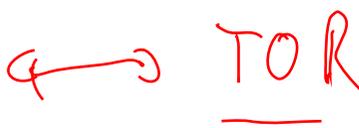


Systeme II

7. Sicherheit

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

- 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?

- 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)

■ 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

"password"
"12345678"
"12345697"

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

Sicherheitsziele ↓	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	

■ 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

- 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



Systeme II

7. Sicherheit

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