Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

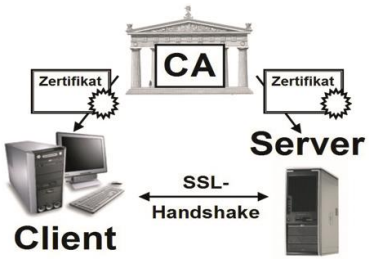
InIT Institut für angewandte Informationstechnologie

Innovative sichere Authentisierungsverfahren fur AXA Winterthur

Diplomierende
Stefanie Pfister
Christian Sandmeier

Dozierende
Marc Rennhard
Karl Rege

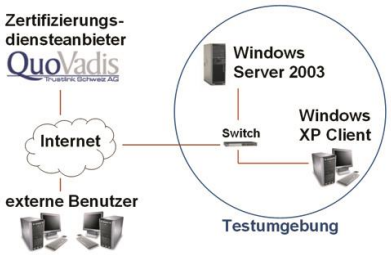
Die vorliegende Diplomarbeit wurde in Kooperation mit der Versicherungsgesellschaft AXA Winterthur erstellt. In dieser Arbeit werden verschiedene Moglichkeiten der Web-Authentisierung auf ihre konkrete Einsatztauglichkeit fur das Versicherungsunternehmen untersucht. Der Fokus wurde auf die derzeit gebrauchlichsten Methoden zur starken Authentisierung, der One Time Passworter und der zertifikatsbasierten Authentisierung, gelegt. In einer Gegenuberstellung der beiden Verfahren unter Berucksichtigung der Sicherheitsaspekte, der Benutzerfreundlichkeit, der Langfristigkeit, Flexibilitat und technischen Konvergenz, sowie einer qualitativen Kostenbetrachtung werden die Starken und Schwachen der jeweiligen Verfahren beleuchtet. Nachfolgend wurde mit Hilfe einer Entscheidungsanalyse, in Anbetracht der Faktoren der Gegenuberstellung, sowie der technischen, betriebswirtschaftlichen und organisatorischen Aspekte, die Wahl fur das geeignetste Authentisierungsverfahren getroffen. Die Entscheidung deckt sich mit dem internationalen Trend, der deutlich in Richtung des Einsatzes zertifikatsbasierter Losungen geht.



Bei der gegenseitigen Authentisierung in SSL wird als erstes das Serverzertifikat validiert. Der Server wiederum verlangt anschliessend das Clientzertifikat. Bei erfolgreicher Authentisierung kann die SSL-Verbindung aufgebaut werden.

Neben den gangigen Losungen werden in einem weiteren Teil verschiedene innovative Varianten fur eine sichere Authentisierung betrachtet. Darunter konnte auch eine eigene Variante der zertifikatsbasierten Authentisierung in Kombination mit Near Field Communication beschrieben werden.

Als Abschluss konnte in Zusammenarbeit mit der QuoVadis Trustlink Schweiz AG, ein in der Schweiz und international akkreditierter Zertifizierungsdiensteanbieter, die Simulation einer Firmenumgebung realisiert werden.



Um ein geeignetes Authentisierungsverfahren zu verdeutlichen und damit die Moglichkeiten und Anforderungen an ein Unternehmen aufzuzeigen, wurde in einer Testumgebung ein Firmennetzwerk simuliert.

Die Schlusselerkenntnisse dieser Arbeit sind zum einen, dass zertifikatsbasierte Authentisierungslosungen in naher Zukunft tendentiell zum Standard fur Unternehmen werden durften. Diese auf asymmetrischer Kryptologie basierende Technologie wird sich dank seiner vielseitigen Anwendungsmoglichkeiten und der Resistenz gegen aktive Attacken tendentiell weiter etablieren. Des Weiteren kann gesagt werden, dass innovative Ansatze fur Authentisierungslosungen vorhanden sind. Diese beziehen sich jedoch grosstenteils auf die Verbesserung der One Time Passwort-Authentisierung. Hier ware die Weiterentwicklung der Zertifikatsverfahren ein interessantes Feld fur weitere Forschung und Entwicklung.