the Internet is for everyone

Some Perspectives on Cyber-Security & the Internet of Things (IoT)

Shernon Osepa

Manager Regional Affairs Latin America & the Caribbean

32nd CANTO Annual General Meeting

Port au Prince, Haiti

2 February 2016

Internet Society

InternetSociety.org

Agenda

- Cyber Security Themes
- Internet of Things
- Questions?

Definition of cyber security

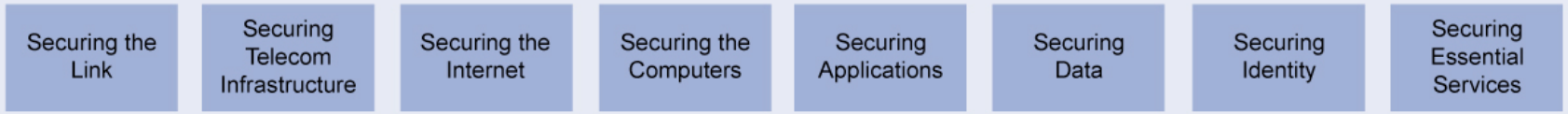
- *"Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way";*

- For the purposes of this presentation, cyber security is defined as "*anything that includes* ***security problems*** *specific to the Internet and their technical and non-technical solutions";*

- Not every crime that occurs on the Internet is covered by the term cyber security. A **crime is a crime**, and simply moving it to the Internet doesn't make it special!

Cyber Security Themes

- Because the scope of cybersecurity is so broad, it is helpful to break it down into these categories



Cybersecurity Themes

Securing the link

- Internet packets inherently have no security
- To prevent unauthorized “sniffing” or eavesdropping sensitive data must be encrypted
- In 2010 Eric Butler demonstrated with “Firesheep” that unencrypted FB traffic could be eavesdropped in public wifi areas
- A few approaches to encrypting this:
  - At the data link layer(MACSec and Wifi Protected Access);
  - At the IP layer(IPSec);
  - At the application layer(SSL/TLS and SSH etc).

Securing the telecoms & Internet infrastructures

- Traditionally a distinction is made between Internet and Telecoms Infrastructure Security because.. they use different technologies and standardization bodies(ITU-T / IETF)
- Telecoms (*highly regulated, few significant players in every market, natural monopolies, etc.*) focusing on securing network:
  - Offices (where switches are located)
  - Cell phones
  - Satellite
  - Broadcast & microwave facilities
- Internet (*no-central control body, unregulated open systems, built on top of multiple national/intl. telecoms infrastructures*) focusing on securing
  - DNS (DNSSEC)
  - Routes (RPKI)

Internet Society
InternetSociety.org

Securing the Internet

The Internet consists of thousands of ***Networks*** all interconnected. The two critical elements are the ***DNS*** and ***Routes***

- The DNS
  - DNSSEC (secure the names)
- The Routes
  - RPKI (secure the routes)

Securing computers

- Whenever a device is connected to the Internet it is susceptible to intrusion
- The most successful attacks from hackers, criminals and other bad actors were against servers and end-user computers
- Many organizations install firewalls and end-point security systems called “anti-malware” or “anti-virus” tools
- Controversy! Computer owners who want to maintain control over their systems and hackers who want these computers and data on them for their own purposes
- No one knows exactly how successful hackers are in their mission. Many attacks are NEVER reported!

Securing computers (2)

- The reasons hackers want to control computer systems have varied over time
- 15-20 years ago it was more for pure vandalisms. Nowadays it has become big business!
- Nowadays: to extort money, steal passwords and financial information (credit card numbers), to build botnets that could be used to sending spam, committing fraud, stealing identity information, executing denial of service on specific websites
- Some of these techniques are also being used but on a much more sophisticated form by some national Governments for espionage, disruption of communications or services or other purposes

Securing computers (3)

- Tools used to attack computers include (trojan horses, malware, botnets, phishing, DDoS and man in the middle attacks
- Several organizations are trying to addressing the challenges
  - Software companies (Eset, FSecure, Kaspersky, McAfee, Sophos, Symantec, and Trend Micro)
  - Firewall companies (Check Point Software, Cisco Systems, Juniper Networks, and SonicWALL)
  - Hardware companies (AMD, Intel)
  - IETF

Securing applications

- Any application on a device, such as a personal computer or a smart phone, connected and communicating over the Internet is an "Internet Application”
- Electronic mail
  - 90 % of email traffic is Spam (it puts a burden on scarce resources)
  - Securing against Spam done by commercial software and appliance vendors (Barracuda networks, Cisco/IronPort, McAfee, Proofpoint, Symantec, Trend Micro)
  - Companies such as Spamhaus provide blacklists and reputations services
- Web browsing

Securing web applications (2)

- The main goal of web application firewalls is to protect both web users and web servers against security faults that may be hidden in the application. For example, a particular type of attack known as “SQL injection” can be used against susceptible web applications to bypass the application and speak directly to the database behind the application.
- SQL injection attacks, when successful, can give the attacker the ability to download private information from web application databases (such as usernames, addresses, passwords, and even credit card numbers) or to upload content to a trusted web site that could place malware on an unsuspecting user’s
- W3C is working on all web application standardization

Securing data

- Internet users expect the data they send and receive will be secured, for example, when communicating with their bank, government or healthcare provider. In other situations, the data they send or receive, for example, the content of entries in Wikipedia may not be secured in transit
- The Data security aspect of cyber security deals with securing this data in transit and while stored

Securing identity

- In the early days of the Internet, it was quickly recognized that for many commercial applications to succeed mechanisms built on principles of trust and secure identity management were needed to authorize and authenticate Internet users.
- A secure link is only good as long as the end points are considered to be legitimate entities that are authorized to carry out a given transaction
- There are a few organizations out there working on this OASIS, W3C, IETF etc.

Securing essential services

- One size does not fit all (“essential services” should be defined per case)
- We agree I guess that power services are essential

It's All About Cooperation & Collaboration "Collaborative Security"

- Both cybersecurity problems specifically and other criminal activity carried out using the Internet are not going to be solved with technology alone!!

- Close cooperation and coordination by all stakeholders is key!!
  - Governments;
  - Businesses;
  - Academia;
  - Organizational and individual users;
  - Law enforcement agencies;
  - Policy makers worldwide.

Internet Society
InternetSociety.org

The Internet of Things (IoT) *"Definition"*

"The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.

There is, however, no single, universal definition!"

Why is it (IoT) important?

- *It's happening now and promises to transform many aspects of the way we work, live, and entertain!*
- *The Internet of Things is an emerging topic of technical, social, and economic significance.*
- *Some analysts predict that by 2025 there will be as many as 100 billion connected devices in the marketplace ($ 11 trillion global economy impact)*
- *The potential for explosive growth in IoT innovation is a testament to the open nature of the Internet's architecture and design (no limits on the kinds of devices connected)*

Why is it (IoT) important? -2nd-

- *ISOC cares about IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives.*

- *An explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges.*

Realizing IoT's Fully Potential Benefits

- Five areas:
  - *Security*
  - *Privacy*
  - *Interoperability/Standards*
  - *Regulatory, Legal and Rights Issues*
  - *Emerging Economy and Development Issues*

Security

- Poorly secured IoT devices and services can be used as entry points for cyber attacks, and can expose user data to theft if data communications and storage are inadequately protected.
- *While security is not a new subject in information technology, the nature of many IoT devices present new and unique security challenges. For example, expected the mass-scale deployment of IoT devices, the ability of some devices to automatically connect to others, unique technical and cost constraints of many IoT products, and the likelihood devices being deployed "in the background" and in unsecure environments.*
- What's more – once a device is *on* the Internet, it becomes *part* of the Internet. Every poorly secured device that is connected potentially affects the security and resilience of the Internet *globally*, not just locally.

Security
-2nd-

- As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm.

- A collaborative approach to IoT security will be needed to develop effective and appropriate solutions to security challenges that are well suited to the scale and complexity of the issues.

Privacy

- Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected.

- In particular, IoT amplifies concerns about the potential for increased surveillance and tracking, the amount of sensitive data that can be collected by devices operating in our home, business, and public environments, and the potential to aggregate IoT data across products to paint detailed and invasive profiles of users, among others.

- Furthermore, they can pose a unique privacy problem for those who are unaware of their presence and have no influence over how information is collected and used.

Privacy -2nd-

- IOT privacy concerns are critical to address because they have implications on our basic rights and our collective ability to trust the Internet and devices that are connected to it.

- In order to realize the opportunities of IoT, strategies need to be developed to respect individual privacy choices across a broad spectrum of expectations and use cases, while still fostering innovation in new technology and services.

Interoperability/Standards

- Interoperability can encourage innovation and provide efficiencies for device manufactures and users, increasing overall benefits and economic value. In fact, McKinsey Global Institute estimates that device interoperability is required to drive up to 40% of the potential value generated by IoT.

- While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, “walled gardens,” and concern over vendor lock-in.

- In short, a fragmented environment of proprietary IoT technical implementations will inhibit value for users as well as industry.

Interoperability/Standards
*-2nd_*

- In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet.

- The development and adoption of appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet.

- The use of generic, open, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol) will support greater user benefits, innovation, and economic opportunity.

Regulatory, Legal and Rights Issues

- IoT raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The rapid rate of change in IoT technology may outpace the ability of the associated policy, legal, and regulatory structures to adapt.

- One set of issues surrounds crossborder data flows, which occur when IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing.

- Further, data collected by IoT devices is sometimes susceptible to misuse, potentially causing discriminatory outcomes for some users.

-

Regulatory, Legal and Rights Issues -2nd-

- Other legal issues with IoT devices include the conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses.

- While the legal and regulatory challenges are broad and complex in scope, adopting the guiding Internet Society principles of promoting a user's ability to *connect, speak, innovate, share, choose*, and *trust* are core considerations for evolving IoT laws and regulations that enable user rights.

- A collaborative governance approach to these challenges, drawing on expertise, engagement and input from across a range of stakeholders, will be needed to develop effective and appropriate solutions.

Emerging Economy and Development Issues

- The Internet of Things holds significant promise for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others.
- *As such, IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals.*
- At the same time, there are often unique challenges in developing regions related to the deployment, growth, implementation, and use of technology. In order for the benefits of IoT to be truly global, the unique needs and challenges of implementation in less-developed regions will need to be addressed.

Emerging Economy and Development Issues -2nd-

- *Some issues for consideration in developing and emerging economies include:*
  - Ensuring the growth and availability of basic infrastructure for IoT, including both wireless and wireline networks, spectrum availability, and the development of data centers, among others.
  - Attracting investment in IoT systems and services, especially in industries and settings that have the prospect for clear, near-term returns (such as natural resource industries.)
  - Developing the skills and capacities to build, deploy, and manage IoT systems locally and encouraging local innovation in developing IoT systems to meet locally-identified needs and challenges.
  - Building capacity for policymakers to develop strategies in addressing IoT policy questions and in building national strategies.


the Internet is for
everyone
Thank You
Shernon Osepa
osepa@isoc.org
Internet Society
InternetSociety.org