Technische Universität Ilmenau 8. April 2024

Vorlesung

Security Engineering

Dr. Peter Amthor

NeXTeX

Vorlesungsmitschrift von
Adrian Schollmeyer

Inhaltsverzeichnis

1 Introduction

1.1 What is Security Engineering?

- Zugriffssteuerung
- Methoden zur Absicherung von Software
- Spezialisierte Methoden für Softwareentwicklung; zieht sich durch alle Schritte des Softwareentwicklungsprozesses, ist also ein *Cross-Cutting-Concern* in der Softwareentwicklung: Security Requirements, Security Model, Security Testing (z. B. SAST), SecDevOps

Konkret ist Security Engineering eine Spezialform der Softwareentwicklung, bei der besondere security-spezifische Teilmethodiken/Artefakte/Modelle benutzt werden, um Sicherheitsanforderungen umzusetzen. Ziel ist die Garantie nichtfunktionaler Sicherheitsanforderungen. Dies umfasst alles von der Technologie bis zum Projektmanagement.

Beispiel: Vertraulichkeit als Anforderung muss zu jedem Zeitpunkt berücksichtigt werden. Im Design müssen verschiedene Benutzerrollen vorgesehen werden, die mit Authentifizierung und Autorisierung umgesetzt werden müssen. Die korrekte Funktion dieser muss getestet werden.

Damit dieser Prozess beherrschbar bleibt, ist Automatisierung mit entsprechenden tools zwingend notwendig.

1.2 Why do we need Security Engineering?

Egal ob Code offen zugänglich oder versteckt ist, sollten wir davon ausgehen, dass Angreifer auf allen Phasen des Softwareentwicklungsprozesses unterwegs waren.

Angreifer laufen den Softwareentwicklungsprozess normalerweise rückwärts ab:

- Ausnutzung einer laufenden Software (z. B. infizierter E-Mail-Anhang wird geöffnet)
- Privilege Escalation: Einsatz eines Programms, um mehr Berechtigungen zu erlangen
- Implementierung von Schadcode auf der Opfer-Infrastruktur, um den Zugang dauerhaft zu erhalten.
- Entwurf von Zielen, die der Angreifer auf dem Opfer-System erreichen will

Wenn jedoch formal gezeigt werden kann, dass die Umsetzung von Sicherheitsanforderungen entlang des Softwareentwicklungsprozesses formal verifizierung lässt, kann man zeigen, dass es nicht am Sicherheitsmodell gelegen haben kann, wenn etwas schief geht. Dies ist allerdings schwierig bis unmöglich zu beweisen.

Literatur

[1] Peter Amthor. “Security Engineering”.