openHPI – Sicherheit im Internet
Sicherheitsziele

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Einführung

- Das Internet bietet eine **offene Kommunikationsinfrastruktur**,
  - jeder kennt die Baupläne und Funktionsprinzipien,
  - jeder kann sich Zugang verschaffen und es
  - für seine Zwecke nutzen
- Offene Kommunikationsinfrastrukturen bieten dem Benutzer grundsätzlich nur **unsichere Kommunikationskanäle**
- Nachdenken über Informationssicherheit im Internet setzt deshalb zunächst eine systematische Analyse der Nutzungswünsche und der dabei gewünschten bzw. erforderlichen Sicherheitsanforderungen voraus → **Sicherheitsziele**
- Sicherheitsanforderungen und Ziele hängen vom jeweiligen Benutzer und von der von ihm jeweils genutzten Anwendung ab

Grundlegende Sicherheitsziele (1/2)

Literatur nennt meist **3 grundlegende Sicherheitsziele: C-I-A**

- **C**onfidentiality – Vertraulichkeit
- **I**ntegrity – Integrität
- **A**vailability – Verfügbarkeit

Vertraulichkeit *(confidentiality)*

Schutz vor unberechtigtem Einblick in vertrauliche Informationen, z.B. Passwörter, Zahlungsinformationen, Gesundheitsdaten, private Korrespondenz, ... beim Transport über offene und deshalb unsichere Kommunikationskanäle wie im Internet

Grundlegende Sicherheitsziele (2/2)

Integrität *(integrity)*

Sicherstellung, dass die beabsichtigte Manipulation und Verfälschung bzw. die unbeabsichtigte Veränderung (Übertragungsfehler) von Informationen beim Transport über offene und demzufolge unsichere Kommunikationskanäle wie im Internet vom Empfänger entdeckt werden können

Verfügbarkeit *(availability)*

Vorsorge, dass Nutzungsberechtige jederzeit und vom rechten Ort auf über offene Kommunikationskanäle wie im Internet bereitgestellte Informationen und Kommunikationsdienste zugreifen können, z.B. auf Internet-basierte medizinische Notdienste, Vertriebskanäle, ...

Weitere Sicherheitsziele (1/4)

Authentifikation (*authentication*)

Feststellung der Identität eines Benutzers, um später entscheiden zu können, ob der berechtigt ist, auf ein über offene Kommunikationskanäle wie dem Internet erreichbares System oder darüber angebotene Informationen und Kommunikationsdienste zuzugreifen

Zugriffskontrolle (*access control*, *accountability*)

Ist der Authentifikation nachgeschaltet und sorgt dafür, dass nur autorisierten Benutzern Zugriff auf Informationen und Ressourcen gewährt wird

...

Weitere Sicherheitsziele (2/4)

...

Anonymität (*anonymity*)

Geheimhaltung der Identität eines Kommunikationsteilnehmers in einem offenen Netz wie dem Internet

Unbeobachtbarkeit (*non-observability*)

Verdeckung eines Kommunikationsvorgangs in einem offenen Kommunikationsnetz wie dem Internet vor Außenstehenden

Privatsphäre *(privacy)*

Kontrolle eines Individuums über den Zugang zu seinen persönlichen Daten (verwandt mit Vertraulichkeit)

...

Weitere Sicherheitsziele (3/4)

...

Verbindlichkeit (*non-repudiation*, *legal enforceability*)

Da bei elektronischer Kommunikation digitalisierte Information und ihr Transportmedium entkoppelt sind, muss ein rechtsverbindlicher Zusammenhang zwischen den übertragenen Daten und der Person, die diese gesendet bzw. empfangen hat, hergestellt werden, z.B. zum

- **Urhebernachweis**
  zur Überprüfung des Ursprungs einer Nachricht
- **Empfängernachweis**
  zur Überprüfung des Empfangs einer Nachricht

...

Weitere Sicherheitsziele (4/4)

...

Kopierschutz (*copy protection*)

Soll sicherstellen, dass Informationen nur von autorisierten Nutzern kopiert werden können. Realisiert z.B. durch Verstecken einer Spezialinformation, mit der das Copyright an einer Software oder einem Audio-/Videoclip nachgewiesen werden kann

Kombination von Sicherheitszielen (1/2)

Es ist unmöglich, Liste der Sicherheitsziele abzuschließen:

- Neue Anwendungen erfordern neuen Sicherheitsziele, z.B.
  - Wahlen im Internet
  - Digitales Geld
  - Schutz der Privatsphäre
  - ...
- In den einzelnen Anwendungen sind die verschiedenen Sicherheitsanforderungen unterschiedlich gewichtet, z.B.
  - Verbindlichkeit
  - Anonymität
  - ...

Kombination von Sicherheitszielen (2/2)

Einzelne Sicherheitsanforderungen können sich widersprechen oder (je nach Anwendungsfall) gar gegenseitig ausschließen, z.B.

- Authentifikation und Anonymität, z.B.
  - Bezahlung mit Kreditkarte schließt Anonymität aus
- Anonymität und Verbindlichkeit, z.B.
  - Verbindliche Handlungen (gerade vor dem Hintergrund der rechtlichen Nachweisbarkeit) setzen immer den Identitätsnachweis einer natürlichen Person voraus
  - Dieser Identitätsnachweis schließt eine anonyme Kommunikationsteilnahme aus
- ...

Kombination von Sicherheitszielen (2/2)

Einzelne Sicherheitsanforderungen können sich widersprechen oder (je nach Anwendungsfall) gar gegenseitig ausschließen, z.B.

- Authentifikation und Anonymität, z.B.
  - Bezahlung mit Kreditkarte schließt Anonymität aus
- Anonymität und Verbindlichkeit, z.B.
  - Verbindliche Handlungen (gerade vor dem Hintergrund der rechtlichen Nachweisbarkeit) setzen immer den Identitätsnachweis einer natürlichen Person voraus
  - Dieser Identitätsnachweis schließt eine anonyme Kommunikationsteilnahme aus
- ...