ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Sicherheit in Rechnernetzen

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Was ist eine Bedrohung?

- **Definition**
  - Eine Bedrohung eines Rechnernetzwerks ist jedes mögliche Ereignis oder eine Folge von Aktionen, die zu einer Verletzung von Sicherheitszielen führen kann
  - Die Realisierung einer Bedrohung ist ein Angriff
- **Beispiele**
  - Ein Hacker erhält Zugang zu einem geschlossenen Netzwerk
  - Veröffentlichung von durchlaufenden E-Mails
  - Fremder Zugriff zu einem Online-Bankkonto
  - Ein Hacker bringt ein System zum Absturz
  - Jemand agiert ohne Erlaubnis im Namen anderer (Identity Theft)

Sicherheitsziele

- **Vertraulichkeit:**
  - Übertragene oder gespeicherte Daten können nur vom vorbestimmten Publikum gelesen oder geschrieben werden
  - Vertraulichkeit der Identität der Teilnehmer: Anonymität
- **Datenintegrität**
  - Veränderungen von Daten sollten entdeckt werden
  - Der Autor von Daten sollte erkennbar sein
- **Verantwortlichkeit**
  - Jedes Kommunikationsereignis muss einem Verursacher zugeordnet werden können
- **Verfügbarkeit**
  - Dienste sollten verfügbar sein und korrekt arbeiten
- **Zugriffskontrolle**
  - Dienste und Informationen sollten nur autorisierten Benutzern zugänglich sein

Angriffe

- **Maskierung (Masquerade)**
  - Jemand gibt sich als jemand anderes aus
- **Abhören (Eavesdropping)**
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- **Zugriffsverletzung (Authorization Violation)**
  - Jemand benutzt einen Dienst oder eine Ressource, die nicht für ihn bestimmt ist
- **Verlust oder Veränderung von Information**
  - Daten werden verändert oder zerstört
- **Verleugnung der Kommunikation**
  - Jemand gibt fälschlicherweise vor nicht der Verursacher von Kommunikation zu sein
- **Fälschen von Information**
  - Jemand erzeugt oder verändert Nachrichten im Namen anderer
- **Sabotage**
  - Jede Aktion, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems einschränkt

Bedrohungen und Sicherheitsziele

Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Terminologie der Kommunikationssicherheit

- **Sicherheitsdienst**
  - Ein abstrakter Dienst, der eine Sicherheitseigenschaft zur erreichen sucht
  - Kann mit (oder ohne) Hilfe kryptographischer Algorithmen und Protokolle realisiert werden, z.B.
    - Verschlüsselung von Daten auf einer Festplatte
    - CD im Safe
- **Kryptographischer Algorithmus**
  - Mathematische Transformationen
  - werden in kryptographischen Protokollen verwendet
- **Kryptographisches Protokoll**
  - Folge von Schritten und auszutauschenden Nachrichten um ein Sicherheitsziel zu erreichen

Sicherheitsdienste

- **Authentisierung**
  - Digitale Unterschrift: Das Datum ist nachweislich vom Verursacher
- **Integrität**
  - Sichert ab, dass ein Datum nicht unbemerkt verändert wird
- **Vertraulichkeit**
  - Das Datum kann nur vom Empfänger verstanden werden
- **Zugriffskontrolle**
  - kontrolliert, dass nur Berechtigte Zugang zu Diensten und Information besitzen
- **Unleugbarkeit**
  - beweist, dass die Nachricht unleugbar vom Verursacher ist

Verschlüsselungsmethoden

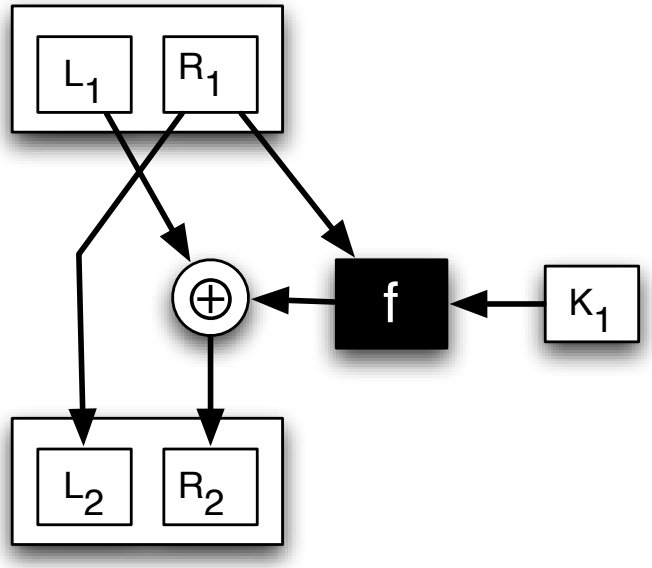
- **Symmetrische Verschlüsselungsverfahren, z.B.**
  - Feistel-Chiffre
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- **Kryptografische Hash-Funktion**
  - SHA-1, SHA-2
  - MD5
- **Asymmetrische Verschlüsselungsverfahren**
  - RSA (Rivest, Shamir, Adleman)
  - El-Gamal
- **Digitale Unterschriften (Elektronische Signatur)**
  - PGP (Phil Zimmermann), RSA

Symmetrische Verschlüsselungsverfahren

- **z.B. Cäsars Code, DES, AES**
- **Funktionen f und g, wobei**
  - Verschlüsselung f:
    - f(schlüssel,text) = code
  - Entschlüsselung g:
    - g(schlüssel,code) = text
- **Der Schlüssel**
  - muss geheim bleiben
  - dem Sender und Empfänger zur Verfügung stehen

Feistel-Chiffre

- **Aufteilung der Nachricht in zwei Hälften L_1, R_1**
  - Schlüssel K_1, K_2, ...
  - Mehrere Runden: resultierender Code: L_n, R_n
- **Verschlüsselung**
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
- **Entschlüsselung**
  - $R_{i-1} = Li$
  - $L_{i-1} = R_i \oplus f(L_i, K_i)$
- **f: beliebige, komplexe Funktion**



Weitere Symmetrische Codes

- **Skipjack**
  - 80-Bit symmetrischer Code
  - baut auf Feistel-Chiffre auf
  - wenig sicher
- **RC5**
  - Schlüssellänge 1-2048 Bits
  - Rivest Code 5 (1994)
  - Mehrere Runden der Feistel-Chiffre

Digital Encryption Standard

- **Geschickt gewählte Kombination von**
  - Xor-Operationen
  - Feistel-Chiffre
  - Permutationen
  - Table-Lookups
  - verwendet 56-Bit Schlüssel
- **1975 entwickelt von Wissenschaftlern von IBM**
  - Mittlerweile nicht mehr sicher
    - leistungsfähigeren Rechner
    - Erkenntnisse in Kryptologie
- **Nachfolger: AES (2001)**

Advanced Encryption Standard

- **Geschickt gewählte Kombination von**
  - Xor-Operationen
  - Feistel-Chiffre
  - Permutationen
  - Table-Lookups
  - Multiplikation in GF[2^8]
  - symmetrischer 128,192 oder 256-Bit Schlüsse
- **Joan Daemen und Vincent Rijmen**
  - 2001 als AES unter vielen ausgewählt worden
  - bis heute als sicher erarchtet

Kryptographische Hash-Funktion

- **z.B. SHA-1, SHA-2, MD5**
- **Ein kryptographische Hash-Funktion h bildet einen Text auf einen Code fester Länge ab, sodass**
  - h(text) = code
  - es unmöglich ist einen anderen Text zu finden mit:
    - h(text‘) = h(text) und text ≠ text‘
- **Mögliche Lösung:**
  - Verwendung einer symmetrischen Kodierung

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer