFlow / NBAR / NSEL

• Collect and analyze
• Up to 4,000 sources
• Up to 240,000 FPS sustained
Cisco AMP – Advanced Malware Protection

AMP Everywhere: See Once, Protect Everywhere
Cisco Umbrella
Visibility on Any Device, Anywhere

CHALLENGES

Multiple Internet Service Providers
Direct-to-Internet Branch Offices
Users Forget to Always Turn VPN On
Different DNS Log Formats
Cisco Umbrella
Visibility on Any Device, Anywhere

BENEFITS

Global Internet Activity Visibility

Network Security w/o Adding Latency

Consistent Policy Enforcement

Internet-Wide Cloud App Visibility
Capabilities vs Solutions

- **Visibility**: ISE, Firepower, Stealthwatch - Network as a Sensor
- **Control**: ISE, AMP, Stealthwatch - Network as an Enforcer
- **Compliance**: Firepower, OpenDNS, CloudLock
- **Segmentation**: ISE, TrustSec, Network as an Enforcer
- **Threat Detection**: Talos, WSA/ESA, AMP, Firepower, Stealthwatch
- **Secure Access**: ISE, AnyConnect VPN, ASA, Firepower
Final thoughts
There is not one Internet of Things, there are many
As always, for security, it starts with designing the right policies & processes
Related sessions

- BRKSEC-2339 - How IoT Threat Defense is protecting the promise of the IoT
  • Mustafa Mustafa, IoT Security Technical Marketing Engineer, Cisco

- PSOSEC-4377 - IoT Threat Defense and Ransomware Defense - Two solutions that address critical business concerns
  • Albert Salazar, Director Enterprise Solutions, Cisco

- BRKIOT-2111 - Power Utilities Energy Automation Design Session
  • Paulo Pereira, Consulting Systems Engineer, Cisco
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKIOT-2112
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you