Hochschule Darmstadt

Zusammenfassung: 1. Semester

IT-Sicherheit

Leonhard Breuer
8. Januar 2024

Inhaltsverzeichnis

1 Grundlagen **3**
- 1.1 Die alltäglichen Probleme . . . 3
- 1.2 By Design . . . 3
  - 1.2.1 Betriebssicherheit/Safety . . . 3
  - 1.2.2 Informationssicherheit/Security . . . 4
  - 1.2.3 Wechselwirkungen . . . 4
- 1.3 Definitionen . . . 5
- 1.4 Schutzziele . . . 5
  - 1.4.1 Übersicht . . . 5
  - 1.4.2 Vertraulichkeit . . . 5
  - 1.4.3 Integrität . . . 6
  - 1.4.4 Authenzität . . . 6
  - 1.4.5 Verbindlichkeit . . . 6
  - 1.4.6 Verfügbarkeit . . . 6
  - 1.4.7 Privatheit . . . 6
- 1.5 IT-Sicherheit . . . 6
  - 1.5.1 Security-Policy . . . 7
  - 1.5.2 Gefahr . . . 7
  - 1.5.3 Bedrohung . . . 7
  - 1.5.4 Schwachstelle/Vulnerability . . . 7
  - 1.5.5 Gefährdung . . . 7
  - 1.5.6 Angriff . . . 7
  - 1.5.7 Angreifer . . . 7

2 Malware **8**
- 2.1 Die Sicht des Anwenders . . . 8
- 2.2 Malware-Typen . . . 8
  - 2.2.1 Computer Virus . . . 8
  - 2.2.2 Trojaner . . . 9
  - 2.2.3 Wurm . . . 9
  - 2.2.4 Ad-/Spyware . . . 10
  - 2.2.5 Rootkits . . . 10
  - 2.2.6 Botnet . . . 10
- 2.3 Advanced Persistent Thread . . . 10

2.3.1 Begriffsbedeutungen 10
2.4 Schutzmaßnahmen 11
2.4.1 Virenscanner 11
2.4.2 Firewall 11
2.4.3 IDS und IPS 11
2.4.4 Honeypot 11
2.4.5 Pentesting 11

3 Kryptologie **12**
3.1 Geschichte der Kryptologie 12
3.1.1 Monoalphabetische Substitutionschiffren 12
3.1.2 Polyalphabetische Chiffren 12
3.1.3 Kerckhoffs Prinzipien 12
3.2 Symmetrische Kryptografie 13
3.2.1 Caesar-Chiffre 13
3.2.2 Schlüsselraum 13
3.2.3 One-time Pad 13
3.2.4 Perfekte Sicherheit 14
3.2.5 Sicherheitsniveau 14
3.3 Zufallszahlen 14
3.3.1 Echte Zufallszahlengeneratoren (TRNG) 14
3.3.2 Pseudozufallszahlengeneratoren (PRNG) 14
3.3.3 Kryptografisch sichere Pseudozufallszahlengeneratoren (CSPRNG) 14
3.3.4 Stromchiffren: 14
3.3.5 Blockchiffren: 15
3.4 Hashfunktionen 15
3.4.1 Kryptografische Hashfunktionen 15
3.4.2 15

Kapitel 1

Grundlagen

1.1 Die alltäglichen Probleme

Täglich werden neue kritische Schwachstellen und Angriffe bekannt. Einige Beispiele:

- September 2020: Shitrix-Anriff
- Dezember 2018: Emotet (Banking Trojaner)
- Januar 2018: Meltdown and Spectre
- Oktober 2017: Return of Coppersmith Attack
- Juli 2015: Jeep Cherokee Hack (Zugriff auf kritische Fahrzeugfunktionen)
- Mitte 2014: Heartbleed (Fehler in OPENSSL)

1.2 By Design

Wegen der sich ständig weiterentwickelnden Technik müssen IT-Sicherheit und Datenschutz von Anfang an berücksichtigt werden.

Security by Design & **Privacy by Design**

1.2.1 Betriebssicherheit/Safety

Die Betriebssicherheit besagt, dass sich das Gerät/System konform seiner speziellen Funktion verhält bzw. das tut, was es soll. Die Safety umfasst auch einen Schutz aus Konsequenzen aus berechtigtem Handeln.

1.2.2 Informationssicherheit/Security

Die Security umfasst einen Schutz vor Konsequenzen aus vorsätzlichen und unberechtigen Handlungen. Gemäß dem **ISO / IEC 2382-1** - Standard gilt:

- Minimierung der Verwundbarkeit von Werten und Ressourcen
- Bewahren eines Systems vor Missbrauch

Informationssicherheit umfasst IT-Systeme (und darin gespeicherte Daten) und _nicht elektronisch verarbeitete Daten.

1.2.3 Wechselwirkungen

Hier einige Beispiele zu Wechselwirkungen von Safety und Security.

Security-Verletzungen können Safety gefährden Security Verletzungen können die Safety gefährden.

1. **Sicherheitsaspekt (Security):** Ein unbefugter Mitarbeiter oder Hacker hat Zugriff auf elektronische Patientenakten im Krankenhausinformationssystem (KIS). Dies könnte durch unzureichende Zugriffskontrollen, Schwachstellen in der Software oder unsichere Passwörter verursacht werden.
2. **Sicherheitsaspekt (Safety):** Die unbefugte Offenlegung oder Manipulation von Patientendaten könnte zu falschen medizinischen Entscheidungen führen. Ärzte könnten falsche Medikamente verschreiben oder lebenswichtige Informationen über Patienten könnten in falsche Hände geraten, was die Sicherheit der Patienten ernsthaft gefährdet.

Security-Maßnahme verletzt Safety Es ist möglich, dass eine zur allgemeinen Sicherheit eingeführte Maßnahme negative Einflüsse auf die Safety hat.

1. **Sicherheitsaspekt (Security):** Einführung biometrischer Zugangskontrollen im Labor, um den Zutritt zu sensiblen Bereichen zu reglementieren und unbefugten Zugriff zu verhindern.
2. **Sicherheitsaspekt (Safety):** Biometrische Systeme können jedoch zu Verzögerungen beim Zugang führen, insbesondere wenn Mitarbeiter dringend auf gefährliche Substanzen oder Notfälle reagieren müssen. Verzögerungen könnten die Sicherheit beeinträchtigen, wenn schnelle Reaktionen erforderlich sind.

Safety-Verletzung gefährdet Security Es ist möglich, dass durch eine Safety-Verletzung Sicherheitsrisiken entstehen.

1. **Sicherheitsaspekt (Safety):** Mitarbeiter erhalten keine angemessene Schulung im Umgang mit den Sicherheitssystemen im Labor, wie z.B. Brandschutzsystemen oder Notausgängen.

2. **Sicherheitsaspekt (Security):** Durch die mangelnde Schulung könnten Mitarbeiter unwissentlich Sicherheitssysteme umgehen oder falsch verwenden, was die Integrität der Sicherheitsinfrastruktur gefährden könnte. Unbeabsichtigte Auslösungen von Sicherheitsmaßnahmen durch ungeschultes Personal könnten zu Fehlalarmen führen und die tatsächliche Sicherheit des Labors beeinträchtigen.

1.3 Definitionen

Information Eine Information hat für den Empfänger i.d.R. einen Neuigkeitsgehalt. In der Informatik/IT-Sicherheit sind Informationen immer schützenswerte Güter.

Daten Repräsentation von Informationen z.B. als

- Bytefolge auf der Festplatte
- als Netzwerkpaket

Datensicherheit ist spezifischer als die Informationssicherheit.

IT-System ist ein dynamisches, technisches System, das Daten verarbeitet und speichert.

IT-Verbund ist die Gesamtheit von ... Objekten, die der Aufgabenerfüllung in einem Aufgabenbereich der Informationssicherheit dienen.

1.4 Schutzziele

1.4.1 Übersicht

- Vertraulichkeit (engl. confidentiality)
- Integrität (engl. entegrity)
- Authenzität (engl. authencity)
- Verbindlichkeit, Zurechenbarkeit (engl. accountability)
- Verfügbarkeit (engl. availability)
- Privatheit (engl. privacy)

1.4.2 Vertraulichkeit

Informationen dürfen nur für **autorisierten Personen** zugänglich sein.
Ein spezielles Problem der Vertraulichkeit sind *verdeckte Kanäle* und *Seitenkanalangriffe*.

verdeckte Kanäle

Verdeckte Kanäle sind Kommunikationswege zwischen Systemkomponenten, die unautorisierte Informationen übertragen, indem sie bestehende Kommunikationsmechanismen oder Ressourcen auf unkonventionelle Weise nutzen, oft in einem Versuch, Sicherheitsmechanismen zu umgehen.

Seitenkanalangriffe

Seitenkanalangriffe sind Angriffsmethoden, bei denen ein Angreifer Informationen aus einem kryptographischen System extrahiert, nicht durch direkte Analyse der verschlüsselten Daten, sondern durch Beobachtung von physikalischen Merkmalen wie Stromverbrauch, Laufzeit oder elektromagnetischer Strahlung während des Verschlüsselungsprozesses.

1.4.3 Integrität

Daten sind vollständig und **unverfälscht**.

1.4.4 Authenzität

Nachweisbarkeit der **Identität** eines Subjektes oder Objektes.

1.4.5 Verbindlichkeit

Ersteller von Daten kann diese Erstellung im Nachhinein **nicht abstreiten**.

1.4.6 Verfügbarkeit

Zugang und Befugnisse bleiben innerhalb der festgelegten Grenzen und werden nicht von unbefugten Dritten beeinflusst.

Berechnung der Verfügbarkeit

$$Verfuegbarkeit = \frac{Gesamtlaufzeit - Gesamtausfallzeit}{Gesamtlaufzeit}$$

1.4.7 Privatheit

Gewährleistung des informa4onellen Selbstbes4mmungsrechts und der Privatsphäre

1.5 IT-Sicherheit

Ziel der IT-Sicherheit ist: *Gewährleistung eines oder mehrerer Schutzziele für Daten, Dienste und Anwendungen*

1.5.1 Security-Policy

Eine Security-Policy besteht aus:

- Festlegung von Schutzzielen und Menge an Regeln.
- Festlegung der Maßnahmen zum Erreichen der Schutzziele.
- Festlegung von Verantwortlichkeiten und Rollen.

1.5.2 Gefahr

Eine Situation oder ein Sachverhalt führt zu negativen Auswirkungen. Es gibt jedoch keinen *zeitlicher*, *räumlichen* oder *personellen* Bezug.

1.5.3 Bedrohung

Eine Bedrohung ist eine **Gefahr** mit *zeitlichem*, *räumlichen* und *personellen* Bezug zu einem Schutzziel.

1.5.4 Schwachstelle/Vulnerability

Eine Schwachstelle ermöglicht das Umgehen der bestehenden Sicherheitsmaßnahmen durch technische oder organisatorische Mängel.

1.5.5 Gefährdung

Möglichkeit des *zeitlichen* oder *räumlichen* Zusammentreffens eines schützenswerten Gutes mit einer Schwachstelle.

1.5.6 Angriff

Ein Angriff ist ein unautorisierter Zugriff oder Zugriffsversuch auf auf IT-Systeme oder Informationen. Angriffe nutzen immer *Schwachstellen* aus.
Man unterscheidet zwei Kategorien von Angriffe:

aktiv Ziel ist *Informationsgewinnung*. Schutzziele *Vertraulichkeit*, *Privatheit*. Beispiel: Abhörung von Datenleitungen

passiv Ziel ist *Informationsveränderung*. Schutziele *Integrität*, *Authenzität*, *Verbindlichkeit* und *Verfügbarkeit*. Beispiel: Vortäuschen einer falschen Identität

1.5.7 Angreifer

Ein Angreifer ist eine *Person*, *System* oder eine *Personengruppe*, die einen Angriff ausführt.

Kapitel 2

Malware

Bei Malware unterscheidet man vorallem zwei wesentliche Aspekte:

- Verbreitungsweg
- Schadroutine

2.1 Die Sicht des Anwenders

Aus der Sicht des Anwenders können selbst im Allgemeinen als *positiv* gesehene Anwendungen b̈osartigesV̈erhalten aufweisen. Solche Fälle von M̈alwarewären dann z.B.

CD-Kopierschutz verhindert das Kopier der Daten auf einer CD

Bundestrojaner

2.2 Malware-Typen

2.2.1 Computer Virus

Ein Virus *infiziert* seinen Wirt durch Einfügen *eigenen* Fremdcodes, um sich selbst zu replizieren.

Phasen

Man unterscheidet bei einer Virus-Infektion zwischen drei Phasen.

Insertion Phase der Virus pflanzt seinen (Schad-)Code in das fremde Programm ein.

Execution Phase der Virus bzw. das Wirtsprogramm wird ausgeführt.

Replication der Virus pflanzt sich fort.

Typen

Viren werden in verschiedene Arten klassifiziert. Es gibt unter anderem:

Bootviren befällt den Computer bei Start des Systems.

Dateivirus befällt eine ausführbare Datei.

Makrovirus befällt Dokumente mit Makrofunktionalität (Excel, Word, Powerpoint).

Erschwerung der Erkennung

Zur Erschwerung der Erkennung von Viren gibt es verschiedene Strategien.

verschlüsselte Viren Der Großteil des Viruscodes ist, bis auf eine Sequenz zum Entschlüssen, mit einem einfachen Verschlüsselungsprozess (wie $VirusBody \oplus 123$) verschlüsselt. Dieses Vorgehen erschwert die Erkennung deutlich, da der Großteil dadurch einfach als ein scheinbar zufälliger String erkannt wird. Es ist jedoch möglich, den Virus über die unverschlüsselte Entschlüsselungsmethode zu erkennen.

polymorphe Viren polymorphe Viren verändern ihr Erscheinungsbild während sie sich replizieren. Wie in der Medizin, mutieren sie. Dies geschieht durch eine sogenannte eine Mutation Engine. Diese nutzt Techniken wie Obfuscation oder fügt Garbage Code ein. Dies macht eine signaturbasierende Erkennung nahezu aussichtslos.

metamorphe Viren metamorphe Viren schreiben sich während der Replikation vollständig selber. Das führt zu einem immer unterschiedlichen Virus Code im RAM.

2.2.2 Trojaner

Ein Trojaner besitzt, neben der bekannten und gewünschten Funktion, eine weitere unerwünschte Funktion (oftmals Backdoor). Ein Trojaner muss allerdings aktiv von einem Benutzer ausgeführt werden, damit es zu einem Effekt kommen kann.

2.2.3 Wurm

Ein Wurm ist ein sich selber replizierendes Schadprogramm.

Verbreitungswege

- E-Mail
- P2P Netze
- Instant Messaging
- IRC
- Wechseldatenträger wie USB-Sticks und Festplatten.

2.2.4 Ad-/Spyware

Ad- und Spyware ist Software, die im Bundle mit anderen Programmen installiert wird und das Verhalten des Nutzers auswertet (Spyware) oder Werbung einblendet(Adware)

2.2.5 Rootkits

Ein Rootkit manipuliert Teile des Betriebssystems um,

- unberechtigte Zugriffe zu ermöglichen
- Anmeldeprozesse und Daten zu verbergen (Prozesstabelle oder Logdateien)
- das System zu überwachen (Keylogger, Netzwerkverkehr).

2.2.6 Botnet

Ein Botnet bezeichnet die Menge automatisierter Schadsoftware auf vernetzten Rechnern.

2.3 Advanced Persistent Thread

Das APT bezeichnet einen *komplexen*, *zielgerichteten* und *effektiven* Angriff über eine lange Zeit.

2.3.1 Begriffsbedeutungen

Advanced Der Angreifer hat erweiterte Kenntnisse, lange Vorbereitungszeit und erhebliche Ressourcen.

Persistent Es gibt einen unberechtigten Zugriff auf Opfersystem über einen langen Zeitraum.

Threat Der Angreifer verfolgt ein klares Ziel und ist hochqualifiziert.

2.4 Schutzmaßnahmen

2.4.1 Virenscanner

Ein Virenscanner ist eine Software zur Erkennung von Viren.

Erkennungsmethoden

Signaturen : Statische Signaturen für bekannte Viren

Heuristiken : Generische Signaturen für Virenfamilien

Sandboxing : Ausführen des Virus in einer isolierten Umgebung.

2.4.2 Firewall

Eine Firewall dient zur Kontrolle des Netzverkehrs zwischen dem Internet und einem internen Netz.

2.4.3 IDS und IPS

Intrusion Detection System (IDS)

Das IDS dient der Erkennung von Angriffen und Generierung von Warnmeldungen.

Intrusion Prevention System (IPS)

Das IPS dient der Unterbindung von Angriffen

Problematiken

Die Problematiken von *IPS* und *IDS* umfassen vorallem falsch **negativ** aber auch falsch **positve** Ergebnisse.

2.4.4 Honeypot

Der Honeypot ist ein scheinbar verwundbares IT-System, das den Angreifer anlocken/vom eigentlichen wichtigen System ablenken soll.

2.4.5 Pentesting

Das Pentesting bezeichnet die *berechtigte* Durchführung von Angriffen zwecks Bewertung von Sicherheitsaspekten auf ein System.

Kapitel 3

Kryptologie

Klassische Kryptologie diente der Geheimhaltung von Nachrichten (*Vertraulichkeit*).

Moderne Kryptologie (seit 1976) dient der sicheren Konzeption und Konstruktion von IT-Systemen. (*Vertraulichkeit, Integrität, Authenzität, Verbindlichkeit*)

3.1 Geschichte der Kryptologie

3.1.1 Monoalphabetische Substitutionschiffren

Verschlüsselung basierend auf Permutation des Alphabetes.
Beispiel: *Caesar-Chiffre*

3.1.2 Polyalphabetische Chiffren

Nutzung mehrerer monoalphabetischer Chiffren.
Beispiel: *Vignenere-Chiffre*

3.1.3 Kerckhoffs Prinzipien

1. Das System musst praktisch unentzifferbar sein.
2. Das System darf öffentlich zugänglich sein, ohne dadurch die Sicherheit zu gefährden.
3. Der Schlüssel muss kommunizierbar sein.
4. Es muss auf Kommunikation anwendbar sein.
5. Es musst durchführbar sein.
6. Das System muss einfach zu nutzen sein.

3.2 Symmetrische Kryptografie

Beide Kommunikationspartner nutzen den gleichen Schlüssel k. Der Schlüssel muss ausgetauscht werden. Es gilt:

$$Dec_k(Enc_k(m)) = m$$

3.2.1 Caesar-Chiffre

Eigenschaften

Schlüsselraum 26

Schwachstelle Brute-Force

Bei der Caesar-Chiffre werden alle Buchstaben des Alphabetes um einen Wert k nach rechts verschoben.

Sicherheit

Das Caesar-Chiffre ist aufgrund von relativ wenig Möglichkeiten des Schlüssels (1-26) sehr schnell zu überwinden. Im Falle eines Brute-Force Angriffes, erhält man allerspätestens nach 25 Durchläufen den Klartext.

3.2.2 Schlüsselraum

Der Schlüsselraum beschreibt die Größe eines Schlüssels und den daraus resultierenden möglichen Kombinationen.
Eine Schlüssellänge von 64 Bit, also ein Schlüsselraum von 2^{64} ist nicht mehr sicher. Das BSI empfiehlt für..

symmetrische Verfahren $k \geq 128$ Bit

asymmetrische Verfahren $\geq$ 3000 Bit (Faktorisierung, diskreter Logarithmus) bzw. $\geq$ 250 Bit (elliptische Kurven)

asymmetrische postquanten Verfahren $\geq$ 15632 Bit (strukturierte Gitter) $\geq$ 524160 Bit (code basiert)

3.2.3 One-time Pad

Das One-Time Pad bietet zwar perfekte Sicherheit, ist jedoch praktisch nicht anwendbar. Der Schlüssel k ist

- zufällig geniert
- nur einmal genutzt
- so lang wie die verschlüsselte Nachricht

Für die Verschlüsselung bzw. Entschlüsselung gilt:

$$c = m \oplus k$$

$$m = c \oplus k$$

3.2.4 Perfekte Sicherheit

Ein Verschlüsselungsverfahren ist *perfekt sicher*, wenn es gegen Angreifer mit unbegrenzten Ressourcen sicher ist.

3.2.5 Sicherheitsniveau

Ein Kryptoverfahren hat ein Sicherheitsniveau von n Bits, wenn ein Angreifer 2^n Versuche benötigt, um das Verfahren zu brechen.

3.3 Zufallszahlen

Zufallszahlen werden in der Kryptografie häufig verwendet. Man unterscheidet zwischen

Echter Zufall basierend auf physikalischen Phänomenen.

Pseudozufallszahlen basierend auf deterministischen Algorithmen.

3.3.1 Echte Zufallszahlengeneratoren (TRNG)

Echte Zufallsgeneratoren erzeugen echte Zufallszahlen basierend auf physikalischen Phänomenen.

3.3.2 Pseudozufallszahlengeneratoren (PRNG)

Pseudozufallszahlengeneratoren erzeugen ausgehend von einem *Seed* eine Sequenz von Zahlen.

3.3.3 Kryptografisch sichere Pseudozufallszahlengeneratoren (CSPRNG)

krypt. s. Pseuzzg. erzeugen nicht vorhersehbare Zufallszahlen. Beispiele: LFSR

3.3.4 Stromchiffren:

Verschlüsseln Daten in Blöcken fester Größe, z.B. AES, durch Anwendung von Schlüssel- und Substitutions-/Permutationsoperationen.

3.3.5 Blockchiffren:

Arbeiten, wie DES, ähnlich wie Stromchiffren, verwenden jedoch eine feste Anzahl von Runden für die Verschlüsselung von Datenblöcken.

3.4 Hashfunktionen

Das Ziel von Hashfunktionen ist die *Integritätsprüfung*. Hashfunktionen bilden einen Bitstring beliebiger Länge auf einen Bitstring fester Länge ab. Ein Nachteil von Hashfunktionen sind mögliche Kollisionen, sodass zwei unterschiedliche Eingangswerte denselben Ausgangswert zur Folge haben.

3.4.1 Kryptografische Hashfunktionen

krypt. Hashfunktionen müssen effizient berechenbar sein, Kollisionsresistent sein und Einwegeigenschaften haben.

3.4.2