IoT...

Internet of Things or Internet of Trust

Presented by

Olaf M. Kolkman
Chief Internet Technology Officer
Internet Society
email: kolkman@isoc.org
twitter: @kolkman

Deck by

Steve Olshansky
olshansky@isoc.org

www.internetsociety.org/IoT

Not starting from scratch… not a done deal either

Frameworks

- **Online Trust Alliance (OTA) IoT Security & Privacy Trust Framework**
  (An Internet Society Initiative)
  - *…includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. ...Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs.*
    https://otalliance.org/iot/
- **ENISA (European Union Agency for Network and Information Security) Baseline Security Recommendations for IoT**
  - *The goal of this report is to elaborate baseline cybersecurity recommendations for IoT with a focus on Critical Information Infrastructures, which encompass facilities, networks, services and physical and information technology equipment.*
    https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Online Trust Alliance IoT Security & Privacy Trust Framework

- June 2015 kick off, consensus driven process with input from industry and policy-makers
- Multi-stakeholder working group – 100 plus participants
- Face-To-Face meetings / Public Call for Comments
- Ongoing refinement
- Working Group Focus
  - Perfection the enemy of good
  - Measureable principles vs. standards development
  - Consumer grade devices (home, office and wearables)
  - Address known vulnerabilities and IoT threats
  - Actionable and vendor neutral

https://otalliance.org/iot/

Online Trust Alliance IoT Security & Privacy Trust Framework

The Framework is broken down into 4 key areas:

1. **Security Principles** – Applicable to any device or sensor and all applications and back-end cloud services.
2. **User Access & Credentials** – Requirement of encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password reset processes and integration of mechanisms to help prevent "brute force" login attempts.
3. **Privacy, Disclosures, & Transparency** – Requirements consistent with generally accepted privacy principles.
4. **Notifications & Related Best Practices** - Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required.

OTA
Online Trust Alliance
an Internet Society initiative

Assumptions/Principles and Instruments

From a discussion organized by NL gov on security of digital soft- and hardware

Assumptions

- Product lifecycle are important
- A portfolio of instruments
- Different Roles and Responsibilities
- Dynamic Equilibrium: Freedom, Security, & Economic growth

Potential Instruments

- Certification
- Monitoring
- In Network clean-up
- Testing
- Research
- Liability
- Enforcement
- Awareness

Internet Invariants: What Makes IoT Possible

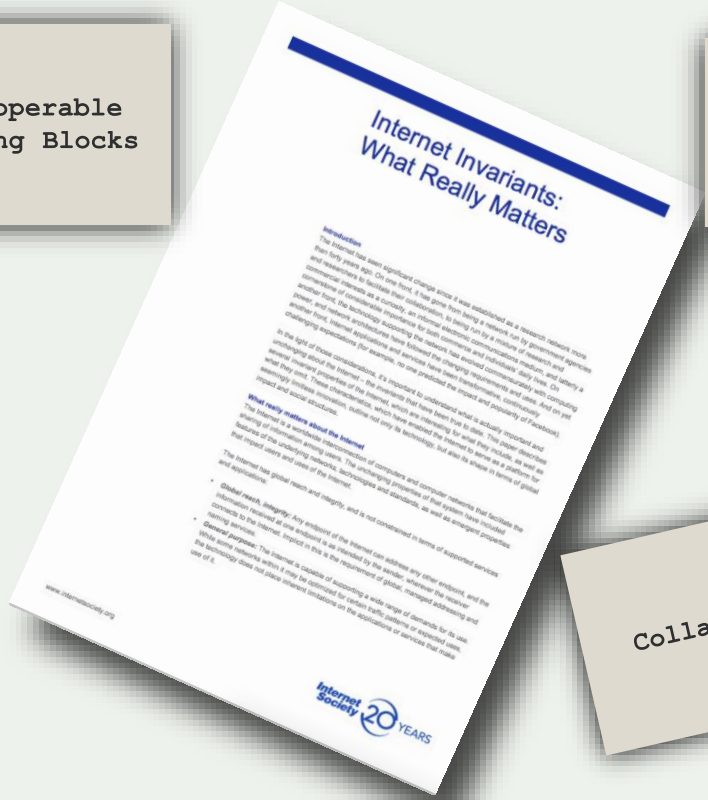
General Purpose

Interoperable Building Blocks

Global Reach & Integrity

Permissionless Innovation

Accessible



No Permanent Favorites

Interoperability & mutual agreement

Collaboration

Frameworks, Certifications, & Trustmarks

- Where can manufacturers and service providers refer to for useful guidance and accepted best practices?
- How best to signal “compliance” to device buyers?
- Which organization(s) have the public recognition and trust, and capability, to do this effectively?
- Complex supply chains pose a real challenge for assessments and certifications
  - How to determine what precisely is in/out of scope?
  - What can any manufacturer actually control and certify?
  - E.g., if a device runs app(s) on Linux, kernel is outside your control…
  - E.g., if a manufacturer sources components or software from other manufacturers/suppliers (a common scenario), how much ability does it have to control and certify?

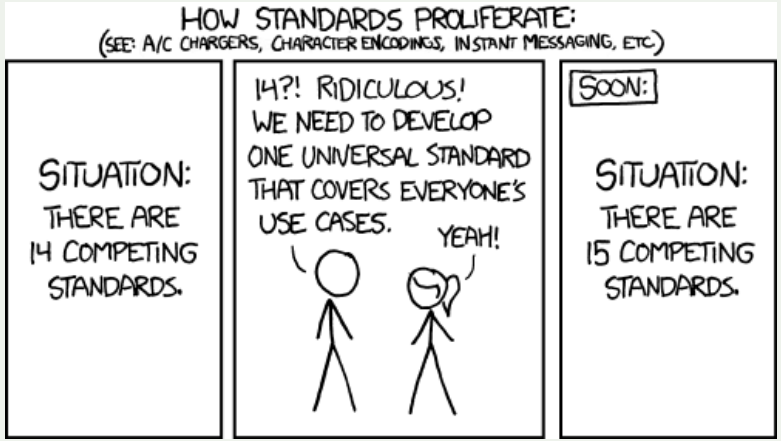
Frameworks, Certifications, & Trustmarks [2]

- Business model(s)? Who pays? Can be quite costly and burdensome, particularly for small companies
- How to manage ongoing testing and certification?
  - An assessment is simply a snapshot, and much can change when a product or service is updated or revised. Thus it needs to be an ongoing process.
- This has the potential to have a significant positive impact, shaping the marketplace by influencing consumer demand. But this is complex…
- But there are significant challenges:
  - Consumer/buyer awareness and education
  - Assessments self-asserted or externally audited? Advantages and disadvantages to both.
  - Exactly what is being evaluated? Are these the correct things? How does this change over time? What is the impact of context?

Interoperability / Standards Considerations

- Complex / Dynamic Service Delivery Chains and Use Cases
- Proliferation of Standards Efforts
  - Land Rush and Schedule Risk – which standards are the “right ones” to follow?
  - Makes security and privacy more challenging
  - Industry coalitions and alliances, SDOs, proprietary development, etc.
  - Open v. Closed standards processes
- Where is Interoperability Needed?
- Reusable Building Blocks
- Preventing “vendor lock-in”
- Best Practices and Reference Models

Ultimately about advancing innovation and user choice.



https://xkcd.com/927/

Interoperability & Standards:
Not Just a Tech Challenge, but also a Market Issue

Barriers include:

- Interoperability and portability
- Integration – (in)compatibility of data formats
- Lack of transparency
  - Data privacy concerns
  - Security concerns
- Standards fragmentation. Examples include:
  - IEEE P2413, ++
  - IETF, W3C, OASIS, ISO/IEC
  - OCF AllJoyn
  - Intel's Open Interconnect Consortium
  - ITU-T SG20 (smart cities)
  - UL 2900 certification (security)
  - Thread (IPv6 networking protocol)

Interoperability between IoT systems is critical. Of the total potential economic value the IoT enables, interoperability is required for 40 percent on average and for nearly 60 percent in some settings.

- McKinsey Global Institute

https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Certification & Trustmarks: Examples

NOTE: These are for reference only, not intended as a complete list or as an endorsement.

- **UL Cybersecurity Assurance Program (UL CAP)**
  https://industries.ul.com/cybersecurity/
- **The Digital Standard**
  https://www.thedigitalstandard.org/
- **Open Internet of Things Certification Mark**
  https://iotmark.wordpress.com/
- **F-Interop**
  http://www.f-interop.eu/
- **Exploring a Trustmark for the Internet of Things (IoT)**
  https://medium.com/thingscon/a-trustmark-for-iot-b4dee8e948e7

ThingsCon

- **Report: A Trustmark for IoT (PDF, 93 pages)**
  https://thewavingcat.com/iot-trustmark/
  https://www.thingscon.com/
- *We propose a trustmark for IoT, a label for consumers to decide which devices they choose to trust and—more importantly—which devices deserve their trust. This empowers consumers to make informed decisions on how to vote with their money and for producers of IoT products to show their commitment to good practices and IoT health.*

Additional Information and Resources

- **Rough Guide to IETF 100: Internet of Things (IETF activities related to IoT)**
  https://www.internetsociety.org/blog/2017/11/rough-guide-ietf-100-internet-things/
- **IEEE IoT Related Standards**
  http://standards.ieee.org/innovate/iot/stds.html
- **Internet Architecture Board (IAB) Internet of Things (IoT) Software Update (IoTSU) Workshop 2016**
  tools.ietf.org/html/draft-iab-iotsu-workshop
  RFC 8240: Report from the Internet of Things Software Update (IoTSU) Workshop 2016
  https://tools.ietf.org/html/rfc8240
- **IETF 97 Technical Plenary – *Attacks Against the Architecture***
  https://www.youtube.com/watch?v=qPaaRaNxIY4
  https://www.ietf.org/proceedings/97/slides/slides-97-ietf-sessb-the-internets-architecture-is-under-attack-ironically-andrew-sullivan-00.pdf
- **MUD – Manufacturer Usage Description Specification**
  https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

Thank you

Steve Olshansky
olshansky@isoc.org
www.internetsociety.org/IoT

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120