TLS/SSL – WebScarab

Raoul
Harlacher

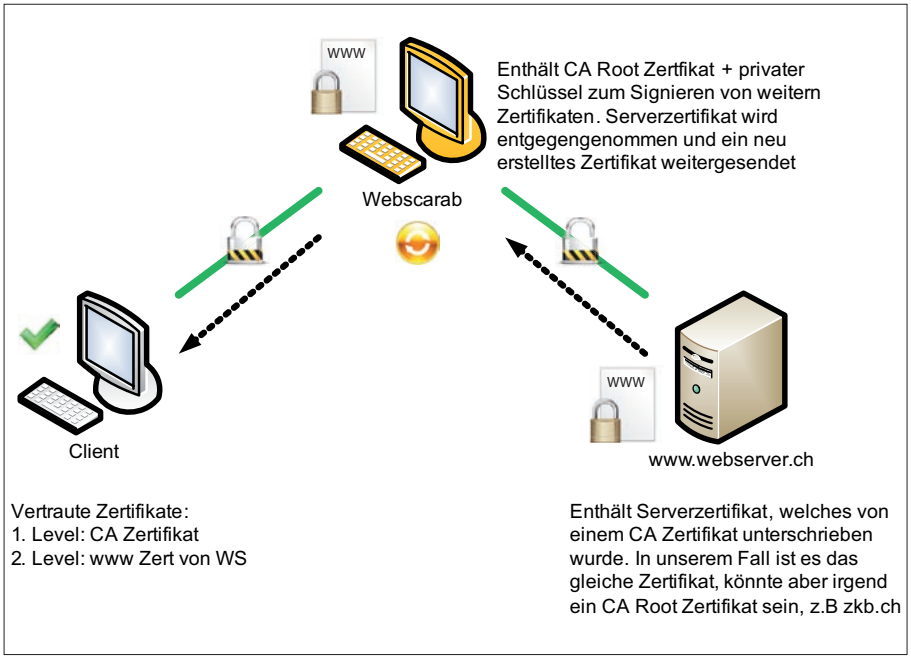
Diplomand	Raoul Harlacher
Examinator	Prof. Dr. Peter Heinzmann
Experte	Dr. Thomas Siegenthaler, CSI Consulting AG, Zürich
Themengebiet	Internet-Technologien und -Anwendungen
Projektpartner	cnlab AG, Rapperswil-Jona SG

Webscarab Logo

Ausgangslage: Der Open-Source Proxy WebScarab wird bei der Software-Entwicklung und bei Sicherheitsüberprüfungen zur Analyse und Modifikation des Datenverkehrs eingesetzt. Leider unterstützt die WebScarab-Version gesicherte Verbindungen (https) nur beschränkt. Ferner kann WebScarab nur eingesetzt werden, wenn der Proxy im Client explizit angegeben wird.

Ziel der Arbeit: Eine Analyse verschiedener Proxies soll deren Vor- und Nachteile hinsichtlich des Einsatzes für Sicherheitsüberprüfungen aufzeigen. Der Proxy WebScarab muss so erweitert werden, dass beim https-Aufruf beliebiger Webseiten on-the-fly ein gültiges Serverzertifikat erstellt wird. Damit kann auch die Analyse verschlüsselter Verbindungen möglich sein. Ferner müsste der erweiterte WebScarab Proxy im transparenten Modus betrieben werden können, um Man-in-the-Middle-Angriffe zu veranschaulichen.

Resultat: Die im Rahmen dieser Diplomarbeit erstellten WebScarab-Erweiterungen ermöglichen die Analyse gesicherter Verbindungen mit beliebigen Servern. Serverzertifikate können innerhalb von 2–3 Sekunden on-the-fly erstellt werden, so



Webscarab Zertifikatserstellung

dass der Client nicht «bemerkt», dass die Verbindung über den Proxy läuft. Die Parameter des generierten Zertifikats können individuell definiert werden.
Ein Zertifikatsspeicher ermöglicht die Wiederverwendung bereits vorhandener Zertifikate, wodurch die Verzögerung auf eine Sekunde reduziert wird. Die neue WebScarab-Version kann als transparenter Proxy eingesetzt werden. Damit sind gesicherte Verbindungen überwachbar, ohne dass auf den Clients ein spezieller Proxy angegeben werden muss. Auf diese Weise lassen sich Man-in-the-Middle Angriffe sehr deutlich veranschaulichen.

Ausblick: Die Anwendung wird künftig beim Industriepartner für Analysen verwendet und soll an der HSR auch für Schulungszwecke genutzt werden. Der neue WebScarab wird öffentlich als Open-Source Projekt auf der Homepage des Industriepartners publiziert.