TOMORROW starts here.
SECURITY EVERYWHERE
Internet Of Things (IoT) Security:
Understanding The Challenges While Mitigating the Risks

Demetris Booth, APJC Lead – Product Management & Product Marketing
Agenda

• Overview & Benefits
• Security Challenges
• Mitigating Challenges
  • High Level View
  • Technical View
• Bringing It All Together
IoT Is Here Now – and Growing!

50 Billion “Smart Objects”

Adoption rate of digital infrastructure: 5X faster than electricity and telephony

Billions of Devices

Timeline

2010 2015 2020

6.8 7.2 7.6

World Population

Inflection point

12.5

25
Relation to Internet of Everything (IoE)

People
Connecting people in more relevant, valuable ways

Process
Delivering the right information to the right person (or machine) at the right time

Data
Leveraging data into more useful information for decision making

Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

IoE: Connecting the Unconnected to Generate Business Value
IoT Delivers Extraordinary Benefits
What Comprises IoT Networks?

Information Technology (IT)  +  Operational Technology (OT)  +  Smart Objects
Smart City

CONNECTED TRAFFIC SIGNALS
- Reduced congestion
- Improved emergency services response times
- Lower fuel usage

PARKING AND LIGHTING
- Increased efficiency
- Power and cost savings
- New revenue opportunities

CITY SERVICES
- Efficient service delivery
- Increased revenues
- Enhanced environmental monitoring capabilities

Safety, financial, and environmental benefits
The Connected Car

**WIRELESS ROUTER**
- Online entertainment
- Mapping, dynamic re-routing, safety and security

**CONNECTED SENSORS**
- Transform “data” to “actionable intelligence”
- Enable proactive maintenance
- Collision avoidance
- Fuel efficiency

**URBAN CONNECTIVITY**
- Reduced congestion
- Increased efficiency
- Safety (hazard avoidance)

Actionable intelligence, enhanced comfort, unprecedented convenience
IoT Transforms Data into Wisdom

Big Data Becomes Open Data for Customers, Consumers to Use
... but it also adds complexity.

New Business Models  Partner Ecosystem

Applications

Application Interfaces

Unified Platform

Infrastructure Interfaces

Infrastructure
… but it also adds complexity.
The Flip Side: Major Security Challenges
We’ve Created the Perfect Storm…

> Device Explosion 
+ > Connectivity Explosion 
+ > Industrialization of Hacking 
+ > State Cyber Programs 
+ > “Hactivism”
Security Challenges

Traditional Security Challenges

- Increased Attack Surface
- Information Breach
- Data Privacy

Smart Objects

- 6 Devices Per Person
- 130 Sensors Per Person
IoT Security Challenges

Superior Visibility
Advanced video analytics, remote management, and multi-site event correlation

Granular Control
Differentiated policy enforcement across the extended network

Advanced Threat Protection
Comprehensive cyber security threat detection and mitigation

Actionable Intelligence
Internetworked security solutions for superior intelligence and rapid response

Automated Decisions
Machine-to-machine enabled security control with no human intervention required
IoT Expands Security Needs

- New Applications
- Threat Diversity
- Impact and Risk
- Remediation
- Protocols
- Compliance and Regulation

IoT CONNECTIVITY

- Converged, Managed Network
- Resilience at Scale
- Security
- Distributed Intelligence
- Application Enablement
Mitigating The Security Risk Across the Extended Network – The 20,000 FT View
IT and OT are Inherently Different

- **IT**
  - Connectivity: “Any-to-Any”
  - Network Posture: Confidentiality, Integrity, Availability (CIA)
  - Security Solutions: Cybersecurity; Data Protection
  - Response to Attacks: Quarantine/Shutdown to Mitigate

- **OT**
  - Connectivity: Hierarchical
  - Network Posture: Availability, Integrity, Confidentiality (AIC)
  - Security Solutions: Physical Access Control; Safety
  - Response to Attacks: Non-stop Operations/Mission Critical – Never Stop, Even if Breached
IT/OT Converged Security Model

IT

DMZ

OT

Enterprise Network

Cloud

Network Security

Application Control

Identity Services

Secure Access

Config Mgmt

Supervisory

Automation & Control
The Secure IoT Architecture – IT Plus OT!

APPLICATION AND BUSINESS INNOVATION

Data Integration  Big Data  Analytics  Control Systems  Application Integration

Application Interfaces

Application Enablement Platform

Infrastructure Interfaces

Application Centric Infrastructure

Device and Sensor Innovation

Services

Cloud-based Threat Analysis / Protection

Network and Perimeter Security

Security

Physical Security

Device-level Security / Anti-tampering

End-to-End Data Encryption

Application and/or its affiliates. All rights reserved.

Presentation ID
Cisco Security Model

**Attack Continuum**

**BEFORE**
- Control
- Enforce
- Harden

**DURING**
- Detect
- Block
- Defend

**AFTER**
- Scope
- Contain
- Remediate

Network

Endpoint

Mobile

Virtual

Cloud

Point in time

Continuous
Security/Attack Continuum - IT

**BEFORE**
- Control
- Enforce
- Harden

**DURING**
- Detect
- Block
- Defend

**AFTER**
- Scope
- Contain
- Remediate

Cloud-based threat detection and prevention; policy enforcement via firewall, VPN and identity services

Quarantine based on real-time analysis and actionable security intelligence from IPS and WSA

Remediate using advanced protection and network behavioral analysis
Security/Attack Continuum - OT

**BEFORE**
- Control
- Enforce
- Harden

**DURING**
- Detect
- Analyze
- Respond

**AFTER**
- Disable
- Contain
- Remove

Networked cyber and physical security solutions with OT-specific policies

Response based on real-time analysis and actionable security intelligence

Lockdown physical spaces or disable access to critical infrastructure
Mitigating The Security Risk Across The Extended Network – Technical View
Exposure In IoT Networks

- **MITM**
  - Sniff traffic
  - Modify data
  - Impersonation

- **Compromise**
  - Unauthorized access
  - Device tampering
  - Service disruption
  - Sniff traffic

- **Compromise**
  - Unauthorized use
  - Malware infection

- **Compromise**
  - Unauthorized access
  - Device tampering
  - Service disruption
  - Sniff traffic

- **Compromise**
  - Unauthorized access
  - Device tampering
  - Service disruption
  - Sniff traffic

- **Compromise**
  - Unauthorized access
  - Device tampering
  - Service disruption
  - Sniff traffic

- **Compromise**
  - Unauthorized access
  - Device tampering
  - Service disruption
  - Sniff traffic

- **Hack Device**
  - Unauthorized device
  - Device tampering
  - Malware infection
Required Security Model for IoT

BEFORE
Control
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network as an Enforcer

Network as a Sensor

Network as a Mitigation Accelerator
BEFORE an attack

DURING

AFTER
BEFORE an attack
BEFORE an attack

Profiling
- ISE builds device database by MAC address
- Profile with SNMP (LLDP), DHCP, NMAP, NetFlow drives MAC-based access policy
- ISE manages policy

Benefit
- Visibility and access control
- MAC linked with device ID and location
- Custom access by device profile
BEFORE an attack

802.1x
- Authenticates device before activating access
- ISE manages policy

Benefit
- Operational simplicity and control
- Dynamic device authentication
- Single policy management
BEFORE an attack

SGT / SGACL
- Tags traffic based on device policy
- Enforces access control based on tag
- ISE manages policy

Benefit
- **Operational simplicity and speed**
- Dynamic, topology-independent enforcement
- Single access control policy
DURING an attack
DURING an attack

NetFlow Analyzer
- Collect full NetFlow across network
- Detect behavioral anomalies
- ISE provides context

Benefit
- Full threat visibility
- Detect threats in any part of network
- Detect access abuse
- Detect attacks missed by security systems
**DURING an attack**

**IPS / AMP**
- Monitor traffic and file threats

**Benefit**
- **Integrated advanced threat detection**
- Detects advanced attacks and malware

Cisco and/or its affiliates. All rights reserved.
**WSA / ESA**
- Reputation-based web threat blocking
- Reputation-based email threat blocking

**Benefit**
- Block advanced web / email threats
- Intelligence-driven threat detection

**DURING an attack**

- **NF analyzer**
- **Policy server (ISE)**
- **Web security**
- **Email security**

- **Firewall**
- **IPS**
- **Advanced malware protection**

- **IoT device**
- **Aggregation**
- **Core**
- **Data center**
- **WAN / Internet [VPN]**
AFTER an attack
AFTER an attack

NF Analyzer
• Record 90 days of communications activity
• Scope extent of breach
• Report policy and compliance

Benefit
• Full Accountability
• Map threat trajectory
• Evidence-based auditing
AFTER an attack

IPS / AMP
- Retrospective analysis of threats
- Contain infected devices and files
- ISE provides quarantine

Benefit
- Fast threat scoping and remediation
- Trace and eliminate infections with the click of a button
- Map threat trajectory
Continuous IoT Threat Protection
Advanced Malware Protection For IoT

The catch? Detection is “in the cloud”.

“On-prem” addresses cloud objections.
Sophisticated and Continuous Protection

Point-in-Time Protection

File Reputation & Sandboxing

Retrospective Security

Breadth and Control points:
- Email
- Network
- Endpoints
- IPS
- Web
- Devices

Telemetry Stream

Continuous feed

File Fingerprint and Metadata
File and Network I/O
Process Information

Continuous Analysis
Analyse The IoT Threat!

1. Submission
Analyst (portal) or system (API) submits suspicious sample to Threat Grid.

2. Proprietary Analysis
An automated engine observes, deconstructs, and analyzes using multiple techniques.

3. Correlation at Unprecedented Scale
System correlates sample result with millions of other samples / billions of artifacts.

4. Enriched Content Integration
Actionable intel generated that can be packaged and integrated into a variety of existing systems.
Global Security Intelligence For IoT

100 TB Intelligence
1.6M sensors
150 million+ endpoints
35% email world wide
FireAMP™, 3+ million
13B web req

180,000+ Files per Day
1B SBRS Queries per Day
3.6PB Monthly though CWS
Bringing It All Together
<table>
<thead>
<tr>
<th></th>
<th>Security Activity</th>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Before</strong></td>
<td>Secure Access</td>
<td>• Role-based access for individuals and groups</td>
<td>• Role-based access to few individuals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VPN/remote access for most systems throughout the network</td>
<td>• VPN to few systems and users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Complex passwords with lockout policies</td>
<td>• Badge readers/integrated sensors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Simplified passwords (except for the most critical systems)</td>
</tr>
<tr>
<td></td>
<td>Security Group Tagging</td>
<td>• Tags traffic based on device policy</td>
<td>• Enhanced segmentation for required groups only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enforces access control based on tag</td>
<td>• Dynamic, topology-independent enforcement</td>
</tr>
<tr>
<td><strong>During</strong></td>
<td>Intrusion Prevention/Detection</td>
<td>IPS – enforces policies</td>
<td>IDS – sends security alert only</td>
</tr>
<tr>
<td></td>
<td>Threat Mitigation</td>
<td>Quarantine affected system</td>
<td>Analysis of the threat to determine appropriate action</td>
</tr>
<tr>
<td></td>
<td>Data Integrity and Confidentiality</td>
<td>Data Loss Prevention (DLP)</td>
<td>Combined physical and cybersecurity access controls</td>
</tr>
<tr>
<td></td>
<td>Network-wide Policy Enforcement</td>
<td>Differentiated actions based on value, function, and location of the device</td>
<td>Centralised remediation and adaptation</td>
</tr>
<tr>
<td><strong>After</strong></td>
<td>Retrospective Security Policies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IoT Can Actually Increase Security Posture

- Network of Security Devices
  - Cyber Security
    - Firewall, IDS
  - Physical Security
    - IP cameras, badge readers, analytics

- Actionable Security Intelligence
  - Automated / M2M
  - Human Response

- Remote Capabilities
  - Configuration and Management
  - Collaboration Between Groups
Conclusion: Securely Embrace IoT!

- New challenges require new thinking!
  - avoid operational siloes
  - networking and convergence are key
  - a sound security solution is integrated throughout
  - build for the future

- Security must be pervasive
  - inside and outside the network
  - device- and data-agnostic
  - proactive and intelligent

- Intelligence, not data
  - convergence, plus analytics
  - speed is essential for real-time decisions