Vorlesung Netzsicherheit

Einführung

Prof. Dr. Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Überblick

- Sicherheit ist nicht nur Kryptographie
- David Kahn: „Das Wettrennen der Codemaker mit den Codebreakern ist gelaufen, die Codemaker haben gewonnen."
  - Stimmt für die reine Kryptographie (3DES und AES sind de facto unknackbar)
  - Aber: Viren, Würmer, Buffer Overflow, PKI, Man-in-the-middle, Seitenkanalattacken, Million-Question-Angriff auf SSL, PPTP geknackt, Berechnung des privaten Schlüssels in OpenPGP, DeCSS, Pay-TV, Telefonkarten, Mobilfunk-Betrug, …
- Die Einbettung von Kryptographie in eine konkrete physikalische oder Protokollumgebung (Oberbegriff: Netzwerk) stellt heute das größte Problem für die Sicherheit dar

Überblick

Ziele dieser Vorlesung:

- NICHT: Abstrakte Theorie der Netzsicherheit
- SONDERN: Sicherheit von konkreten Netzen an Beispielen aus der Praxis:
  - Pay-TV
  - Mobilfunk
  - WLAN
  - Internet:
    - OpenPGP, S/MIME, XML
    - SSL, PKI
    - IPSec, PPTP
  - CSS, DRM, TCPA
  - …

Gliederung

I. Alles außer WWW

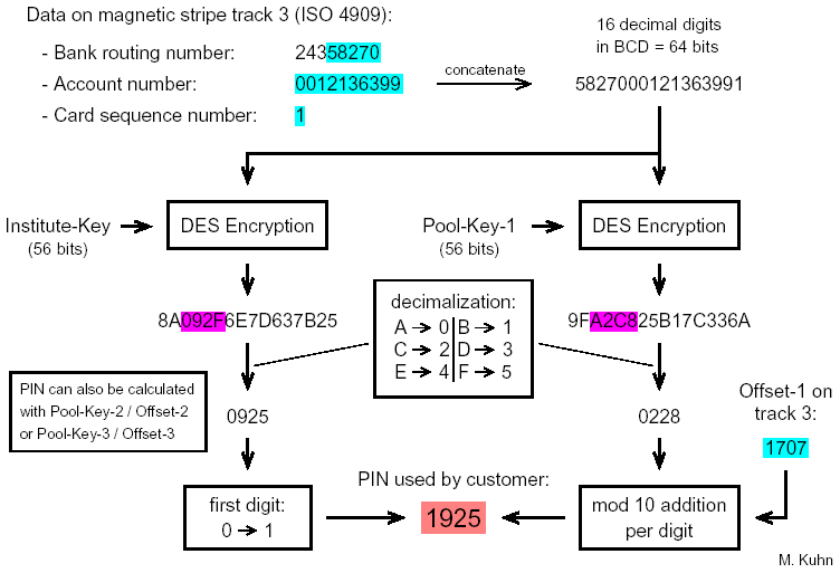
- Mobilfunk: GSM und UMTS
- WLAN
- PPP-Erweiterungen, RADIUS und AAA
- Contentsicherheit (1): DVD-Verschlüsselung mit CSS
- Contentsicherheit (2): Broadcast Encryption
- Contentsicherheit (3): Pay-TV
- Chipkarten
- Zertifikate und PKI
- OpenPGP
- S/MIME
- IPSec
- IP Multicast und Gruppenkommunikation

Gliederung

II. Sicherheit im WWW

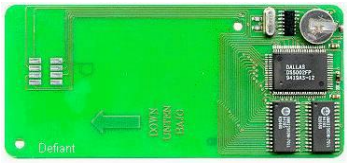
- http, HTML (5)
- XSS, CSRF, SQLi
- SSL/TLS
- Single-Sign-On-Systeme
  - Microsoft Active Directory und Passport
  - SAML SSO, OpenID
- DNSSEC
- XML-Sicherheit: Signatur, Verschlüsselung, Schlüsselmanagement
- WS-Security
- Firewalls, Intrusion Detection Systeme
- Malware: Drive-by-Downloads

PIN Calculation for EuroCheque ATM Debit Cards



Pay-TV

- Militärische Systeme wurden in fremdem Umfeld verwendet
- Diverse neuartige Angriffe



Contentsicherheit: CPSA

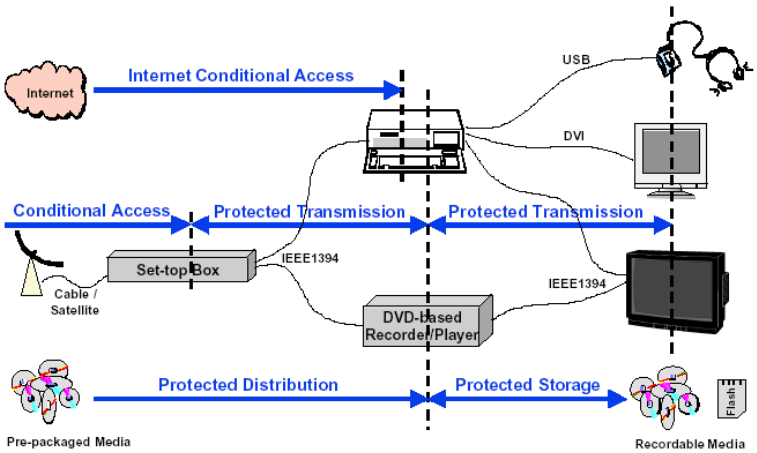
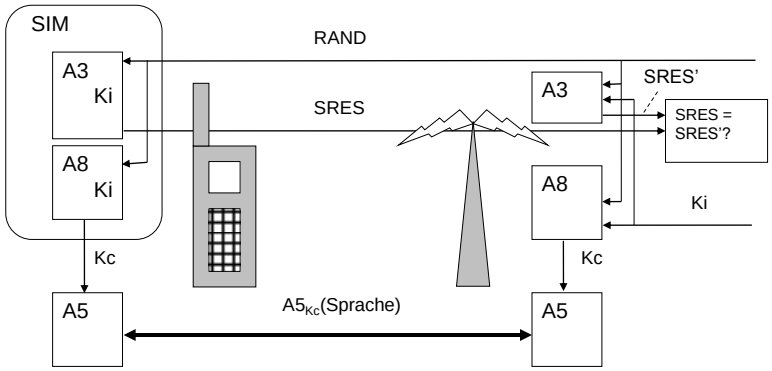


Figure 1. Digital Content Protection Chain

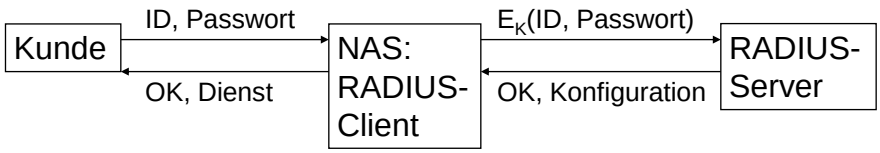
Mobilfunk: GSM-Sicherheit



RADIUS: AAA

Authentication, Autorisation, Accounting

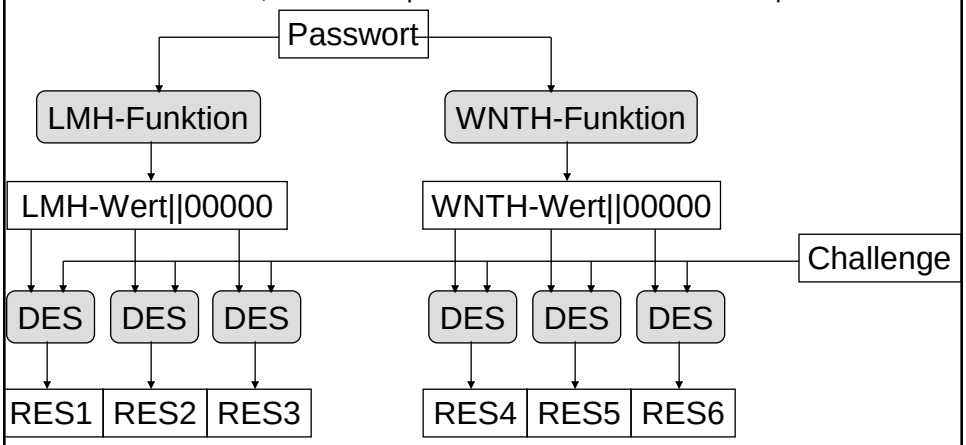
- RFC 2058: RADIUS (Lucent Technologies)
  - Client-Server-Lösung zur Authentisierung von Kunden



- SecureID: Produktlinie von RSA Inc.
  - Alle 10 s wird in Token und Server neue Zufallszahl generiert
  - Server überprüft, ob gesendete Zufallszahl im Zeitfenster liegt.

PPTP

- PPTP (Microsoft) verlängert das Einwahlprotokoll PPP durch das Internet; Sicherheitsprobleme durch Rückwärtskompatibilität



WLAN

WEP (Wired Equivalent Privacy)

- Symmetrisches Schlüsselmanagement (Schlüssel müssen manuell in Notebooks und Access Points eingetragen werden
  - Folge: I.d.R. nur ein Schlüssel in einem Netzwerk, der z.B. nach Reparatur eines Notebooks als allgemein bekannt gelten darf
- Stromchiffre RC4 ohne Vorgaben zur Wahl des IV
  - Interessante XOR-Angriffe, z.B. Verändern der bekannten IP-Zieladresse eine Pakets
- Schwächen von RC4 kommen voll zum Tragen
  - Fluhrer, Mantin und Shamir konnten WEP kryptologisch brechen; dies wurde in Tools (z.B. WepCrack) umgesetzt

PGP: Angriff auf DSA

95**01D7**043A8D29DF11**0400**F2E02A396A14E137085DA859B3569AF4027EA379682F46780920B7212
7C88787DDC1BFF9FDB59E564B741FD5FC98856679F1C041CB71895CB6975E7FE6E15A6D4B705145
60E11A25637F3FBA35E89E5F1FA272A2707F4865EA106EE402973D4969A276DA4911005B968B815
48621CEBBB5771A35C5A785F7F480E47277D2BAB5**00A0**FF04303152BD2A9AD963E063A3FE34A8A5
534F3F**0400**CD8580F20AA821A6D2FF5255DFD02E4F4C8D8DA3731517476BEE096F7B104B01B6CE1
C4DE586BAEA30D82B50DCB3F0D20B0F0D07D8384C09F12CBF079887CEB696E822D753A48584F2BC
573C84E8490AB310FDBCC40EAEBCD05973B3F2A1A479FFE0E4B63026E066B6E936F1B2B7F1C91C6
5CBA0F27B4C0D22254BBC852DEDE1**0400**AC756BB6EB82313A0FE91F47A36D1425D89FB124CD0ACB
A082E8B2C2B048BE92C5CE7A5FAA5AF317DCC086150B98AB504C0DA6BF1D87FAB73C8F8D0FC821B
D8902CA6927338CF0D682E7C9E3E8D89A3D00D53224C301E6C932ADA7562FA15E9027E105F80304
3D4CBC08807A8FB71FEF9B27EE6A0722C4BF601D032CC59F6FE4**FF09030213CF38106B7BCA3F603
F59437C3860B98DA3A1A3F02A4D2754075B494CAC156E38E1282705FB0BBD68940A1653457E161A**
B00187B428566C617374696D696C204B6C696D612C20445353203C762E6B6C696D6140646563726
F732E637A3EB00303FFFF89005A04101102001A05023A8D29DF050901E13.....shortened....
0167

Ursprüngliche Datei secring.skr; p,g und verschlüsselte Daten hervorgehoben

95**00FF**043A8D29DF11**009F**538000000000000000000000000000000000000000001**00A0**FF04303152BD2
A9AD963E063A3FE34A8A5534F3F**009E**31AC85291FF814E625E4B88C8C5047A7DB2F0E45**0400**AC75
6BB6EB82313A0FE91F47A36D1425D89FB124CD0ACBA082E8B2C2B048BE92C5CE7A5FAA5AF317DCC
086150B98AB504C0DA6BF1D87FAB73C8F8D0FC821BD8902CA6927338CF0D682E7C9E3E8D89A3D00
D53224C301E6C932ADA7562FA15E9027E105F803043D4CBC08807A8FB71FEF9B27EE6A0722C4BF6
01D032CC59F6FE4**FF09**030213CF38106B7BCA3F603F59437C3860B98DA3A1A3F02A4D2754075B49
4CAC156E38E1282705FB0BBD68940A1653457E161AB00187B428566C617374696D696C204B6C696
D612C20445353203C762E6B6C696D6140646563726F732E637A3EB00303FFFF89005A0410110200
1A05023A8D29DF050901E13..... shortened..... 0167

Modifizierte Datei secring.skr; modifizierte p,g und unmodifizierte verschlüsselte Daten hervorgehoben

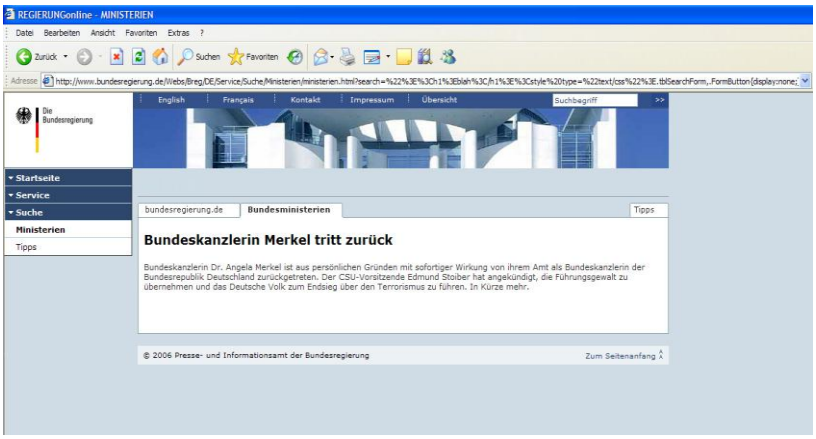
Angreifermodell 1: WW2

- 2. Weltkrieg und kalter Krieg: Abhören verschlüsselter, per Funk übertragener Gespräche

- Wichtig, aber nicht mehr ausreichend (GEMATIK!)

Angreifermodell 2: WWW

- XSS, CSRF und SQLi



Angreifermodell 3: Malware

DigiTask ?

G DATA

... und viele weitere moderne Angreifermodelle

- Seitenkanalangriffe
- Fehlerangriffe
- Angriffe auf Zertifizierungsstellen (DigiNotar)
- Social Engineering
- ...