CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

7. Sicherheit

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg
(Version 14.07.2014)

UNI FREIBURG

CoNe Freiburg

Sicherheit in Rechnernetzwerken

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

UNI FREIBURG

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
- Beispiel:
  - 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 unautorisiert 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
  - 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

- Maskierung (Masquerade)
  - Jemand gibt sich als ein anderer aus
- Abhören (Eavesdropping)
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- 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, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems reduziert

CoNe Freiburg

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	

CoNe Freiburg

Terminologie der Kommunikationssicherheit

- Sicherheitsdienst
  - Ein abstrakter Dienst, der eine Sicherheitseigenschaft zur erreichen sucht
  - Kann mit (oder ohne) Hilfe 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 um ein Sicherheitsziel zu erreichen

UNI FREIBURG

CoNe Freiburg

Sicherheitsdienste

- 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

UNI FREIBURG

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Systeme II

7. Sicherheit

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg

UNI FREIBURG