Dismantling MIFARE Classic

F. Garcia, G. de Koning Gans, R. Muijrers,
P. van Rossum, R. Verdult, R. Schreur, B. Jacobs

13th European Symposium on Research in Computer Security (ESORICS 2008),
LNCS 5283, pp. 97-114, 2008.

DOI: 10.1007/978-3-540-88313-5_7

Nathan Wood

Summary

This paper focuses on the security vulnerabilities of the MIFARE contactless smartcard, and how to exploit those vulnerabilities with a few example attacks.

Appreciation

High level of detail would enable any person reading the paper to follow the experiement

Method fully explained

Vulnerabilities fully explained

Enables the reader to be able to understand the MIFARE classic enough to perform their own attacks

Criticism

No discussion from an ethical framework. The paper includes comments such as:

"We have successfully executed these attacks against real systems, including the London Oyster Card and the Dutch OV-Chipkaart."

However there is no mention as to the ethics of performing such attacks on real systems

Criticism

Under Pfleeger's basic moral principles:

The right to know
The right to privacy
The right to fair compensation for work

The writers of the paper are abusing their right to know without any respect for the right to the privacy of the companies which are using the MIFARE system.

Criticism

The paper contains a Consequences and Conclusions section where this information could be placed. It only mentions:

- Some potential of the MIFARE classic is not being used in public
- In most cases it is not the only security mechanism in place

Could contain information on the ethics behind why they are performing the attack, or at least the possible future applications of their paper.

Question

Can you think of an ethical framework in which performing attacks on real life systems such as the London Underground and explaining how do to so would be acceptable?

What do you think the implications of releasing such information might be?