Repetitionsblatt 1

Security Requirements

21.06.2019

Inhaltsverzeichnis

Erklären Sie den Unterschied zwischen Security und Safety und wie die beiden Begriffe zusammenhängen.

- Security: Schutz des Systems vor Unfug und Schabernack
- Safety: Schutz der Umwelt vor Systemen, die schlecht / falsch funktionieren (Flugzeugabsturz)

Security *kann* Auswirkungen auf Safety haben.

Was versteht man unter Perimeter Security und warum reicht die nicht aus?

Sicherheitsmassnahmen, die an der Aussengrenze eines Systems getroffen werden, z.B. Firewall, Authentifizierung... Diese reichen i.d.R. nicht aus: Insider Threads, Schutz *nach* dem Eindringen, Aussengrenze kann oft nicht mehr genau definiert werden etc.

Massnahmen, die *nicht* Perimeter Security sind:

- Netzwerksegmentierung
- System Monitoring
- ...

Erklären Sie die Begriffe Vulnerability (Schwachstelle) und Exploit.

- *Vulnerability*: Ein generelles Sicherheitsrisiko; eine Situation, die nicht vorgesehen war. Kann in der Software, Konfiguration usw. liegen.
- *Exploit*: Ein Weg, die Schwachstelle auszunützen.

Warum muss Security von Beginn an in einem Software-Entwicklungsprojekt berücksichtigt werden?

- Grundsätzliches Design kann nachträglich oft nicht mehr geändert werden.
- Nachträgliche Anpassungen kosten mehr.

Erklären Sie den Unterschied zwischen Anforderungsanalyse, Spezifikation und Design.

- Anforderungsanalyse: Anforderungen an System, Kundenwünsche (*Wofür*)
- Spezifikation: (*Was*)
- Design: (*Wie*)

Was ist ein Prozessmodell der Software-Entwicklung und welche Modelle gibt es?

Beschreibt die zeitliche Anordnung, Schritte.

- Wasserfall-Modell
- V-Modell
- Unified Process
- Scrum
- Devops
- ...

Was sind die 7 Phasen des MS Security Development Lifecycles (SDL)?

1. Training (projektunabhängig)
2. Requirements
3. Design

4. Implementierung
5. Verifikation: Testen
6. Release: Rahmenbedingen, Anleitungen, Setup-Programme für die Installation
7. Response (projektunabhängig): Patch-Zyklen etc.

Welche Festlegungen müssen im Trainingsprogramm für SDL getroffen werden?

- Mindestanforderungen (*Inhalt*) definieren.
- Grad (*Prozentsatz der geschulten Programmierer*)

Was ist ein Bug Bar?

a) Käfer-Beiz
b) Wie viele der Threats müssen behandelt sein. (z.B: 100% der High Risks, 50% der Low Risk Bugs)

Was versteht man unter Threat Modeling?

Bedrohungsanalyse. Aus der Sicht des Angreifers (was kann angegriffen werden) + Massnahmen (*Mitigations*).

Was ist der Unterschied zwischen funktionalen und nicht-funktionalen Sicherheitsanforderungen? Geben Sie jeweils einige Beispiele.

- Funktionale Sicherheitsanforderungen: Können als Funktion implementiert werden. (Verschlüsselte Übertragung, Passwort-Anforderungen, ...)
- Nicht-funktionale Anforderungen: Qualitative Anforderungen, die nicht mit einer einzelen Funktion abgedeckt werden (Performance, abhörsicher)

FA beschreiben *was* gemacht werden muss, NFA beschreiben *wie*.

Beispiele für NFA:

- Security

- Safety
- Performance
- Maintainability

Nicht-funktionale Anforderungen sollten wenn möglich auf funktionale Anforderungen heruntergebrochen werden, und klare Testfälle definiert werden.

Abhörsicher (NFA) –> Verschlüsselte Übertragung (FA), Authentifizierung (FA)

Welche Hilfsmittel/Dokumente können zum Identifizieren von Bedrohungen herangezogen werden?

Wichtige Standard-Kataloge:

- OWASP (Web)
- Common Criteria
- Bestimmte Dokumente (müsste man auf den Folien schaun)
- ...

Wo findet man wichtige Standardkataloge für mögliche Bedrohungen?

Auf den Folien.

Was versteht man unter einem Protection Profile (Schutzprofil)? Nennen sie zumindest zwei Beispiele für Schutzprofile.

- allgemeine Zusammenstellung von Sicherheitsanforderungen (gemäss Common Criteria)
- Dokument, das Teil des Zertifizierungsprozesses ist
- dient Herstellern zur Erklärung der Sicherheitsfunktionen ihrer Produkte und zur Orientierung bei deren Entwicklung
- Beispiel: Sicherheitsanforderungen an intelligente Stromzähler; Auslesen von Reisepässen; Tachometer (BSI)

Was ist der spezielle Fokus der OWASP-Dokumente?

Webapplikationen

Gibt es gesetzliche Vorschriften, die Security-Maßnahmen bei der Software-Entwicklung erfordern? Geben Sie zumindest 2 Beispiele.

Ja. Zum Beispiel:

- Datenschutz, Privatsphäre
- PCIDSS
- Finanzbranche: Sarbanes Oxley Act
- Medizin

Was ist der Unterschied zwischen einem Threat (Bedrohung), einer Vulnerability (Schwachstelle) und einer Mitigation?

- *Threat*: Situation, bei der eine Schwachstelle ausgenutzt wird
- *Vulnerability*: Angriffspunkt
- *Mitigation*: Geplante Gegenmassnahme, um diesen Angriff zu erschweren

---

Aus welchen Schritten besteht der Threat Modeling Prozess?

1. Identify the Assets: Was muss ich schützen?
2. Systemanalyse / Architektur
3. Applikation unterteilen
4. Bedrohungen feststellen
5. Schwachstellen
6. Gegenmassnahmen

Was sind Trust Boundaries?

Dort wo zwei Vertrauensgrenzen aneinander stossen. Wo habe ich Einfluss auf die Sicherheit und wo nicht?

- Päulis Webshop & Payment Service Provider

Was sind die 6 Elemente der STRIDE Attack Classification? Erklären Sie diese 6 Elemente einzeln.

- *Spoofing*: Ausgeben als andere Person / System
- *Tampering*: Daten ändern (Kontonummern, Rechnungsbeträge etc.)
- *Repudiation*: Massnahmen zur Abstreitbarkeit (Logfiles manipulieren, andere Benutzerkonten verwenden etc.)
- *Information disclosure*: Daten zugänglich machen
- *Denial of service*: Überlastung von System / Diensten
- *Elevation of Privilege*: Höhere Rechte aneignen

Führen Sie für jedes dieser 6 Elemente geeignete Mitigation Maßnahmen an.

- *Spoofing*: Passwörter schützen, Authentifikation etc
- *Tampering*: Authorization, Hashes, digitale Signaturen
- *Repudiation*: Digitale Signaturen, Timestamps, Audit trails, sicheres Logging
- *Information disclosure*: Authorizazion, sichere Protokolle, Verschlüsselung, Schutzmassnahmen, Don't store secrets.
- *DoS*: Throttling, Filtern, Authentication / Authorization
- *Elevation of Privileges*: Run with least privileges