National Institute of Standards and Technology

Cybersecurity and Privacy for the Internet of Things

Program Overview

April 2017
NIST Research

NIST IT Laboratory has expertise related to IoT
Examples of research areas include:

- Security and Privacy
- Networking
- Data Analytics
- Time and Space

Our “Cybersecurity for IoT” Program builds on the decades of cybersecurity research and experience on the technological underpinnings of the IoT

ITL Cybersecurity for IOT Program

- **Program purpose**
  - Cultivate trust in IoT and promote U.S. leadership in IoT through:
    - Definitions, guidance, and best practice documentation
    - Research, producing IoT reference data and enabling software tools
    - Coordination of standards within and across sectors in the digital economy;

- **Stakeholders**
  - Industry
  - Academia
  - Standards Development Organizations
  - International bodies
  - Government
Multiple definitions exist within industry

No clear definition of IoT as it represents a convergence of multiple areas of technology

- Mobile
- Embedded Systems
- Cloud
- Traditional IT

Functions within the IoT ecosystem

- Sensors
- Actuators
- Compute
- Communication

Gartner Says:

"IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment"
The nature of IoT is raising the stakes

**Market Conditions**
- 30 Billion Devices expected by 2020
- Estimated over 500 billion in sales by 2020
- Only 8% of businesses are using 25% of their IoT data today

**Anticipated massive market growth**

**New Operational Uses**
- Health care providers improperly diagnosing or treating patients based on modified health information or manipulated sensor data
- Intruders gaining physical access to homes or commercial businesses through attacks against electronic, remote controlled door lock mechanisms.
- Loss of vehicle control caused by denial-of-service against internal bus communications

**New risks**
- including personal safety

“How do we secure “things” and ensure proper processing of the data they generate and transmit to protect privacy?”
SECURITY AND PRIVACY CHALLENGES
### Barriers to IoT security/privacy – market factors

<table>
<thead>
<tr>
<th>Market Access</th>
<th>Developers push for first to market or early to market in blooming market segment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Focus on features and functionality first, tying user into ecosystem</td>
</tr>
<tr>
<td></td>
<td>Massive price pressure (more so in consumer vs industrial). We are talking about shaving fractions of pennies off of supply chain and hardware costs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First to market</th>
<th>Cheap processing readily available, such as: Arduino, Raspberry PI, Quark, many more</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An idea, a few dollars, and access to a maker space (with tools such as 3D printers) and service such as GoFundMe, Kickstarter, IndieGoGo, all can lead to quick prototypes</td>
</tr>
<tr>
<td></td>
<td>These nascent entrepreneurs often lack security expertise or resources to implement security</td>
</tr>
</tbody>
</table>

| Diversity | Vendors often use different hardware, software, APIs, third-party service providers, and patching mechanisms |
## Barriers to IoT security – device constraints

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Consumption</strong></td>
<td>Many IoT devices require a long battery life, without access to a permanent power supply.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Power efficient hardware often lacks additional capabilities such as ability to support encryption or hardware security mechanisms</td>
</tr>
<tr>
<td><strong>Low Cost</strong></td>
<td>The perceived value of an IoT device by customers greatly depends on the cost to purchase and implement the device. Market drivers often require that companies produce devices at a very low cost.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Low Processing capabilities, limited support for security</td>
</tr>
<tr>
<td><strong>Lifecycle</strong></td>
<td>Some sensors are short lived, others need to last decades.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Over time devices may become hardware constrained, can’t be updated. Built in security mechanism maybe found vulnerable or be deprecated, i.e. old encryption suites</td>
</tr>
<tr>
<td><strong>Limited Transmission</strong></td>
<td>Transmission is costly re: power and compute. Many IoT devices only transmit when needed or very infrequently.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>When the device is not processing or sending data, it may be in a sleep mode that limits the ability to scan, conduct diagnostics, update or patch.</td>
</tr>
</tbody>
</table>
Well publicized IoT related attacks

Mirai

- Malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers
- Gets command and control by attempting 62 different commonly used username and passwords – surprising or maybe not so surprisingly very effective.

9/21/2016 DDoS on Brian Krebs
- Security Researcher Brian Krebs known for his coverage of profit-seeking cybercriminals (re: bitcoin, silkroad, black market credit cards) and often a target for cyber attacks
- Servers hosting his blog were hit with DDoS using Mirai Attack generated traffic up to 655 Gbps, largest ever seen at the time

9/25/2016 DDoS on OVH
- Hosting company OVH hit with Mirai with traffic generation maxing at 799Gbps, breaking record set a few days prior

9/21/2016 DDoS on DYN
- DNS provider DYN hit with DDoS with traffic generation maxing at 1.2 Tbps
- Sites such as Twitter, Reddit, Netflix unavailable
- 4 days later Senator Mark Warner (VA), co-chair of senate cybersecurity caucus, reach out to FTC, FCC and DHS on possible solutions and responses to the security threat from IoT
## Privacy Challenges

<table>
<thead>
<tr>
<th>NIST Privacy Engineering Objective</th>
<th>Definition</th>
<th>IoT Data Actions</th>
<th>Potential Privacy-related Problems for Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictability</td>
<td>Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by a system.</td>
<td>It may be difficult for individuals to know what data devices are collecting about them and how the information will be processed after collection, especially if user interfaces are limited. De-centralized data-processing functions can contribute to complex automated systems and data flows IoT systems can act on human behavior directly. For example, traffic systems can influence or control where vehicles move. Environmental systems can influence behavior or movement in buildings.</td>
<td>When individuals lack awareness about what is happening in a system it can create problems around loss of self-determination -individuals may have difficulty participating in meaningful decisions about the use of their information -may create “chilling effects” on ordinary behavior and activity.</td>
</tr>
</tbody>
</table>
# Privacy Challenges

<table>
<thead>
<tr>
<th>NIST Privacy Engineering Objective</th>
<th>Definition</th>
<th>IoT Data Actions</th>
<th>Potential Privacy-related Problems for Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manageability</td>
<td>Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure.</td>
<td>The ubiquity of IoT sensors and devices in public and private environments can contribute to the aggregation and analysis of enormous amounts of data about individuals. Even non-identifying information can become identifying when combined with other information.</td>
<td>Information can be deeply sensitive and provide detailed insights into individuals’ lives in ways that individuals did not anticipate and do not find beneficial. Decentralization can contribute to difficulty in ensuring the quality and management of data and could lead to inaccurate or damaging determinations about individuals or difficulty in providing redress.</td>
</tr>
</tbody>
</table>
# Privacy Challenges

<table>
<thead>
<tr>
<th>NIST Privacy Engineering Objective</th>
<th>Definition</th>
<th>IoT Data Actions</th>
<th>Potential Privacy-related Problems for Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disassociability</td>
<td>Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.</td>
<td>Devices may collect information indiscriminately even when information about individuals is not necessary for the purpose of the system. Securing data is predominantly focused on data at rest in a system or data in motion between two known parties. Decentralizing data processing may be complicated by the low-power and low-processing capabilities required by many sensor use cases.</td>
<td>Processing identifying information even when not operationally necessary can increase the capability for tracking and profiling individuals. In a de-centralized system, encryption that relies on known parties/devices (as opposed to just trusted parties/devices) can create information-rich data trails about individuals.</td>
</tr>
</tbody>
</table>
NIST IoT Cybersecurity and Privacy Activities
Existing IoT security-related efforts at NIST

- **IoT-Specific**
  - Lightweight Encryption
  - Network of Things
  - Vehicle-to-vehicle transportation
  - Cybersecurity for Smart Grid Systems
  - Cybersecurity for Cyber Physical Systems
  - BLE Bluetooth

- **Directly Supporting IoT**
  - Wireless Medical Infusion Pumps
  - RFID Security Guidelines
  - Guide to Industrial Control Systems (ICS) Security
  - Security for Time
  - Supply Chain Risk Management
  - Blockchain
  - Hardware Roots of Trust
  - Galois IoT authentication & PDS Pilot
  - Cloud security

- **Indirectly Supporting IoT**
  - Cybersecurity Framework
  - CSF Profile for Manufacturing
  - National Vulnerability Database
  - Security of Interactive and Automated Access Management Using Secure Shell (SSH)
  - Digital Identity Guidelines
  - Security Content Automation Protocol (SCAP) Standards and Guidelines
  - Software Assessment Management Standards and Guidelines
  - Cyber Threat Information Sharing
  - Privacy Engineering and Risk Management
## IoT security-specific work

<table>
<thead>
<tr>
<th>Status</th>
<th>Effort</th>
<th>Additional Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document</td>
<td>Lightweight Encryption (IR 8114)</td>
<td>Need to identify the classes of IoT devices that can’t do full-strength crypto.</td>
</tr>
<tr>
<td>Document</td>
<td>Network of Things (SP 800-183)</td>
<td>Provides a model and terminology for describing IoTs. Opportunity to map the model to lower-level architectures and designs.</td>
</tr>
<tr>
<td>In Progress</td>
<td>Vehicle-to-vehicle transportation</td>
<td>Participating in international standard development for vehicle cybersecurity, consulting domestically on automotive security, and developing CSF profile for transportation.</td>
</tr>
<tr>
<td>Document</td>
<td>Cybersecurity for Smart Grid Systems (IR 7628 Rev 1)</td>
<td>Possible explosive growth in numbers of sensors and actuators, with security requirements. Opportunity to map to IoT models (like SP 800-183)</td>
</tr>
<tr>
<td>Document</td>
<td>Cybersecurity for Cyber Physical Systems (framework document)</td>
<td>Opportunity to map to IoT models (like SP 800-183)</td>
</tr>
<tr>
<td>Document</td>
<td>BLE Bluetooth (SP 800-121)</td>
<td>Protecting IoT communication.</td>
</tr>
<tr>
<td>Status</td>
<td>Effort</td>
<td>Additional Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>In Progress</td>
<td>NCCoE - Wireless Medical Infusion Pumps</td>
<td>Working with industry partners to develop implementation guidance for wireless medical infusion pumps use case (<a href="http://nccoe.nist.gov/projects/use_cases/medical_devices">http://nccoe.nist.gov/projects/use_cases/medical_devices</a>).</td>
</tr>
<tr>
<td>Document</td>
<td>RFID Security Guidelines (SP 800-98)</td>
<td>Information disclosure issue; impoverished version of an IoT</td>
</tr>
<tr>
<td>In Progress</td>
<td>Supply Chain Risk Management (SP 800-161)</td>
<td>Supply chain risk management practices</td>
</tr>
<tr>
<td>In Progress</td>
<td>Blockchain</td>
<td>How do fundamental blockchain features and resource requirements relate to IoT? (e.g. “proof of work”)</td>
</tr>
<tr>
<td>Document</td>
<td>Hardware Roots of Trust (SP 800-147)</td>
<td>Assured boot and state attestation.</td>
</tr>
<tr>
<td>In Progress</td>
<td>Galois IoT authentication &amp; PDS Pilot</td>
<td>Pilot deploying strong authentication for IoT-connected smart building. Enables access to IoT devices and sharing device data across organizational entities.</td>
</tr>
<tr>
<td>Document</td>
<td>Cloud security (SP 800-144)</td>
<td>Cloud definition.</td>
</tr>
</tbody>
</table>
## Indirectly supporting IoT security and privacy

<table>
<thead>
<tr>
<th>Status</th>
<th>Effort</th>
<th>Additional Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document</td>
<td>CSF Profile for Manufacturing (white paper)</td>
<td>Profile maps manufacturing processes to the cybersecurity framework. Multi-laboratory effort within NIST.</td>
</tr>
<tr>
<td>Document</td>
<td>Security Systems Engineering (SP 800-160)</td>
<td>Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems</td>
</tr>
<tr>
<td>Document</td>
<td>Software Assessment Management Standards and Guidelines (IR 8060)</td>
<td>Maintain an inventory of installed software (and maybe hardware) for an organization. SWID tag.</td>
</tr>
<tr>
<td>Document</td>
<td>Cyber Threat Information Sharing (SP 800-150)</td>
<td>Guidance for organizations generating and/or consuming cyber threat information.</td>
</tr>
<tr>
<td>Document</td>
<td>Introduction to Privacy Engineering</td>
<td>Report introducing concepts for privacy engineering and risk</td>
</tr>
</tbody>
</table>
Potential future NIST efforts on IoT Security (1)

- “NIST Publication on The Status of International Cybersecurity Standardization for the Internet of Things (IoT)” The Cybersecurity Enhancement Act of 2014 directs NIST to ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security and shall ensure consultation with appropriate private sector stakeholders.

- “IoT Publications and Industry Initiatives Survey”: Set of references (standards, academic papers, industry white papers, etc.) describing current IoT technology and anticipated use cases. Will describe active industry initiatives.

- “IoT Definition, Vocabulary, and Conceptual Architecture”: Describes IoT-specific aspects of a device or set (network) of devices (and backend support systems), building on existing industrial resources and NIST Network of Things (SP 800-183).

- “Use-Case and Sector-Specific IoT Architectures and Key Features”: Describes IoT across sectors and key use cases. Demonstrates how the architecture and key features of each can be generalized to an overarching IoT architecture.
Potential future NIST efforts on IoT Security (2)

- “NIST Cybersecurity Framework application to IoT”: Describes how the NIST Cybersecurity Framework can be used to apply security practices and security controls (e.g., SP800-53) to IoT system components.

- “IoT Threat Modeling”: Describes how to apply threat modeling to IoT systems, mapping architectures and key functions to security and privacy capabilities.

- “Risk Management for IoT”: Guidance for system developers, owners, and operators for managing risks using the suitable risk management framework (e.g., NIST RMF).

- National Thing Behavior Database (NTBD): Make available, on a national basis, behavioral information on IoT devices (such as signatures), as a service similar to the National Vulnerability Database. Industry standard specifications (e.g., MUD (Manufacturer Usage Description) IETF draft) as starting points.
Potential future NIST efforts on IoT Security (3)

• “Configuration Scanning for Consumer-Owned IoT”: Guidance for standardized data formats and protocols for applications that scan and perform configuration analysis when connected to consumer-owned IoTs. Primary goal is to provide a level of safety and security to consumers without requiring they apply IoT expertise themselves; will also benefit experts.
Other IOT program research
(beyond cybersecurity considerations but complementary)
IoT Networking Research

The IoT demands scalability, reliability, and interoperability of communications. Networking standards are critical to enable interoperable systems of systems, and support innovation at the application layer.

- Software Defined Networking (SDN) and Information Content Networking (ICN) approaches for improving security, interoperability, and congestion control.
- Analysis of network control systems to identify where wireless infrastructure can reduce wiring costs without impacting performance.
- Controlled mobility algorithm for communication of smart cells in public safety networks.
- Ultra-Wide-Band Channel Model for Smart Pills connectivity
- Body area networking, and energy harvesting
IoT Data Research

The IoT will generate vast amounts of data for decision making, prediction, and autonomous physical action.

- NIST Big Data Interoperability Framework – Big Data Public Working Group – Phase II - Interfaces
  - Seven volumes: 1 - Definitions; 2 - Taxonomies; 3 - Use Cases and General Requirements; 4 - Security and Privacy; 5 - Architectures White Paper Survey; 6 - Reference Architecture; 7 - Standards Roadmap

- Developing methods and testing infrastructure to measure and compare the performance of data analytic algorithms.
IoT Time & Space Research

It’s estimated that there will be over 30 billion devices connected to the IoT by 2020, resulting in trillions of interactions presenting localization and interoperability challenges. Some devices will need to be synchronized in real time.

- Research in timing standards including security,
- Interoperability, localization, and real-time data analysis for IoT systems.
Other research under consideration

- **Usability and Human Interface.** IOT systems won’t be adopted unless they are usable. We need ...
  - Research: how should IoT components best interact with users?
  - Guidance: to aid developers in creating useable designs.

- **Sensors.** Sensors are critical components. We need ...
  - Research on best practices for sensor data exchange
  - New methods for remote sensor calibrations and quality control.
Contact

Naomi Lefkovitz, Senior Privacy Policy Advisor
nbl@nist.gov
301-975-2924