IoT Security Update Resources

November 2017

The documents presented here examine key issues for security update capability for Internet of Things (IoT) devices.

The four documents below cover 1) technical standards for IoT updatability, 2) steps to secure IoT updates, 3) communicating to consumers about IoT security updates, and 4) incentives and trade-offs for stakeholders considering actions on IoT updates. Each document functions as a standalone resource, but all four documents are also available in consolidated format as one multifaceted resource.

I. Background

The proliferation of devices and growth in the Internet of Things (IoT) provides the opportunity for technical advances that could dramatically improve people's lives. As devices become increasingly integrated into society, security and safety risks to individuals, businesses, and society may increase without appropriate security measures.

Like virtually all computers and software, IoT devices inevitably carry security vulnerabilities of varying severity, which can create risk until those vulnerabilities are mitigated. Security updates are a key way to protect IoT devices when vulnerabilities are discovered and attacks evolve, though the method and capability of IoT devices to receive security updates varies across devices, services, and deployments. Security updating is not the only (or, depending on the system, the most critical) solution for reducing cybersecurity risk, nor does it provide complete device protection, but it is an important feature to consider for IoT security.

In Oct. 2016, the National Telecommunications and Information Administration (NTIA) launched a process to develop resources on IoT security updates. NTIA's goal was to strengthen private sector coordination on IoT security updates and help foster a market offering consumers more devices and systems that support security updates. The process was open to the public, transparent, and voluntary – facilitated by NTIA but led by participants that included diverse experts from industry and non-governmental organizations (NGOs). The participants identified issues related to IoT updates that they considered to be both critical and achievable opportunities, and ultimately produced the resources presented here by group consensus.

The intended audience for these resources is generally manufacturers and developers of IoT hardware, software, and services, but also can be used by those across the ecosystem, from ISPs to civil society. The recommendations put forth by the working groups are meant to be informative and voluntary, do not describe or replace any domestic or international regulation, and are not intended to create a legal standard of care for the IoT ecosystem, or to provide a foundation for future regulatory or statutory obligations.

We recognize that integrating and maintaining security update capability in IoT devices is not a trivial undertaking. It is the hope of the multistakeholder process participants that these resources will nonetheless be broadly helpful in promoting greater security for IoT devices and transparency for consumers. If there are any questions or feedback on these resources, IoT

update capability in general, or the NTIA multistakeholder process, please feel free to contact NTIA's Allan Friedman: afriedman@ntia.doc.gov.

Finally, an acknowledgement to the participants, commenters, and other stakeholders that provided input and effort to creating and disseminating these resources – thank you.

II. Resources on IoT Update Capability

Below are the four resources on IoT security update capability developed by the NTIA multistakeholder process.

1) Title: Catalog of Existing IoT Security Standards

Description: This resource is a catalog of existing standards and initiatives as they apply to IoT security patching and upgradability. This review focused on global standards initiatives and specifications primarily from industry groups, self-regulatory organizations, and non-governmental organizations. The intent is leverage ongoing efforts and properly document existing best practices, rather than reinventing redundant guidance.

Last Updated: September 12, 2017

2) Title: Voluntary Framework for Enhancing Update Process Security

Description: This resource is designed to support manufacturers in identifying and selecting appropriate, risk-based security features to mitigate vulnerabilities in the update process, as well as educating enterprise-level procurement decision makers on what to look for. Part I of this document provides an overview of basic security steps in an update process. Part II reviews the security risks of each step, and offers voluntary guidance on how they might be mitigated.

Last Updated: October 31, 2017

3) Title: Communicating IoT Device Security Update Capability to Improve Transparency for Consumers

Description: This resource outlines basic information that manufacturers can communicate to consumers about whether and how IoT devices receive security updates. The information is divided into two parts: 1) Three key elements that manufacturers should consider communicating to consumers prior to purchase (such as through, for example, product packaging labels, online retailer item description, or

other consumer-facing media), and 2) Three additional elements that may be communicated before or after purchase.

Last Updated: July 14, 2017

4) Title: Incentives and Barriers to Adoption of IoT Update Capabilities

Description: This resource provides an approach to identifying and analyzing incentives and barriers associated with IoT security update capability. The resource describes factors that contribute to IoT manufacturers and developers to embrace or resist device updatability, and proposes an approach to weigh security concepts in such deliberations.

Last Updated: November 2, 2017

END