Why Software Updates Are More Than a Security Issue

Challenges for IETF CoRE and the W3C Web of Things

Matthias Kovatsch
Siemens AG / ETH Zurich
matthias.kovatsch@siemens.com

Andreas Scholz
Siemens AG
andreas.as.scholz@siemens.com

Johannes Hund
Siemens AG
johannes.hund@siemens.com

Abstract—Software updates have become an integral part in modern software development, rollout, and support. In the desktop and mobile world, they are essential for security updates of networked systems. This aspect is just as important for the Internet of Things (IoT). Yet there is more: Firmware of IoT devices often represents the competitive edge in products, and hence needs to be confidential. This increases the requirements on resource-constrained devices, but also the infrastructure to roll out updates for billions of devices. Solutions such as BitTorrent are not available for constrained environments and approaches from Wireless Sensor Networks do not scale with the heterogeneity of the IoT. Finally, there are no best practices for the IoT yet. Given the lack of adequately large testbeds and the inaccuracy of simulations, we need to mature IoT devices and networks in the field. This is challenging the software update mechanism itself, but necessary to harden the IoT architecture in all its aspects.

Introduction

Multiple organizations are working architectures for the Internet of Things. oneM2M and OMA LightweightM2M, for instance, emerged from the domain of mobile network and equipment operators, which have a long history with device management. The IETF Constrained RESTful Environments (CoRE) Working Group and W3C Web of Things (WoT) Interest Group and envisioned Working Group, for instance, belong to the organizations that together realized the classic Internet and Web. All of them bring a lot of expertise to the table, yet all of them still have to investigate how the Internet of Things differs from their current know-how and best practices.

The Internet of Things is expected to be disruptive, allowing for whole new economy [1]. For this, disruptive technology needs to be deployed, breaking with old paradigms. At Internet scale, this requires experiences in the field to get architectures and technologies right. Simulations turned out to be too inaccurate to be fully prepared for deployment [2]; a lesson learned multiple times in Wireless Sensor Networks, a domain that has shaped today's idea of the IoT [3]. This domain also clearly identified the necessity of over-the-air updates to make deployments successful. However, the IoT is more than Wireless Sensor Networks and more complicated than mobile equipment alone. As members of the IETF CoRE Working Group, the IRTF Thing-to-Thing Research Group (a long-term support group for the IETF IoT cluster), and W3C WoT Interest Group, we are interested in discussing the best practices of today to investigate the right paths toward IoT software updates.

Challenges

Firmware, that is, software for embedded devices, often contains company secrets, as it provides large parts of the competitive edge in products. For instance, it might contain on-device analytics or optimized motor controls that were learned from privileged big data sets over a long period and optimized to meet the hardware constraints of the device. Thus, firmware updates need to be treated with confidentiality in some industrial scenarios. This burdens resource-constrained devices with a higher load. Furthermore, it complicates the distribution of updates.

This could be solved by splitting a monolithic firmware into modules that have different levels of criticality. This, however, also makes it hard for trust relations on embedded devices, which usually lack support for memory management, sandboxing, etc. In particular when application modules are safety-critical, they need a trusted platform to ensure correct behavior. In the context of IoT, trusted platforms go way beyond digital rights management. They need to provide a reliable level of accountability and digital forensics to answer questions such as who is liable when an IoT-enabled traffic system fails and leads to casualties. This has a direct impact on software updates, which may lead to various combinations of different modules and versions.

Another safety concern of IoT software updates is correct scheduling. A train must not become unresponsive due to updates in progress. Careful scheduling, e.g., only when in a depot, is necessary for such systems. This conflicts with the whole idea of automated and scalable updates.

In the desktop and mobile world, we have come up with powerful mechanisms to enable software updates at scale. Technologies such as BitTorrent or Avalanche allow for efficient distribution of software. However, they are not designed for constrained nodes and networks. Solution such as Deluge [4] for sensor networks can deal with the resource constraints. However, they assume a batch of identical devices that all run the same firmware. The heterogeneity of IoT devices enables new applications and business models, but also needs new approaches to software updates.

Conclusion

The different domains such as mobile, Web, and Wireless Sensor Networks can all provide valuable insights from different angles on the topic of software updates. For the IoT, their long history has to be reviewed together, so that new approaches can evolve that can also deal with the new challenges within the Internet of Things.

References

[1] C. MacGillivray, V. Turner, and D. Lund. “Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars” *Market Analysis 243661*. IDC, 2013.

[2] Gnawali, Omprakash, et al. "Collection Tree Protocol." *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2009.

[3] Barrenetxea, Guillermo, et al. "The Hitchhiker's Guide to Successful Wireless Sensor Network Deployments." *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*. ACM, 2008.

[4] Hui, Jonathan W., and David Culler. "The Dynamic Behavior of a Data Dissemination Protocol for Network Programming at Scale." *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*. ACM, 2004.