Dismantling MIFARE Classic

Flavio D. Garcia,
Gerhard de Koning Gans,
Ruben Muijrers,
Peter van Rossum,
Roel Verdult,
Ronny Wichers Schreur,
and Bart Jacobs

13th European Symposium On Research In Computer Security
(ESORICS 2008)

Presented by Oran Ryan

Summary

- Description of MIFARE Classic
  - Its use in public transit systems
- Reverse Engineering of the MIFARE Classic chip
  - Through recording / studying the communication between the card and reader
- Successfully recovers encryption and authentication protocols
- Found concrete vulnerabilities!
  - These are used to propose & execute two attacks on the reader to recover it's secret key

Appreciative

- Paper follows a very clear, logical structure
- Progresses from general description of MIFARE through stages of analysis & examination
  - Beneficial, as it describes the practical reverse engineering of the device.
    - Allows the reader to follow logic of the researchers, even if the reader is not experienced in field specifically.

Critical

- Consequences & Conclusions section
  - Unlike previous sections of the paper, this section is rather disjointed.
  - Particularly, mentions specific capabilities of the MIFARE chip, which are unreferenced anywhere else in the paper:
    - Decrement only counters
    - Random Sector authentication
      - But, an entire section was spent on Multiple Sector Authentication for the attacks, why not Random Sector Authentication?

Question

- Should the developers of contactless smart cards be required to publish their cryptographic systems prior to their use in public systems?