Repetitionsblatt 2

Security Requirements

21.06.2019

Inhaltsverzeichnis

DREAD: Erklären Sie die Begriffe *Damage*, *Reproducibility*, *Exploitability*, *Affected Users* und *Discoverability*

- Damage: *how bad would an attack be?*
- Reproducibility: *how easy is it to reproduce the attack?*
- Exploitability: *how much work is it to launch the attack?*
- Affected Users: *how many people will be impacted?*
- Discoverability: *how easy is it to discover the threat?*

Nennen Sie wenigstens 5 Punkte aus der OWASP Threat List.

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Corss-Site Scripting (XSS)
8. Insecure Deserialization
9. Using components with known vulnerabilities
10. Insufficient Logging & Monitoring

Was sind die 4 Hauptkategorien beim OWASP Risk Rating?

- Thread Agent
  - *skill level*
  - *motivation*
  - *opportunity*
  - *size*
- Vulnerability
  - *ease of discovery*
  - *ease of exploit*
  - *awareness*
  - *intrusion detection*
- Technical impact
  - *loss of confidentiality*
  - *loss of integrity*
  - *loss of availability*
  - *loss of accountability*
- Business impact
  - *financial damage*
  - *reputation damage*
  - *non-compliance*
  - *privacy violation*

Was versteht man unter einem Attack Tree?

Ein *Attack Tree* ist ein konzeptuelles Diagramm, das aufzeigt, wie ein Ziel angegriffen werden kann.

Besteht aus einem `root` (*Ziel des Angriffs*) und `nodes` (*notwendige Schritte zum Ziel*).

Die Knoten können mit OR (Standard) oder AND (mit Bogen) verbunden sein. Bei AND-Verknüpfungen müssen beide erfüllt sein um den Parent auf `true` zu setzen. Der Wert ist bei AND die Summe der beiden Knoten, bei OR der kleinere der beiden Werte.

Welche Knotenbewertung können in einem Attack Tree vorgenommen werden. Nennen Sie mindestens 4 Möglichkeiten.

1. Möglich / unmöglich

2. Angriffskosten
3. Nötige Zeit für den Angriff / für die Abwehr
4. Wahrscheinlichkeit für gelungene Attacke
5. Wahrscheinlichkeit für erneuten Angriffsversuch

Wenn in einem Attack Tree ein Knoten N zwei Folgeknoten N1 und N2 hat, die mit UND verbunden sind und N1 eine Bewertung von 300 für die Kosten des Angriffs hat und N2 eine Kostenbewertung von 500, welche Bewertung bekommt N?

Bei AND Verbindungen wird die Bewertung aus der Summe der beiden Knoten berechnet:

$$Wert = 300 + 500 = 800$$

** Wenn in einem Attack Tree ein Konten N zwei Folgeknoten N1 und N2 hat, die mit ODER verbunden sind und N1 eine Bewertung vvon 300 für die Kosten des Angriffs hat und N2 eine Kostenbewertung von 500, welche Bewertung bekommt N?**

Bei einer OR Verbindung ist die Bewertung der Wert gleich Wert des tiefsten Knotens:

$$Wert = 300$$

Was sind Misuse Cases?

Use Case, der von einem Attacker ausgeführt wird, und einen regulären Use Case bedroht oder ausgenutzt wird.

Beispiel: “Sniffing Attack” als Misuse Case für den Use Case “Mit Benutzername und Passwort anmelden”

Was sind Mitigation Use Cases?

Ein *Mitigation Use Case* ist ein Use Case, der einen Misuse Case mitigiert.

Warum sollen in einem Use Case DIagramm auch Misuse Cases modelliert werden?

Zum Aufzeigen, wie ein Use Case ausgenutzt / bedroht werden kann.

Was sind die wesentlichen Teile einer Misuse-Case-Beschreibung?

- Misuse Case Name
- Misuser Profile (Angreifer)
- Beschreibung
- Pfad
- Alternativpfade
- Auslöser
- Annahmen
- Mitigations

Was versteht man unter Input Validation?

Prüfen von Eingaben (Benutzereingaben, Anfragen an ein System), Plausibilitätsprüfung (Sanity Check):

- Datentyp
- Wertebereich/Wertemenge
- Länge/Grösse

Warum besteht bei einer Schnittstellen-Kommunikation eine Problem, wenn die Entschlüsselung der Verschlüsselung einer Nachricht geringfügig von der originalen Nachricht abweicht?

Kryptografische Verfahren arbeiten mit dem avalanche Effect, wonach kleinste Abweichungen in der Eingabe signifikante Abweichungen in der Ausgabe zur Folge haben, sodass man das Verfahren nicht mittels Annäherung angreifen kann.

Eine falsch entschlüsselte Nachricht weicht deshalb sehr stark von der originalen, verschlüsselten Nachricht ab.

Definiert man die Eingabe für ein System als formale Sprache mit Hilfe einer Grammatik - welche Eigenschaft sollte diese Sprache bzw. doe Grammatik aus Sicherheitsgründen haben?

Eine definierte Menge an erlaubten Zeichen.

In welcher Form sollte die Input Validation einer Eingabesprache implementiert werden?

Whitelisting ist besser als *Blacklisting*.

Was versteht man unter einem Parser-Generator?

Ein Parser-Generator ist ein Programm, as aufgrund einer Syntax-Spezifikation ein Parser-Programm erstellt.

Warum sind Längenfelder in Protokollen problematisch?

Gefälschte / falsche Längenfelder können dazu führen, dass falsche Speicherstellen referenziert werden (–> Heartbleed), was zur Herausgabe heikler Daten führen kann (Auslesen von Arbeitsspeicher).