Communicating IoT Device Security Update Capability to Improve Transparency for Consumers

07/18/17

Communicating Upgradability and Improving Transparency Working Group,
NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching,
Working Group Co-Chairs: Harley Geiger (Rapid7), Aaron Kleiner (Microsoft), Beau Woods (Atlantic Council)[1]

I. Introduction and Scope

Security of Internet of Things (IoT) devices is increasingly important to the security and safety of consumers, businesses, and others. 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. Consumers of IoT devices may desire basic information about their devices' security capabilities, particularly with regard to whether and how devices receive security updates. There is also interest on the part of many policymakers and technologists for promoting transparency for consumers about the security needs and capabilities of internet-enabled devices.[2] In support of this concept, some stakeholders have urged the development of an accessible means of communicating security information to consumers prior to purchase. Ideas include product packaging labels, consumer-facing websites, and more.

To advance that dialogue, this document outlines information that manufacturers can communicate to better inform consumers and the marketplace about IoT devices' capability to receive security updates (i.e., the "elements of updatability"). This document is not intended to recommend exact language manufacturers must use, nor a specific method or vehicle for communicating the elements to consumers.

It is also important to note that updates and patches do not offer complete device protection and are not the sole security measures IoT manufacturers or consumers should take. Manufacturers may also consider advising consumers and industry partners on additional security practices and policies that apply to the device, including prudent steps consumers should take to maintain device security – such as password management, physical security,

[1] This document is the output of a public-private sector working group convened by the National Telecommunications and Information Administration (NTIA), as part of NTIA's multi-stakeholder process to address IoT security upgradability. For more information about the multi-stakeholder process, please see NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (last accessed Jan. 13, 2017). This document does not describe or supersede domestic or international regulation and is not intended to create a legal standard of care for IoT device manufacturers, sellers, or others in the ecosystem, or to provide a foundation for future regulatory or statutory obligations.

[2] See, e.g., Commission on Enhancing the National Cybersecurity, Report on Securing and Growing the Digital Economy, Action Item 3.1.1, White House, Dec. 1, 2016, pg. 30, https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf. See, e.g., Department of Homeland Security, Strategic Principles for Securing the Internet of Things, Nov. 16, 2016, pg. 11, https://www.dhs.gov/securingtheiot.

securing home wireless networks, privacy protection, and more.[3] However, this document focuses on device security updates and does not discuss additional topics in detail.

To help identify the elements of IoT device updatability, this working group leveraged a broad range of inputs. The working group looked to IoT security guidance from government sources (e.g., Federal Trade Commission, Department of Homeland Security), non-profit organizations (e.g., Online Trust Alliance), and corporations (e.g., Microsoft), as well as public reporting about IoT security developments (e.g., Mirai botnet).[4] The working group also considered participants' personal and anecdotal experiences with internet-connected devices. The elements listed below represent the working group's consensus recommendations, drawn from participants' perspectives as technologists, public policy specialists, and other relevant disciplines.

II. Elements of IoT security updatability

The working group developed two categories of information about updatability that IoT device manufacturers should consider communicating: key elements and additional considerations. The first category lists what we determined to be the most important elements for transparency and informed choice, information that manufacturers should consider communicating to consumers prior to purchase. The second category lists considerations that may be helpful for consumers but are not as fundamental to updatability as the first category, and which may be made available to consumers before or after purchase.

The working group observed that the elements below can be communicated in a variety of ways, though consideration should be given to context and ease of understanding. For all these issues, the ideal level of detail and the method of communication may differ across manufacturers, software providers, and product and service categories, as well as across buyer types. These voluntary communications may evolve over time as threats, solutions, and products change, and as needed to be consistent with consumers' familiarity, expectations, and security needs.

[3] This information can draw, as appropriate, on government and private sector education efforts, and may include reference to best practices. See, e.g., Federal Trade Commission, Consumer Information, Online Security, https://www.consumer.ftc.gov/topics/online-security (last accessed Feb. 10, 2017). See also Federal Bureau of Investigation, Cyber Tip: Be Vigilant with Your Internet of Things (IoT) Devices, Oct. 13, 2015, https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices. See also Online Trust Alliance, Internet of Things Trust Framework, Jan. 5, 2017, https://otalliance.org/initiatives/internet-things.

[4] This document reflects input and comments on earlier draft versions that were received from various stakeholders participating in the NTIA's multistakeholder process, including comments provided by the Federal Trade Commission. See Federal Trade Commission, Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers", Multistakeholder Process on Internet of Things Security Upgradability and Patching, National Telecommunications & Information Administration, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf (last accessed June 25, 2017). We encourage readers to review the FTC's comments for the agency's perspective on IoT security updatability and related issues.

A. Key elements that manufacturers should consider communicating to consumers prior to purchase

A.1. Describe whether the device can receive security updates

This description could provide a simple statement of whether the device is capable of receiving security updates.

A.2. Describe how the device receives security updates

This summary could address the following questions:

- Can the device receive security updates automatically? Consumers may have different preferences about updates and security management. For example, those without a high degree of technical expertise may be interested in automatic updates.

- What user action is required to ensure the device is updated correctly and in a timely fashion? Understanding the steps consumers must take to keep the device updated might provide some indication of the level of end user commitment needed to maintain the device. If consumers must pay additional costs as a normal part of update support, such as a subscription or mechanics' fee to install each update, this might be helpful to note.

A.3. Describe the anticipated timeline for the end of security update support

Support for routine security updates typically ends as a device or software reaches the end of its lifecycle. If may be helpful to describe how long can consumers expect, at a minimum, the device to receive security update support. A specific date for when support begins or ends (e.g. Jan. 1, 2025, or one year after date of registration) may be preferable to a general time period, though companies may describe their product lifecycles differently. If the device will be supported indefinitely without foreseeable end, or if the duration update support is unknown, manufacturers might indicate this.

B. Additional elements that manufacturers should consider communicating to consumers before or after purchase

B.1. Describe how the user is notified about security updates

Does the manufacturer indicate to the user that an update is needed for the device, such as through an “action needed notification”? For example, this can be in the form of a “dashboard light”, email, optional subscription service offering affirmative notifications, or other channel of communication with the user. This information could also include the timing of updates, such

as if updates are available on a regular schedule. Manufacturers that wish to communicate this type of information could do so as a part of the description in element A.2, above.

B.2. Describe what happens when the device no longer receives security update support

Manufacturers may want to communicate when or whether the device ceases to operate or loses functionality when security support ends, whether the manufacturer charges for extra support with an extended subscription or turns over security update authority to another party, or whether the device continues to function without security updates and the user operates it at the user's own risk.

B.3. Describe how the manufacturer secures updates, or explain how the process is reasonably secure

Buyers may want to understand how manufacturers evaluate, verify or test the source, security or functionality of updates. The manufacturer may choose to reference a specific secure update standard or solution, but should consider balancing clarity and ease of understanding with completeness.

END