Communicating IoT Security Updatability

NTIA Multistakeholder Process on IoT Security Upgradability

Apr. 26, 2017

Presenter – Harley Geiger, Rapid7

Communicating Upgradability And Improving Transparency Working Group

Co-Chairs:

Harley Geiger (Rapid7)
Aaron Kleiner (Microsoft)
Beau Woods (Atlantic Council)

Working Group Mandate

Problem statement:

Internet of Things (IoT) users and consumers have difficulty determining the extent of security support for an IoT device without clear information regarding the manufacturer's commitments to security patching and updatability.

Mandate:

This Working Group will identify the critical elements of information that should be communicated to IoT users and consumers regarding device updatability, and will explore potential means of clearly communicating that information.

To Dispel The Preliminary Terrors

Footnote 1:

- The document is output of the multistakeholder process;
- The document does not describe or supersede any regulation;
- The document is not intended to create a legal standard of care or foundation for future regulation.

To Dispel The Preliminary Terrors

Intro and Scope:

- IoT methods and capabilities to receive updates vary widely;
- Not intended to recommend exact language manufacturers must use or a specific method for communicating;
- Updates are just one security measure and do not offer complete protection;
- Notes working group inputs.

Elements Of IoT Updatability

Two categories:

A. **Key elements** that could be communicated to consumers prior to purchase; and

B. **Additional elements** that could be communicated before or after purchase.

A. Key Elements

(that manufacturers should consider communicating to consumers prior to purchase)

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

- Simple statement.
- Allows for possibility that the device cannot receive updates.

A. Key Elements

A.2. Describe how the device receives security updates

- Manual or automatic?
- What user action is required for updates? Additional costs?

A. Key Elements

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

- Minimum period consumers can expect security updates.
- Specific date is preferable, if possible.
- If support timeline is indefinite or unknown, 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

- Proactive indication to user that an update is needed?
- Can be combined with A.2.

B. Additional Elements

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

- Does the device lose functionality?
- Extended subscription or third party support available?
- Or user may continue operating at user's own risk?

B. Additional Elements

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

- How does manufacturer verify source or test functionality of updates?
- Manufacturer may choose to reference a standard or solution.

Potential Additional Work

Examples of IoT security updatability transparency

- Existing communications in the wild, and/or
- Theoretical mock-ups demonstrating the elements in action.

Elements Of IoT Security Updatability

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

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

A.2 – Describe how the device receives security updates

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

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

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

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

Thank You!

Harley Geiger
Director of Public Policy, Rapid7
HGeiger [at] Rapid7 [dot] com
@HarleyGeiger

Draft available at:

https://www.ntia.doc.gov/files/ntia/publications/draft-communicating_iot_security_update_0426.pdf