Nichts ist wahr, alles ist erlaubt!

Hacking Chipcards

auf die eine oder andere Methode

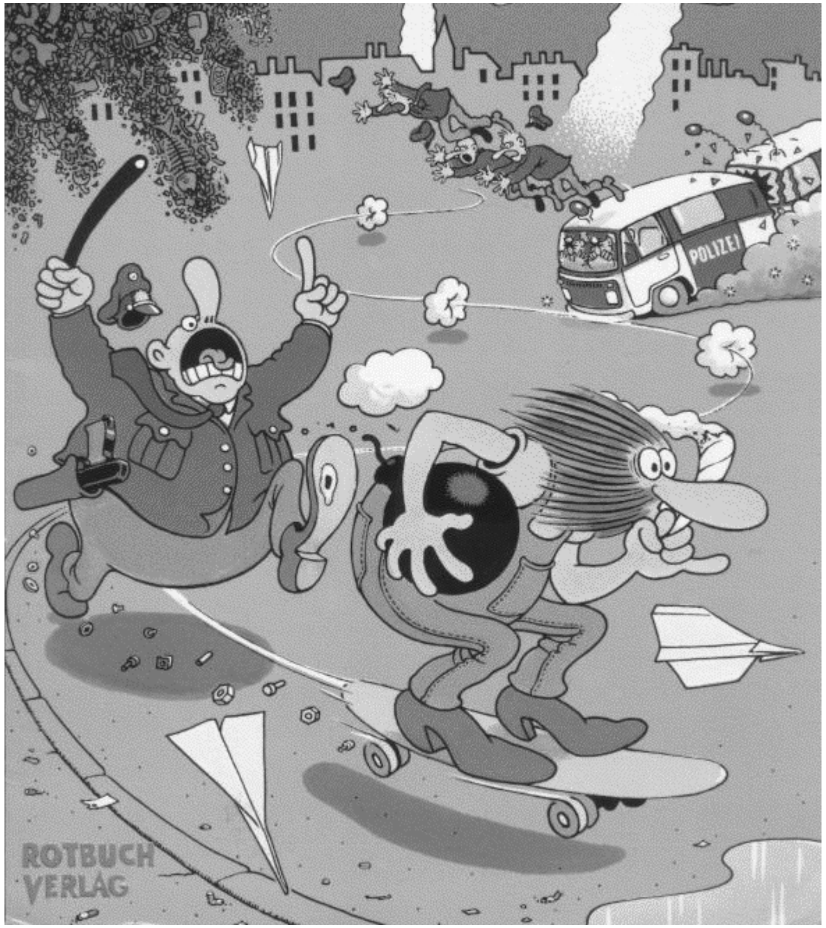
CHAOS COMPUTER CLUB

Communication Congress '97

Sonntag, 28.12. Workshop-Raum 1

Hacking Chipcards: Gewaltfrei

10 Uhr (Mitten in der Nacht!!!)



Referent:

Rüdiger Weis

“Lockpicking chipcards“

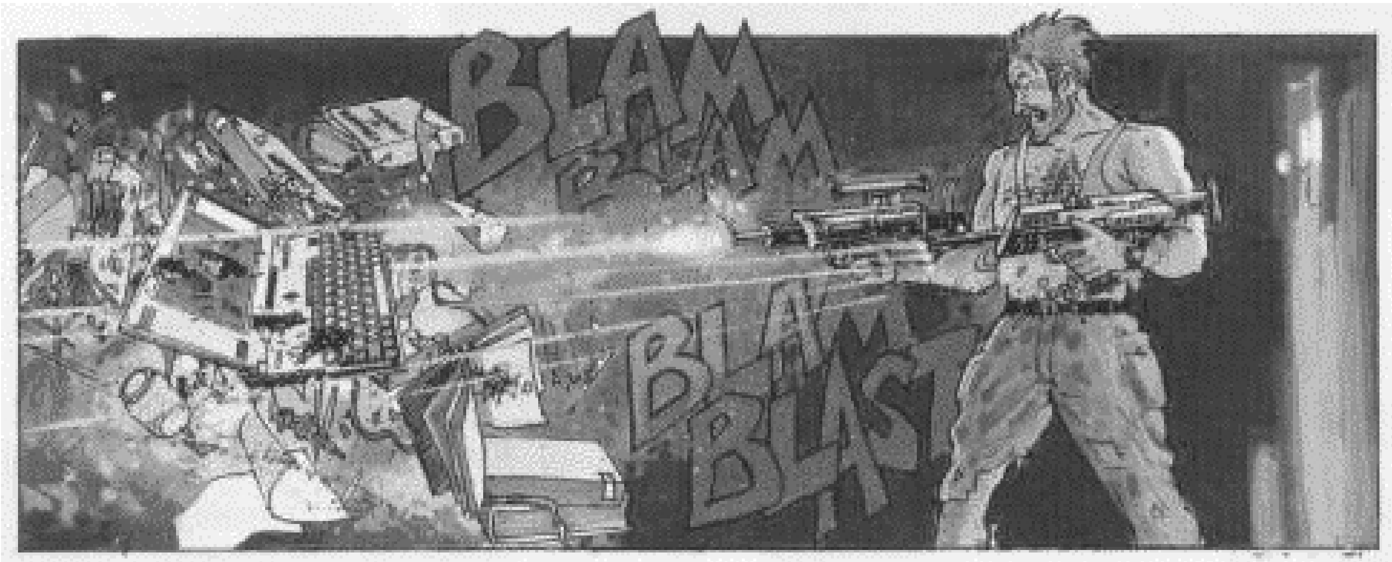
Hacking Chipcards: Gewalttätig

12 Uhr

Referenten: Markus Kuhn, Tron

Eher hardwareorientierte Methoden des schöpferisch kritischen Umgangs mit Chipkartentechnologie...

< Wir erlauben uns vorr. die Veranstaltung mit rechtlichen Hinweisen zu würzen.>



Hacking Chipcards: Anwendungen

16 Uhr

Referenten: Andreas Bogk, Markus Kuhn, Rüdiger Weis, Tron

Hacking Chipcards

auf die eine oder andere Methode
Teil 1: "Gewaltfrei"

Dipl.-Math. Rüdiger Weis

Lehrstuhl für Praktische Informatik IV

Rechenzentrum der Universität Mannheim

Agenda

- Exkurs: Probleme auf der Algorithmenebene
- Die Timing-Attack von Paul Kocher
- Die Differential Fault Attack (Bellcore)
- RSA(CRT)-Unsicherheit
- Zusammenfassung

Hacking Chipcards auf die eine oder andere Methode

- Analytische Angriffe
- Hardware-Angriffe
- Kombinierte Angriffe

Exkurs:

Probleme auf der Algorithmenebene

Unwissenheit, falsche Politik und Schwerfälligkeit der Verantwortlichen führen zu strukturellen Sicherheitsproblemen.

Würden Sie diesen jungen Leuten Ihre EC-PIN-Nummer anvertrauen?

Nein?

Aber warum lassen Sie sich dann von Ihrer Bank einen 56-Bit Schlüssel gefallen?

So einen knacken sie gerade mal wieder:

http://www.uni-mannheim.de/studorg/gahg/rweis/jungeleute.html

... und was sagt die Bundesregierung?

Deutscher Bundestag Drucksache 13/7753, 13. Wahlperiode 22.05.97

Antwort der Bundesregierung auf die Kleine Anfrage
des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS90/DIE GRÜNEN - Drs. 13/ 7594

Lage der IT-Sicherheit in Deutschland

"
...

* 40-Bit-Verfahren können - allerdings mit hohem zeitlichen und apparativen Aufwand mittels Hochleistungsrechnern oder auf dem Wege des "verteilten Rechnens" entziffert werden. Die genaue Höhe des Aufwandes ist verfahrensabhängig.

* **56-Bit-Verfahren erfordern zu ihrer Entzifferung den Einsatz von Spezialrechnern, die eigens zu diesem Zweck konstruiert werden müssen. Bei deren entsprechender Dimensionierung läßt sich der zeitliche Aufwand auf die Größenordnung von Stunden begrenzen.**

...
" (Hervorhebungen R.Weis)

DES ist unsicher!!!

Einfaches DES ist

mit 56 Bit Schlüssellänge

unsicher

gegen Brute-Force-Angriffe!!!

Stromchiffrierer RC4

- Erfinder: Ron Rivest 1987

- Variable Schlüssellänge
- 40 Bit exportierbar
- 1994 veröffentlicht (cypherpunks)
- Interessante neue Idee
- Zu wenig analysiert
- Eurocrypt ´97: Statistische Schwächen

RC4-Source

```
#!/usr/local/bin/perl -0777-- -export-a-crypto-system-sig -RC4-3-lines-PERL
@k=unpack('C*',pack('H*',shift));for(@t=@s=0..255){$y=($k[$_%@k]+$s[$x=$_
]+$y)%256;&S;}$x=$y=0;for(unpack('C*',<>)){$x++;$y=($s[$x%=256]+$y)%256;
&S;print pack(C,$_^=$s[($s[$x]+$s[$y])%256]);}sub S{@s[$x,$y]=@s[$y,$x];}
```

Beschreibung:

http://www.informatik.uni-mannheim.de/~rweis/rgp/rc4/

Blockchiffrierer RC2

- Erfinder Ron Rivest
- Variable Schlüssellänge
- 40 Bit exportierbar
- "Firmengeheimnis"

Veröffentlicht durch Posting in sci.crypt-Newsgroup

Internet-Draft

Internet Draft	Ron Rivest
draft-rivest-rc2desc-00.txt	RSA Data Security, Inc.
Created 1987	
Revised March 12, 1992	
Revised June 23, 1997	Expires December 22, 1997

A Description of the RC2(r) Encryption Algorithm

Properitäre Algorithmen

Nicht veröffentlichte Algorithmen sind

unsicher!

Wer Ihnen anderes erzählt ist ein

Scharlatan

oder

Geheimdienstmensch!

Die Timing Attack von Paul Kocher

Am 7. Dezember 1995 veröffentlichte Paul C. Kocher einen “gewaltfreien”Angriff auf verbreitete kryptographische Verfahren mittels Zeitmessung.

Angriffsszenario

- "Keine Gewalt"
- Der Angreifer kann die Zeit für die kryptographischen Operationen messen.

Diese Voraussetzung ist insbesondere bei der Analyse von Chipkarten gegeben.

Gefährdete Verfahren

Verfahren mit unterschiedlichem Zeitverbrauch für die kryptographischen Basisoperationen

insbesondere:

- Assymetrische Verfahren
  - RSA
  - DLP
- Symmetrische Verfahren
  - Rotationen (RC5, SPEED)
  - Tabellenzugriffe (DES, Blowfish, SEAL)
  - ...

Straigt forward RSA (I)

M	zu unterschreibende Nachricht
N	RSA Modulus
e	öffentlicher Exponent
d	geheimer Exponent der Länge w
E	Unterschrift

Straigt forward RSA (II)

- Zur Signatur einer Nachricht M wird M mit dem geheimen Schlüssel **d** potenziert:

$$E = M^d \bmod N$$

- Wegen der Symmetrie des Algorithmus kann der öffentliche Schlüssel **e** zur Verifikation der Signatur verwendet werden.

$$\begin{aligned} E^e &= M^{de} \bmod N \\ &= M \bmod N \end{aligned}$$

square-and-multiply

```
s[0] := 1;
(* es sei d der geheime Exponent mit Bitlänge w *)
FOR k = 0 TO w-1 DO
   BEGIN
   IF (k.Bit von d) = 1
      THEN
            r[k] = (s[k] * m) mod n
            (* Multipliziere *)
      ELSE
            r[k] = s[k] mod n;
            (* Multipliziere nicht *)
      s[k+1] = SQR (r[k2]) mod n; (* Quadriere *)
   END;
ModularExp:=r[w-1]; (* Ergebnis *)
```

Kochers Ergebnisse

- Pentium 120 mit einer RSAREF-Implementierung
- 512-Bit Modulus mit einem geheimen 256 Bit Exponenten
- ungefähr 2000 Signaturen
- erfolgreicher Angriff mit Bitkorrelation von über 95%.

RSASDI-Stellungnahme

http://www.rsa.com/rsaqa.htm:

- Q: Will this require a software change for manufacturers?

- *A: RSA recommends that its customers add "blinding" to their implementations as soon as is practical, however, because the described attack is as yet only theoretical, most manufacturers can probably safely wait to make the necessary modifications in the next regular release of their software.*

Blinding

- Die benötigte Zeit kann durch die Verwendung einer Zufallszahl **r** verschleiert (Blinding) werden.
- Statt der normalen RSA-Verschlüsselung

$$E = M^d \bmod N$$

sollte

$$E = r^{-1} (Mr^e)^d \bmod N$$

berechnet werden.

- Hierdurch soll es dem Angreifer unmöglich (“impossible”) gemacht werden, die Zeitabweichungen zu verwerten. Der zusätzliche Aufwand wird von RSASDI mit 10-20% beziffert.

Lösung: Worst Time

- Das Blinding benötigt einen "echten" Zufallsgenerator.
  (vgl. Kocher 96, Weis 97)
- Sicherste Lösung:
  "Maximal mögliche Dauer benötigen"

Differential Fault Analysis

Die “Alarm”-Nachricht, die am 27. September 1996 vom Technologieberatungsunternehmen Bellcore verbreitet wurde, löste ein mittleres Beben in der Geschäfts- und Wissenschaftswelt aus.

Eine Kombination von physikalischen und kryptoanalytischen Techniken liefert einen wissenschaftlich fundierten Angriff auf “einbruchsichere” Chipkartensysteme.

Der Bellcore-Angriff

Richard Lipton, Rich DeMillo, Dan Boneh

- "**On the Importance of Checking Computations**"
- Now, Smart Cards Can Leak Secrets (25.09.96)
- Bellcore Media Advisory (27.09.96)
  New Threat Model Breaks Crypto Codes
- Eurocrypt ´97

Eli Biham/Shamir

- A New Cryptanalytic Attack on **DES**: Differential Fault Analysis (18.10.96)
- The next Stage of Differential Fault Analysis: How to break completely **unknown cryptosystems** (30.10.96)
- Identifying the Structure of Unknown Ciphers Sealed in **Tamper-Proof Devices** (10.11.96)
- Crypto ´97

Anderson/Kuhn

- Improved Differential Fault Analysis
- Tamper Resistance - a Cautionary Note
- Ross Anderson: A serious weakness of DES Draft - (2.11.1996)

RSA(CRT)-Sicherheit gefährdet:
“One strike and you’re out

(Hardware)-Fehler stellen die Sicherheit der
meisten RSA-Implementierungen (CRT)
in Frage.

RSA Implementierungen mit dem Chinesischen Restsatz

- Verbreitet insbesondere auf Chipkarten
- Referenzimplementierung RSAREF
- Durch eine **einzige fehlerhafte** RSA-Unterschrift kann mit hoher Wahrscheinlichkeit der RSA-Modulus N **faktorisiert werden.**

(Damit kann der private Schlüssel bestimmt und beliebige Nachrichten gelesen bzw. Signaturen gefälscht werden.)

Realistische Fehlerannahme

- Praktisch beliebige Bitfehler
- Fehlerzeitpunktannahme realistisch

Zusatzproblem:

- Fehler fällt “Angreifer“ sofort auf

Sicherheit von RSA(CRT) bei Fehlern

- Boneh, DeMillo, Lipton (Bellcore):

  “On the Importance of Checking Cryptographic Protokolls for Faults”,

  EUROCRYPT ‘97 (Internetveröffentlichung: Sept ‘96)

  Eine falsche und eine korrekte Unterschrift

- Einfache Gegenstrategie möglich: random-padding

Lenstas Memo

- Arje Lenstra:

"Memo on RSA signature generation
in the precence of faults"

28. September 1996
Bei gleicher Fehlerannahme:

Eine *fehlerhaft RSA-Unterschrift reicht!*

Mathematische Begründung (I)

M	zu unterschreibende Nachicht
N	RSA Modulus
p, q	Primfaktoren von N
e	öffentlicher Exponent
F	sei die fehlerhafte Unterschrift
E	sei die korrekte Unterschrift

Mathematische Begründung (II)

Fehlermodell:

$$F = E \bmod q$$

$$F <> E \bmod p$$

Dann gilt

$$GGT(M-F^e, N) = q$$

und damit ist N = pq faktorisiert!

Lösung

- Überprüfung der Ausgabe durch **Verifizieren** der Signatur.

- **Problem:**
  Längere Signaturzeit
- **Alternative:**
  Protokolländerung: Randompadding mit **starkem** Zufallsgenerator
  (vgl. Weis 97)

Lage der IT-Sicherheit in Deutschland

Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDIS90/DIE GRÜNEN, Drs. 13/ 7594
"

Lage der IT-Sicherheit in Deutschland

...

51 .Welcher Sicherheitswert kann nach Auffassung der Bundesregierung Verschlüsselungsverfahren zugemessen werden, bei denen der Schlüssel auf Chipkarten gespeichert ist und damit die Analyse durch die "Differential Fault Analysis" erlauben?

Was meinen die “Experten“?

Deutscher Bundestag Drucksache 13/7753, 13. Wahlperiode, 22.05.97

Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDIS90/DIE GRÜNEN, Drs. 13/ 7594

Bis heute ist nicht nachgewiesen worden, daß eine “Differential Fault Analysis” - bei unbezweifelbarer theoretischer Machbarkeit - tatsächlich durchgeführt werden kann. **Sie erfordert im übrigen auch, daß der Schlüssel nicht nur auf der Chipkarte gespeichert ist, sondern dort auch verarbeitet wird.** Ferner kann diese Analysetechnik durch entsprechend redundante Systemarchitektur weitgehend blockiert werden.

(Hervorhebung RW)

Hauptvorteil von Chipkarten

Der geheime Schlüssel muß die Karte nicht verlassen!

Vorgeschrieben u.a. im Signaturgesetz!

Eine Bemerkung zur Geldkarte

- Kleingeldbeträge
  auf “sicherer” Chipkarte
- Trotzdem:
  Schattenkonto
- Fazit:
  Der Kunde ist immer der Dumme!?

Zusammenfassung

Es gibt keine
"einbruchsichere Hardware"

Weitere Informationen

- Zahlreiche und ständig aktualisierte Informationen zu den hier diskutierten Themen finden man unter

  http://www.informatik.uni-mannheim.de/~rweis/

  Danke für Eure Aufmerksamkeit!

ruediger.weis@informatik.uni-mannheim.de
PGP fingerprint = C8 B5 52 AC 05 EA C7 2A EB 31 E3 FB 65 DD 7A 76