

# TAN-Generatoren mit optischer Schnittstelle (Flickercode)

Andreas Schiermeier (schiirmi)

E-Mail: [andreas@schiermeier.name](mailto:andreas@schiermeier.name)

DECT: 3693

Jabber: [aschiermeier@imfarkt.de](jabber:aschiermeier@imfarkt.de)

# Ursprung & Verbreitung

- Weiterentwicklung aktuell kaum verbreiteter TAN-Generatoren
- Eingabe des Startcodes und Transaktionsparameter wird durch optische Übertragung ersetzt
- spezifiziert durch den ZKA (HBCI, FinTS, Geldkarte, ...)
- Marketingbezeichnungen
  - Sm@rt TAN optic (VR Banken)
  - chipTAN comfort (Sparkassen)

# Motivation

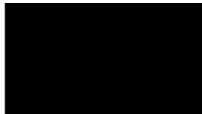
- Wie spielen die einzelnen Komponenten zusammen? Prüfsummenberechnung?
- Ergeben sich aus der Implementierung Angriffsmöglichkeiten?
  - Redteam Pentesting (MITM, 23. Nov 2009)
- Anwendungsbereiche neben dem Onlinebanking?

# Komponenten

- Lesegerät
  - Zifferntastatur
  - alphanummerisches Display
  - fünf Fototransistoren auf der Rückseite
    - Takt & binäre Stellenwerte: 1, 2, 4 & 8 => 0..F
  - Hersteller: ReinerSCT, VASCO, Kobil, Gemalto, etc.
- Bankkarte mit SECCOS-Chip („Geldkarte“)
- Flickercode (in Webbanking oder Onlinebankingapplikation)



# Flickercode

- Anzeigeoptionen in Webbanking
  - Javascript
  - Flash
  - animated GIF
- Eingabeparameter für Flickerroutine
  - z.B.: 0F04871851260333555414302C303106
- Übertragung mittels Blinkcode von Takt und vier Bits | 

# erster Schritt: Flickercode

- Spec nicht öffentlich zugänglich (HHD 1.3.2)
- optische Übertragung
  - Schleife aus Synchronisationssequenz und Datensequenz
  - Synchronisation

① ② ④ ⑧

① ② ④ ⑧

① ② ④ ⑧

① ② ④ ⑧

① ② ④ ⑧

① ② ④ ⑧

① ② ④ ⑧



# Flickercode

- optische Übertragung

- Daten

- Eingangsparameter: 0F0487...

- Übertragungsreihenfolge: F0 40 78 ...

F: **0 1 2 4 8**      0 1 2 4 8

0: **0** 1 2 4 8      0 1 2 4 8

4: **0** 1 2 **4** 8      0 1 2 **4** 8

0: **0** 1 2 4 8      0 1 2 4 8

7: **0 1 2 4 8**      0 **1 2 4 8**

8: **0** 1 2 4 **8**      0 1 2 4 **8**

...



# Aufbau Eingabeparameter

- Am Beispiel 0F 04 87185126 03 335554 14 302C3031 0 6
  - 0F: Anzahl nachfolgender Bytes (15 Bytes => 30 Nibbles => 30 hexadezimale Stellen 30\*4bit)
  - 0: Kodierung der nachfolgende Daten in BCD (0=BCD, 1=ASCII)
  - 4: Länge der Maskendefinition in Bytes
    - 87185126: Maskendefinition (sog. Startcode)
      - 8 = freie Maskengestaltung
      - 7 = Anzeige des Kontos
      - 1 = Anzeige des Betrages
      - 85126 = Zufallszahl
  - 0: Kodierung der nachfolgenden Daten in BCD (0=BCD, 1=ASCII)
  - 3: Länge des ersten Maskeninhalts in Bytes
  - 335554: Erster Maskeninhalt (hier: Empfänger-Kontonummer)
  - 1: Kodierung der nachfolgenden Daten in ASCII (0=BCD, 1=ASCII)
  - 4: Länge des zweiten Maskeninhalts in Bytes
  - 302C3031: zweiter Maskenparameter (hier: Betrag)
    - 30 = ASCII (hex): 0
    - 2C = ASCII (hex): , (Komma)
    - 30 = ASCII (hex): 0
    - 31 = ASCII (hex): 1
    - 0: unbekannte Prüfsumme
  - 6: XOR Prüfsumme über alles bis auf 0 und 6

- Wie berechnet sich die vorletzte Ziffer (Prüfsumme)?

# Links & Kontakt

- Slides & Listen mit validen Eingabewerten für die Flickerroutine

<http://bitinfarkt.de/chiptan/>

- Aufbau von Startcodes (<http://tinyurl.com/ya49qk4>)

[http://www.hbci-zka.de/dokumente/spezifikation\\_deutsch/Belegungsrichtlinien%20](http://www.hbci-zka.de/dokumente/spezifikation_deutsch/Belegungsrichtlinien%20)

- oberflächliche Beschreibung (<http://tinyurl.com/yddsq7z>)

<http://www.reiner-sct.com/index.php?option=content&task=view&id=162>

- Redteam Pentesting: Man-in-the-Middle-Angriffe auf das chipTAN comfort-Verfahren im Online-Banking (<http://tinyurl.com/yaua9b3>)

<http://www.redteam-pentesting.de/de/publications/MitM-chipTAN-comfort/-man-in-t>

# TAN-Generatoren mit optischer Schnittstelle (Flickercode)

Andreas Schiermeier (schiirmi)

E-Mail: [andreas@schiermeier.name](mailto:andreas@schiermeier.name)

DECT: 3693

Jabber: [aschiermeier@imfarkt.de](jabber:aschiermeier@imfarkt.de)