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

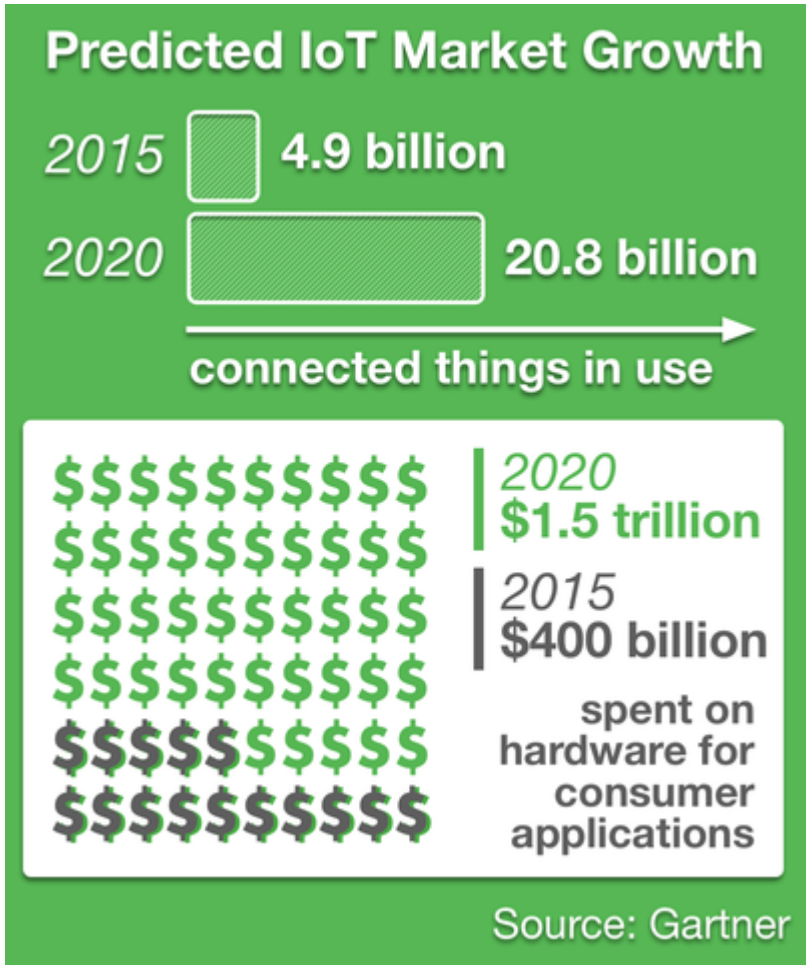
NIST Cybersecurity for IoT Program

Program Overview

[Date]

IoT on the Rise

Just as there are a variety of new uses, the IoT ecosystem brings new security considerations.



The Challenge

Fostering security for devices and data in the internet of things (IoT) ecosystem, across industry sectors and at scale

Program Mission

Cultivate trust in the IoT and promote U.S. leadership through standards, guidance, and related tools

NIST's **Cybersecurity for IoT Program** supports the development & application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.

By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and promote U.S. leadership in IoT.

IoT Activities

There are a number of IoT and IoT-related initiatives across NIST

IoT Work

Technical Needs

- Lightweight Encryption
- Advanced networking
- Cybersecurity for Cyber Physical Systems
- Systems BLE Bluetooth
- RFID Security Guidelines
- Guide to Industrial Control Systems (ICS) Security

Specific Uses

- Connected Transportation
- Smart Cities
- Cybersecurity for Smart Grid Systems
- Wireless Medical Infusion Pumps

IoT-Related Work

- Cybersecurity Framework
- Cybersecurity Framework Profile for Manufacturing
- National Vulnerability Database
- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- Security Systems Engineering
- Digital Identity Guidelines
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- Software Assessment Management Standards and Guidelines
- Cyber Threat Information Sharing
- Supply Chain Risk Management
- Cloud security

Ongoing Program Efforts

IoT Task Group of the Interagency International Cybersecurity Standardization Working Group (IICS WG)

- NIST co-chairs the IoT Task Group stood up under the National Security Council's Cyber Interagency Policy Council

Purpose

- In keeping with its charter to coordinate on major issues in international cybersecurity standardization, the IICS WG established at task group to determine the present state of international cybersecurity standards development for IoT.
  - IoT Task Group has 54 federal employee participants representing 13 agencies.

Next Steps

- The IICS Working Group is convening in early December and will determine next steps for the current draft report
- NIST is prepared to leverage NIST IR process to publish report on the state of International Cybersecurity Standards for IoT.
- Private industry input is key to providing a more complete view of the current state of IoT standards, especially in areas such as industry adoption or implementation barriers.
- Inform NIST standards engagement strategy for IoT security, depending on the report.

Ongoing Program Efforts

Cybersecurity for IoT Colloquium

- NIST hosted an IOT Colloquium inviting members from industry, academia and government to hear from the community to better understand the overall risk and security and privacy threat landscape as well as understand what NIST can do to support these areas.
- We plan to publish the proceedings from the colloquium but some early themes that emerged are:
  - The threat landscape is varied and broadening, without an authoritative set of security and privacy guidance. The IoT space is wide with some common risks and threats across the IoT, but there are also application specific risks and threats. It is likely that there will need to multiple solutions applied across the ecosystem commensurate with capabilities and risks.
  - Incentives for better security are needed in the marketplace. How can we ensure that organizations that 'do the right thing' can get the recognition for doing so. There were suggestions that currently, IoT manufacturers are not incentivized to provide high security products. LPTA (least price, technically accessible) with a much stronger emphasis on price. Definition for technically accessible isn't including security and is not well defined.·
  - Acknowledgment/awareness of privacy issues with IoT devices. Informed consent involves becoming fully aware of consequences. The IoT landscape is making this increasing difficult and making consent revocation and data deletion increasingly harder to attain.
  - Talking and working with industry (including using global standards) is the best way to mitigate risk without stifling innovation

Ongoing Program Efforts

Guidance to federal agencies on considerations for managing security and privacy risk for the IoT

- NIST publication covering Internet of things (IoT) Security and Privacy considerations for Federal Agencies

Purpose

- To educate federal agencies on common high-level security and privacy risks for IoT, and to introduce practical risk management considerations for IoT product selection, deployment, protection, and operation.
- To engage with federal government as well as industry stakeholders both during the development process

Next steps

- We plan to hold town halls to gather industry feedback during the concept and guidance development process.
  - Our first town hall is tentatively collocated at CES.
- Plan to begin socialization process with federal agencies through the Federal Computer Security Managers' Forum and through the Federal Privacy Council

Contact

#IoTSecurityNIST

iotsecurity@nist.gov

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program