

Recherche

Einfache Suche

Erweiterte Suche

Browsen

Fraunhofer-Publica > Neue Suche > Suche / Trefferliste > Vollanzeige

Fraunhofer-Publica

Suche

■ Einfache Suche

Erweiterte Suche

Browsen

Neue Publikationen

Volltextzugang

RSS Feed

Fraunhofer-Gesellschaft

Fraunhofer-ePrints

Kompetenz-Suchsystem

Auswahl 1 von 1.

Seite: [1]

Volltextzugang

Drucken

Hilfe

Java-Security in Mehrbenutzersystemen*Autor(en):* Bäcker, R.*Herausgeber:* Peters, J.**Erschienen** Frankfurt, 2006, 72 S.
Frankfurt, Provadis Hochschule, Bachelor-Arbeit, 2006**Sprache** Deutsch**Dokumentart** Bachelor-Arbeit**Institut** [Fraunhofer IGD](#)Signatur: Q/b/47 ([zur Institutshomepage](#))**Schlagwörter** Java security; [risk analysis](#); [service oriented architecture](#)**Abstract**

Sicherheit wird in der Informationstechnik groß geschrieben. Da Anwendungen häufig das Ziel von Angreifern sind, müssen diese analysiert und auf Schwachstellen untersucht werden. Nach dieser Untersuchung müssen die Schwachstellen beseitigt werden.

Die Plattform SicAri, die den ubiquitären Internetzugang ermöglichen soll, ist die Anwendung, die in der Bachelor-Thesis von Renée Bäcker betrachtet wird. Die Arbeit gliedert sich in drei Hauptbereiche: Im ersten Bereich werden die Grundlagen zum Thema "Sicherheit" gelegt. Dabei werden die Ziele im Allgemeinen und die Sicherheitsmechanismen der Programmiersprache Java im Speziellen beleuchtet. Im zweiten Hauptbereich wird die Plattform SicAri mit ihren Komponenten vorgestellt. Dabei wird hauptsächlich auf die implementierten Sicherheitsmechanismen eingegangen. Für die Sicherheitsanalyse und Untersuchung auf Schwachstellen wurde der Bootstrapping-Vorgang von SicAri betrachtet. Die Ergebnisse der Analyse und wie die Schwachstellen behoben wurden, wird im dritten Teil der Bachelor-Thesis angesprochen.

Der Bootstrapping-Vorgang von SicAri ist der Teil, dem in dieser Arbeit besondere Aufmerksamkeit gewidmet wurde. Die SicAri-Kernbestandteile werden in einem JAR-Archiv gespeichert. Beim Start der Plattform muss überprüft werden, ob dieses Archiv korrupt ist oder nicht. Für diese Überprüfung wurde ein Tool geschrieben, da es bei Java einen Bug gibt, der es erlaubt, nicht-signierte Dateien in ein signiertes JAR-Archiv zu speichern; und diese nicht-signierte Datei wird dann als signiert erkannt. Weiterhin wurden in einem Bootstrapper die Dienste festgelegt, die für den Startvorgang benötigt werden. Ein Angreifer kann somit diese besonderen Dienste nicht mehr ersetzen.

Zusätzlich findet jetzt jede Aktion in SicAri unter einem Benutzerkontext statt, während in der vorherigen Version nur bestimmte Aktionen - z.B. starten eines Dienstes - unter dem Kontext des aktuell angemeldeten Users stattfand. Alle anderen Aktionen liefen ohne Kontext.

[English](#)[Kontakt](#)[Impressum](#)[Sitemap](#)