Systeme II

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

Christian Schindelhauer
Sommersemester 2006
20. Vorlesung
13.07.2006
schindel@informatik.uni-freiburg.de

Sicherheit in Rechnernetzwerken

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

- **Spielt eine Rolle in den Schichten**
  - Bitübertragungsschicht
  - Sicherungsschicht
  - Vermittlungsschicht
  - Transportschicht
  - Anwendungsschicht
- **Was ist eine Bedrohung (oder ein Angriff)**
- **Welche Methoden gibt es**
  - Kryptographie
- **Wie wehrt man Angriffe ab?**
  - Beispiel: Firewalls

Was ist eine Bedrohung

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

- **Definition:**
  - Eine Bedrohung eines Rechner-Netzwerks ist jedes mögliche Ereignis oder eine Folge von Aktionen, welches zu einer Verletzung von Sicherheitszielen führen kann
  - Die Realisierung einer Bedrohung ist ein Angriff
- **Beispiel:**
  - Ein Hacker erhält Zugang zu einem geschlossenen Netzwerk
  - Veröffentlichung von durch laufenden E-Mails
  - Fremder Zugriff zu einem Online-Bank-Konto
  - Ein Hacker bringt ein System zum Absturz
  - Jemand agiert unautorisiert im Namen anderer (Identity Theft)

Sicherheitsziele

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

- **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**
  - Jedem Kommunikationsereignis muss ein Verursacher zugeordnet werden können
- **Verfügbarkeit**
  - Dienste sollten verfügbar sein und korrekt arbeiten
- **Zugriffskontrolle**
  - Dienste und Informationen sollten nur autorisierten Benutzern zugänglich sein

Angriffe

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

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

Bedrohungen und Sicherheitsziele

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

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

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

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

Sicherheitsdienste

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

- **Authentisierung**
  - Digitale Unterschift: 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

Kryptologie

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

- **Kryptologie**
  - Wissenschaft der geheimen Kommunikation
  - Von griechisch kryptós (versteckt) und lógos (Wort)
  - Kryptologie beinhaltet:
    - Kryptografie (gráphein = schreiben): die Lehre des Erzeugens von geheimer Kommunikation
    - Krypto-Analyse (analýein = lösen, entwirren): die Lehre des Entschüsselns geheimer Information

Verschlüsselungs-methoden

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

- **Symmetrische Verschlüsselungsverfahren**
  - z.B. Caesers Code
  - Enigma
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- **Kryptografische Hash-Funktion**
  - SHA-1, SHA-2, MD5
- **Asymmetrische Verschlüsselungsverfahren**
  - RSA (Rivest, Shamir, Adleman)
  - Diffie-Helman

Symmetrische Verschlüsselungsverfahren

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

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

Kryptografische Hash-Funktion

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

- **z.B. SHA-1, SHA-2, MD5**

- **Ein kryptografische Hash-Funktion h bildet einen Text auf einen Code fester Länge so ab,**
  - h(text) = code
  - dass es unmöglich ist einen anderen Text zu finden mit:
    - h(text‘) = h(text) und text $\neq$ text‘
- **Mögliche Lösung:**
  - Verwendung einer symmetrischen Kryptografie-Methode

Asymmetrische Verschlüsselungsverfahren

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

- **z.B. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977**
  - Diffie-Hellman, PGP
- **Geheimer Schlüssel `privat`**
  - kennt nur der Empfänger der Nachricht
- **Öffentlichen Schlüssel `offen`**
  - Ist allen Teilnehmern bekannt
  - Wird erzeugt durch Funktion
    - keygen(`privat`) = `offen`
- **Verschlüsselungsfunktion f und Entschlüsselungsfunktion g**
  - sind auch allen bekannt
- **Verschlüsselung**
  - f(`offen`,`text`) = `code`
  - kann jeder berechnen
- **Entschlüsselung**
  - g(`privat`,`code`) = `code`
  - nur vom Empfänger

Ende der 20. Vorlesung

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

Systeme II

Christian Schindelhauer

schindel@informatik.uni-freiburg.de