Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

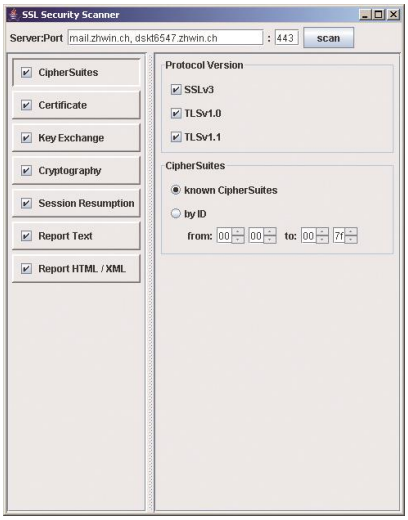
InIT Institut für angewandte
Informationstechnologie

SSL/TLS Security Scanner

Diplomierende
Martin Rasera
Patric Sauter

Dozent
Marc Rennhard

Das Wachstum des Internets und die damit verbundenen Kommunikationsmoglichkeiten nehmen stetig zu. Massnahmen zur Sicherheit im Internet sind in den letzten Jahren diesem Wachstum gefolgt, weil immer mehr Anwendungen, wie z.B. E-Banking, eine sichere Kommunikation erfordern und zugleich das Bewusstsein fur Internet Security der Anwender und Service Provider gewachsen ist. Die aktuell wichtigsten Protokolle in diesem Zusammenhang sind Secure Sockets Layer (SSL) - und dessen Nachfolger Transport Layer Security (TLS). Sie gelten als sichere Verschlusselungsprotokolle fur Datenubertragungen im Internet und werden von Fachleuten standig uberpruft und weiterentwickelt. Schwachstellen konnen jedoch bei der fehlerhaften Implementierung dieser Protokolle und bei der Konfiguration des Systems entstehen, wodurch ein Angreifer die Sicherheit dieser Protokolle aushebeln konnte. Deshalb ist die korrekte Implementierung und Konfiguration von SSL/TLS Komponenten sehr wichtig und erfordert bei der Umsetzung besondere Aufmerksamkeit. Es existieren bis heute jedoch keine Tools, welche daraus resultierende Sicherheitslucken umfassend und automatisiert testen konnen.
Um solche Schwachstellen aufzudecken, haben wir einen SSL/TLS Security Scanner in Java implementiert. Dieser Scanner besitzt eine eigens erstellte Implementation von SSL und TLS, die detaillierte Analysen bis in die Protokollschicht ermoglicht und einfache Wart- und Erweiterbarkeit garantiert. Der Scanner ubernimmt dabei die Rolle eines Clients und fuhrt Tests an SSL/TLS Servern durch. Die verschiedenen Scans sind im Stil von Plug-Ins realisiert und geben Informationen uber die Konfiguration und ob sich der Server standardkonform verhalt.
Das langfristige Ziel ist, den SSL/TLS Security Scanner als Open Source Anwendung zur Verfugung stellen, um damit einen wichtigen Beitrag zur sicheren Kommunikation im Internet zu leisten.



Graphische Benutzeroberflache des SSL/TLS Security Scanners