Klassische Sicherheitsprinzipien

Dozent: **Prof. Dr. Michael Eichberg**
Kontakt: michael.eichberg@dhbw-mannheim.de
Version: 2024-02-16

Klassische Sicherheitsprinzipien

(Jerome Saltzer and Michael Schroeder, 1975)

Principle of Economy of Mechanism (aka Principle of Simplicity):

Die Sicherheitsmechanismen sollten so einfach wie möglich sein.

Principle of Fail-Safe Defaults:

Standardmäßig sollte der Zugriff auf Ressourcen verweigert werden.

Principle of Complete Mediation:

Jeder Zugriff auf eine Ressource sollte überprüft werden.

Klassische Sicherheitsprinzipien

Principle of Least Authority (aka POLA)/ Principle of Least Privilege:

Jedes Programm und jeder Benutzer sollte nur die für seine Aufgabe unbedingt notwendigen Rechte besitzen.

Principle of Separation of Privilege:

Ein System sollte in mehrere POLA konforme Komponenten unterteilt sein. Sollte eine Komponente kompromittiert sein, dann sind die Möglichkeiten des Angreifers dennoch begrenzt. (Eng verwandt mit dem POLA.)

Klassische Sicherheitsprinzipien

Principle of Least Common Mechanism:

Die Sicherheitsmechanismen sollten über Nutzer hinweg möglichst wenig Gemeinsamkeiten haben.

Principle of Open Design (vgl. Kerckhoffs Prinzip):

Die Sicherheit des Systems sollte nicht von der Geheimhaltung der Sicherheitsmechanismen abhängen (sondern nur vom Schlüssel).

Beispiel - Principle of Least Common Mechanism

z.B. sollten keine gemeinsamen Speicherbereiche verwendet werden und es ist deswegen sinnvoll - wenn möglich - auf Implementierungen im Kernel zu verzichten und statt dessen auf User-Space-Implementierungen zu setzen.

TCP Connection Hijacking Angriffe wird bzw. wurden z.B. durch die Implementierung des TCP Stacks im Kernel ermöglicht (⇔ „Principle of Least Common Mechanism”).

Wiederholung: Klassische Sicherheitsprinzipien

Principle of Psychological Acceptability:

Die Sicherheitsmechanismen sollten einfach zu verstehen und zu benutzen sein.

Principle of Isolation:

Die Sicherheitsmechanismen sollten so entworfen sein, dass Fehler in einem Teil des Systems nicht die Sicherheit des gesamten Systems gefährden; d.h. die einzelnen Komponenten sollten möglichst unabhängig voneinander sein und nur über wohldefinierte Schnittstellen miteinander kommunizieren und entsprechende Sicherheitsüberprüfungen durchführen.

Beispiel - Principle of Isolation:

Typischerweise kommuniziert zum Beispiel ein Basebandchip (WIFI, LTE, 5G, ...) mit dem Betriebssystem über eine minimale Schnittstelle über die nur Nachrichten übermittelt werden können, die leicht auf ihre Korrektheit überprüft werden können. Insbesondere erfolgt kein direkter Zugriff auf den Speicher des Betriebssystems.

Einen Angreifer ist es somit ggf. möglich den Basebandchip anzugreifen und ggf. zu kompromittieren, aber er kann nicht direkt auf das Betriebssystem zugreifen und Nachrichten, die bereits auf Betriebssystem oder Anwendungsebene verschlüsselt werden, sind weiterhin sicher.

ergänzende Sicherheitsprinzipien

Principle of Modularity:

Die Sicherheitsmechanismen sollten so entworfen sein, dass sie unabhängig voneinander implementiert und geprüft werden können.

Principle of Layering:

Die Sicherheitsmechanismen sollten in Schichten organisiert sein.

Principle of Least Astonishment:

Die Sicherheitsmechanismen sollten so entworfen sein, dass sie keine Überraschungen für die Benutzer bereithalten.

Beispiel für ein Schutzsystem für Netzwerke, dass mehrere Schichten verwendet:

- einfache (und effiziente) Paketfilter auf unterster Ebene
- zustandsbehaftete Paketfilter auf der nächsten bzw. der Anwendungsebene