Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Sicherheitsanalyse der hochsicheren Internet-Applikation M1

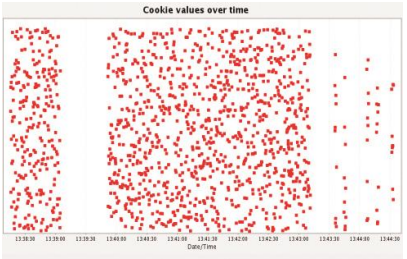
Diplomierende
Simon Furrer
Michael Tschannen

Dozent
Marc Rennhard

Diese Diplomarbeit beschreibt eine ausfuhrliche Sicherheitsanalyse des momentan bestehenden Prototypen einer Java-basierten Webapplikation mit internem Codenamen M1. Es handelt sich hierbei um eine hochsichere Anwendung, welche als Applet in allen gangigen Browsern lauft und dem Benutzer Security SaaS ("Software-as-a-Service")-Elemente bietet. Die nun abgeschlossene Momentaufnahme soll einen Uberblick uber den aktuellen Stand von ausgewahlten, sicherheitskritischen Elementen sowie der Qualitat der Sicherheitsarchitektur geben. Auftraggeber und Industriepartner war eine Schweizer IT-Security-Unternehmung. Die gesamte Diplomarbeit wurde bereits initial als vertraulich eingestuft.

Login-Maske der getesteten Webapplikation M1

Der erste Teil der Arbeit beinhaltete eine allgemeine Bedrohungsanalyse in Bezug auf aktuelle Attacken im Zusammenhang mit Webapplikationen. Das Ergebnis war eine Zusammenstellung von gesamthaft 82 Attacken, welche wir bewerteten und rangierten. Im zweiten Teil wurden von uns aktive Angriffe auf M1 wie auch allgemeine, kritische Betrachtungen der Sicherheitsarchitektur durchgefuhrt und beschrieben. Hierbei gelang uns die erfolgreiche Durchfuhrung von Attacken auf verschiedenen Ebenen, vom Modifizieren der Java Runtime Environment uber MITM-Attacken bis hin zu Attacken auf die Applikation selbst. Besonders interessant fur uns war, festzustellen, wie einfach selbst signierte Java-Applets manipuliert werden konnen und wie schwierig es ist, serverseitig die Echtheit eines Applets zu uberprufen. Im letzten Teil der Arbeit haben wir konkrete Verbesserungsvorschlage zur kunftigen Verhinderung dieser Attacken formuliert.



Output einer Attacke auf die Session-Implementation mit WebScarab

Zusammenfassend konnen wir sagen, dass sich M1 auf einem guten Weg befindet. Es ist uns zwar gelungen, verschiedene Attacken erfolgreich durchzufuhren, die hierbei gefundenen Schwachstellen sind aber grosstenteils behebbar. Die von uns formulierten Verbesserungsvorschlage sollten letztendlich dazu beitragen, M1 nochmals einen Schritt weiterzubringen, sodass die endgultige Version den hohen Anforderungen gerecht werden kann.

Fur uns selbst bleibt die Erkenntnis, dass eine nicht angreifbare Webapplikation auch mit viel Aufwand und Fachwissen kaum entwickelt werden kann - Angreifer finden immer wieder neue Wege, um Attacken auf verschiedenen Ebenen erfolgreich durchzufuhren. Aus diesem Grund ist es besonders wichtig, solche Sicherheitsanalysen regelmassig durchzufuhren.