FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Diplomarbeitspräsentation

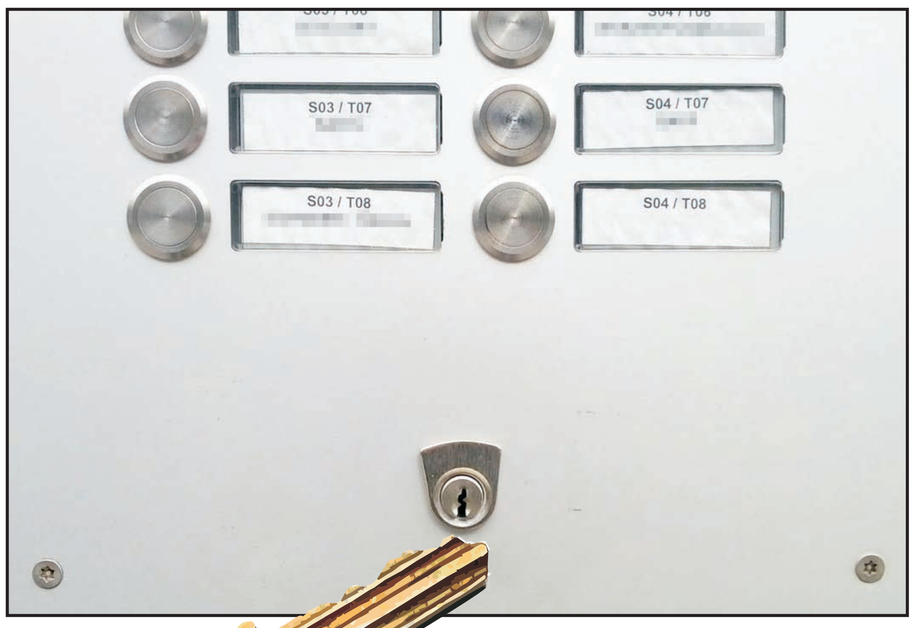
Security Analysis of Metropolitan Locking Systems Using the Example of the City of Vienna

Masterstudium:
Software Engineering & Internet Computing

Adrian Dabrowski

Institut für Rechnergestützte Automation
Arbeitsbereich: Automatisierungssysteme
Betreuer: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Wolfgang Kastner
Mitwirkung: Dipl.-Ing. Mag.rer.soc.oec. Dr.techn. Gilbert Wondracek

1 Introduction



The large circulation of “Z” or “BG” keys makes many people uncomfortable.

In Vienna, 92% of residential buildings are equipped with a system to allow access for postal delivery, emergency services and maintenance personnel. The mechanical key is currently available for €10-20 at many locksmiths under the counter. Since 2006, house owners can replace the old mechanical key by an RFID based system named “BEGEH”.

The new system promises more control: Only accredited companies are handed over RFID keys. The house owner can allow certain user groups (e.g. mail service) but deny others (e.g. advertisements).

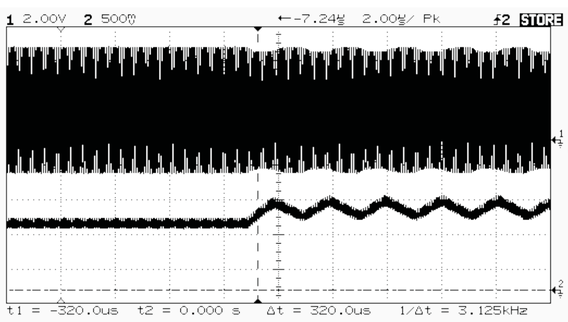
2 Analysis and Contribution

1) Normal user cards can easily be read out, but require a card simulator for exploitation because they are UID dependant. We built one ourselves for €20.

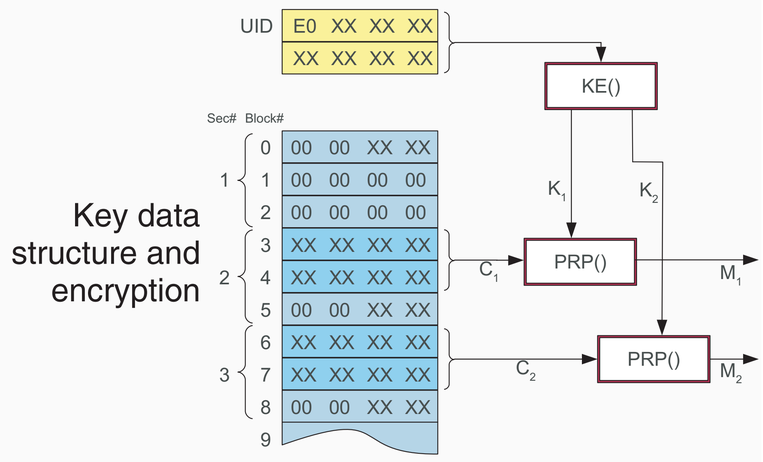
2) A specific card type (Baucard) can be manufactured out of any compatible transponder, such as an old ski ticket.

3) Cards have low UID entropy.

4) The blacklist feature is not updated frequently enough to be effective.



Sniffing card communication

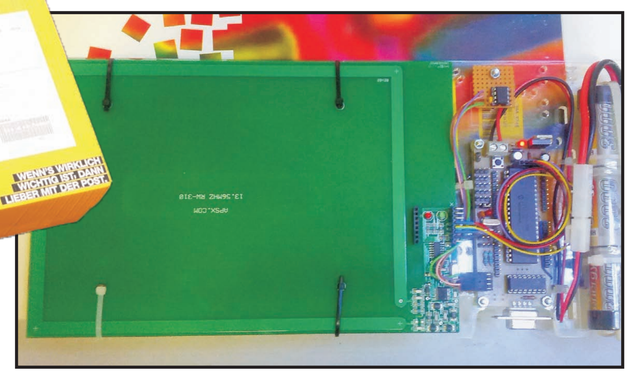


Key data structure and encryption

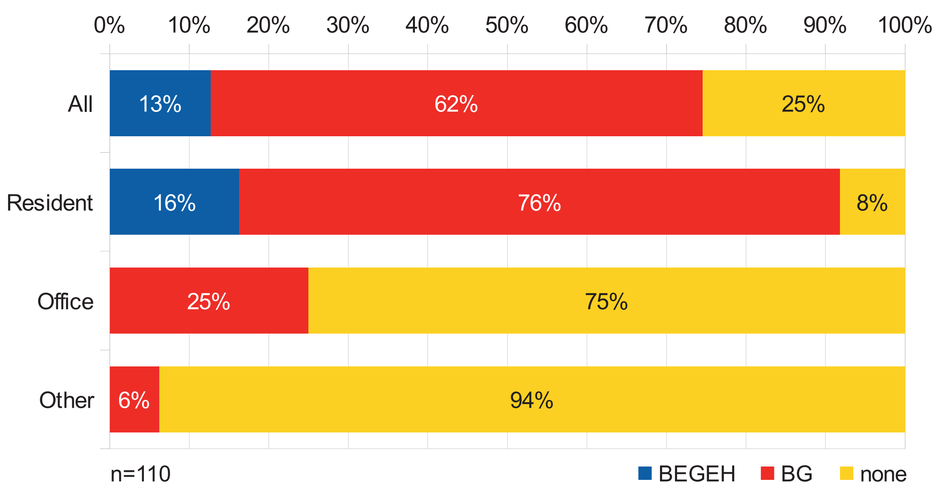
3 Experiment

In an experiment, we put a mid-range RFID reader into a post package and sent it to a building equipped with the BEGEH system. We successfully recorded the key. Later, we used the gained data with a card simulator.

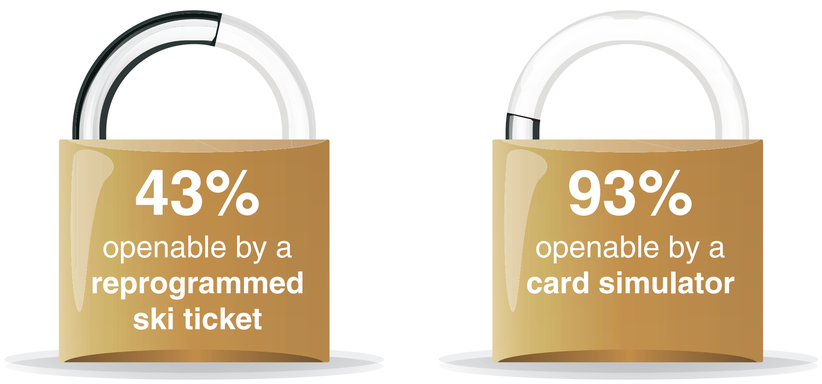
Pressefoto: Post.at



4 Field Test Results and Outcome



Results: 16% of residential buildings in Vienna switched to the electronic RFID system by the end of 2012.



Of these RFID installations, 43% can be opened using a manipulated ski ticket and 93% by simulating a post access card or fire brigade card.

Opening a house entrance to a staircase using an old reprogrammed ski ticket.

COMET Competence Centers for Excellent Technologies

secure sba-research.org

iseclab

Kontakt: dabrowski@seclab.tuwien.ac.at