Analyse des Studentenausweises und daraus resultierende Hacks

03.06.13 - Gerhard K.

Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Relevanz

- InterCard wird verwendet in:
  - Universitäten
  - Hochschulen
  - Studentenwerke
  - Unternehmen, Kliniken, Freizeit
  - Bibliotheken
- Studentenausweis ersetzt Bargeld in vielen Unis/Hochschulen
- Studentenausweis wird als Schlüssel zu Räumen genutzt

Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

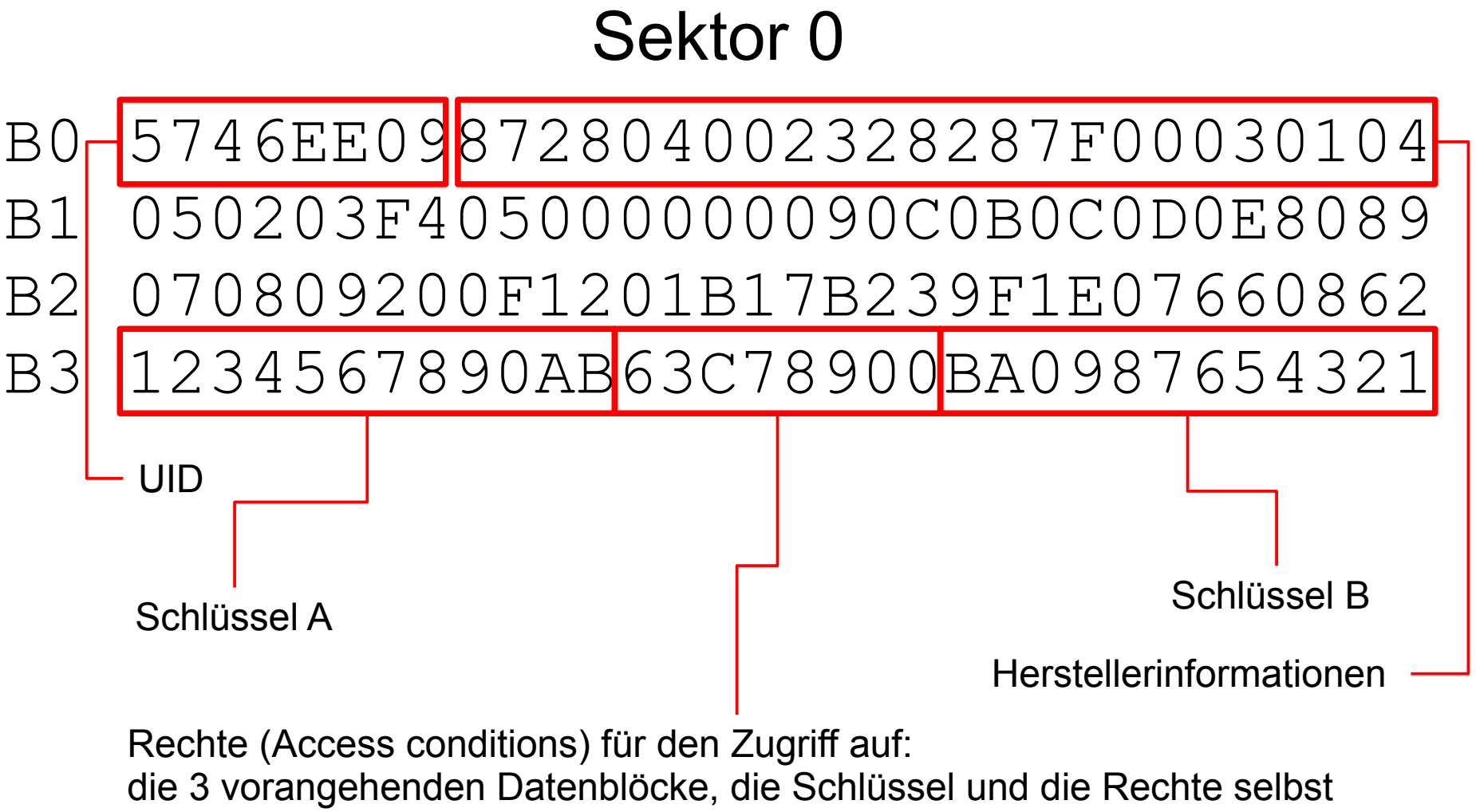
MIFARE

- *„MIFARE von NXP Semiconductors ist die weltweit meistgenutzte kontaktlose Chipkartentechnik“* - Wikipedia
- MIFARE = Mikron Fare Collection System (Ursprünglich für den Nahverkehr gedacht)
- Bei sehr vielen Studentenausweisen im Einsatz, da billig
- Verschlüsselung (Classic) seit 2008 unsicher (Danke an Plötz & Nohl & Co, CCC ;-))

MIFARE - Technik

- RFID-Technik (ISO/IEC 14443a) auf 13,56 Mhz
- MIFARE Classic 1K:
  - 16 Sektoren
  - 4 Blöcke pro Sektor (3xDaten, 1xSectorTrailer)
  - 1 Block hat 16 Byte
  - 2 Schlüssel (KeyA/KeyB) für jeden Sektor
  - Rechte:
    (read/write für 'A', 'B', 'A|B' oder 'never')
    - Datenblockzugriff (für jeden Block einzeln)
    - Schlüssel- und Rechtezugriff

MIFARE - Beispielsektor



MIFARE - Value Block

- Besondere Formatierung für „increment“ und „decrement“ Operationen

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	value				value				value				adr	$\overline{\text{adr}}$	adr	$\overline{\text{adr}}$

Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Annahme - Raumzugang

- Zugang wird geregelt ohne Zugriff auf die Karte
  - Zugang über Freischaltung der MatrikelNr.
  - Möglicherweise noch weitere Daten (z.B. UID)
- Zugang verfällt nach einem Semester
  - Kartengültigkeit auch als Datensatz auf Karte enthalten
  - Oder: Zugänge werden zentral zurückgesetzt

Annahme - Kartenverlust

- Karte kann bei Verlust gesperrt werden
  - Sperrung anhand der UID
  - Sperrung anhand andere Daten auf der Karte

Annahme - Konten

- Geld- und Kopien-Konten vermutlich ähnlich
- Sinnvoll: Konten in „Value Block“-Format
- Möglicherweise nicht auf der Karte
- (Kontostände sind bekannt)

Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Schlüssel knacken

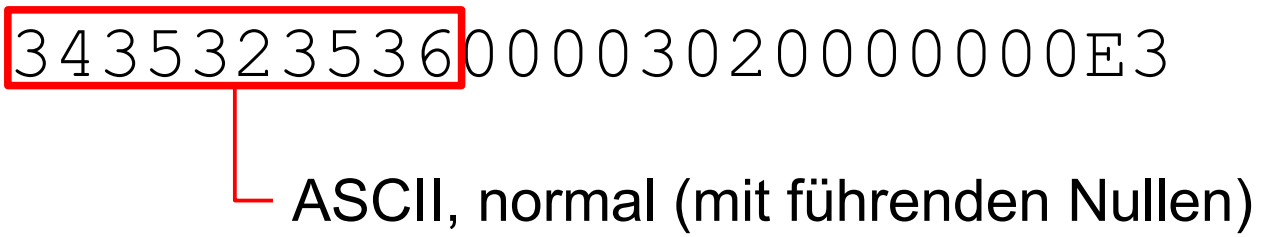
- Darkside Attack (Differential Attack)
  - Kann jeden MIFARE Schlüssel knacken
  - Dauer (auf Proxmark3) ca. 5-10 Minuten
- Nested Authentication
  - Wenn ein Schlüssel bekannt ist, können die anderen alle schnell errechnet werden
  - Dauer (auf Proxmark3) für 16 Sektoren ca. 10 Minuten

Inhalt

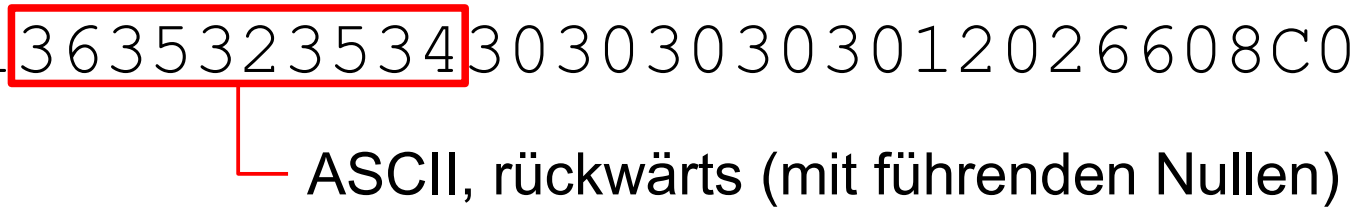
- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Analyse - MatrikelNr. (45256)

- Erstes Auftreten
  - Sektor 05, Block 0
  - Bsp. `303030343532353600003020000000E3`

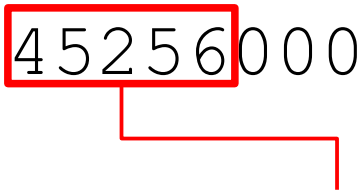


- Zweites Auftreten
  - Sektor 04, Block 0 und 1 (redundant)
  - Bsp. `313635323534303030303012026608C0`



Analyse - MatrikelNr. (45256)

- Drittes Auftreten
  - Sektor 03, Block 1
  - Bsp. `3100000000452560000040C10000067101A`

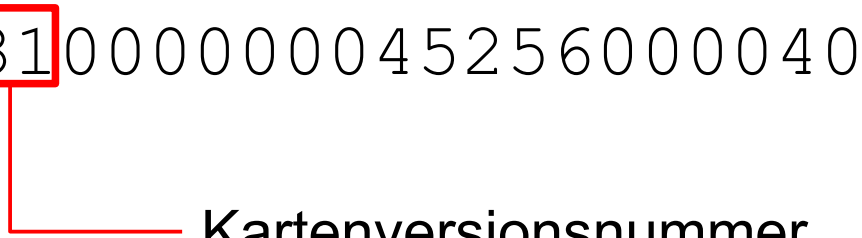


Hex aber dezimal lesbar (mit führenden Nullen)

Anmerkung: Abhängig von der Einrichtung kann die MatrikelNr. an ein oder mehreren Stellen durch eine KartenNr. (oder ähnliches) ersetzt sein.

Analyse - Kartenverlust

- Kartenversionsnummer
  - Sektor 03, Block 0
  - Bsp. 310000000045256000040C10000067101A



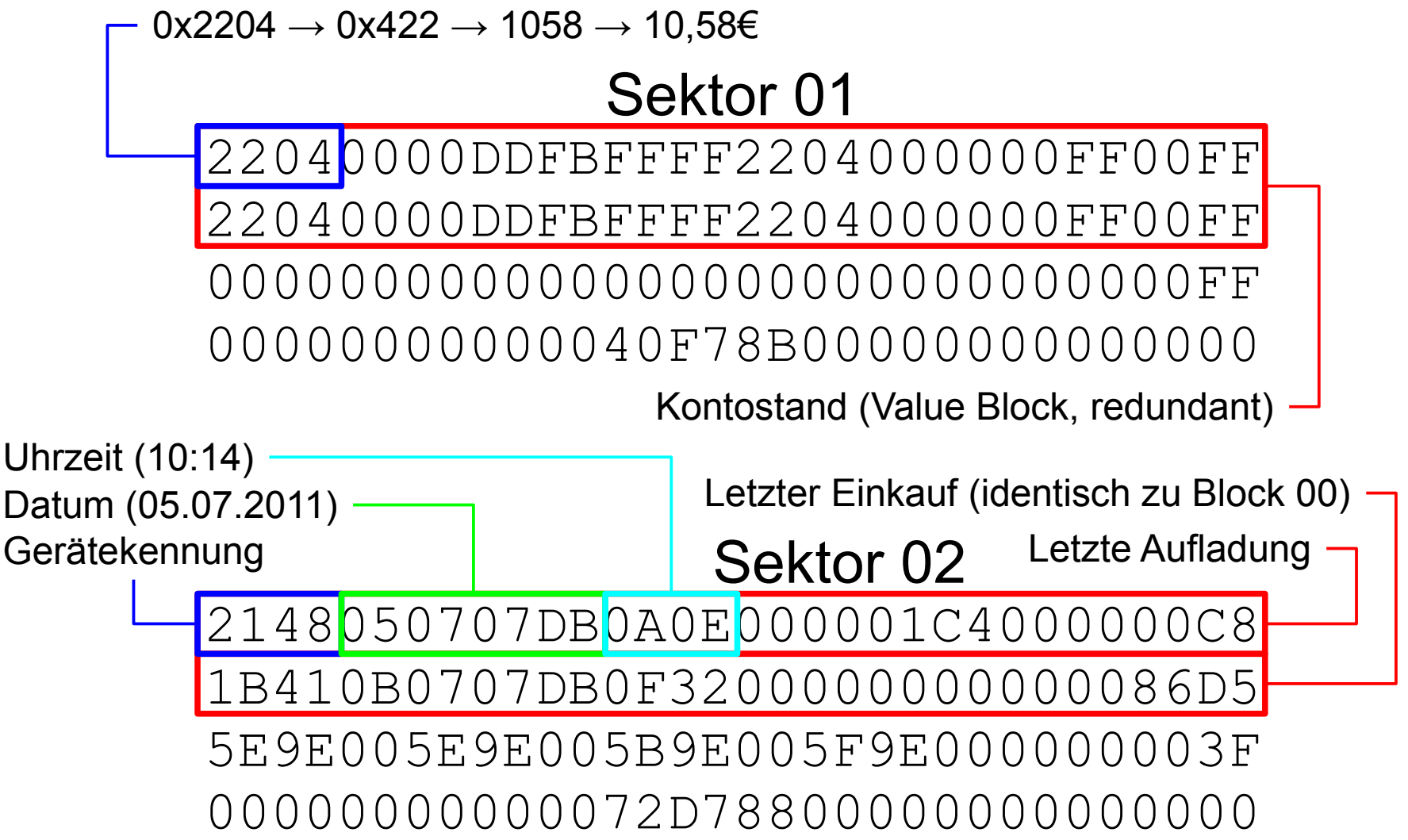
  - Sektor 04, Block 0 und 1 (redundant)
  - Bsp. 313635323534303030303012026608C0

Analyse - Konten

- Geld und Kopien sind identisch organisiert
- „Value Block“-Format
- Redundant (Block 00 und 01 eines Sektors)
- Folgesektor enthält
  - Gerätekennung
  - Zeitstempel

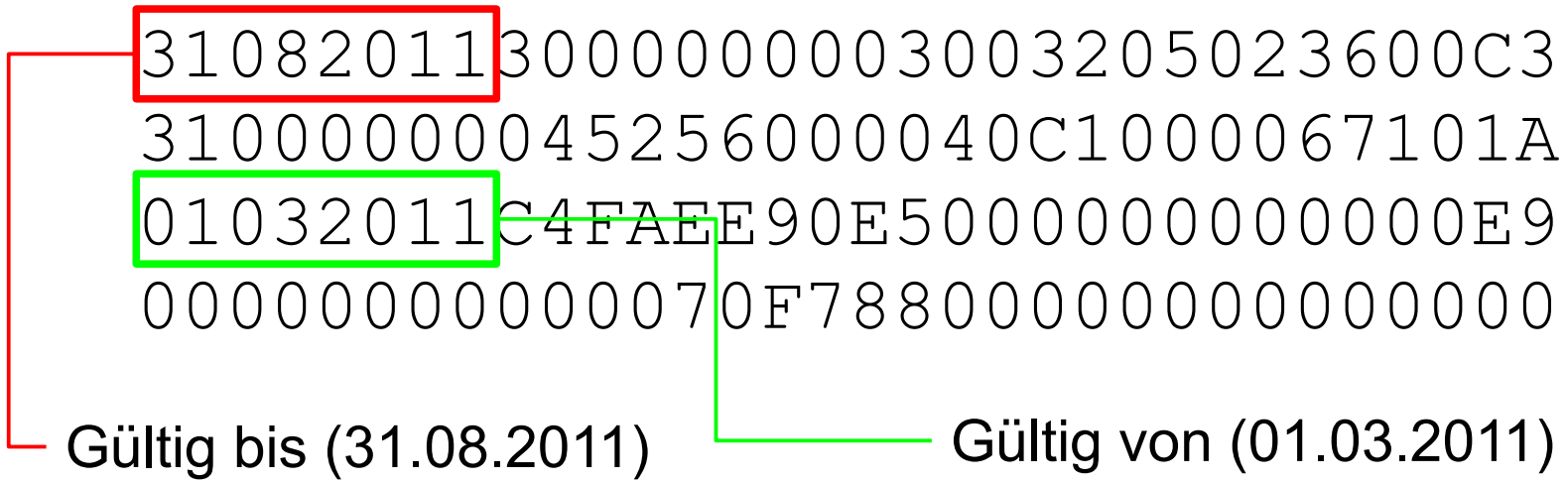
  der letzten Nutzung (Block 01) und Aufladung (Block 00)

Analyse - Konten - Beispiel



Analyse - Kartengültigkeit

- Kartengültigkeit (Sektor 03, Block 0, 2)



Analyse - Sonstige

- Es gibt mehrere ungenutzte aber initialisierte Konten
  - Gleiche Automatenkennung bei verschiedenen Hochschulen → Karten immer von InterCard initialisiert
- Ungenutzte Sektoren haben immer den gleichen Schlüssel
- Immer gleicher Schlüssel für Sektor 0 bei verschiedenen Einrichtungen
  (Wenn eigenes „InterCard MAD“ genutzt wird)

Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Hacks - Clone

- UID wird nicht (immer) beachtet
- Und selbst wenn:
  - Mit dem Proxmark3 kann eine komplette Karte (incl. UID) emuliert werden
  - Spezielle Karten erlauben das schreiben der UID und Herstellerinformationen

Hacks - MatrikelNr.

- Problem: Prüfsumme (1 Byte)

  `2148050707DB0A0E000001C4000000`**`89`**

  Prüfsummenbyte (hat fast jeder Block)

- Lösung:

```
B15 = 0xFF - (B0 v B1 v B2 v B3 v B4 v B5 v B6
     B7 v B8 v B9 v B10 v B11 v B12 v B13 v B14)
```

- Danach: Identitätsdiebstahl durch Manipulation der MatrikelNr. möglich

Hacks - Konten

- Problem: Jedes Gerät hat ein Ethernet Port! Wird das Konto zusätzlich auf einer Datenbank geführt? (Netzwerkabgleich mit Schattenkonto)
- → Ja!

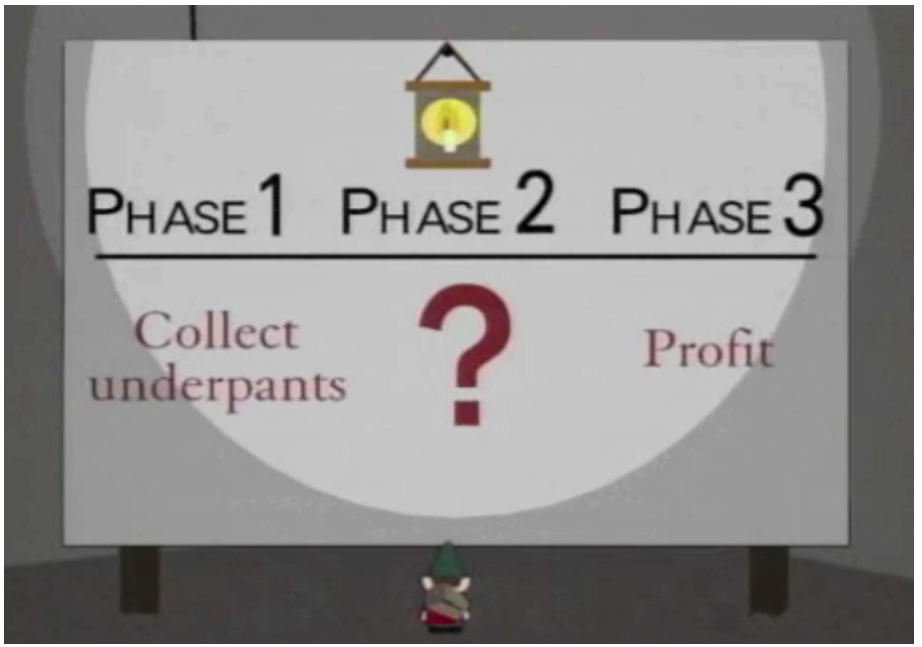
Hacks - Konten

Hacks - Konten

- Mögliche Probleme für ein Hack:
  - Was wird abgeglichen? Kontostand? UID? MatrikelNr.?
  - Was passiert wenn Daten nicht stimmen?
  - Wann wird abgeglichen?
- Lösung (Timo Kasper et. al):
  - Abgleich wird (vermutlich) **nach** Kartenzugriff durchgeführt
  - Manipulierte Kontostände werden angenommen
  - Falsche Personendaten werden angenommen

Hacks - Konten - Worst Case

- **Phase1:** Gastkarte besorgen (anonym)
- **Phase2:** Kontostand manipulieren (z.B. auf 50€)
- **Phase3:** An anderer Stelle die Gastkarte abgeben und verbleibendes Geld ausbezahlen lassen



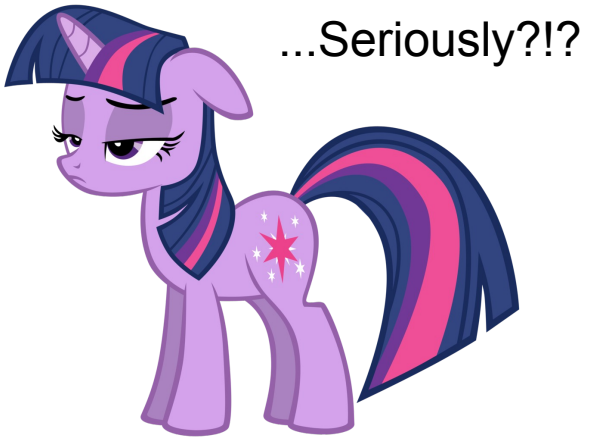
Inhalt

- Relevanz
- MIFARE
- Annahmen (Vorabanalyse)
- Schlüssel knacken
- Analyse der Daten
- Hacks
- Fazit

Fazit

- **MIFARE Classic**
- **Kontostand manipulierbar & virtuelles Geld ausbezahlbar**
- **Prüfsumme nicht kryptografisch (→ MAC)**
- **Schlüssel immer gleich (innerhalb einer Einrichtung)**

- UID wird nicht beachtet
- Karten Gültigkeit (Datum) wird beim Raumzugang nicht überprüft
- Schlüssel für ersten Sektor kundenübergreifend gleich
- Persönliche Erfahrung: Verlorene Karte wurde nicht gesperrt (nur vergessen!?)



Danke, Fragen?