NISTIR 8201

Internet of Things (IoT) Cybersecurity Colloquium

A NIST Workshop Proceedings

Katerina Megas
Ben Piccarreta
Danna Gabel O'Rourke

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8201

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

NISTIR 8201

Internet of Things Cybersecurity Colloquium

A NIST Workshop Proceedings

Katerina Megas
Ben Piccarreta
Applied Cybersecurity Division
Information Technology Laboratory

Danna Gabel O'Rourke
Deloitte & Touche LLP
Arlington, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8201

December 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8201
12 pages (December 2017)

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8201

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: iotsecurity@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This report provides an overview of the topics discussed at the "Internet of Things (IoT) Cybersecurity Colloquium" hosted on NIST's campus in Gaithersburg, Maryland on October 19, 2017. It summarizes key takeaways from the presentations and discussions. Further, it provides information on potential next steps for the NIST Cybersecurity for IoT Program.

Keywords

Internet of Things (IoT); Connected devices; Cybersecurity; Privacy

Acknowledgments

The authors gratefully acknowledge the speakers for their thoughtful contributions: Andrea Arias, Carlos J. Bosch, Matthew Eggers, Jeremy Grant, Arabella Hallaway, Joe Jarzombek, Gilad Rosner, Yasser Shoukry, and Andrew Sullivan. In addition, the authors would like to thank Suzanne Lightman for her support in planning and executing the Colloquium.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose. Content was derived from Colloquium discussions captured by note takers and aggregated for the purposes of summarizing the event. Any misrepresentation of comments or concepts is unintentional.

Table of Contents

List of Appendices

1 Introduction

On October 19, 2017, the National Institute of Standards and Technology (NIST) hosted the Internet of Things (IoT) Cybersecurity Colloquium at its Gaithersburg campus to convene stakeholders from across government, industry, international bodies, and academia. The goal was to better understand the concerns and risks associated with the rapidly expanding landscape of connected devices, known as the Internet of Things. Over 220 people participated, with more than 120 in-person attendees; webcast attendees followed the livestream from the US, Canada, Colombia, Israel, and Argentina.

1.1 About the NIST Cybersecurity for the Internet of Things Program

NIST's Cybersecurity for IoT Program [Program] supports the development and 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 foster an environment that enables innovation on a global scale.

The expanding IoT landscape is subject to an equally expanding list of risks, attacks, and corresponding outcomes. As the Program learned through stakeholder outreach, the list of risks is extensive. It includes – but is far from limited to – opportunities for malicious actors to highjack communication channels, change sensor data, access sensitive information, disrupt vital services, and alter signals and data for nefarious purposes. Outcomes vary and may include the collection of bad data, and actual, physical harm. Stakeholders have expressed interest in NIST producing guidelines to help organizations understand and manage cybersecurity and privacy risks associated with the use of IoT.

1.2 About the IoT Cybersecurity Colloquium

The IoT Cybersecurity Colloquium [Colloquium] focused on challenges organizations face in managing the cybersecurity and privacy risks associated with the Internet of Things. Speakers from industry, academia, international bodies, and government explored the current threat landscape, as well as challenges and considerations specific to the IoT ecosystem. Speakers also discussed practical risk management considerations for IoT deployment, protection, and operation over the course of the device lifecycle.

Time	Topic
9:00 AM	**Opening Session** **James St. Pierre** *Deputy Director, Information Technology Lab* **Katerina Megas** *Program Lead, NIST Cybersecurity for IoT Program*
9:30 AM	**Andrew Sullivan** *Fellow, Oracle Dyn* "The Internet of Infrastructure Threats"

Time	Topic
10:00 AM	**Yasser Shoukry** *Assistant Professor, University of Maryland* "Sensor Spoofing: Attacks and Consequences"
10:30 AM	**Joe Jarzombek** *Global Manager, Software Supply Chain Solutions, Synopsys Software* "IoT Supply Chain Management: Reducing Attack Vectors & Enabling Cybersecurity Assurance"
11:00 AM	**Jeremy Grant** *Managing Director of Technology Business Strategy, Venable* "Identity and the Internet of Things"
11:30 AM	**Carlos Bosch** *Head of Technology, GSMA North America* "Mobile IoT Security"
12:00 PM	**Matthew Eggers** *Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce* "IoT Cyber Policy"
12:30 PM	Lunch
1:30 PM	**Gilad Rosner** *Founder, Internet of Things Privacy Forum* "The IoT Privacy Threat Landscape"
2:00 PM	**Andrea Arias** *Bureau of Consumer Protection, Federal Trade Commission* "Internet of Things: Consumer Landscape"
2:30 PM	**Arabella Hallawell** *Senior Director, Advanced Threat, Arbor Networks* "Devices Without Identity: Internet of Things in the Enterprise Network"
3:00 PM	**Adjourn**

IoT Cybersecurity Colloquium Agenda

In holding the Colloquium, NIST sought to hear from stakeholders about IoT cybersecurity and privacy concerns, and understand practical cybersecurity and privacy risk management considerations for IoT. To facilitate this, the Program asked attendees to come prepared to share their perspectives on a variety of questions, presented in the "Security and Privacy Considerations for IoT" Pre-Read Essay [Essay].

Video and the slides from each presentation are available on the IoT Cybersecurity Colloquium web page. Based on feedback collected from stakeholders, this report provides a summary of key conversation points and a general discussion of possible follow-on activities for the Program.

2 Summary and Key Takeaways

The summary below identifies takeaways and observations from the event. It does not necessarily indicate attendees' unanimous support, nor is it intended to represent all the thoughts, opinions, and suggestions provided during the sessions.

2.1 Defining the Internet of Things

There is no consensus amongst industry on how to define the Internet of Things, which the Colloquium reflected. Some speakers provided a description or scope of IoT, while others left it open-ended. One speaker described IoT as "'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate, or transmit information with or between each other through the internet." Another speaker said that "devices or things are not full-fledged computers" but are instead "purpose-built items" that "have sensors… can communicate over networks… [and] bridge the physical world with the electronic one." Furthermore, there was no consensus on whether developing such a definition would be useful. While some thought scoping IoT would have benefits for cybersecurity and privacy discussions (e.g. to determine an organization's goals), others argued that any set definition would be too limiting in a rapidly evolving field.

2.2 IoT Cybersecurity and Privacy Risks

The IoT ecosystem poses cybersecurity and privacy risks that extend beyond traditional data security. Over the course of the Colloquium, speakers addressed IoT-specific cybersecurity and privacy risks – including those posed by cyber, physical, and human elements. This section provides an overview of the IoT cybersecurity and privacy risks discussed at the Colloquium.

Speakers discussed how the introduction of IoT to networks and infrastructure has changed the cybersecurity and privacy risks organizations are facing, and how managing these cybersecurity and privacy risks has become increasingly difficult for IT security departments.

From a cybersecurity perspective, while once there was only a need to focus on protecting servers and databases from intrusion, CISOs and front-line professionals are now tasked with defeating well-funded attacks that in some cases can cause immediate physical harm. A single enterprise can have hundreds if not thousands of sensors, and monitoring for attacks in real time is resource-intensive. Traditional IT security systems offer very little defense against these cyber-attacks that can shut down power grids, smart traffic systems, and automobiles.

The ubiquity of IoT devices poses challenges for managing the personal information they collect and helping people understand how that information is processed by a system. IoT can – intentionally or unintentionally – lead to the direct collection of sensitive personal information such as geolocation, financial account numbers, and health information. Many consumers are unaware that devices already in homes can surreptitiously record and process their information. As speakers pointed out, from personal health information on wearables to cameras on baby monitors, consumers have an expectation of privacy that is currently not met.

When assessing their particular set of risks, an organization must consider the nature of a specific IoT device and how it is being used in order to identify any associated cybersecurity threats or

privacy problems. Over the course of the Colloquium, speakers demonstrated that the list of risks is extensive. It includes – but is far from limited to – opportunities for malicious actors to hijack communication channels, spoof sensor data, access sensitive information, disrupt vital services, and alter signals and data for nefarious purposes. Furthermore, while cybersecurity and privacy risks are present and need to be addressed throughout a device's lifecycle, cybersecurity and privacy are often an afterthought and not considered throughout the system development lifecycle.

Over the course of the Colloquium, speakers and attendees expressed a need for a framework or other type of guidance for assessing and scoping IoT cybersecurity and privacy risks in order to provide an informed approach to securing devices and the ecosystems in which they are deployed.

2.3 IoT-Specific Risks

Over the course of the Colloquium, speakers covered the cybersecurity and privacy challenges posed by a variety of facets of the IoT ecosystem. This section provides an overview of IoT-specific risks discussed during the presentations and conversations, but not a comprehensive review of all IoT cybersecurity and privacy challenges.

2.3.1 Need for Incentives

Speakers indicated that there is a lack of incentives to build cybersecurity and privacy into IoT devices. Cybersecurity is often an afterthought to getting to market, with price and features prioritized. There is also a general lack of consumer education leading to a lack of demand for better cybersecurity and privacy. There are guidelines available to help manufacturers mitigate the risk, but a lack of incentives to adhere to them. Furthermore, there is a communication gap between technical and executive professionals. Speakers noted this gap will likely continue to exist until executives and technical professionals are more aware of the potential consequences of an IoT cybersecurity breach or failure.

2.3.2 Sensors

Speakers noted that with the rapid proliferation of IoT devices comes a rapid accumulation of data – data that offers a host of insights while also posing a host of security and privacy risks. With such an increase in the volume of data, organizations have to consider how the data is processed. While there are methods for analyzing anomalies in data, it can be difficult to analyze massive amounts of data to find discrepancies in real time (which many IoT applications need), especially when dealing with a sensor attack.

The volume of sensor data can also be used by both attackers and legitimate users to compromise users' security and privacy. For example, smart meters can be analyzed to learn a person's TV watching habits; gyroscope orientation can be used to get the password or text from a phone based on how a user's hand is tilted while typing; and a bad actor can even learn health and religious information from a smart phone GPS location.

One of the speakers demonstrated how sensors are now a feasible attack vector, as they are used to understand a physical environment and gather information. This data informs decisions and

actions, and any spoofing can lead to unanticipated consequences. A spoofing attack could affect things such as a GPS in a boat, the anti-lock braking system in a car, or a pacemaker located in a human body. Even an attack on a phasor measurement unit, which measures electrical waves, could destabilize portions of a power grid.

2.3.3 Supply Chain

Supply chain threats are a concern in the IoT ecosystem as many manufacturers do not create the entire device. Speakers discussed how manufacturers often use components produced elsewhere, and that these components may be produced by suppliers whose cybersecurity practices are unknown to the manufacturer. Many threats exploit vulnerabilities in IoT components that were acquired via the supply chain during the development, modification, or support of these devices.

Component suppliers often have poor cyber hygiene, and these vulnerabilities are more of an issue than the ingenuity of the attackers. From these vulnerabilities, edge devices, IoT platforms, and the enterprise are all subject to hacking, snooping, and tampering.

2.3.4 Identity

A speaker explained that identity is critical to IoT because

- Most IoT devices connect to the cloud at some point;
- Human control of, and access to, these devices is generally controlled by traditional identity solutions; and
- A full-lifecycle approach to identity is needed to govern access to things on the Internet.

Most IoT devices are controlled by traditional identity solutions – most commonly username and password. Because bad actors frequently leverage weak identity management practices to access devices, it is necessary to take a full-lifecycle approach to identity management in the IoT – that is, considering cybersecurity and privacy in every stage of the device lifecycle, from design to deployment to retirement. Furthermore, these devices often come hard-coded with default passwords that cannot be changed.

2.3.5 DDoS

Analysis of recent attacks reveals that the scale of distributed denial-of-service (DDoS) attacks has rapidly increased in recent years. IoT devices are frequently leveraged in these attacks. According to the speakers, there are two types of DDoS attacks: one is a large volume of attacks against the service itself, and the other is a reflection attack where traffic is sent towards a targeted service. This rise is driven, in part, by profitability: this takes the form of bad actors using devices for attacks on individuals' banking information, as well as people who hire bad actors for espionage and to cause chaos, often making payments with bitcoin and stolen credit cards.

2.3.6 Patch Management

There were also discussions on the role of patching. While patching is important for ongoing device cybersecurity, it is not sufficient. There are too many exploits for patching alone to work, and there is concern about running out of time and money before bad actors do, given how quickly IoT changes.

3 Next Steps

In response to the concerns raised both in this Colloquium and in other Program activities, the NIST Cybersecurity for IoT Program will continue collaborating with stakeholders as we begin drafting guidance for IoT cybersecurity and privacy. The Program intends for the document to have broad applicability to address common high-level cybersecurity and privacy risks for IoT, and to introduce practical risk management considerations for IoT product selection, deployment, protection, and operation. As part of the guidance development process, the Program will engage with stakeholders for input. Furthermore, the Program will continue working with the NIST National Cybersecurity Center of Excellence on projects to demonstrate secure and privacy-enhancing IoT solutions.

Updates on Program activities and collaboration opportunities are available on the NIST Cybersecurity for IoT Program website.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
IoT	Internet of Things
NIST	National Institute of Standards and Technology

Appendix B—References

[Colloquium] IoT Cybersecurity Colloquium, National Institute of Standards and Technology, [Website], https://www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium.

[Essay] "'Security and Privacy Considerations for IoT' Pre-Read Essay," *NIST Cybersecurity for IoT Program*, https://www.nist.gov/sites/default/files/documents/2017/10/10/iot_colloquium_pre-read_1.pdf.

[Program] NIST Cybersecurity for IoT Program, [Website], https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program