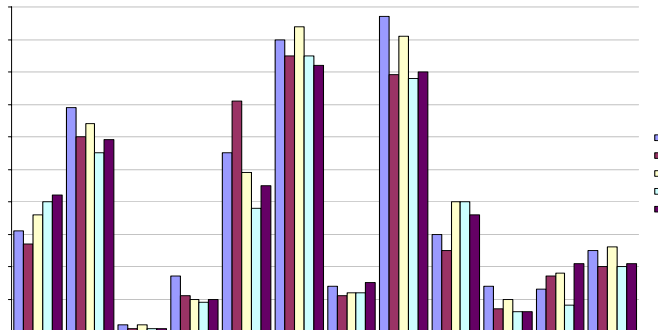


Was ist schon sicher ...

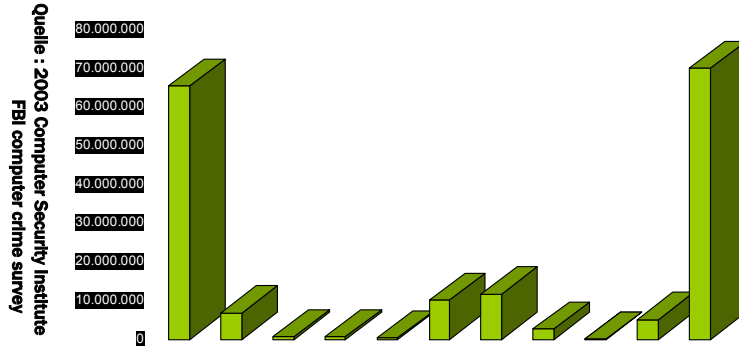
Jürgen Ecker
Computer- und Mediensicherheit
FH Hagenberg

Sicherheitsmängel

Quelle : 2003 Computer Security Institute
FBI computer crime survey



Schaden durch Sicherheitsmängel



11.05.2004

Wie großen Schaden richten Hacker wirklich an?

mi2G (computer security, Lodon):
Schäden weltweit im Oktober 2003

- Spam: \$ 10.4 Mrd.
- Viren und Würmer: \$ 8.4 Mrd.
- Hacker: \$ 1 Mrd.

Quelle: The Washington Times; 2003/11/10

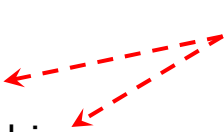
11.05.2004

The weakest link

Sicherheitsprobleme können an allen Enden auftreten, nur in den wenigsten Fällen, kann man Sicherheit garantieren.

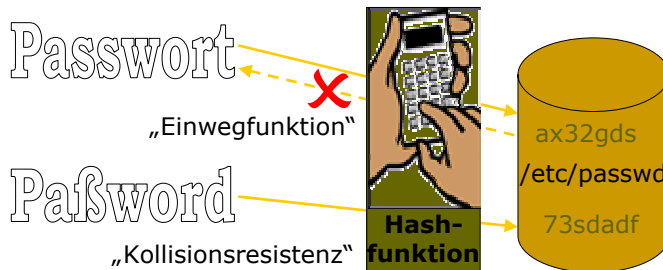
- Ungepatchte Software und Implementierungsfehler
- User
- Protokolle
- Kryptographie

Beweise für Sicherheit



11.05.2004

Hashfunktionen, Einwegfunktionen, Kollisionen



11.05.2004

Hashfunktionen

- MD2 (128 Bit)
 - keine Kollisionen bekannt
 - langsam
- MD4 (128 Bit)
 - Kollisionen in weniger als 1 Minute
 - sehr schnell
- MD5 (128 Bit)
 - Kollisionen in 4-5 Wochen (mit Hardware um €1 Mio.)
 - Pseudokollisionen bekannt
 - schnell
 - für „mittlere“ Sicherheit

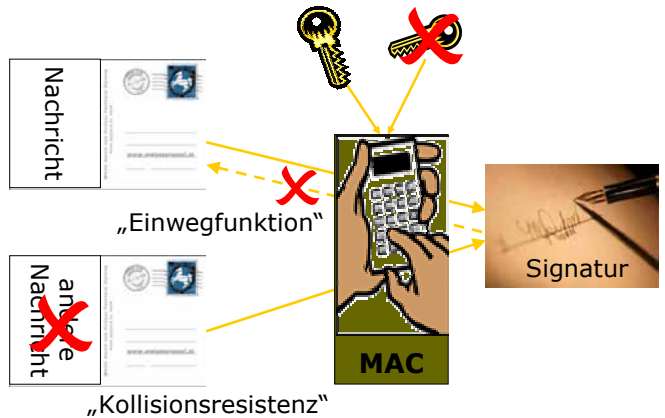
11.05.2004

Hashfunktionen (2)

- SHA-x (160, 256, 354, 512 Bit)
 - keine Kollisionen bekannt
 - schnell
- RIPEMD-160 (160 Bit)
 - noch sicherer als SHA-x
 - schnell
- Tiger (196 Bit)
 - keine Kollisionen bekannt
 - längerer Digest als RIPEMD-160
- Die Kollisionsresistenz all dieser Funktionen ist nur empirisch erwiesen.
- Sonst nur wenige Funktionen, die überhaupt hinreichend genau untersucht wurden.

11.05.2004

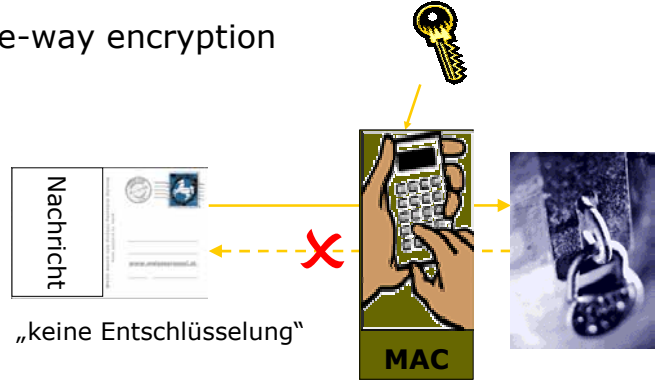
MACs (message authentication codes) Signature View



11.05.2004

MACs (message authentication codes) Encryption View

- One-way encryption



- kann im CFB- und OFB-Mode symm. Verschlüsselung ersetzen

11.05.2004

MACs vs. Symm. Encryption

□ MACs

- + schnell
- + einfach
- + keine Import- oder Exportbeschränkungen
- + kann im OFB (full feedback oder counter) mode zum Verschlüsseln verwendet werden
- wenig untersucht

□ Symmetrische Verschlüsselung

- + universell
- + gut untersucht
- komplex
- schnell

Für keinen der gängigen MACs symmetrischen Chiffren ist die Sicherheit theoretisch bewiesen. Es gibt nur empirische Beweise.

11.05.2004

Beweise für die Sicherheit von RSA und DH

□ RSA

- zerlege eine n-Bit Zahl in ein Produkt
- n – security parameter, zur Zeit $n \geq 1024$
- z.Z. $n \geq 1024$
- kein Beweis, dass das schwierig ist
- kein Beweis, dass das notwendig ist, um RSA vollständig zu brechen

□ DH

- gegeben g , p , g^a und $g^b \text{ mod } p$, berechne $g^{ab} \text{ mod } p$
- p n-Bit Primzahl
- n – security parameter, zur Zeit $n \geq 1024$
- kein Beweis, dass das schwierig ist

11.05.2004

Was lässt sich beweisen?

- Es ist nicht bekannt, ob es Einwegfunktionen, kollisionsresistente Hashfunktionen oder MACs, sichere symmetrische oder public-key Verschlüsselungsverfahren gibt.
- Aber:
Gibt es eins davon, so gibt es auch alles andere.
- Aber²: All das macht die Implementierung dieser Systeme nicht einfacher und sicherer.

11.05.2004

Wie beweist man Sicherheit?

Was ist Sicherheit?

- Was kann der Angreifer?
 - KPA (known plaintext): kennt Verschlüsselungen von bekannten Klartexten
 - CPA (chosen plaintext): kennt Verschlüsselungen von selbstgewählten Klartexten (typischerweise bei asymm. Verfahren)
 - CCA (chosen ciphertext): kennt Klartext zu selbst gewählten Chiffraten
 - nicht-adaptiv (CCA1): kann nach Klartexten zu selbstgewählten Chiffraten fragen, bis sein Angriff beginnt
 - adaptiv (CCA2): kann auch dann noch weiterfragen

11.05.2004

Wie beweist man Sicherheit?

Was ist Sicherheit?

- Was ist ein erfolgreicher Angriff?
 - total break: findet den geheimen Schlüssel
 - partial break: findet einzelne Bits des Schlüssels
 - SINGLE MESSAGE: entschlüsselt eine Nachricht
 - klassisch (partiell): findet einzelne Bits der Nachricht
 - semantic security: findet zwei Nachrichten, so dass sie die zugehörigen Chiffre unterscheiden kann
 - non-malleability: gegeben $c = E_K(m)$, findet eine Relation \sim und c' , so dass $E^{-1}(c') \sim m$, mit größerer Wahrscheinlichkeit als vor der Attacke.

11.05.2004

Beispiel: Klassisches RSA ist SINGLE-MESSAGE-CCA2 unsicher

- A (Angreifer) soll Chiffre c entschlüsseln
- A wählt x rel. prim zu n und berechnet $y = c/x \pmod n$
- A lässt sich x und y entschlüsseln, erhält a und b
- Dann ist ab der gesuchte Klartext
- Bemerkung: RSA-Verschlüsselung gemäß PKCS#1 v2.0 und später (mit OAEP) ist beweisbar CCA2-sicher

11.05.2004

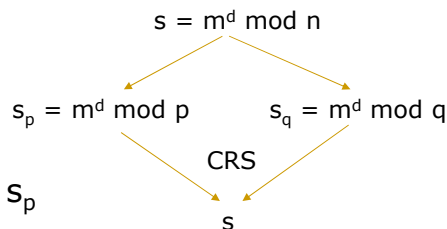
Side Channel Attacken auf RSA-Verschlüsselungs- und Signatursysteme

- Timing Attacks
 - [Kocher 96]
 - Reject Timing Attack auf EPOC-2 [Dent 02]
- Fault Induction Attacks
 - [Joye, Lenstra, Quisquater 99]
 - Memory Dump Attack [Kim e.a. 01]
- SPA (Simple Power Analysis)
 - [Messerges, Dabbish, Loan 99]
 - Novak Attack [Novak 02]
- DPA (Differential Power Analysis)
 - [deBoer, Lemke, Wicke 02]

11.05.2004

Fault Induction

- Chosen message Attacke auf RSA
 - Angreifer kann Signatur erstellen
 - Ziel: Bestimmung des Signaturschlüssels
- $n = p \cdot q$
 $ggT(e, (p-1)(q-1)) = 1$
 $d = 1/e \text{ mod } (p-1)(q-1)$
- Idee: störe die Berechnung von s_p



11.05.2004

Fault Induction

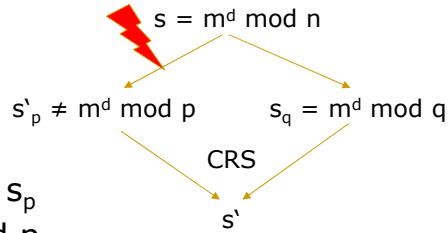
Chosen message Attacke auf RSA

- Angreifer kann Signatur erstellen
- Ziel: Bestimmung des Signaturschlüssels

$$n=p \cdot q$$

$$ggT(e,(p-1)(q-1))=1$$

$$d=1/e \text{ mod } (p-1)(q-1)$$

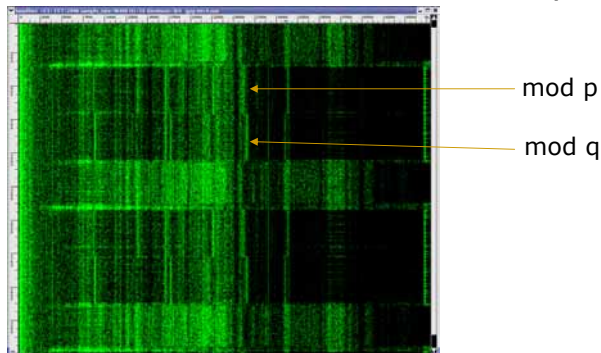


- Idee: störe die Berechnung von s_p
- Nun ist $s' \neq s \text{ mod } p$ und $s' = s \text{ mod } q$. Daher ist $ggT(s'-s,n)=q$.

11.05.2004

Und wann muss man den Fehler machen?

- [Tromer, Shamir 04]: ein Mikrophon genügt, um festzustellen, was der Prozessor gerade tut. (www.wisdom.weizmann.ac.il/~tromer/acoustic)

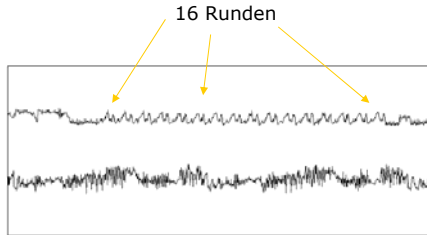


Frequenzspektrum GPG-Signieren

11.05.2004

Power Analysis (DES)

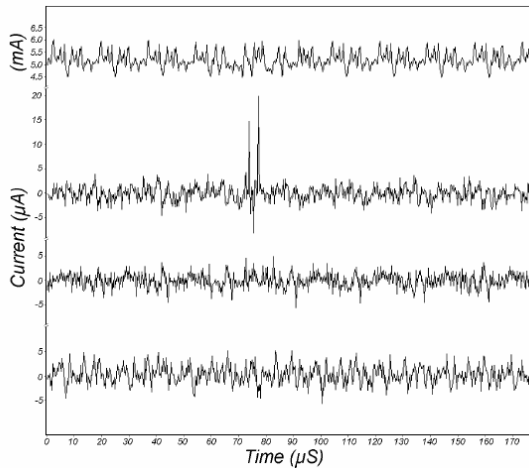
- Stromaufnahme während einer DES-Verschlüsselung



11.05.2004

Differential Power Analysis

- DES normal
- Rundenschlüssel erraten
- Rundenschlüssel nicht erraten



11.05.2004

Side channel attacks auf ECC

- SPA
 - Angriffe und Countermeasures [Coron 99]
- DPA
 - weitere Angriffe [Okeya, Sakurai 00]
 - Goubin's Attack [Goubin 03]
 - ZVP-Attack [Takagi 03]
- Workshop on Cryptographic Hardware and Embedded Systems CHES

11.05.2004

Simple Power Analysis auf ECC

- Beispiel: ElGamal
- Ziel: Ermittlung des geheimen Exponenten
- Verschiedene Formeln für Addition und Verdopplung
- Diese Unterschiede sieht man auch am Power Consumption Chart
- ... und kann so die Bits des Exponenten einzeln ablesen.

11.05.2004

Literatur

(Side Channel Attacks, Auswahl)

- den Boer, B., ea., „A DPA attack against the modular reduction within a CRT implementation of RSA“, CHES 2002, LNCS 2523, 228-243, 2003
- Coron, J., „Resistance against differential power analysis for elliptic curve cryptosystems“, CHES 99, LNCS 1717, 292-302, 1999
- Dent, A., „An implementation attack against the EPOC-2 public-key cryptosystem“, Electronics Letters, 38(9), 412ff., 2002
- Goubin, L., „A refined power analysis attack on elliptic curve cryptosystems“, PKC 2003, LNCS 2567, 199-211, 2003
- Joye, M., ea., „Chinese remaindering based cryptosystems in the presence of faults“, Journal of Cryptology, 12(4), 241-245, 1999
- Kim, S., ea., „Strong adaptive chosen ciphertext attacks with memory dump“, Cryptography and Coding, 8th IMA Conf., LNCS 2260, 114-127, 2001
- Kocher, C., „Timing attacks on implementations of DH, RSA, DSS, and other systems“, Crypto 96, LNCS 1109, 104-113, 1996
- Novak, R., „SPA-based adaptive CCA on RSA implementation“, PKC 2002, LNCS 2274, 252-262, 2002
- Okeya, K. & Sakurai, K., „Power analysis breaks elliptic curve cryptosystems even secure against the timing attack“, Indocrypt 00, LNCS 1977, 178-190, 2000

11.05.2004

Literatur

(Sicherheitsbeweise, Auswahl)

- Bellare, M., „Practice oriented provable security“, ISW 97, LNCS 1396, 1997
- Bellare, M., Rogaway, P., „Optimal asymmetric encryption – How to encrypt with RSA“, Eurocrypt 94, LNCS 950, 92-111, 1995
- Bellare, M., ea., „Relations among notions of security for public key encryption schemes“, Crypto 98, LNCS 1462, 26-45, 1998
- Bleichenbacher, D., „Generating ElGamal signatures without knowing the secret key“, Eurocrypt 96, LNCS 1070, 10-18, 1996
- Dolev, D., ea., „Non-malleable cryptography“, SIAM J.Comp., 30(2), 391-437, 2000
- Goldreich, O., „Foundations of Cryptography. Vol.1: Basic Tools“, Cambridge University Press, 2001
- Goldreich, O., „Foundations of Cryptography. Vol.2: ???“, Cambridge University Press, 2004
- Goldreich, O., ea., „How to construct random functions“, J. of the ACM, 33(4), 792-807, 1986
- Goldwasser, S., Micali, S., „Probabilistic encryption“, J. of Computer and System Sciences, 28, 270-299, 1984
- Naor, M., Yung, M., „Public key cryptosystems provably secure against chosen ciphertext attacks“, Proc. 22nd STOC, 427-437, 1990

11.05.2004