Datensicherheit, Lösungsvorschlag Prüfung WS 2022/23

Henry Haustein, Dennis Rössel

Schutzziele, was bedeuten Sie?

Schutzziele:

- Vertraulichkeit: nur der bestimmte Empfänger kann die Nachricht lesen
- Integrität: die Daten sind nicht manipuliert worden
- Verfügbarkeit: [nicht mit Kryptografie erreichbar]

Wie funktioniert ein symmetrisches Authentikationssystem? Wie wird die MAC geprüft?

Neben der Nachricht wird auch eine MAC mitgeschickt. Die MAC wird berechnet, indem die Nachricht mit einem Schlüssel verschlüsselt wird. Auf Empfängerseite kann dann einfach die empfangene Nachricht auch verschlüsselt werden und es wird verglichen, ob das mit der MAC übereinstimmt.

Was ist ein IT-Sicherheitskonzept? Anforderungs- und Risikoanalyse, Maßnahmen

IT-Sicherheitskonzept:

- Was, Wovor und Wie schützen?
- Anforderungsanalyse:
  - Welche Objekte (Anwendungen, Netze, Informationen, ...) relevant
  - Schutzbedarf (normal, hoch, sehr hoch)
- Risikoanalyse:
  - Risiko-Identifikation (Bedrohungen und Schwachstellen)
  - Risiko-Einschätzung (Eintrittswahrscheinlichkeit)
  - Risiko-Bewertung (Einstufung Risiko + Ausmaß für Maßnahmen)
- Maßnahmen

Wie ist die Risikoanalyse klassifiziert? (qualitativ, quantitativ, Risikomatrix)

quantitativ: Eintrittswahrscheinlichkeit · Schadenshöhe → schwierig zu schätzen

qualitativ mittels Risikomatrix: Risikoklassen gering, mittel, hoch, sehr hoch → Einschätzung, was tragbar ist und was nicht mehr tragbar ist

Was ist Sicherheit? Gibt es einen Endpunkt?

Sicherheit ist ein Prozess ohne Endpunkt. Es gibt keine 100%-ige Sicherheit, da es immer neue Schwachstellen gibt, die behoben werden müssen.

Was ist Steganographie? Wo wird es eingesetzt? Welche Methoden gibt es?

Bei der Steganographie geht es darum, eine Nachricht in unverdächtigen Daten zu verbergen. Man schützt nur die Existenz der Nachricht, nicht den Inhalt.

Methoden:

- LSB-Ersetzung
- Inkrementieren/Dekrementieren
- synthetische Steganographie (Erstellen von Coverdaten passend zur Nachricht)
- selektive Steganographie (Suchen von Coverdaten, die die Nachricht bereits enthalten)

Ist die LSB-Ersetzung sicher? Welche Angriffe gibt es dagegen?

LSB-Ersetzung ist nicht sicher, es gibt eine Vielzahl von Angriffen, da das Verfahren bereits gut untersucht wurde. Beispiele für Angriffe:

- visueller Angriff: LSB-Ebene visualisieren
- Histogramm auf LSB-Ebene: Werte, die sich nur im LSB unterscheiden, werden angeglichen
- große Datenmengen + statistische Analysen + KI → Unentdeckbarkeit schwierig