675.55.8

Working Paper
Updating firmware of embedded systems in the Internet of Things

62nd meeting, 27-28 November 2017, Paris (France)

Introduction

Estimates vary considerably as to the number of Internet of Things (IoT) devices that will be online by 2020, ranging from 26 billion[1] to 50 billion[2]. Regardless of which number is correct, the fact remains that there will be an enormous increase in the number of Internet connected devices over the next few years.

There is no single agreed definition for the term "Internet of Things". One source[3] defines the IoT as "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*". The Internet Society interprets IoT in a broad sense as "*the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers*".[4]

The defining characteristic of devices comprising the IoT is their connectivity to a network and the ability to collect and transmit data, either wired or wirelessly, across the Internet. Connecting these

[1] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, Gartner news release dated 12 December 2013, available online at http://www.gartner.com/newsroom/id/2636073

[2] *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, Cisco White Paper dated April 2011, available online at* http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] Overview of the Internet of things, ITU Telecommunication Standardization Sector Recommendations http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[4] The Internet of Things: An Overview, The Internet Society, 2015, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

devices to the Internet provides benefits such as remote control, remote sensing and automation capabilities but also increases the risk that these devices, and the information they process, may be compromised.

The IoT ecosystem is far reaching and crosses many industry boundaries including, but not limited to, IT and Networks, Security and Public Safety, Retail, Transport, Industry, Healthcare, Consumer and Home, Energy, Buildings and more. IoT devices will typically be comprised of, or include, one or more embedded systems (stand-alone computing modules), each typically with a single dedicated processing purpose which together provide the necessary processing functionality of the IoT device. Such embedded systems will have limited CPU, memory, and power resources (so-called constrained devices) with "*specific design constraints including cost, size, weight, and other scaling factors*".[5] These constraints often mean that manufacturers don't incorporate a software/firmware update mechanism in their devices. Examples of IoT devices include connected environmental sensors (temperature, humidity, and pressure), light-bulbs, printers and cameras within a home security system.

Manufacturers of IoT devices tend to source components, such as embedded systems, for their products from third party suppliers. The upstream vendors of these sub components can produce millions of embedded systems in a given year, and any change in this supply chain is both time consuming and expensive. Due to the time-lagged nature of this supply chain, individual software components may be months to years old before being assembled into the final product.

The ubiquity of IoT devices, the variety of sensors they may include and their proximity to individuals, including the possibility of being embedded in the human body, significantly increases the likelihood that these devices will process (collect, manipulate, store, transmit) information about all aspects (e.g., physiological, behavioral, locational, etc.) of an individual's life. Given that many of these devices communicate on a device-to-device level, bypassing human interaction altogether, they give rise to significant potential risks to the fundamental rights and freedoms of individuals.

This Working Paper focuses on risks associated with the failure to update the firmware controlling the behaviour of an IoT device. It will also touch on some of the implications of successful updating (e.g., introduction of new capabilities unbeknownst to the individual). These risks include the potential for unauthorized collection, modification or disclosure of personal data captured by the device, as well as exploitation of device vulnerabilities for the purposes of using the device as a tool to compromise the integrity of other systems processing or protecting personal data. Devices such as desktop PCs, tablets, smartphones, smart TVs, entertainment systems in connected vehicles, etc. are excluded from the scope of this paper.

What is firmware?

Embedded systems will typically contain one or more microcontrollers with limited memory and processing power. The software installed on the microcontroller is highly specialized for the particular specifications of the microcontroller and for the specialized purpose. This type of software is commonly referred to as firmware and it provides the necessary instructions for how the device com-

[5] Terminology for Constrained-Node Networks, https://tools.ietf.org/html/rfc7228

municates with other computer hardware or the wider network. Firmware is stored in non-volatile memory (flash or read-only memory (ROM)) on the device.

Why does firmware need updating?

All types of software, even the most tested, can have errors. Some may be known by the manufacturer but not fixed in order to meet a manufacturing deadline, while others may only come to light after the device has been shipped. These errors, or bugs, will vary in severity. Some will be very minor and not cause any significant impact on the normal operation of the device. Others will be severe and may even cause the device to display abnormal behavior.

As with any software, there are a number of reasons why the firmware might need to be updated:

a) To add new **features**;
b) To **reconfigure** based on changing Internet protocols;
c) To fix firmware **bugs**; or
d) To replace **weak cryptographic algorithms** or **keys** (all cryptographic algorithms have an expiry date).

Bugs, which can allow an attacker to breach the security[6] of a device (i.e., a software vulnerability), can introduce threats to the wider network and, ultimately, to the data being processed by the device and to the individual(s) to which that data relates.

How can firmware be updated?

Ensuring that firmware is updated in a timely and correct manner is challenging enough with traditional computing devices. The characteristics that define embedded systems within IoT devices compound these challenges and present new ones.

Embedded systems often lack the means to offer the individual a simple or automated firmware update process, which can be used once the device leaves the manufacturer. This can be due to a number of factors, including the specification or design of the device. Firmware updates, if they are made available by the manufacturer, are typically posted to a support page for the individual to download and manually install. Manual installation often begins with the transfer of the firmware image by way of a standard or proprietary protocol, which may or may not authenticate the persons authorized to initiate this process. It will require transferring the firmware image to the IoT device, possibly by connecting to a web server built into the device, by connecting a USB stick to the device or by some other method. Note that some IoT devices may not have a traditional user interface, or may not have any user interface. Applying the update may be as simple as unpacking an archive of files, but may also require putting the device into a special state due to the security-sensitive nature of the firmware update. In this process, the configuration or personalization of the device by the individual, including any privacy settings, may or may not be overwritten, and require restoration. In any event, updating IoT device firmware may be very challenging for the average individual.

[6] A security breach is defined as exerting a negative effect on either confidentiality or availability.

Firmware update issues

There are a number of issues which must be considered in order to deliver a trusted and secure firmware update process, including but not necessarily limited to:

1. Devices may not be readily accessible, either physically or logically, making delivery of firmware updates difficult or impossible;
2. Devices may simply not be updateable, perhaps due to technical constraints, and therefore devices may need to be physically replaced with ones containing the updated firmware;
3. A heterogeneous network of devices (i.e., from multiple manufacturers) will receive updates on a different schedule with vulnerabilities fixed at different rates (or not at all) leaving the security of the network as a whole constantly in doubt;
4. Ownership or responsibility for updating devices owned by multiple organizations and individuals may be unclear or undefined;
5. Individuals need to be made aware that firmware updates are available and for these to be installed in a timely and consistent manner;
6. Firmware updates can change device functionality in unexpected, undesirable ways;
7. Firmware updates can fail, resulting in an unusable device which cannot be restored (e.g., the device may be “bricked”);
8. Even if only part of the firmware code needs to be updated, the update mechanism may not support partial or differential updates;
9. The firmware update process may be vulnerable to manipulation (e.g., manipulated code from untrusted sources can be unwittingly installed instead of the published firmware image, which may result in a security breach or corruption of the device);
10. The device may no longer be supported by the original manufacturer and the expected firmware update may no longer be available;
11. If a device cannot be updated or has become compromised, it may need to be isolated from the network; and
12. If the firmware update process is complex or time-consuming, individuals may choose the convenience of not updating over the marginal increase in privacy and security resulting from an update – especially if they do not understand how the update makes their device more secure.[7]

[7] See Arunesh Mathur & Marshini Chetty, *Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates*, Thirteenth Symposium on Usable Privacy and Security, at 175, July 12-14-2017, https://www.usenix.org/system/files/conference/soups2017/soups2017-mathur.pdf (mobile app updates). See also Kami Vaniea & Yasmeen Rashidi, *Tales of Software Updates: The Process of Updating Software*, 2016, https://vaniea.com/papers/chi2016.pdf (PC updates) and M. Fagan, et al., *A Study of Users’ Experiences and Beliefs About Software Update Messges*, 51 J. of Computers in Human Behavior 504 (2015), https://dl.acm.org/citation.cfm?id=2805432 (same).

Privacy and data protection risks

R1. Vulnerabilities in device firmware might provide attackers direct access to the sensors of the device, allowing them to activate the sensors and capture sensor data (e.g., camera pictures or audio recordings), or retrieve such data if they are stored in the device. Conspicuous targets are voice-controlled devices, IP cameras[8] and even toys[9].

R2. Attackers may try to exploit vulnerabilities in IoT devices to gain control over them and use them as a proxy for further illegal activities, which pose risks to privacy and data protection.[10]

R3. Attackers may also try to access other stored data derived from sensor data, like indications about when a particular person was present in the vicinity of the device.

R4. Attackers may also retrieve credentials stored on the device for access to background systems and possibly access sensor data stored there, or they may retrieve or manipulate cryptographic keys used to protect the communications of the device to allow for the capture of data in transit.

R5. If the IoT device is placed in a private home, sensor and derived data may contain information about the daily routine of people in the household, their behavior and habits. The information may cover long periods of time, but be retrieved in a single access operation.

R6. IoT devices placed in homes might also store other credentials of individuals (e.g., those used for sending emails or posting information in social networks on behalf of the individual), which may fall prey to an attack. These credentials would open the way for further intrusions.

Recommendations

When considering firmware updates in the context of embedded systems, it is important to take the security and data privacy aspects as a whole into account. The challenge is to adopt the same common security practices traditionally used to combat security threats within the IT industry (e.g., as secure booting, access control, device authentication, firewalls and intrusion protection systems, and updates) and apply them to the IoT domain.

In order to address the issues outlined in this Working Paper, the following recommendations are made:

Regulators, legislators and oversight bodies

M1. Promote the development and adoption of firmware update mechanisms across embedded systems;

M2. Promote efforts to educate businesses and individuals on issues regarding firmware updates;

M3. Promote projects which address device security vulnerabilities;[11]

[8] http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html

[9] Bundesnetzagentur removes children's doll "Cayla" from the market https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422

[10] https://krebsonsecurity.com/2016/iot-devices-as-proxies-for-cybercrime/

M4. Set requirements for the security of IoT devices marketed to individuals that include a duty to supply information about the firmware installed, about the time period within which updates for the firmware of the devices are made available for known vulnerabilities, and about the procedure individuals need to follow in order to guarantee that the latest security updates are applied to the product; and

M5. Set requirements for certification of IoT firmware update procedures according to relevant industry standards. These standards should take into account the various types of IoT devices. Certification is intended to address the variety of risks to be mitigated and to introduce security and privacy controls into firmware updates.

Device manufacturers

M6. Develop and implement a secure firmware update mechanism for devices which incorporates the possibility for seamless and rapid deployment of updates, preferably automatic updates, that minimizes the burden on individuals;

M7. If the firmware update process can be provided in an automated fashion, consideration must be given to privacy and security-friendly defaults and the maintenance of configuration options previously set by the individual whilst including provisions that allow individuals to select which updates to allow or refuse and the timing of those updates;

M8. Consider whether the update mechanism requires that only updates provided by authorized parties can be installed (automatically or otherwise) on authorized devices and ensure code integrity;

M9. Provide appropriate information to individuals regarding the security dangers of installing updates from unauthorized sources, as well as the dangers of not installing authorized updates, and the benefits of installing updates or enabling automatic updates;

M10. Develop and/or use open standards for common functionality, such as cryptography, and network connectivity;

M11. Adopt widely recognized good practices for security and privacy risk assessment as part of the device development lifecycle;

M12. Ensure that all third party suppliers provide on-going support to any firmware that might be included in the components they supply to the manufacturer;

M13. Inform individuals about the firmware installed, about the time period within which updates for the firmware of the devices are made available for known vulnerabilities, and about the procedure individuals need to follow in order to guarantee that the latest security updates are applied to the product;

M14. Establish and communicate a clear security support period for all devices developed. Tell individuals before purchase what security support they will receive and remind individuals when security support is about to end;

[11] The FTC hosted a prize competition that challenged the public to create a technical solution, or tools, that consumers could use to guard against security vulnerabilities in software found on the Internet of Things (IoT) devices in their homes. https://www.ftc.gov/iot-home-inspector-challenge.

M15. Provide timely updates to all devices within their supported lifespan;

M16. Consider low-cost alternatives for continuing support, such as releasing source code under an open source license for those devices which have an expired lifespan;

M17. Adopt a transparent approach to updates by providing full and comprehensive information regarding bug fixes and new features within software updates and any shift in the location where the processing takes place as a result of the firmware update;

M18. Allow for individuals to remain informed about firmware vulnerabilities and provide information on how to mitigate risks whilst updates are being developed; and

M19. Sufficiently test all firmware prior to deployment and rigorously test all updates to the same high standards.

Device owners (organizations)

M20. Acquire only devices for which security information and firmware updates are made available by manufacturers in a timely fashion, or mitigate any possible risks that may ensue due to firmware vulnerabilities in another well-defined way;

M21. Organizations should maintain an asset list, such that devices can be physically and logically located;

M22. Organizations should maintain a record of the architecture of their systems, the security safeguards they have implemented, and the nature and extent of data processed (including justification for that processing) by devices;

M23. Organizations should ensure they are alerted to the announcements of security vulnerabilities published by device manufacturers and act on such alerts in a timely manner;

M24. Organizations should have a documented and auditable process for the installation of firmware updates across all types of devices, including across multiple manufacturers, that includes integrity checks for any updates to be rolled out, and verifies that security and privacy related configuration settings are maintained or, respectively, newly set after the roll-out;

M25. Organizations should consider whether further testing over and above that conducted by the device manufacturer is required prior to installation;

M26. In the event that an organization considers it is not appropriate to install a firmware update, this decision should be documented with any mitigation measures that have been applied; and

M27. Organizations should have a defined policy outlining the process to shut down, isolate and/or quarantine devices from the network in the event of a serious vulnerability or security breach or at the time the maker of the device stops providing security information and updates for the product.

Device owners (individuals)

M28. Individuals should contact the device manufacturer if they have any questions about firmware updates for devices they own;

M29. Individuals should consider the published device lifespan and be aware that no updates may be available after this date;

M30. Individuals should consider enabling automatic firmware updates (where provided) or otherwise maintain the firmware of devices up to date;

M31. Individuals should obtain firmware updates only from trusted sources (such as directly from the device manufacturer’s website) or through the provided secure update mechanism, and verify their integrity if possible; and

M32. Individuals should be aware that rejecting the firmware update, perhaps through a fear of loss of functionality or stability, subjects the device itself and the wider network to unnecessary security vulnerabilities and, therefore, creates additional risks for themselves and all others coming into contact with the device.