INFO-F-514 - Conference Report #1
Atos Wordline

Université Libre de Bruxelles

Hakim Boulahya

June 10, 2018

1 Introduction

During the conference of 28 March, Cedric Meuter talk about his activity in Atos Worldline company. The subject of the conference was the use of cryptographic technology within cashless banking payment. In this paper, we will propose a summary of the content of the conference. We will first describe fundamentals of security. Then we will propose a description of the important cryptographic protocol uses in the domain. Then an important part of the job in banking is to handle the keys used during the communication of the devices during a payment, we will then describe the key management as presented by Atom Worldline company. Finally we will propose some interesting details about engineering in security.

2 Fundamentals of security

It is important for a company to analyse the risk of the infrastrucutre deployed. Two important questions must be asked for (1) How likely an attacker will try to compromise you and acquire your data (2) What's the impact of the compromisation of your data. A good example of of an attack that highlights the importance of such risk analysis is the Sony Playstation Network Attack [Rai12]. Sony acknowledge that personal informations were stolen, including credit cards number. There are three important fundamentals of security: (1) Confidentiality (2) Integrity (3) Authenticity. With this informations, the goal of the protocols presented in the next section is to respect those fundamentals.

3 Cryptographic protocols and key management

The Payment Card Industry (PCI) must rely on standard to make sure that the transactions follow the fundamentals of security. Those standards used by the PCI are defined by different institution, such as NIST, FIPS or ANSI. An important protocol used in terminal payment is the DUKPT protocol defined in the ANSI X9.24 standard [ANS14].

3.1 DUKPT

DUKPT or Derived Unique Key Per Transaction, is at it's named says to generate a unique key per transaction. The goal of such a protocol, if a single transaction is compromised, it will not compromised the all infrastructure. To do so, it is necessary to have a centralized server, usually a Hardware Security Module, a centralized server that stores the keys and provides cryptographic functions. The algorithms need a secret key, called a Base Derivation Key or

BDK, to be able to generate a key for each terminal. Storing the BDK is very costly because if they are compromised, they can compromised a lot of devices. Therefore store new keys, developer must request to add a new key, and this will be done during a Key Ceremony, that will add the key to the HSM.

Each terminal as a secret key, based on the serial number, generate at factory by the HSM. To encrypt a transaction and process secret information, such as a PIN code, the terminal generate a number of key, and each key will only be used for only one transactions. Then the terminal send the encrypted data and it's serial number to the HSM. The HSM will be able to retrieve the key from the terminal, and regenerate the key used for the transaction, since it provides the cryptographic functions, and the key of the terminal was generated by the HSM.

3.2 Hardware Security Modules

The HSM is the devices (server), that allows to generate key for the terminals, and provides crypto-functions to handle the payements. The HSM stores multiple Base Deriviation Key, and with those will be able to generate per terminal keys, called Initial Key (IK). Those keys are loaded in factory in each terminal and will allow the terminals to generated the Trasanctions Keys.

References

[ANS14] Ansi x9.24 - pin security requirements. Standard, American National Standard Institute, 2014.

[Rai12] Costin Raiu. Cyber-threat evolution: the past year. *Computer Fraud & Security*, 2012(3):5–8, March 2012.