Gregor Engels, Regina Hebig, Matthias Tichy (Hrsg.): SE 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 123

Identifizierung von Vertraulichkeitsproblemen mithilfe von Angriffsausbreitung auf Architektur[1]

Maximilian Walter[2], Robert Heinrich[3], Ralf Reussner[4]

Keywords: Angreiferpropagation, Software-Architektur, Sicherheit

1 Einleitung und Übersicht

Wir sind dabei immer mehr verschiedene Bereiche unseres täglichen Lebens zu digitalisieren. Diese Systeme haben gemeinsam, dass sie häufig dynamische Zugangskontrollsysteme zusammen mit einer Vielzahl verschiedener verbundener Elemente, wie Komponenten oder Geräte, verwenden. Jedoch sind diese Systeme häufig verwundbar. Angreifer können die einzelnen verwundbaren Elemente zusammen mit legitimen Zugriffsberechtigungen nutzen, um einen verketten Angriffspfad durch die Architektur zu bilden. Daher ist es sinnvoll, diese Abhängigkeit zwischen Zugangskontrollrichtlinien und Schwachstellen zu analysieren. Zwar gibt es bereits Ansätze für die automatische Generierung von Angriffspfaden auf der Grundlage von Schwachstellen und Zugriffskontrolle, wie z.B. Bloodhound[5] bei Active Directory, doch sind Ansätze sehr auf einen Anwendungsbereich bezogen oder setzen häufig ein lauffähiges System voraus und können nicht während der Entwurfszeit oder der Wartung des Systems verwendet werden. Daher haben wir eine architekturgetriebene Angreiferpropagationsanalyse [Wa22] entwickelt, welche mögliche Ausbreitungen von Angreifern berechnen kann. Dabei haben wir die existierende Architekturbeschreibungssprache das Palladio-Komponentenmodell (PCM) [Re16] mit einer Zugriffskontrollmodellierung und einer Verwundbarkeitsmodellierung erweitert. Dies wird in unserer Analyse genutzt, um von einem möglichen Startpunk alle erreichbaren Architekturelemente zu identifizieren. Wir haben den Ansatz anhand verschiedener Fallstudien evaluiert und erhielten eine hohe Genauigkeit.

[1] Diese Arbeit wurde duch die DFG mit der Projektnummer 432576552, HE8596/1-1 (FluidTrust) und dem Forschungsbereich Engineering Secure Systems (46.23.03) der Helmholtz Gemeinschaft (HGF) durch KASTEL Security Research Labs unterstützt.

[2] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, maximilian.walter@kit.edu
[3] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, robert.heinrich@kit.edu
[4] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, ralf.reussner@kit.edu

[5] `https://bloodhoundenterprise.io/`

2 Modellierung und Analyse

Die Verwundbarkeitsmodellierung passiert auf gängige Standards wie z.B. CVSS[6] und die Zugriffskontrollmodellierung folgt dem Konzept der Attributbasierten-Zugriffskontrolle [Hu15]. Wir haben diese Konzepte in das PCM übertragen. Dies ermöglicht Software-Architekt:innen Verwundbarkeiten und Zugriffsrichtlinien direkt in der Software-Architektur zu spezifizieren. Die Wiederverwendung von bereits gängigen Konzepten unterstützt auch die Möglichkeit existierendes Wissen über die Klassifizierung von Schwachstellen und die Modellierung von Sicherheitseigenschaften wiederzuverwenden.

Die Analyse basiert auf dem KAMP-Ansatz [Ro]. Dieser wurde um neue Ausbreitungsregeln für Angreifer und Änderungen erweitert. Die Analyse berechnet iterativ von einem Startpunkt alle Nachbarelemente und überprüft, ob sie diese kompromittieren kann. Dies ist möglich, wenn es entweder eine Schwachstelle gibt, die die Analyse ausnutzen kann oder die Analyse die passende Zugriffsberechtigung hat. Dabei prüft die Analyse für jede Schwachstelle, ob sie die passenden Fähigkeiten hat. In jedem Iterationsschritt kann zudem die Analyse neue Zugriffsberechtigungen durch das Ausnutzen von Schwachstellen oder gespeicherten Passwörtern sammeln. Am Ende wird eine Liste mit allen potenziell betroffen Elementen zurückgegeben. Diese können Architekt:innen nutzen, um Stellen für Schutzmaßnahmen in die Software-Architektur zu identifizieren, damit diese Angriffspfade brechen können.

3 Data Availability

Wir stellen die Evaluationsdaten öffentlich zur Verfügung [Wa]. Dies umfasst die Modelle, die erwarteten Modelle sowie den Quellcode der Analyse inklusive einer virtuellen Maschine zum Ausführen der Analyse.

Literatur

[Hu15] Hu, V. et al.: Attribute-Based Access Control. Computer 48/2, S. 85–88, Feb. 2015, ISSN: 0018-9162.

[Re16] Reussner, R. et al.: Modeling and Simulating Software Architectures – The Palladio Approach. MIT Press, Cambridge, MA, 2016.

[Ro] Rostami, K. et al.: Architecture-Based Change Impact Analysis in Information Systems and Business Processes. In: ICSA'17. S. 179–188.

[Wa] Walter, M. et al.: Dataset - Architectural Attack Propagation Analysis for Identifying Confidentiality Issues, URL: https://doi.org/10.5445/IR/1000141655.

[Wa22] Walter, M. et al.: Architectural Attack Propagation Analysis for Identifying Confidentiality Issues. In: ICSA'22. IEEE, S. 1–12, 2022.

[6] https://www.first.org/cvss/