NRENs and IoT Security: Challenges and Opportunities

Internet Society

Karen O'Donoghue

TICAL 2018 Cartagena

4 September 2018

The number of IoT devices and systems
connected to the Internet will be more than

5x the global population

by 2022 (IHS).

As more and more devices are connected, privacy and security risks increase.

New devices, new vulnerabilities

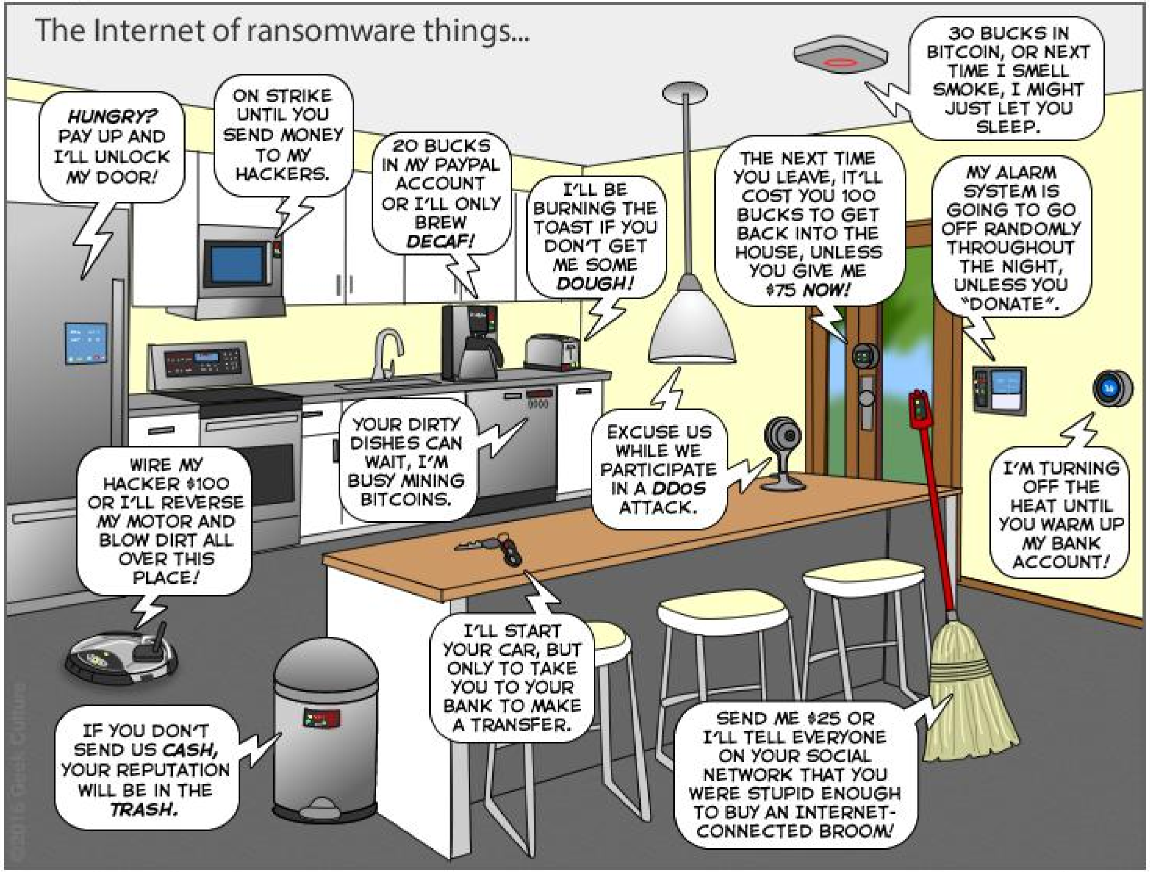
The attributes of many IoT devices present new and unique security challenges compared to traditional computing systems.

- Device Cost/Size/Functionality
- Volume of identical devices (homogeneity)
- Long service life (often extending far beyond supported lifetime)
- No or limited upgradability or patching
- Physical security vulnerabilities
- Access

- Limited user interfaces (UI)
- Limited visibility into, or control over, internal w
- Embedded device
- Unintended uses
- Bring Your Own

The threats are everywhere…

The Joy of Tech™ by Nitrozac & Snaggy


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture

You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

A connected world offers the promise of convenience, efficiency and insight, but creates a platform for shared risk.

Many of today’s IoT devices are rushed to market with little consideration for basic security and consumer safety protections.

Inward Security

Focus on potential harms to the health, safety, and privacy of device users and their property stemming from compromised IoT devices and systems

Outward Security

Focus on potential harms that compromised devices and systems can inflict on the Internet and other users

Internet Invariants

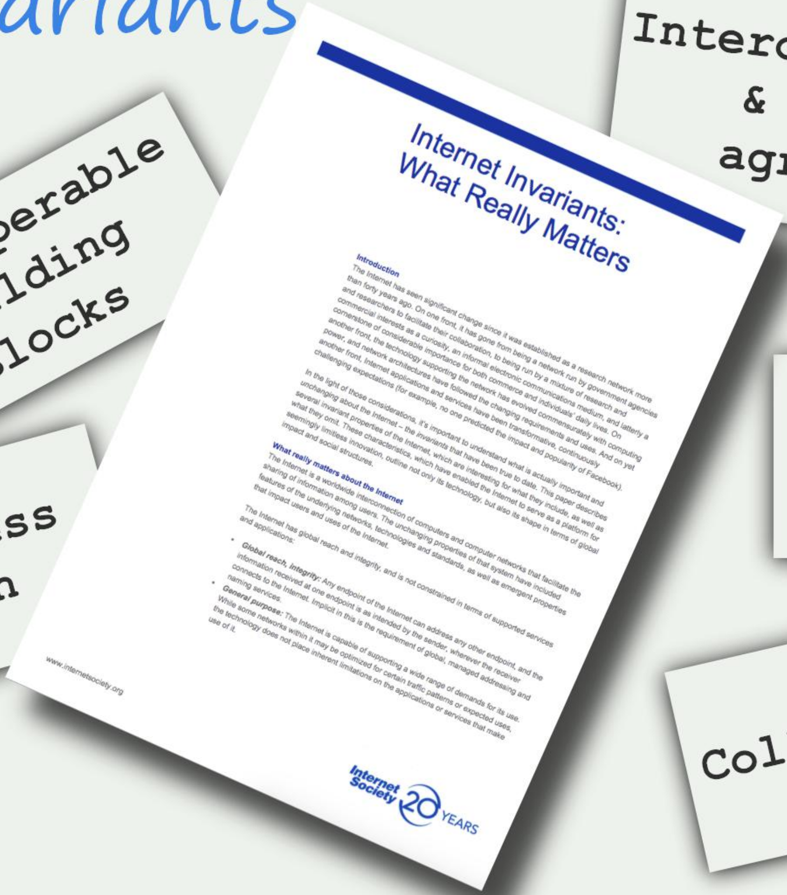
General Purpose

Interoperable Building Blocks

Global Reach & Integrity

Permissionless Innovation

Accessible



Internet Invariants: What Really Matters

Introduction

The Internet has seen significant change since it was established as a research network more than forty years ago. On one front, it has gone from being a network run by government agencies and researchers to facilitate their collaboration, to being run by a mixture of research and commercial interests as a curiosity, an informal electronic communications medium, and latterly a cornerstone of considerable importance for both commerce and individuals' daily lives. On another front, the technology supporting the network has evolved commensurately with computing power, and network architectures have followed the changing requirements and uses. And on yet another front, Internet applications and services have been transformative, continuously challenging expectations (for example, no one predicted the impact and popularity of Facebook).

In the light of those considerations, it's important to understand what is actually important and unchanging about the Internet – the invariants that have been true to date. This paper describes several invariant properties of the Internet, which are interesting for what they include, as well as what they omit. These characteristics, which have enabled the Internet to serve as a platform for seemingly limitless innovation, outline not only its technology, but also its shape in terms of global impact and social structures.

What really matters about the Internet

The Internet is a worldwide interconnection of computers and computer networks that facilitate the sharing of information among users. The unchanging properties of that system have included features of the underlying networks, technologies and standards, as well as emergent properties that impact users and uses of the Internet.

The Internet has global reach and integrity, and is not constrained in terms of supported services and applications:

- **Global reach, Integrity:** Any endpoint of the Internet can address any other endpoint, and the information received at one endpoint is as intended by the sender, wherever the receiver connects to the Internet. Implicit in this is the requirement of global, managed addressing and naming services.
- **General purpose:** The Internet is capable of supporting a wide range of demands for its use. While some networks within it may be optimized for certain traffic patterns or expected uses, the technology does not place inherent limitations on the applications or services that make use of it.

www.internetsociety.org

Internet Society 20 YEARS

Interoperability & mutual agreement

No Permanent Favorites

Collaboration

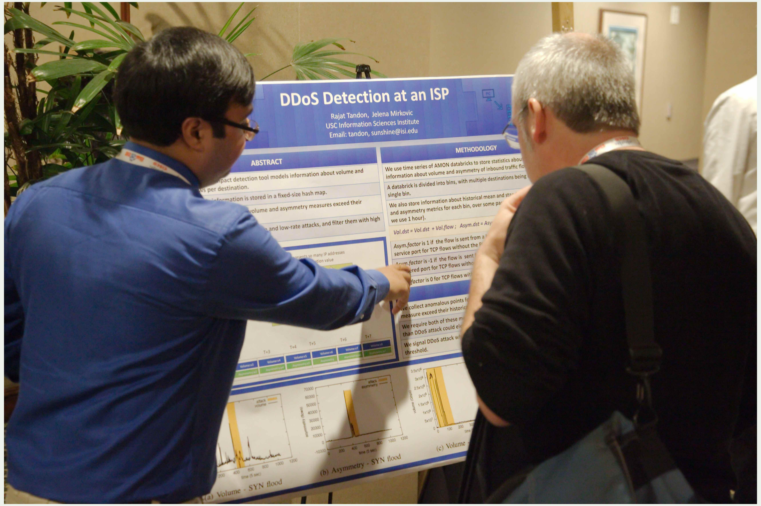
https://www.internetsociety.org/internet-invariants-what-really-matters/

How do we improve things?

- □ Research and Innovation
- □ Open Standards
- □ Frameworks and Best Practices
- □ Certifications and Trustmarks
- □ Policy and Regulation

Research and Innovation

Fear and Logging in the Internet of Things
Qi Wang, Wajih Ul Hassan, Adam Bates, Carl Gunter
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
NDSS Symposium 2018
Feb 19, 2018
NDSS SYMPOSIUM '18 25 YEARS


DDoS Detection at an ISP
Rajat Tandon, Jelena Mirkovic
USC Information Sciences Institute
Email: tandon, sunshine@isi.edu
ABSTRACT
METHODOLOGY
(a) Volume - SYN flood
(b) Asymmetry - SYN flood
(c) Volume

Open Standards Grou

IEEE

I E T F®

ITU

zigbee alliance

industrial internet® CONSORTIUM

oma SpecWorks
For a Connected World

ISO

OASIS
Open standards. Open source.

LoRa Alliance™

... and many more

Frameworks and Best Practices

OTA
Online Trust Alliance
an Internet Society initiative

IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to
product purc
well as the te
Security upda
when vulnera
Framework p
transparency
and a range o

Core to addre
entire device
the backend /
components
chain security

Serving as a r
foundation fo
these standar
decisions. The

The Framewo

- **Security F** cloud ser process t supply ch principles
- **User Acce** shipment processes
- **Privacy, D** privacy p capability applicable addresses
- **Notificati** mechanis include re communi accessibil

© 2017 Online

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity
(首相官邸Webサイトの検索システ

General Framework for Secure IoT Systems

National center of Incident readiness and Strategy for Cybersecu
Governme
Augu

1. General Framework Objective

Internet of Things (IoT) systems consist of connected things and networks and t
be regarded as an integrated system of IT with physical components. It is importan
physical safety in addition to existing information security measures. It is essent
systems are designed, developed and operated under the principle of "Security b
while looking ahead to the future where many individual systems are interconn
new vulnerabilities possibly introduced. To rationally accomplish this, a two-ste
is appropriate: instituting general requirements on design, development, and o
all IoT systems, in addition, sector-specific requirements for development and
based on characteristics of respective sectors.

Based on this concept, this framework aims to clarify the fundamental and essent
requirements for secure IoT systems.

It is expected that this framework will contribute to promoting the indust
involvement in the development of secure IoT systems and will create an envir
which IoT systems users can utilize the systems with a condition that security and safety is assured, by promoting the interoperability of IoT systems and the implementation of security requirements.

enisa

Baseline Securit
Recommendati
in the context of Critical Informati

NOVEMBER 2017

www.enisa.europa.eu European Union Agency For N

Secure by Design Report

Department for
Digital, Culture
Media & Sport

Secure by Design: Improvi
security of consumer Intern
Report

Singapore Standards Council

TR 64 : 2018
(ICS 35.030)

TECHNICAL REFERENCE
Guidelines for IoT security for smart nation

Published by
Enterprise Singapore

IoTA
IoT Alliance Australia

INTERNET OF THINGS
SECURITY GUIDELINE

IoT SECURITY GUIDELINE V1.2
November 2017

Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.

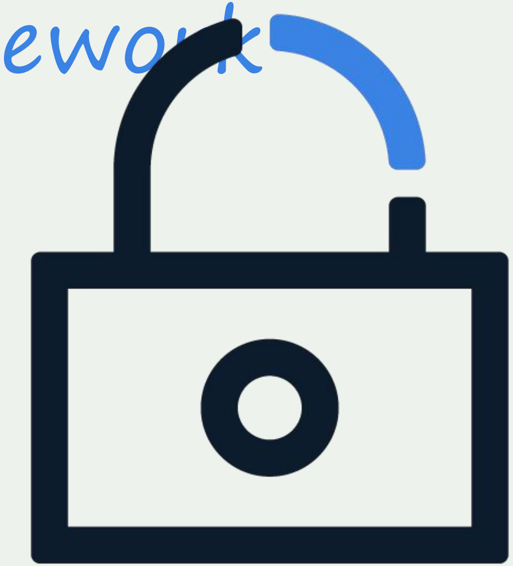
The Interagency International Cybersecurity Standardization Working Group (IICS WG) has developed this draft report based upon the information available to the participating agencies. Comments are being solicited in order to augment that information, especially on the information about the state of cybersecurity standardization for IoT that is found in Sections 8, 9, 10, and Annex D.

Reviewers are requested to submit comments to NISTIR-8200@nist.gov using the comment template at https://csrc.nist.gov/publications/detail/nistir/8200/draft. Comments will be posted at https://www.nist.gov/itl/comments-draft-nistir-8200 as they are received.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Frameworks:
The OTA IoT Trust Framework

- Measurable principles vs. standards development
- Consumer grade devices (home, office and wearables)
- Address known vulnerabilities and IoT threats
- Actionable and vendor neutral



https://www.internetsociety.org/iot/trust-framework//

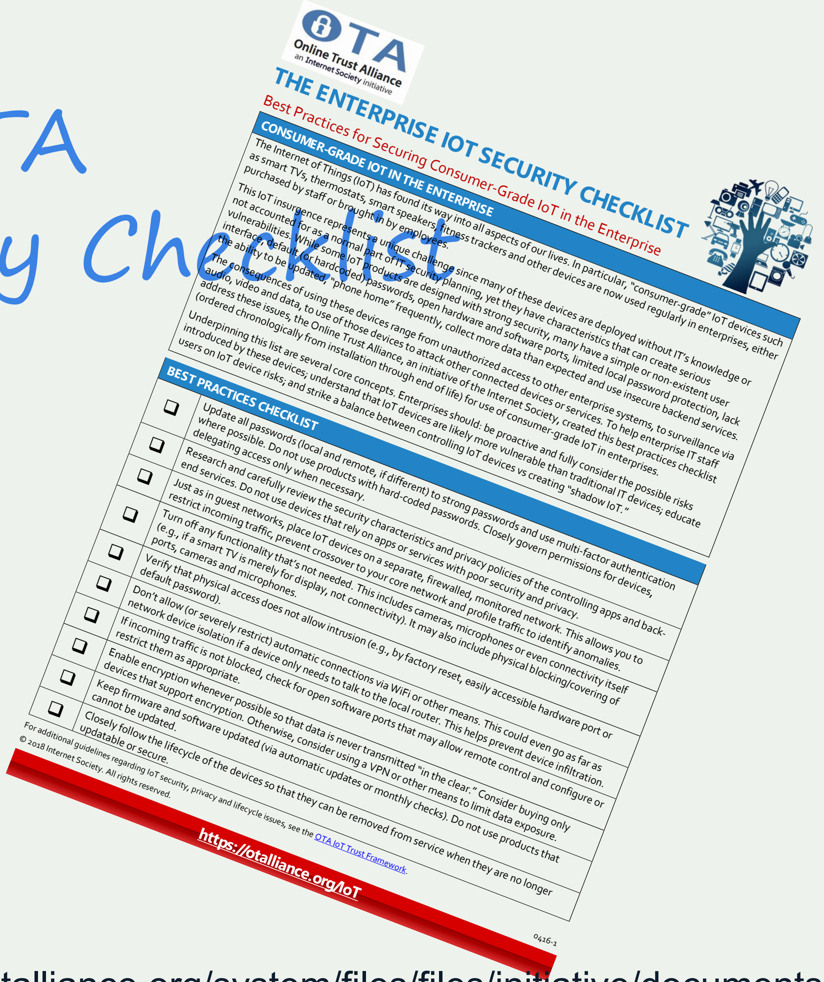
The Online Trust Alliance's IoT Trust Framework principles address

- Authentication
- Encryption
- Security
- Updates
- Privacy
- Disclosures
- Control
- Communications

Best Practices: The OTA Enterprise IoT Security Checklist

Set of Best Practices for Enterprises

- be proactive and fully consider the possible risks introduced by these devices;
- understand that IoT devices are likely more vulnerable than traditional IT devices;
- educate users on IoT device risks; and
- strike a balance between



OTA Online Trust Alliance an Internet Society initiative

THE ENTERPRISE IOT SECURITY CHECKLIST

Best Practices for Securing Consumer-Grade IoT in the Enterprise

CONSUMER-GRADE IOT IN THE ENTERPRISE

The Internet of Things (IoT) has found its way into all aspects of our lives. In particular, "consumer-grade" IoT devices such as smart TVs, thermostats, smart speakers, fitness trackers and other devices are now used regularly in enterprises, either purchased by staff or brought in by employees.

This IoT insurgence represents a unique challenge since many of these devices are deployed without IT's knowledge or not accounted for as a normal part of IT security planning, yet they have characteristics that can create serious vulnerabilities. While some IoT products are designed with strong security, many have a simple or non-existent user interface, default (or hardcoded) passwords, open hardware and software ports, limited local password protection, lack the ability to be updated, "phone home" frequently, collect more data than expected and use insecure backend services.

The consequences of using these devices range from unauthorized access to other enterprise systems, to surveillance via audio, video and data, to use of those devices to attack other connected devices or services. To help enterprise IT staff address these issues, the Online Trust Alliance, an initiative of the Internet Society, created this best practices checklist (ordered chronologically from installation through end of life) for use of consumer-grade IoT in enterprises.

Underpinning this list are several core concepts. Enterprises should: be proactive and fully consider the possible risks introduced by these devices; understand that IoT devices are likely more vulnerable than traditional IT devices; educate users on IoT device risks; and strike a balance between controlling IoT devices vs creating "shadow IoT."

BEST PRACTICES CHECKLIST

☐ Update all passwords (local and remote, if different) to strong passwords and use multi-factor authentication where possible. Do not use products with hard-coded passwords. Closely govern permissions for devices, delegating access only when necessary.

☐ Research and carefully review the security characteristics and privacy policies of the controlling apps and back-end services. Do not use devices that rely on apps or services with poor security and privacy.

☐ Just as in guest networks, place IoT devices on a separate, firewalled, monitored network. This allows you to restrict incoming traffic, prevent crossover to your core network and profile traffic to identify anomalies.

☐ Turn off any functionality that's not needed. This includes cameras, microphones or even connectivity itself (e.g., if a smart TV is merely for display, not connectivity). It may also include physical blocking/covering of ports, cameras and microphones.

☐ Verify that physical access does not allow intrusion (e.g., by factory reset, easily accessible hardware port or default password).

☐ Don't allow (or severely restrict) automatic connections via WiFi or other means. This could even go as far as network device isolation if a device only needs to talk to the local router. This helps prevent device infiltration.

☐ If incoming traffic is not blocked, check for open software ports that may allow remote control and configure or restrict them as appropriate.

☐ Enable encryption whenever possible so that data is never transmitted "in the clear." Consider buying only devices that support encryption. Otherwise, consider using a VPN or other means to limit data exposure.

☐ Keep firmware and software updated (via automatic updates or monthly checks). Do not use products that cannot be updated.

☐ Closely follow the lifecycle of the devices so that they can be removed from service when they are no longer updatable or secure.

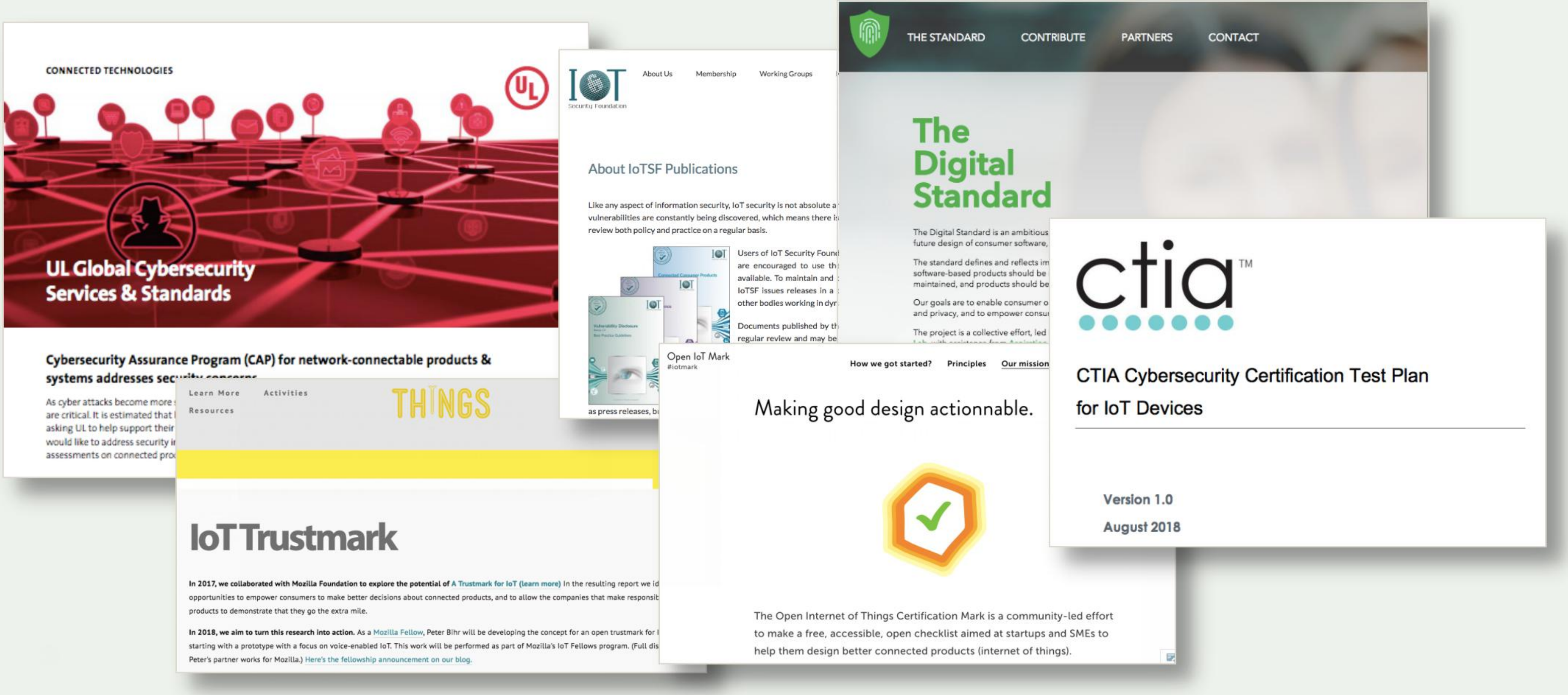
For additional guidelines regarding IoT security, privacy and lifecycle issues, see the OTA IoT Trust Framework.

https://otalliance.org/IoT

0416-1

https://otalliance.org/system/files/files/initiative/documents/enterprise_iot_checklist.pdf

Certifications and Trustmarks



CONNECTED TECHNOLOGIES

UL Global Cybersecurity Services & Standards

Cybersecurity Assurance Program (CAP) for network-connectable products & systems addresses sec

As cyber attacks become more
are critical. It is estimated that
asking UL to help support their
would like to address security i
assessments on connected pro

About Us Membership Working Groups

IoT Security Foundation

About IoTSF Publications

Like any aspect of information security, IoT security is not absolute a
vulnerabilities are constantly being discovered, which means there is
review both policy and practice on a regular basis.

Users of IoT Security Found
are encouraged to use th
available. To maintain and
IoTSF issues releases in a
other bodies working in dyn

Documents published by th
regular review and may be

as press releases, b

THE STANDARD CONTRIBUTE PARTNERS CONTACT

The Digital Standard

The Digital Standard is an ambitious
future design of consumer software,

The standard defines and reflects im
software-based products should be
maintained, and products should be

Our goals are to enable consumer o
and privacy, and to empower consu

The project is a collective effort, led

Learn More Activities
Resources

THINGS

IoT Trustmark

In 2017, we collaborated with Mozilla Foundation to explore the potential of A Trustmark for IoT (learn more) In the resulting report we id
opportunities to empower consumers to make better decisions about connected products, and to allow the companies that make responsib
products to demonstrate that they go the extra mile.

In 2018, we aim to turn this research into action. As a Mozilla Fellow, Peter Bihr will be developing the concept for an open trustmark for I
starting with a prototype with a focus on voice-enabled IoT. This work will be performed as part of Mozilla's IoT Fellows program. (Full dis
Peter's partner works for Mozilla.) Here's the fellowship announcement on our blog.

Open IoT Mark
#iotmark

How we got started? Principles Our mission

Making good design actionable.

The Open Internet of Things Certification Mark is a community-led effort to make a free, accessible, open checklist aimed at startups and SMEs to help them design better connected products (internet of things).

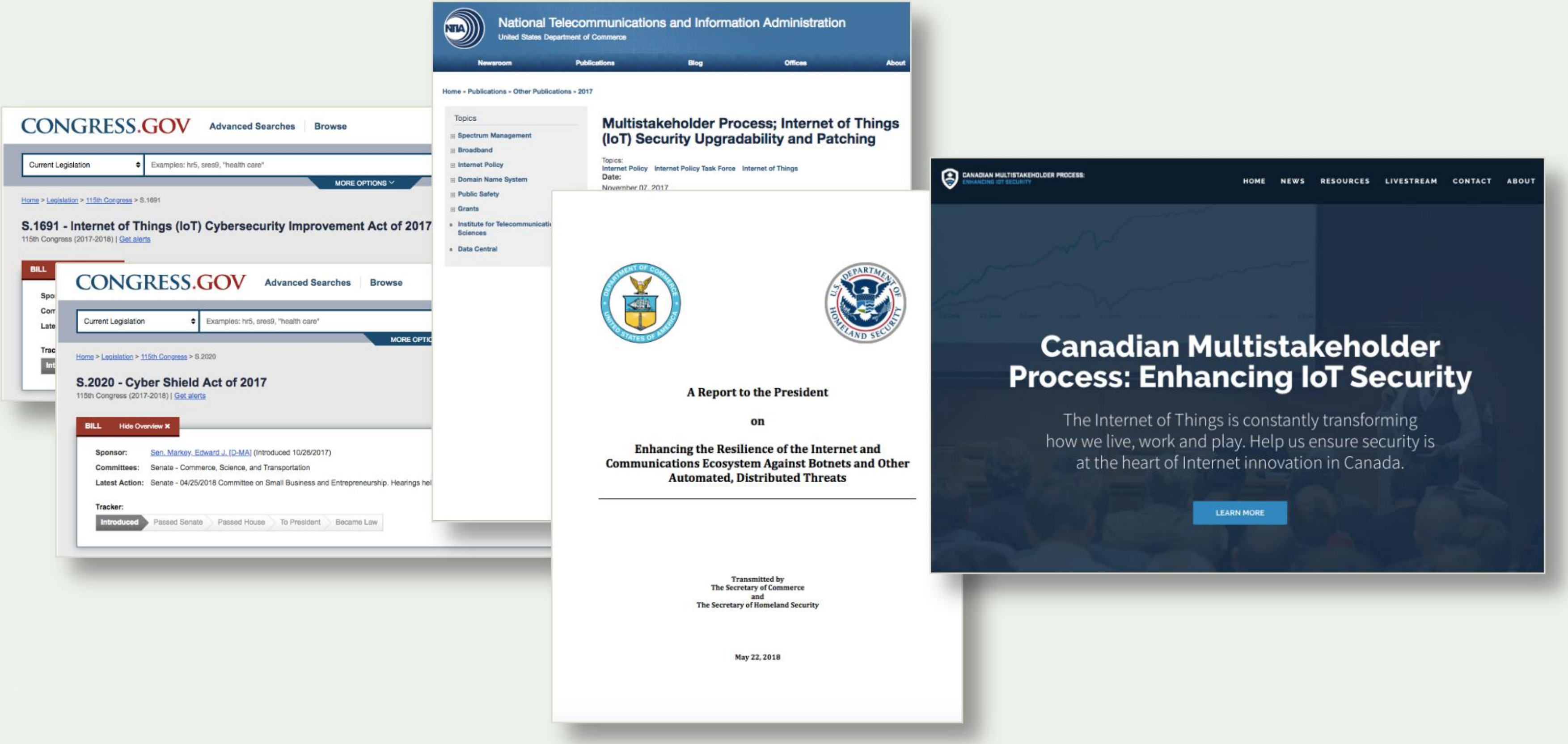
ctia™

CTIA Cybersecurity Certification Test Plan for IoT Devices

Version 1.0

August 2018

Policy and Regulation:



CONGRESS.GOV Advanced Searches Browse

Current Legislation | Examples: hr5, sres9, "health care"

MORE OPTIONS

Home > Legislation > 115th Congress > S.1691

S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017

115th Congress (2017-2018) | Get alerts

CONGRESS.GOV Advanced Searches Browse

Current Legislation | Examples: hr5, sres9, "health care"

Home > Legislation > 115th Congress > S.2020

S.2020 - Cyber Shield Act of 2017

115th Congress (2017-2018) | Get alerts

BILL Hide Overview ✖

Sponsor: Sen. Markey, Edward J. [D-MA] (Introduced 10/26/2017)

Committees: Senate - Commerce, Science, and Transportation

Latest Action: Senate - 04/25/2018 Committee on Small Business and Entrepreneurship. Hearings hel

Tracker: Introduced | Passed Senate | Passed House | To President | Became Law

National Telecommunications and Information Administration

United States Department of Commerce

Newsroom | Publications | Blog | Offices | About

Home » Publications » Other Publications » 2017

Topics

- Spectrum Management
- Broadband
- Internet Policy
- Domain Name System
- Public Safety
- Grants
- Institute for Telecommunicati Sciences
- Data Central

Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching

Topics:
Internet Policy | Internet Policy Task Force | Internet of Things

Date:
November 07, 2017

A Report to the President

on

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

CANADIAN MULTISTAKEHOLDER PROCESS:
ENHANCING IOT SECURITY

HOME | NEWS | RESOURCES | LIVESTREAM | CONTACT | ABOUT

Canadian Multistakeholder Process: Enhancing IoT Security

The Internet of Things is constantly transforming how we live, work and play. Help us ensure security is at the heart of Internet innovation in Canada.

LEARN MORE

Policy and Regulation:

Policies and Regulations may be needed.

Let's help to ensure these rules and regulations are correct, necessary and sufficient.

https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

19 April 2018

IoT Security for Policymakers

"Cybersecurity will be the most pressing challenge of the next decade, and IoT will play a critical role in it."

Internet Society 2017 Global Internet Report

Internet Society

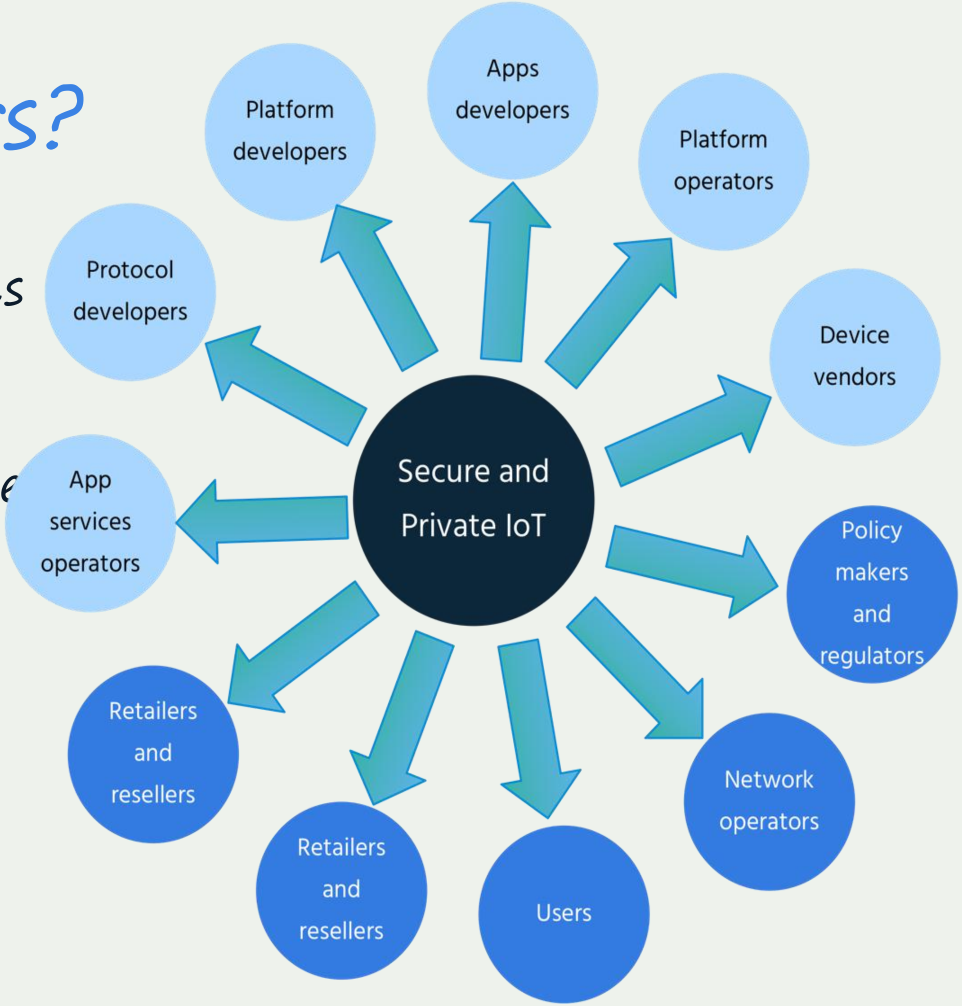
IoT Security & Privacy – A Collective Responsibility

- IoT vendors and their supply chain
- Distribution channels
- Policymakers and governments
- Consumer testing and product review organizations
- Consumers and enterprises

Who are the players?

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itse to potential harm

To scale up we need a collective approach, addressing security challenges on all fronts.



Secure and Private IoT

Protocol developers

Platform developers

Apps developers

Platform operators

Device vendors

Policy makers and regulators

Network operators

Users

Retailers and resellers

Retailers and resellers

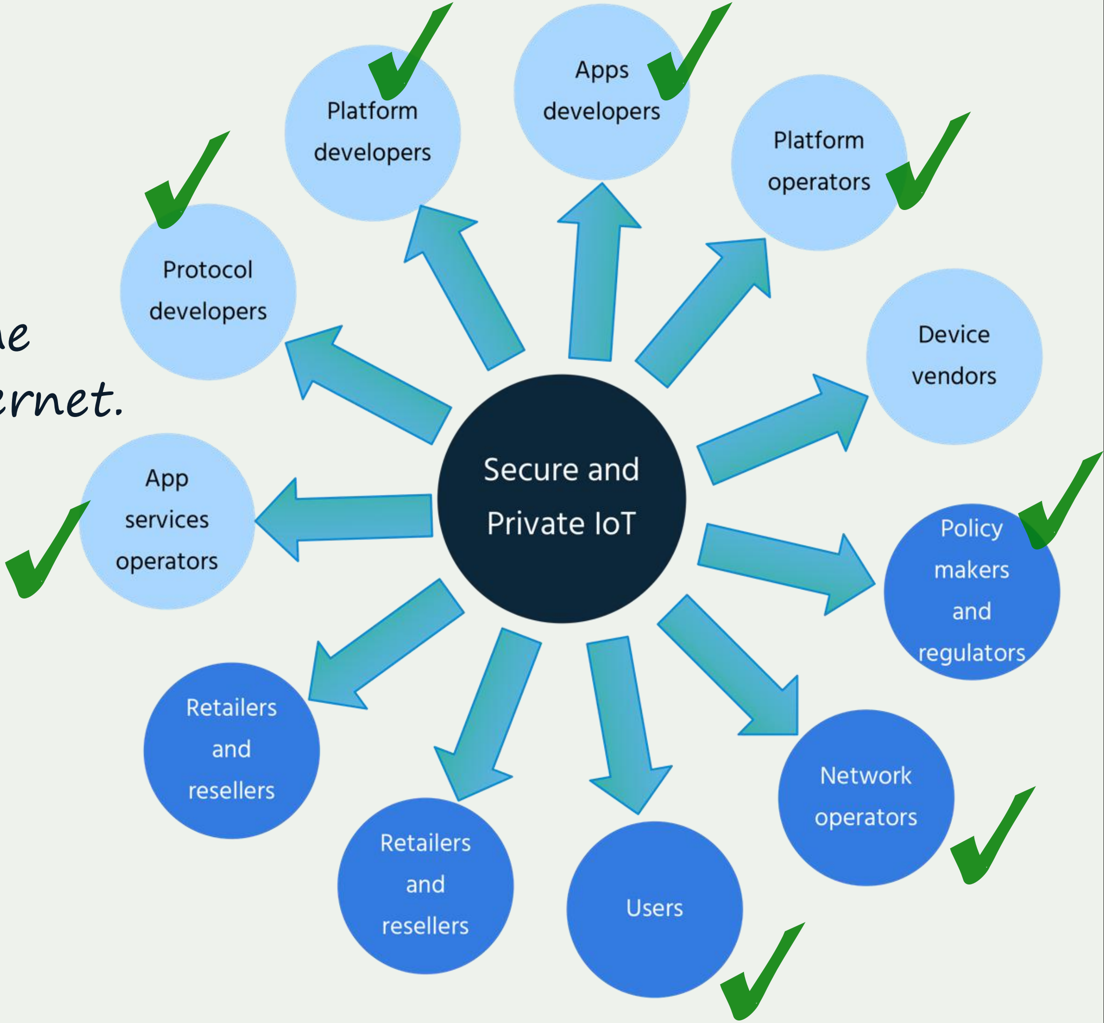
App services operators

Where do NRENs fit into this picture?

NRENs have historically led the way in innovation for the Internet.

NRENs are:

- Consumers
- Operators
- Policy makers
- Developers
- Technical Leaders



Possible NREN Roles and Actions

Consumers power → Exercise procurement

Possible NREN Roles and Actions

Consumers → Exercise procurement

power →

Operators Build smartly

Possible NREN Roles and Actions

Consumers → Exercise procurement

power →

Operators → Build smartly

Policy makers Rule wisely

Possible NREN Roles and Actions

Consumers	→	Exercise procurement
power	→	
Operators	→	Build smartly
Policy makers	→	Rule wisely
Developers		Implement cautiously

Possible NREN Roles and Actions

Consumers → Exercise procurement

power →

Operators → Build smartly

Policy makers → Rule wisely

Developers → Implement cautiously

Technical Leaders Participate

A Word on Privacy (in IoT)

Need strategies that **respect individual privacy choices** across a broad spectrum of expectations, while **still fostering innovation** in new technologies and services.

- Traditional online privacy models may not fit
- Challenges in achieving basic privacy principles, such as:
  - Transparency/Openness
  - Meaningful Choice
  - Data Minimization
  - Use Limitation
  - Opportunities to opt out

Hot off the presses…

[Clearly Opaque
Privacy Risks of the Internet of]

Authors:

Dr. Gilad Rosner and Erin Kenneally, J.D.

https://www.iotprivacyforum.org/clearlyopaque/

CLEARLY OPAQUE

PRIVACY RISKS OF THE INTERNET OF THINGS

THE INTERNET OF THINGS PRIVACY FORUM

May 2018

Final thoughts…

The Internet of Things is here and growing (be wary but not afraid).

NRENs are uniquely positioned to help lead the way forward to a healthy Internet ecosystem.

Use your NREN super powers wisely to:

Buy, Build, Rule, Implement, and Participate

in the emerging IoT Ecosystem

Questions?

© Octavio Aburto/Caters

http://www.dailymail.co.uk/news/article-2284287/Youre-going-wrong-way-Moment-confused-fish-tried-swim-opposite-direction-hundreds-companions-enormous-shoal.html

Thank you

Karen O'Donoghue
odonoghue@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