the Internet is for everyone

Some Perspectives on Cyber-security

Shernon Osepa

Manager Regional Affairs Latin America & the Caribbean

2nd National Conference on Cyber Security & Data Protection

Kingston, Jamaica 20-21 November 2014

Internet Society

InternetSociety.org

Agenda

- What is the Internet Society (ISOC)
- On the IETF
- Cyber Security Themes
- Cooperation and collaboration
- Questions

Internet Society

- Founded in 1992 by Internet pioneers
- Not for profit international organization
  - 110+ organizational members
  - 60.000+ individual members
  - 100+ local chapters worldwide
  - Offices: Africa, Asia, Europe, LAC, USA
- ISOC's mission is "to assure the open development, evolution and use of the Internet for the benefit of all people throughout the world"

- We do this by working in the areas of technical standards, policy development and education/capacitybuilding

Internet Society
InternetSociety.org

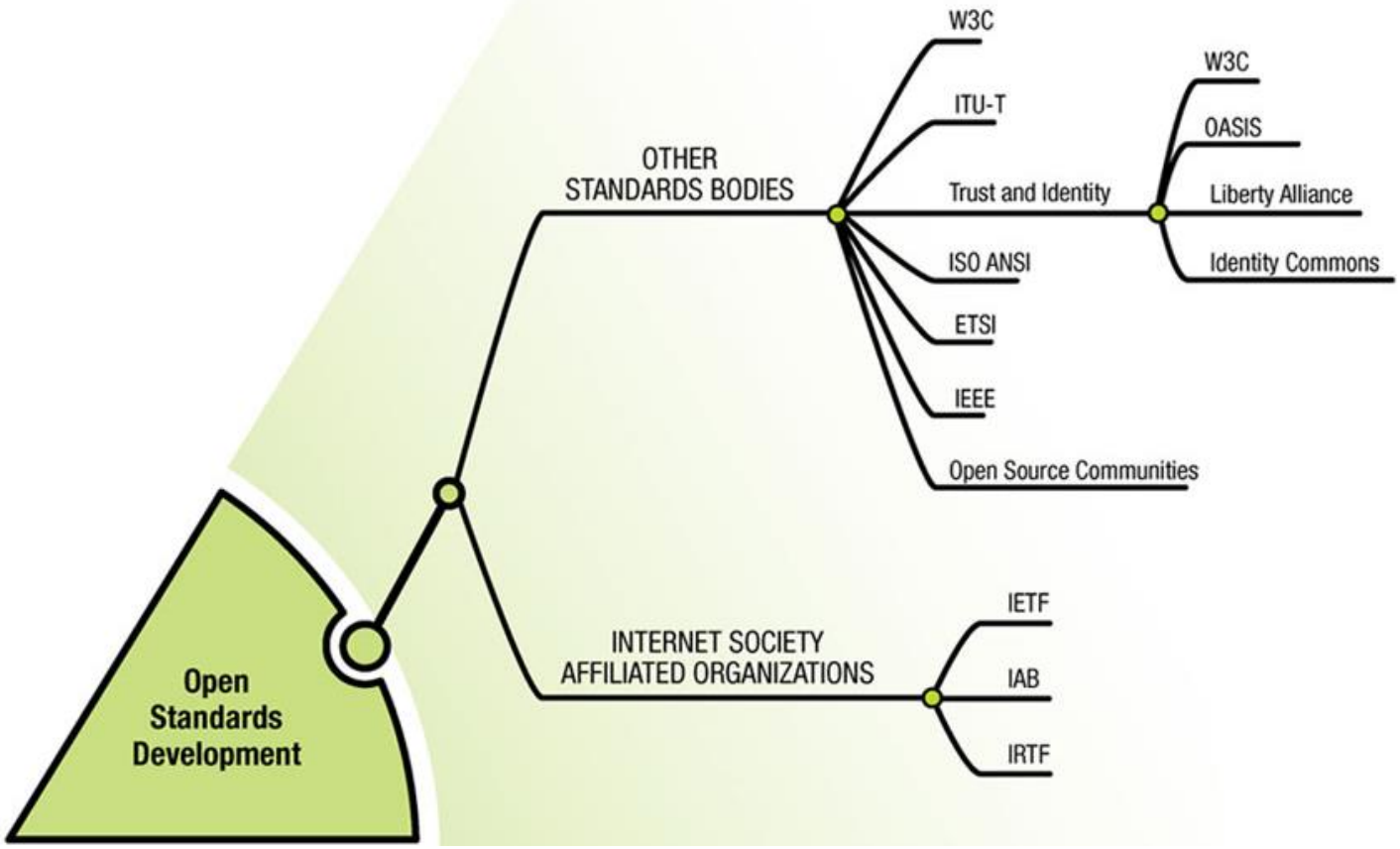
What Made Internet Society Unique?

- 20 years of leadership at the intersection of *Internet technology, development, and public policy*

- Organizational home of the *Internet Engineering Task Force* (IETF), which sets global Internet Standards
- Trusted reputation as *neutral and unbiased advocates* for the Internet
- Broad engagement across stakeholders including industry, government, universities, and civil society
- Expert contributors to the World Economic Forum, United Nations bodies, Internet Governance Forum(IGF), OECD, etc.
- Access to an *international network of experts*

Internet Society
InternetSociety.org

Open Standards Development (ecosystem)


Open
Standards
Development
OTHER
STANDARDS BODIES
W3C
ITU-T
Trust and Identity
ISO ANSI
ETSI
IEEE
Open Source Communities
W3C
OASIS
Liberty Alliance
Identity Commons
INTERNET SOCIETY
AFFILIATED ORGANIZATIONS
IETF
IAB
IRTF

On the Internet Engineering Task Force

- ***Challenges in LAC region***

Weakness

- The region is underrepresented!

Opportunities

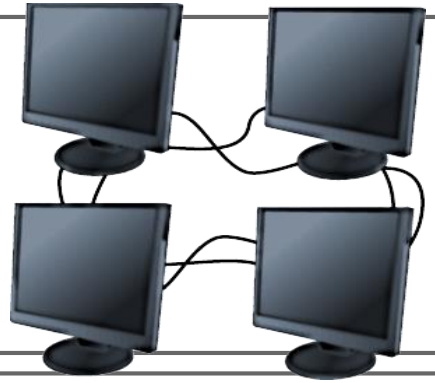
- And there are many working groups where our engineers can contribute (based on their own experiences);
- There is a need in the IETF for more operators;
- There is interest in the IETF on reaching out the open source communities;

Addressing the challenges

- In order to address the geographic diversity there is a campaign to encourage participation from Latin America and the Caribbean in preparation for the IETF in Buenos Aires in 2016 (first one in the LAC region).

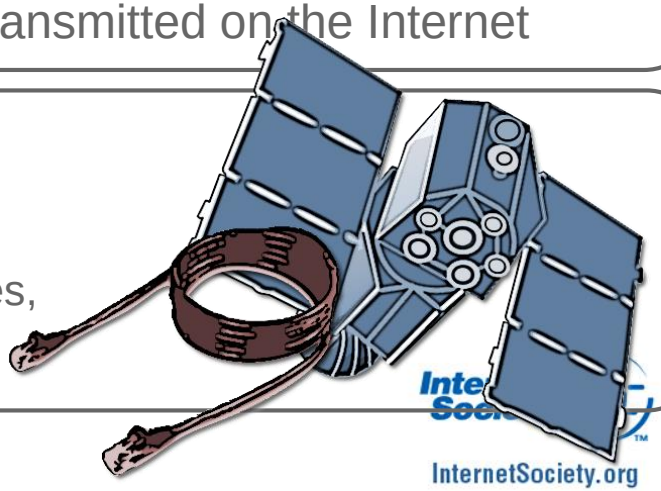
Internet's Three Operating Layers

Content and applications standards (HTML, XML, Java) – Promotes creativity and innovation in applications leading to email, World Wide Web, ebanking, wiki, Skype, Twitter, Facebook, Yahoo, Google, YouTube and much more



Internet protocols and standards (TCP/IP, DNS, SSL) – TCP/IP, controls traffic flow by dividing email and web data into packages before they are transmitted on the Internet

Telecommunications infrastructure – Physical network made up of underwater cables, telephone lines, fiber optics, satellites, microwaves, wi-fi, and so on Facilitates transfer of electronic data over the Internet



Definition of cyber security

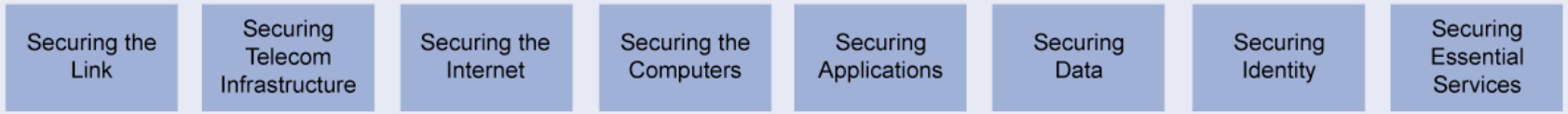
- *"Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way";*

- 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 scare 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

- 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.

It's All About Cooperation & Collaboration

- 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.

Thank You

Shernon Osepa
osepa@isoc.org

Internet Society
InternetSociety.org