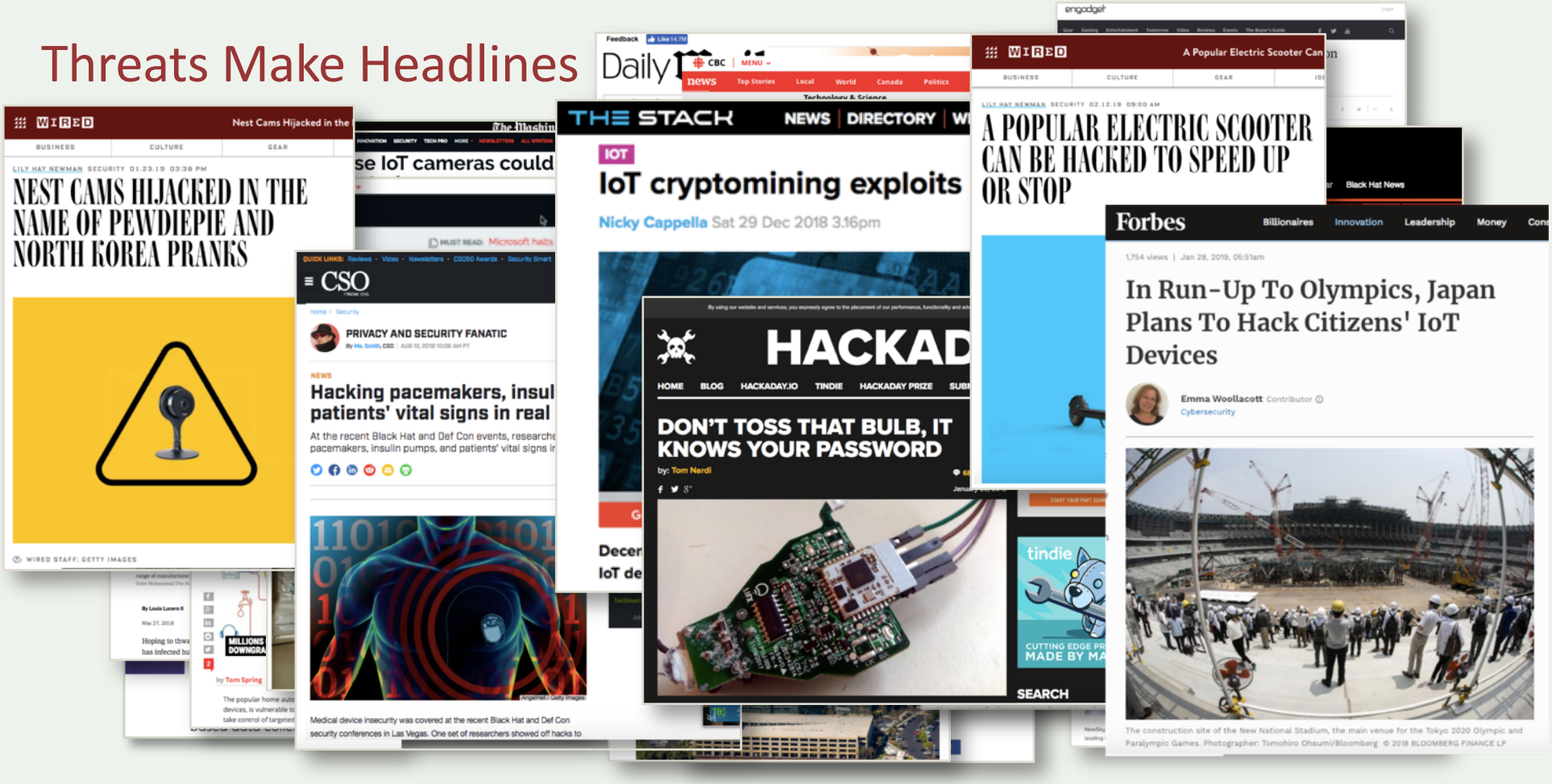
TNC19
18-June-2019
Tallinn, EE

Consumer IoT Security and Privacy Frameworks, Trustmarks and Certifications: Useful, or Useless?

Steve Olshansky
olshansky@isoc.org

Threats Make Headlines



Context

- IoT devices are proliferating on our networks (including BYOIoT), and in many cases central IT has little or no control and often no knowledge until problems occur – and they will occur.
- A growing number of organizations and government agencies are actively working on developing or promoting IoT security and privacy frameworks, and related trustmark and certification programs, around the world.
- There is a great deal of commonality/overlap in the principles in these various frameworks.
- What do they mean for R&E? How can we leverage these frameworks to address the threats to our networks and infrastructure stemming from the proliferation of IoT devices?

Proposals

- Bring facilities management, contracts/purchasing, and central IT together to improve communication and collaboration, and to break down silos.
- Use the leverage of your purchasing power - include security and privacy requirements in RFPs and contracts.

Some Framework Examples:

- IoT Trust Framework - Internet Society / Online Trust Alliance (OTA)
- UK Code of Practice for Consumer Internet of Things (IoT) Security
- ETSI TS 103 645 - Cyber Security for Consumer Internet of Things
- IoT Security Guidelines – GSMA
- US National Institute of Standards and Technology (NIST):
  - Cybersecurity Framework
  - NISTIR 8228 (DRAFT) - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Some Framework Examples [2]:

- Securing Consumer Trust in the Internet of Things - Consumers International)
- Consumer IoT Trust by Design 2019 - Consumers International / Vodafone
- The Digital Standard - Consumer Reports, US
- IoT Security Compliance Framework - IoT Security Foundation (IoTSF)
- Baseline Security Recommendations for IoT - ENISA (EU Agency for Cybersecurity)

Some Trustmark/Certification Examples:

- EU Cybersecurity Certification Framework (forthcoming, cf. ENISA Baseline Security Recommendations for IoT)
- Trustable Technology Mark - w/Mozilla
- Cybersecurity Assurance Program (CAP) - UL
- IoT Cybersecurity Certification Program – CTIA (U.S. wireless communications industry)
- GSMA IoT Security Assessment

This is big! Congratulations to our friends at the EU Agency for Cybersecurity!

The EU Cybersecurity Act will come into force on 27th June 2019. In a shift towards a role that adds more value to the European Union, ENISA, which will henceforth be known as the EU Agency for Cybersecurity and will receive a permanent mandate. Find out more: https://europa.eu/!bX86Fp.

The EU Cybersecurity Act establishes a European cybersecurity certification framework for ICT products, services and processes.

https://www.enisa.europa.eu/news/enisa-news/the-eu-cybersecurity-act-a-new-era-dawns-on-enisa

In February 2019, ETSI, the European Standards Organisation, published Technical Specification 103 645, the first globally-applicable industry standard for consumer IoT security. This industry standard builds on the Code of Practice, but has been designed to work for European and wider global needs. The standard is set to inform, at home and abroad, the development of regulation and industry-led certification schemes.

For businesses with an international supply chain and customer base, the standard provides an avenue to pursue a harmonised approach to implementing good security practice for their products.

https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security

https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Questions**

- How can we know, with confidence, the security and privacy aspects of the devices (and associated cloud services) we buy and use?
  - A: We can't. Thus we need to be proactive in monitoring their behavior and protecting our networks and users. One promising approach is under development: Manufacturer Usage Description Specification (IETF RFC 8520)
- Are self-asserted trustmarks (by manufacturers and related service providers) valuable, or should the focus be on externally audited certification programs managed by known and trusted organizations?
  - A: Self-asserted trustmarks are indeed useful so long as we keep them in perspective as to what they do and do not convey. And a lot has to do with how much trust we can place in the manufacturer, given their history etc.
- What can actually be assessed in IoT products and related services, and what cannot?
  - A: This is a very thorny topic. The short answer is that assessments are by their nature limited, and at best only a snapshot in time. E.g. many may be "desk exercises."

** Answers reflect my own opinions after a deep dive into these topics, but much will depend upon your particular circumstances and environment…

[2] Questions**

- What happens when products are updated (HW/SW/FW) – how much of a change is meaningful toward requiring a new assessment?
  - A: This is very hard to answer in a general way. A lot depends upon the specifics of course, but it is incumbent upon us to do our due diligence and fully understand the issues.
- Should assessment be focused instead or in addition on the company's "trustworthiness" and privacy and security posture, and HW/SW/FW development processes?
  - A: Arguably these aspects are at least as valuable, if not more so.

** Answers reflect my own opinions after a deep dive into these topics, but much will depend upon your particular circumstances and environment…

Tänan väga

Quai de l'île 13
CH-1204 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Sin El Fil, Dekwaneh Highway
Aramex Building, 2nd Floor
Beirut, Lebanon

Science Park 400
1098 XH Amsterdam
Netherlands

internetsociety.org
@internetsociety

9 Temasek Boulevard
#09-01 Suntec Tower Two
Singapore 038989