Christian
Schellenberg

Livio
Schirru

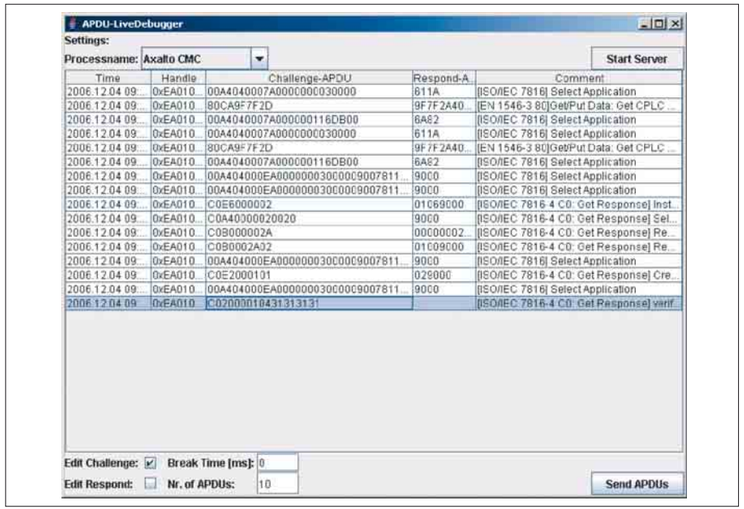
Smartcard Security

Diplomanden	Christian Schellenberg, Livio Schirru
Examinator	Ivan Bütler
Experte	Dr. Benjamin Fehrensen, UBS, Zürich
Themengebiet	Internet-Technologien und -Anwendungen
Projektpartner	Compass Security AG

Verschiedene Smartcards

Aufgabenstellung: Bei der Anmeldung an ein E-Banking oder andere kritische Applikationen ist es wichtig, dass der PC frei von Viren und Trojanern ist. Aufgrund der vielseitigen Möglichkeiten zur Einflussnahme auf PCs haben sich in jüngster Vergangenheit neue Kleinstcomputer in Form von Smartcards durchgesetzt, welche diese Security Operationen übernehmen. Eine solche Smartcard sieht optisch aus wie eine EC-Karte für den Bankomat-Bezug, ist aber im Grunde ein eigenständiger PC mit Software Verteilung und Input Devices.
Diese Arbeit analysiert die Sicherheit von Smartcards und zeigt Schwachstellen bei deren Nutzung und Gebrauch auf.

Ziel der Arbeit: Die Diplomarbeit beschäftigt sich mit dem Security Modell von Smartcards und versucht mögliche Angriffspunkte sowohl theoretisch als auch praktisch aufzuzeigen. Dabei werden sowohl die Voraussetzungen als auch die Ergebnisse für Hacking Attacken analysiert und praktisch ausgetestet. Am Schluss soll ein Entscheidungsträger beurteilen können, ob der Gewinn an Sicherheit wirklich real vorhanden ist und somit diese Investitionen gerechtfertigt sind.



APDU LiveDebugger

Lösung: Die Projektgruppe hat bei der Arbeit folgende Smartcards untersucht:

- Axalto
- Gemplus
- SafeNet

Für spezielle Hacking-Versuche wurde der APDU LiveDebugger entwickelt (siehe Bild links), welcher die Kommunikation zwischen PC und Smartcard sowohl analysieren als auch beeinflussen kann.
Die Sicherheit wird hauptsächlich durch die praktische Nutzung bestimmt. Die Nutzung von Smartcards in einem ungeeigneten Setup bringt keinen Mehrwert. Falls man aber gewisse Rahmenbedingungen erfüllt, erachtet das Projektteam die Smartcards als nächsten, unumgänglichen Schritt für den Schutz der Identität, Integrität und Vertraulichkeit.