Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

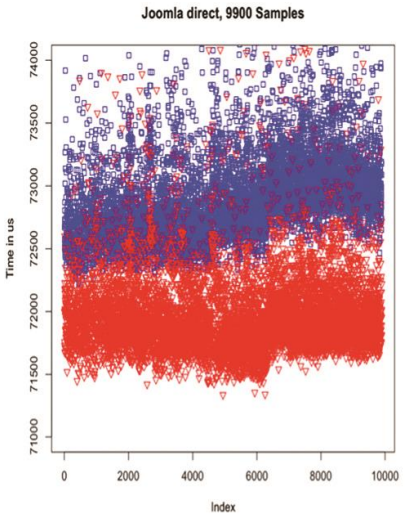
InIT Institut für angewandte Informationstechnologie

Side Channel Vulnerabilities in Web Application Firewalls

Diplomierende
Stefan Kuch
Simon Lehmann

Dozent
Marc Rennhard

Die Analyse von Side Channels ist ein noch sehr junges Forschungsgebiet, welches erst in den letzten Jahren an Bedeutung gewann. Das Ziel einer entsprechenden Side Channel Attacke ist, durch gezielte Interaktion mit einen zu analysierenden System - in der vorliegenden Arbeit eine Web-Applikation - an sensitive Informationen zu gelangen. Diese neue Art von Attacken wird von vielen Web-Entwicklern nicht als Sicherheitsrisiko betrachtet und entsprechend sind meist keine Abwehrmassnahmen implementiert. Eine populäre Massnahme zum Schutz von Web-Applikationen ist eine vorgelagerte Web Application Firewall (WAF) und in dieser Arbeit soll die Frage beantwortet werden, inwiefern das kommerzielle WAF-Produkt des Wirtschaftspartners dieser Arbeit vor Side Channel Attacken Schutz bietet.
Zur Beantwortung dieser Frage wurden zuerst verfügbare Arbeiten zu Side Channel Attacken untersucht und dann konkrete Attacken auf die WAF angewendet. Der Fokus liegt auf Timing-Attacken auf den Authentisierungsvorgang, d.h. man kann anhand unterschiedlicher Antwortzeiten der von der WAF geschützten Web-Applikation irgendwelche relevanten Rückschlüsse ziehen. Zu diesem Zweck wurde eine Testumgebung installiert, welche die gezielte Verzögerung bestimmter Pakete zulässt, um so ein Authentisierungssystem mit unterschiedlichen Antwortzeiten zu simulieren. Die bei den anschliessenden Analysen gemessenen Antwortzeiten wurden statistisch ausgewertet, grafisch dargestellt und beurteilt. Dadurch konnte aufgezeigt werden, wie gut die WAF vor Side Channel Attacken auf den Authentisierungsvorgang zu schützen vermag.
Es hat sich gezeigt, dass die untersuchte WAF zwar Schutzmechanismen implementiert, diese aber nur begrenzt vor Side Channel Attacken schützen. Selbst dann, wenn die WAF alle implementierten Abwehrmassnahmen verwendet, können Timing-Attacken durchgeführt werden. Dies ist der Fall wenn sich die Antwortzeiten des Authentisierungssystems bei Verwendung eines existierenden bzw. nicht-existierenden Benutzers signifikant (> 10 ms) unterscheiden. Als Gegenmassnahme schlagen wir eine Modifikation der von der WAF implementierten Abwehrmassnahmen vor, womit Timing-Attacken praktisch verunmöglicht werden könnten.



Die Grafik zeigt die unterschiedlichen Zeiten bei Messungen auf joomla, einem bekannten open source Content Management System. Die blaue Punktewolke stellt die Antwortzeiten (inus) bei bekanntem Benutzernamen dar. Die rote diejenigen bei unbekanntem Benutzernamen. Dabei wurde in beiden Fällen ein falsches Passwort angegeben. Die Messungen wurden direkt auf dem Login-Formular der Applikation durchgeführt. Sie zeigen also die Situation, in welcher die Applikation nichtdurch eine WAF geschützt wird.