IoT Security Challenges and Ways Forward

Marcel Medwed
NXP Semiconductors Austria GmbH
Mikronweg 1
Gratkorn, Austria
marcel.medwed@nxp.com

ABSTRACT

Today 2.9 billion people, or 40% of the world's population are online. By 2020, at least 40 billion more devices will become smart via embedded processors. The impact of such Internet of Things (IoT) on our society will be extraordinary. It will influence most consumer and business sectors, impact education, healthcare and safety. However, it certainly will also pose a challenge from a security point of view. Not only will the devices themselves become more complex, also the interaction between devices, the networks and the variance in topology will grow. Finally, with increasing amounts of data and assets at stake the incentive for attackers will increase. The costs of cyber attacks in such setting are estimated to reach about 2 trillion USD by 2020.

Today, the IoT is just beginning to emerge. Unfortunately, when looking at its security, there is lots of room for improvement. Exploits reported at a steady pace clearly suggest that security is a major challenge when the world wants to successfully switch from an IoT hype to a real IoT deployment. Security, and security risk awareness, insufficiently present in today's consumer and developer mindset, are only a starting point. Once the requirement for strong security is widely accepted, there will be still the economical question of who is going to pay for security and its maintenance. Without enforcing certain standards by means of third party evaluation this problem is expected to be hard to get under control.

However, awareness and obligatory security levels do not remove the complexity from creating secure solutions. Therefore, most of the complexity needs to be abstracted by suitable platforms. Amongst other vital features such platforms need to provide a secure software update mechanism, a secure, yet convenient device pairing mechanism and the integration into a trust provisioning infrastructure. Furthermore, standards need to be decimated to an interoperable set which can be supported by such platforms.

Another interesting question evolves around hardware versus software security. In particular, it is debated whether requirements like tamper and fault resistance are relevant. In practice, there are several arguments for taking them into account. First and most importantly, every additional ring of defense renders carrying out unforeseen attacks harder. Second, we already know some and can expect more network attacks exploiting physical attack phenomenons, like for instance cache attacks, timing attacks or even faults induced by the Row hammer approach to come. Third, even though physical attacks are not directly seen as a requirement for smart home applications, IPR protection and the prevention of easy code exploit discovery might create a demand for code confidentiality. For this reasons it will be advantageous and more sustainable if such requirements can be fulfilled at very little costs. We present one way how this could be achieved for symmetric cryptographic primitives.

Keywords

IoT security, physical security

TrustED'16 October 28-28 2016, Vienna, Austria

© 2016 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-4567-5/16/10.

DOI: http://dx.doi.org/10.1145/2995289.2995298