The Internet of Things and Security

Chuck DePalma
CISSP CISM | Network and Cloud Security Architect

The Internet of Things

1998 Adoption of “Mosaic” Browsers 0ver 250 Millions of Internet Connected Devices

2007 Introduction of the iPhone: 2009 Wide Adoption of Smart Phones, Over a Billion Devices connected to the Internet

“We believe the number of internet connected devices has reached 8.7 Billion” Cisco November, 2012

June, 2015: there are 25 Billion total devices connected to the Internet:

4.9 Billion Internet of Things devices connected **

By 2020, it is estimated that there will be 75 Billion total devices, 25 Billion of which will compromise the Internet of Things (IoT)**

CenturyLink™ Business

Why Does It Matter?

- The Potential Market of the IoT and generated Big Data will exceed $11 Trillion Dollars by 2020
- January 2013: FTC Releases “Internet of Things: Privacy and Security in a Connected World”
- March 2015: EU initiated the creation of “Alliance for Internet of Things Innovation (AIOTI)”
- DEF CON 23 (August 6th – 9th , 2015) in Las Vegas, attendees compete to hack IoT devices.

CenturyLink™ Business

The Internet of Today, 2020 and Beyond

- Here in Michigan, a “Smart Freeway, 20 miles of I-96 and I-696, Cameras and Sensors have been deployed to provide Intelligent Communications with Connected Vehicles.”

- Various Pharmaceutical Manufactures have developed “Smart Medicine” to be deploy as needed. Items such as Insulin Pumps that adapt to real time Blood Sugars and provide Insulin as needed.

- Both Homes and Cars can be remotely controlled via smart phones or other portable devices

- We can either become the Connected World of the Future….Or a Horror Writers vision of Chaos”

CenturyLink™ Business

What's Important

- Threat Modeling
- Threat Intelligence
- The Security of IoT

CenturyLink™ Business

Threat Modeling

- Everyone does Threat Modeling everyday
  - Risks to your home
  - Risks to your person
  - Risk to your Business

- You know your environment, be it personal or Company better than anyone else

- In both Corporate and Personal instances basic Security Rules apply:
  - Protect what is important
  - Identify threats
  - Mitigate threats

CenturyLink™ Business

Threat Intelligence

- Basic Business Model
  - Tools: Firewalls, IDS, Log Management, SIEM
  - People: Incident Response; Mitigation
  - Governance: Executive Direction (CISO) and Policy

- IoT
  - New Tools: Complex, Intelligent Security appliances and devices
  - New Dynamics: Merger of Personal and Corporate Interaction
  - Cooperative Governance of devices deployed by businesses for Consumers use

CenturyLink™ Business

The Security of IoT

- Zero Trust Networks*
- Next Generation Firewalls
  - PKI
  - Certificate Authority
- SSL / TLS
  - Matrix SSL
  - Matrix SSL Tiny
- Certificates and Beyond

* Forrester Concept November of 2014

CenturyLink™ Business

Zero Trust Networks

- Basic Premise: Eliminate “Trust side of Firewall”
- Utilizes Micro-VLANs: Every Device has it own VLAN
- Requires Authentication at all points
- Requires Fast Authentication mechanism
- Requires High Backplane Speed Firewalls to support fast Authentication
- Requires native Security Elements: Not Bolt-on Security Solutions

CenturyLink™ Business

Next Generation Firewalls

- Much like initial Securely deployed WiFi networks were deployed in Corporate environments and moved to other environments NGF's being deployed in todays Corporate environments will move to other environments as well.
- NGF's can natively support Certificate Authorities, supporting PKI
- NGF's have High Speed Backplanes
- Via CA's NGF's can natively support fast Authentication, such as PKI
- NGF's support Commercial and Privately signed PKI Certificates
- PKI can facilitate more secure Authentication
- PKI can provide secure communications for both Outside and Inside "Untrust" networks for Internet connected devices

CenturyLink™ Business

SSL: Secure Socket Layer / TLS: Transport Layer Security

- SSL / TLS allows for implementation of IoT devices to encrypt their transmissions across the internet
- Helps Secures against Man in the Middle (MTM), such as eavesdropping and DDoS Misuse Attacks
- Matrix SSL – Open Source embedded SSL/TLS designed for small footprint, for Web Servers to implement encryption layer for Secure Management of remote devices (>50KB)
- Inside Secure' s Matrix SSL / DTLS Tiny – Supports IP Stack, TLS; if no IP and UDP only, DTLS. Designed for a tiny memory footprint of Security to be integrated into Applications. (>10KB)

CenturyLink™ Business

Certificates and Beyond

Digital Certificates:
•Prevalent for Authentication and Encryption
•Becoming smaller, but yet maintaining an appropriate level of Security
•1st Step in Securing IoT

Threat Modeling and Intelligence
•Needs to be part of the overall Security Landscape
•Needs to be integral to Security planning

Bottom Line
•Security is pivoting every 6 months. We have a continuous stream of new tools evolving and at our disposal. There is an unprecedented opportunity to get ahead of the curve and start to secure the IoT as it evolves, as opposed to an after thought.

CenturyLink™ Business