Jacob Fenton

Fitzwilliam

jf574

Computer Science Tripos – Part II – Draft Project Proposal

**Efficient Asymmetric Cryptography for RFID Access Control**

11th October 2017

**Project Originator:** Dr Markus Kuhn

**Project Supervisor:** Dr Markus Kuhn

**Director of Studies:** Dr Robert Harle

**Overseers:** Dr Sean Holden and Dr Neel Krishnaswami

**Introduction**

The current university access control system is based on the MIFARE Classic smart card, which conforms to ISO 14443 Type A, a standard for contactless integrated circuit cards to communicate with a “coupling device” (i.e. a smart card reader) over radio frequency. There are huge numbers of this particular card in existence – over 200 million are in use today.

The cryptography used in the card, a scheme named CRYPTO-1, was developed in-house by the manufacturer of the MIFARE Classic, NXP Semiconductors. NXP chose to keep the scheme secret, a practice known as security by obscurity. Such practice is eschewed by the security community because naturally, all cryptographic schemes are bound to have weaknesses and if researchers (or others) are not able to analyse a scheme, then they cannot provide advice as to how flaws within said scheme can be fixed. Furthermore, obscurity does not prevent others from deducing the scheme by observing it in operation and indeed, this was the case for CRYPTO-1. In December 2007, a presentation at the Chaos Communication Congress (an annual security conference) by two German researchers, Nohl and Plötz, described a partial reverse engineering of CRYPTO-1, as well as some weaknesses. They managed to do this by reconstructing the card’s electronic circuit from photos of the chip. They then verified their reconstruction by eavesdropping on the reader-card communication. Just a few months later, in March 2008, the Digital Security group at Radboud University Nijmegen revealed a complete reverse engineering of the scheme and were able to clone and manipulate the contents of a MIFARE Classic card. The most serious attack they detailed in their paper can recover the card’s cryptographic key in under a second using only a laptop, without any pre-computation.

Talk about how symmetric enc makes system very vulnerable after just one card being compromised.

**Starting point**

**Substance and structure of the project**

**Success criteria and evaluation**

**Possible extensions**

**Timetable**

**Resources declaration**