Chapter 75
Where Do All My Keys Come From?

Andreas Daniel Sinnhofer
Graz University of Technology, Austria

Felix Jonathan Oppermann
NXP Semiconductors Austria GmbH, Austria

Christian Steger
Graz University of Technology, Austria

Klaus Potzmader
NXP Semiconductors, Austria

Christian Kreiner
Graz University of Technology, Austria

Clemens Orthacker
NXP Semiconductors, Austria

ABSTRACT

Nowadays, cyber-physical systems are omnipresent in our daily lives and are increasingly used to process confidential data. While the variety of portable devices we use excessively at home and at work is steadily increasing, their security vulnerabilities are often not noticed by the user. Therefore, portable devices such as wearables are becoming more and more interesting for adversaries. Thus, a robust and secure software design is required for the implementation of cryptographic communication protocols and encryption algorithms. While these topics are well discussed and subject to further research activities, the issue of provisioning the initial device setup is widely uncovered. However, the protection of the initial setup is as important as the protection of the confidential data during the time in use. In this work, the authors will present solutions for a secure initialization of security critical integrated circuits (ICs).

INTRODUCTION

Cyber-physical systems (CPS) and Internet of Things (IoT) devices are increasingly used in our daily lives. Generally speaking, IoT refers to the connection of our everyday objects with a network like the internet. Each of these devices is usually equipped with different kind of sensors to observe its environment, making the device a smart object. In combination with embedded systems, IoT promises to increase the quality of our daily lives by taking over simple tasks like controlling the room temperature and cooking coffee (Nest Labs, 2016). On the other hand, smart objects like wearables are becoming

DOI: 10.4018/978-1-7998-7705-9.ch075

more and more interesting for adversaries due to their increasing functionalities like internet capabilities, cameras, microphones, GPS trackers and other senor devices.

Furthermore, such smart objects are often deployed in unsupervised and untrusted environments raising the question about privacy and security to a crucial topic. Thus, a robust and secure software design is required for the implementation of cryptographic communication protocols and encryption algorithms. Moreover, tamper-proof solutions like secure elements and trusted platform modules are necessary to securely calculate cryptographic functions and to store confidential data or cryptographic keys. While cryptographic protocols and secure hardware architectures are well discussed and subject to further research activities, the issue of provisioning the initial confidential device setup is widely uncovered. However, the protection of this initial setup is as important as the protection of the confidential data during the time in use. Especially the protection of master keys is essential, because otherwise all security measures, which are based on such keys, are futile.

Due to the high quantity of produced chips – e.g. 8.8 billion secure elements for smartcard chips in 2014 (IHS Markit, 2014) – it is obvious that automatic methods are required to generate the trusted data needed for each chip. Otherwise an economical and practical production is infeasible. On the one hand, the system creating this data has to be designed flexible since every product can support different cryptographic protocols and thus, require different keys. On the other hand, the personalization system needs to fulfil high security requirements to prevent the risk that the generated data leaks during the production process to an operator – or even worse – to an adversary.

As revealed in 2015 by Edward Snowden, the secret master key of SIM cards, securing the 3G and 4G mobile communication channels was subject to such an attack (Begley & Scahill, 2015; Scahill, 2015):

The American "National Security Agency" (NSA) and the British spy agency "Government Communications Headquarters" (GCHQ) perpetrated an attack and hacked into the network of Gemalto. Gemalto produces, amongst other things, Smart Cards in the form of SIM cards and EMV (Europay, MasterCard, and Visa) chip cards. More precisely, the company generates and inserts an individual cryptographic key (a symmetric encryption key) into each SIM card during the personalization process of the manufacturing process. The inserted cryptographic key is used to secure the communication between the mobile phone and the cell tower of the mobile network operator. Mobile network operators purchase SIM cards in bulks with pre-loaded keys by Gemalto. Additionally, the mobile network operators get a copy of each key from Gemalto in order to allow their networks to recognize an individual's phone. For this purpose, Gemalto provided a file containing the cryptographic keys for each of the new SIM cards to the mobile network operator. The primary goal of this hack was to steal millions of such symmetric encryption keys to wiretap and decipher the encrypted mobile phone communication. By using the stolen symmetric encryption keys, the national agencies can decrypt any mobile phone conversation or text message sent by a mobile phone having a Gemalto SIM card. With this heist, no assistance from the mobile operators, or permission from the legal official court was necessary. To get inside Gemalto's network, social engineering attacks like phishing and scouring Facebook posts where used to take over the employee's PCs (Begley & Scahill, 2015). Once inside the network, the agencies were able to retrieve the cryptographic keys because Gemalto sent them via unencrypted FTP to the Smart Card manufacturing factories. According to Begley & Scahill (Begley & Scahill, 2015), millions of keys where stolen by GCHQ in a three-month period in 2010. This is a good example showing the impact of insecure data handling and how many users can be affected by hacking the personalization system of secure integrated circuits.