HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**I**
Name der Studierenden	**Philip Bötschi** **Adrian Dörig**
Studienjahr	**2007**
Titel der Studienarbeit	**Web Inspection with SmartCard** **HTTPS Proxy mit Zugriff auf SmartCard Client Certificate**
Examinatorin / Examinator	**Ivan Bütler, Compass Security AG**

Kurzfassung der Studienarbeit

Aufgabenstellung

Zur Analyse der Sicherheit von Web Anwendungen arbeitet Compass Security AG mit dem Tool „Paros Proxy“(www.parosproxy.org). Mit dem Proxy, welcher zwischen Browser und Internet geschaltet wird, können HTTP Requests/Respones beobachtet, angehalten und manipuliert werden.
Vermehrt setzen Firmen für die Authentifizierung bei Web Anwendungen auf Client Certificates. Paros kann mit dateibasierenden Certificates(PKCS#12 Format) ohne Probleme umgehen. Immer mehr Kunden von Compass Security AG liefern aber nur noch Certificates auf SmartCard's aus. Dies wird von Paros aber nicht unterstützt. Wie können in Zukunft solche Anwendungen getestet werden?

Vorgehen

Es wurden zwei mögliche Lösungsvarianten analysiert:
Proxy Variante: den Paros Proxy um die SmartCard Funktionalität erweitern
Systemnahe Variante: Programm schreiben, dass zwischen Browser und Verschlüsslungssystem platziert wird

Es wurde entschieden die Proxy Variante zu realisieren. Mit dieser Lösung kann während der verfügbaren Zeit ein ausreichend getestetes Endprodukt realisiert werden.

Lösung

Das Endprodukt ist eine um SmartCard Funktionalität erweiterte Paros Proxy Version. Das Client Certificates Handling wurde komplett neu programmiert und damit einiges verbessert. Beim Zugriff auf die SmartCard setzt die neue Version auf die SmartCard Schnittstelle PKCS#11, welche unter anderen von Firefox verwendet wird. Die von der Programmierung und vom Bedienungskomfort bessere, unter Windows angebotene Crypto API Schnittstelle, konnte leider nicht integriert werden. Dies aus dem Grund, dass die bei der Implementierung aufgetretenen Probleme in der vorgegeben Zeit nicht lösbar waren.