Sicherheit digitaler Systeme

Prof. Dr. Christian Forler

Berliner Hochschule für Technik

Dezember 2023

Organisatorisches

- Stellen Sie Fragen!
  - Unterricht,
  - E-Mail `mailto:cforler@bht-berlin.de`,
  - Büro: D134,
  - ...
- Dozenten sind fehlbar.

  $\Longrightarrow$ Bei Unklarheiten stellen Sie Fragen

Sonstiges

- Machen Sie sich Notizen und annotieren sie die Folien
- Benutzung von Handys ist in der Vorlesung nicht erwünscht
- Stellen Sie Fragen
- Bereiten Sie die Vorlesung nach

Übung

- Bereiten Sie die Übungsaufgabe für die Übung vor.
- Bereiten Sie Fragen zum Stoff der Vorlesung/Übung vor.
- Die Übungsaufgabe werden in der Übung besprochen.
- Stellen Sie sich darauf ein Ihre Lösung zu präsentieren.
- Nehmen Sie aktiv an der Übung teil.
- Durch das Üben lernen Sie die Inhalte der Vorlesung.

Klausur

- n Minuten (n Punkte)
- Punkte entsprechen der Bearbeitungszeit in Minuten.
- Ein handgeschriebener Spickzettel (Din A4) ist erlaubt.
- Termin: 25. Januar 2024

Relevanz von IT-Sicherheit (1/2)

IT-Sicherheit (*Security*) wird zunehmend wichtiger

- Analyse von Sicherheitsanforderungen. Wo sind die Sicherheitslücken?
- Gegeben einen Ansatz, die Lücken zu stopfen. Welche Probleme bleiben ungelöst, welche neuen Probleme treten auf?

Hauptproblem der IT-Sicherheit

IT-Sicherheit kann nicht gemessen werden.

Lösungsansatz

Indirekte Definition von IT-Sicherheit durch Schutzziele.

- Vertraulichkeit (engl. confidentiality, data privacy)
  Schutz gegen unbefugte Informationsgewinnung
- Integrität (engl. (data) integrity)
  Schutz gegen unbefugte Veränderung der Daten
- Verfügbarkeit (engl. availability)
  Schutz gegen unbefugte Beeinträchtigung der Funktionalität

Vertraulichkeit

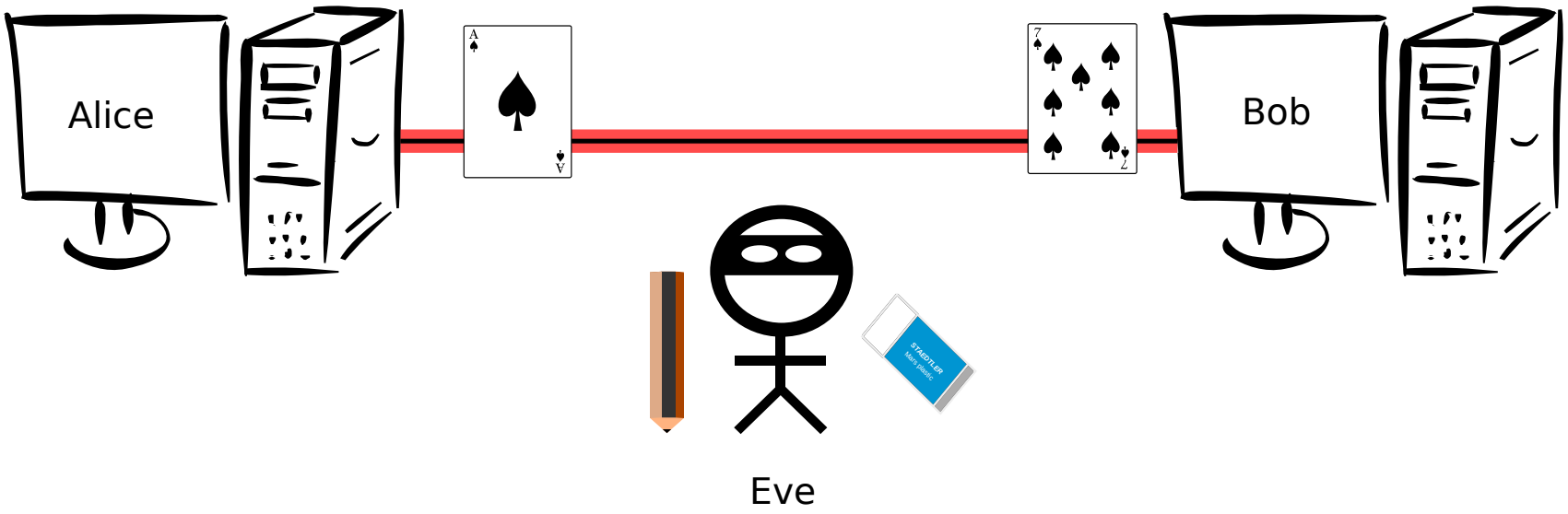
- Geschützte Daten können nur von Berechtigten genutzt werden.
- Vertraulichkeit gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten (Angreifer) eingesehen werden können
- In vernetzten Systemen ist zu betrachten
  - Der Transport von Daten (über Rechnernetze)
  - Speicherung von Daten (inkl. Backup)
  - Verarbeitung von Daten
- Typische Sicherheitsmaßnahme: Verschlüsselung
- Kontext Dienste: Vertrauliche IT-Dienste können nur von autorisierten Anwendern genutzt werden

Vertraulichkeit: Visualisierung

Integrität

- Geschützte Daten können nur von Berechtigten verändert werden.
- Integrität verletzt, wenn Daten von einem Angreifer unbemerkt verändert werden können.
- Wiederum bei Transport, Speicherung und Verarbeitung sicherzustellen!
- Typische Sicherheitsmaßnahme: Kryptographische Prüfsummen
- Kontext Dienste: Integre IT-Dienste haben keine (versteckte) Schadfunktionalität.

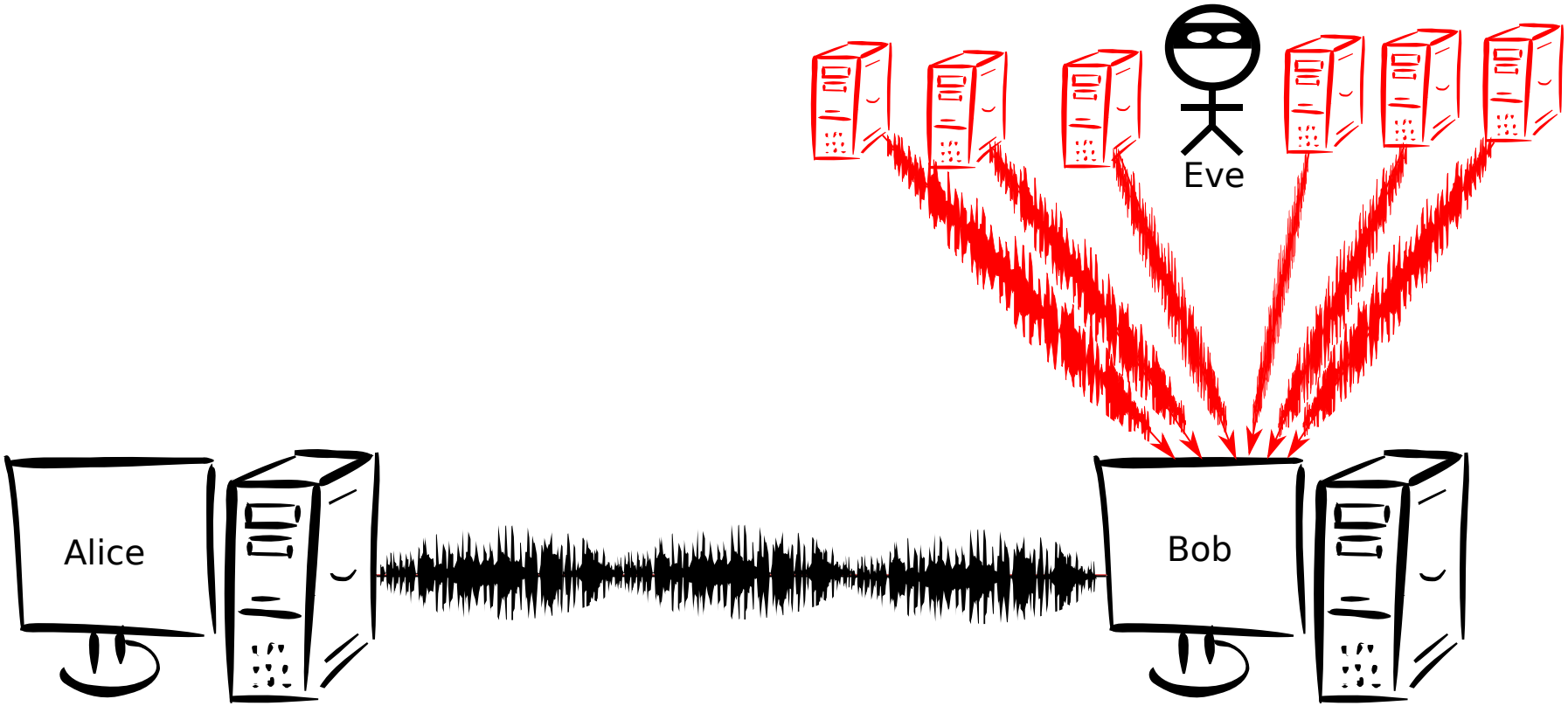
Integrität: Visualisierung



Verfügbarkeit

- Daten sind für berechtigte Nutzer verfügbar.
- Verfügbarkeit verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender einschränkt.
- Typische Sicherheitsmaßnahme: Redundanz (z.B. Daten-Backups), Overprovisioning (z.B. mehr als genug Server).
- Bezieht sich nicht nur auf Daten, sondern z.B. auch auf Dienste und ganze IT-Infrastrukturen.

Verfügbarkeit: Visualisierung



Inhalte der Vorlesung

1. Grundlagen des sicheren Programmierens in C
2. Grundlagen der Kryptographie
3. Einführung in die symmetrische Kryptographie
4. Einführung in die asymmetrische Kryptographie

Acknowledgments

Disclaimer

Die Folien dieser Veranstaltung sind inspiriert von Prof. Stefan Lucks und Prof. Helmut Reiser.