Cyber Security and the Internet of Things

UNSW AUSTRALIA Canberra

Never Stand Still

ACCS

Professor Jill Slay

Director Australian Centre for Cyber Security

UNSW Canberra

- **Draws on the work of Professor Greg Austin of ACCS and Ian Farquar of Gigamon**

ADFA AUSTRALIAN DEFENCE FORCE ACADEMY

Agenda

- The difficulties with cyber security
- Complexity caused by the Internet of Things

What is cyber security?

The term “cyber security” covers a multitude of quite diverse considerations. Each country, and even actors within one country, will focus on a different combination of these considerations because they will have different organisational priorities and quite distinct economic and security potentials.

- In broad terms, “cyber security” has at least eight “ingredients” or foundation elements, some of which are narrowly technical (but which all involve human input and institutions) and others of which are simultaneously technical but deeply dependent on non-technical inputs. One view of these ingredients is captured here which describes them as vectors of attack and response.
- This begins to answer the question “what shapes security in cyber space”

Eight Vectors of Attack and Response*

Cyber security must address a range of political, social, legal, technical, management and personnel issues.

*Source: adapted from a Bell Labs graphic

What is difficult about security, why is there a problem?

There is a problem because of:

- Targeted attack
- Weaponisation of the Internet
- Offensive Cyber Warfare
- Lack of understanding / lack of security culture
- Large numbers of SMEs who have little or no protection
- Poor management
- Poor communications between engineering / IT, IT Sec/ Physical Security, IT Sec / Management

Problem and Approach

- We are basically dealing with people, processes and tools.
- We can draw on models to help us broaden our thinking

Access Control

Telecommunications and Network Security

Information Security Governance and Risk Management

Software Development Security

Cryptography

Security Architecture and Design

Physical (Environmental) Security

Problem and Approach

Operations Security

Business Continuity and Disaster Recovery Planning

Legal, Regulations, Investigations and Compliance

Does the Internet of Things add Complexity?

- There is no agreed-upon formal definition yet – many informal definitions
- Scott McNealy: putting Java into light bulbs (2000)
- A subset of the “Internet of Everything” – all Internet connected devices
- ABI Research says:
  - 10 billion wirelessly connected devices (2013)
  - Over 30 billion devices expected by 2020

Devices per head of population:

  - 2013: 7 billion (1.43 devices per person)
  - 2020: 7.7 billion (3.90 devices per person)

The Challenge We Face

- As yet there is no consensus on how to secure IoT devices, and no comprehensive solutions have appeared to date.
- Looking futuristically we large scale acceleration of use of IoT sensors, an excitement about their use, some development of security standards but no obvious engagement with potential disruption

Characteristics

Without a formal definition, let's look at the characteristics of an IoT device

- A "thing": possessing a physical existence
- Connected to "the Internet", although this might only mean the local broadcast domain
  - IPv4 and IPv6 – maybe also control via proprietary networks through an IP gateway
  - Doesn't have to be wireless: wired connections possible (Ethernet, CAN, powerline networking, even IP over legacy industrial, process and building control networks)
  - Doesn't have to be RF wireless: LiFi and other technologies possible too
- Power management is very important unless the unit is mains-powered

Security Approaches

Observation: IoT devices are just endpoints on a network

How are we going securing existing (non-IoT) endpoints?

- Arguably, not very well (endpoint security vendors would disagree, but the stats say otherwise)

Counter-argument: the limited functionality of the majority of IoT devices should make the attack surface smaller

- The evidence to support this assertion is thin (at best)
- Consider how easily IoT devices are penetrated by even basic pen testing

Challenge in our complex cyber environment

- The embedded OS(s) will have security vulnerabilities
- The embedded hardware may have security vulnerabilities
- These devices may run for decades
- They will be built to price, with time-to-market a major consideration (security?)
- They may be covered by stringent regulation and testing (eg. Medical devices), or very little at all
- The people who “own” them may not even be aware they’re present, and if they are, how to upgrade them
- Yet they will possess network connectivity and the required operating system and hardware environment to support that
- This is a major challenge – yet are inevitable with major benefits

Example: Using IoT for DDOS

- 665 gigabit per second (Gbps) distributed denial of service (DDoS) attack that targeted Brian Krebs' website
- Recently source code being released demonstrating how this kind of targeting carried out on IoT devices
- Routers, cameras, light bulbs, fridges
- Milking machines, street lights, agricultural machinery. (http://www.theregister.co.uk/2016/06/21/plane_hacker_cows_milk_and_honey/)

- Solutions are given as strong passwords, remove default user names and passwords.

Suggested Approaches

Deny/ignore the problem: “make the money and run”

Address it on a per-device basis (the predominant approach) : Extremely expensive.

Standards: Assumes that security is a fixed state. Security isn’t.

“Encryption”: This is not really an approach, just a “make the problem go away” buzzword. It’s actually “deny/ignore” in disguise.

Platformization: How did that work out for Android? I can still buy devices running Android 2.x! It has worked for Apple, but how do we scale that beyond a single company?

Containment: Attack Detection; Local Network Gateway Controls, SP routing