Seminarangebot SWA-SEC

Sichere Architekturen

Stand 2026-03

Architektur ist die Menge der Entscheidungen, die später schwierig, wenn nicht sogar aus ökonomischer oder technischer Sicht unmöglich, zu ändern sind. Oftmals müssen aber viele davon bereits zu Beginn eines Projektes getroffen werden.

Insbesondere die Qualitätsmerkmale eines Systems werden von solchen schwierigen Entscheidungen geprägt. In der Regel ist es deutlich einfacher einen weiteren Anwendungsfall umzusetzen als z.B. die Performance drastisch zu verbessern oder die Bedienbarkeit spürbar zu steigern. Oder nachträglich Sicherheit einzubauen.

Im Gegensatz zu Sicherheitslücken, welche durch bloße Implementierungsfehler entstehen, sind Sicherheitsprobleme in der Architektur meist nur mit erheblichem Umstrukturierungsaufwand zu beheben, im schlimmsten Fall werden wesentliche Sicherheitskonzepte überhaupt nicht abgedeckt.

In diesem Seminar erarbeiten wir, wie du Sicherheitsaspekte beim Systementwurf von Anfang an berücksichtigst, ohne dabei „Big Design Up Front“ zu betreiben. Da die Umsetzung von Sicherheitsmaßnahmen oft den Einsatz von Kryptografie erfordert, erlernst du die für die Architektur wichtigsten Konzepte, von Hashing bis PKI, Kryptoagilität bis Post-Quanten-Kryptografie. Immer genau in der Detailtiefe, die du für deine Architekturentscheidungen benötigst.

Du wirst alles, was du theoretisch erlernst, direkt in einem praktischen Beispiel anwenden. Im Verlauf der Schulung wirst du eine Architektur entwerfen, diese strukturiert mit unterschiedlichen Vorgehensmodellen zur Bedrohungsanalyse auf Schwachstellen untersuchen und iterativ verbessern.

Am Ende wird deine Architektur so gut sein, dass du am liebsten gleich ein Start-Up gründen möchtest. Wäre da nicht dieser kleine Haken an der Sache…

Software Security
Hannes Molsen
Wieselgang 7 | 23683 Scharbeutz
mail@sosec.de | 0162/7160342
Steuernummer 25/077/04553

INHALT

Einführung und Analyse

- Begrifflichkeiten, CVEs, CWEs, CVSS, …
- Schutzziele
- Sicherheit als Qualitätsmerkmal
- Richtlinien und Zertifizierungen

Bedrohungsanalysen

- Assets identifizieren, Angriffsbäume erstellen, STRIDE

Sicherer Design-/Entwicklungsprozess

- Frameworks: OpenSAMM, MS SDL, BSIMM
- Input Validation und Output Escaping
- Zugriffskonzepte
- Security-Analyse: SAST, DAST, IAST, SCA
- Incident Management

Angewandte Kryptographie

- Grundbegriffe
- Symmetrische und asymmetrische Kryptographie, Hashfunktionen
- Schlüsselaustauschverfahren, PKIs, Trust on First Use
- Sichere Zufallszahlen
- Transport Layer Security

Web: Technische Grundlagen

- OAuth, OpenID Connect, SAML2, JWT

Web: Mögliche Angriffsvektoren

- Injection-Angriffe
- DoS / DDoS-Angriffe
- Machine-in-the-Middle-Angriffe
- Social Engineering

Web: Security und Infrastruktur

- Web Application Firewalls
- Intrusion Detection / Intrusion Prevention, Logging und Monitoring

VORAUSSETZUNGEN

Es sind keine besonderen Vorkenntnisse erforderlich.

TEILNEHMERINNENZAHL

Das Seminar kann für 4-10 Personen angeboten werden.

RAHMENBEDINGUNGEN

Das Seminar findet an 3 aufeinanderfolgenden Tagen statt und kann sowohl als Präsenzveranstaltung wie auch remote als Live Online Seminar durchgeführt werden.

Tag 1:	9:00 – 16:30
Tag 2:	9:00 – 16:30
Tag 3:	9:00 – 15:30

LIVE ONLINE SCHULUNG

Online-Schulungen finden über Zoom statt. Die Einwahldaten werden etwa eine Woche vor der Schulung übermittelt.

Ich empfehle, dass du dich im Vorfeld mit der Plattform Zoom vertraut machst. Damit auch alle benötigten Zoom-Features zur Verfügung stehen, muss eine App ausgeführt werden. Vor der Schulung solltest Du testen, ob alles funktioniert: https://zoom.us/test.

Apps gibt es für PC, Mac, iOS oder Android. Für die Bildschirmfreigabe empfiehlt sich aber eine Teilnahme vom Rechner (PC, Mac): https://zoom.us/download.

Im Notfall geht es auch per Browser, der Funktionsumfang ist jedoch reduziert und Gruppenübungen sind dann nur eingeschränkt möglich.

Bitte schalte während der Schulung deine Kamera ein. Das visuelle Feedback ist für eine interessante und den Teilnehmenden angepasste Schulung unerlässlich.