IoT Security and Risk Management

Tyson Macaulay
Chief Security Strategist, Fortinet
IoT Security is a BIG STORY!
Security as a % of IT Budget

Source: Gartner: 2005 to 2015

20 Billion+ devices?
85% of global organizations are considering, exploring, or implementing an IoT strategy.

IoT deployments are on the rise. How many connected devices do you have in your organization?

- 85% of organizations are fully confident that their connected devices are secure.

Source: AT&T, March 2016
Customers looking for IoT security services

- Significant demand already exists: 23.5%
- Within the next year: 19.4%
- In 1-2 years: 28.6%
- In 2-3 years: 21.4%
- Not for at least 3 years: 7.1%

Source: Fortinet, May 2016
Threat Agents in the IoT

- Criminals
- Hacktivists
- Industrial Spies
- Nation States

- Terrorists
- Insiders
- Chaotic Actors & Vigilantes
- Regulators
Top Threats to the IoT (the short list)

Regulatory and Legal
- Privacy
- Data assurance
- Resource allocation
- Audit failures

Competitive
- Skills shortages
- Failure to use “big data” effectively
- Market disruptors
- Unstable suppliers and partners

Financial
- Subscriber fraud and theft of service
- Social engineering (accounts info)
- Fines (regulatory vs SLA)
- Liability and insurance

Internal Policy
- Standards vacuum
Zoom in! - IoT Transaction Use-case

- Energy Spot-market settlement
- Stored value and loyalty
- Fuel currencies
- Pay as you go feed stock by inventory managers
- Micro-payments for utilities
- Automated prescription fulfillment
- Food ordering
- P2P lending
- Enterprise Services IoT
- Consumer/Home IoT
- Internet

- Local cellular switching and breakout
- Local gateway switching
A wants to send currency, updated service information or device ownership to B

The transaction grouped with many other transactions occurring in the same period as a "block"

The block is broadcast to every verifying party in the network for agreement that "double spending" or false transactions are not present

The block is encoded with a hash of the previous block and then can be added to the end of the former block to form a chain, which provides an indelible and transparent record of transactions

Those in the network approve the transaction is unique and valid

The money/service information or device ownership moves from A to B

Zoom in! – Blockchain IoT Transaction Use-case

RSA Conference 2016 Singapore
Big Threat #1 – Device to Device Attacks

- Infected/compromised devices attack internally and externally
- Infected device enters the home and attacks adjacent devices – which in turn launch attacks
Big Threat #2 – IoT as the Weakest Link

- Social engineering in the IoT
- Compromise of one device leads to all adjacent systems

Messages pushed to device manager “Upgrade now for your own safety”

Malware Drop

Fetch “patches” = malware

Man-in-the-Middle or compromise Cloud

IoT Cloud services

Internet

Sabotage or privacy invasions

Attack on information-rich devices

Personally Identifiable Info
Big Threat #3 – Interdependency and Complexity

- IoT ecosystem has many stakeholders and service providers at each point in the architecture
- Cascading impacts almost impossible to project or monitor
- Assumptions will fail

**Gateway**
- Service function owner
- Gateway owner
- Gateway manager
- Gateway maker
- Supply chain

**End point**
- Device user(s)
- Device owner
- Device manager
- Device maker
- Supply chain

**Network**
- Network provider
- Network owner
- Network manager

**Cloud / DC**
- Service tenant
- Software owner
- Software manager
- Software vendor
- Platform owner
- Platform manager
- Supply chain
- Infrastructure owner
- Infrastructure manage
- Infrastructure vendors
Case Study - 4G to 5G Security Evolution to Support IoT
4G/IoT Security Today
IoT/5G – Heavy Growth Across Infrastructure
4G versus 5G requirements

Source: Mobile Experts LLC, Feb 2015
IoT/4G Evolving to IoT/5G – More Challenges
WHERE DO THE IOT SECURITY ANSWERS LIE?

PARTIALLY WITH THE IOT DEVICES THEMSELVES.

BUT MOSTLY WITH THE NETWORK.
A Cooperative Security Fabric in the Enterprise

- Global Intelligence
- Client Security
- IoT
- Secure WLAN Access
- Secure LAN Access
- Network Security
- Cloud Security
- Application Security
- Alliance Partners
- Local Intelligence
End-to-End: IoT Security Reference Model

Virtualization

Distributed Network Function Virtualization (D-NFV)

Network Function Virtualization (NFV)
Evolving IoT Infrastructure
Evolving IoT Infrastructure with Security

Micro-segmentation (by subscriber)
Form factor: Virtual

Internet Breakout

Internet

Core Network

Consumer Access

Micro-segmentation (by in-home service)
Form factor: Virtual

RSA Conference 2016 Singapore
Apply: Call to Action for IoT Risk Management

- IoT devices require new approaches to security
- Look to the network for better security
  - Gateways, Transport networks, DC / Clouds
- Network virtualization brings opportunities for better security, not just operational savings
  - Increased automation, Scalability and license management