



Christian Schellenberg



Livio Schirru

Smartcard Security

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

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 Smart-

cards 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.



Verschiedene Smartcards

Time	Handle	Challenge-APDU	Respond-A	Comment
2006.12.04 09:	0xEA010	00A4040007A000000030000	611A	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	80CA9F7F2D	9F7F2A40	[EN 1546-3 8U]GetPut Data: Get CPLC ...
2006.12.04 09:	0xEA010	00A4040007A000000116DB00	6A82	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	00A4040007A000000030000	611A	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	80CA9F7F2D	9F7F2A40	[EN 1546-3 8U]GetPut Data: Get CPLC ...
2006.12.04 09:	0xEA010	00A4040007A000000116DB00	6A82	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	00A404000EA00000030C0009007811	90C0	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	00A404000EA00000030C0009007811	90C0	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	C0E600002	01C69C00	[ISO/IEC 7816-4 C0: Get Response] Inst...
2006.12.04 09:	0xEA010	C0A40300020020	90C0	[ISO/IEC 7816-4 C0: Get Response] Sel...
2006.12.04 09:	0xEA010	C0B000002A	00C00C02	[ISO/IEC 7816-4 C0: Get Response] Re...
2006.12.04 09:	0xEA010	C0B0002A32	01C09C00	[ISO/IEC 7816-4 C0: Get Response] Re...
2006.12.04 09:	0xEA010	00A404000EA00000030C0009007811	90C0	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	C0E2000101	028000	[ISO/IEC 7816-4 C0: Get Response] Cre...
2006.12.04 09:	0xEA010	00A404000EA00000030C0009007811	90C0	[ISO/IEC 7816] Select Application
2006.12.04 09:	0xEA010	C020000104313131	90C0	[ISO/IEC 7816-4 C0: Get Response] verif...

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.