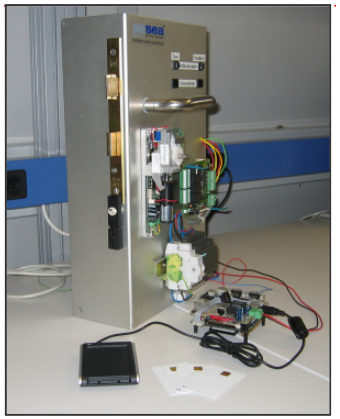
Building Access Control

A PKI Approach Using Contactless Smart Cards

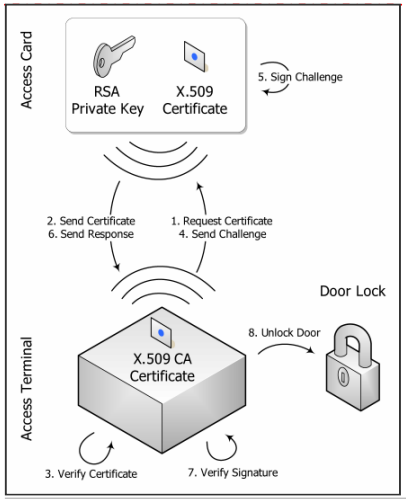
Diplomand / in	Jonas Schwertfeger
Examinator / in	Prof. Dr. Andreas Steffen
Experte / in	Dr. Ralf Hauser
Themengebiet	Security, Pervasive Computing
Projektpartner	



Motorenschloss, Terminal und Karten

Problemstellung: Heutige Verfahren zur berührungslosen Zutrittskontrolle bei Gebäuden beruhen auf Mechanismen, die einen gemeinsamen geheimen Schlüssel auf der Zutrittskarte und dem Zutrittsystem benötigen. Diese Mechanismen besitzen den grossen Nachteil, dass der geheime Schlüssel jeder Karte bei allen Zugangspunkten eines Gebäudes hinterlegt werden muss. Des Weiteren erlauben es die Verfahren auch nicht, dass die gleiche Karte bei mehreren verschiedenen Zutrittssystemen verwendet werden kann. Eine solche Verwendung hätte zur Folge, dass die Betreiber des einen Zutrittssystem durch die Kenntniss des geheimen Schlüssels auch Zutritt zum anderen System erlangen könnten.

Ziel der Arbeit: Es wird der Prototyp eines neuartigen Zutrittssystem entwickelt, das Personen durch ein berührungsloses *Public-Key Challenge/Response*-Protokoll authentifiziert. Bestandteil der Arbeit ist dabei die Software für die Karten als auch die Software für das Zutritts-Terminal. Des Weiteren wird ein Programm zur Konfiguration der Karten benötigt.



Schematische Darstellung einer Authorisierung

Zu Demonstrationszwecken wird die Terminal-Software auf einem Embedded-Computer unter Linux installiert. Der Embedded-Computer ist mit einem Motorenschloss verbunden, das bei erfolgreicher Authentifizierung geöffnet wird. Die Installation und Konfiguration des Linux sowie die Ansteuerung des Schlosses gehören ebenfalls zur Aufgabenstellung.

Lösung: Die Entscheidung für die Karten fiel auf berührungslose JCOP Smartcards. Diese basieren auf einem Philips IC mit Kryptographie-Koprozessor und führen dadurch Public-Key-Operationen in angemessener Zeit aus. Für diese Karten wurde ein Javacard-Applet entwickelt, das mehrere Authentifizierungsprofile verwalten kann. Zusätzlich zur erwähnten Challenge-Response-Funktionalität erlaubt das Applet für jedes Profil die Definition einer PIN und die Speicherung beliebiger binärer Daten. Dadurch ist nebst der geforderten *Public-Key*-Authentifizierung auch eine Drei-Faktor-Authentifizierung möglich.

Die Terminal-Software besteht aus einem in C++ geschriebenen *Multi-Threaded-Daemon*, der simultan mehrere angeschlossene Kartenleser verwalten kann. Nähert sich eine Smartcard einem Kartenleser, so initiiert der Daemon zunächst einen Authentifizierungs- und anschliessend einen Authorisierungsvorgang. Sind diese erfolgreich wird als Zutrittsaktion ein Motorenschloss geöffnet. Die Architektur des Daemons wurde so gewählt, dass dieser auf einfache Weise um zusätzliche Authentifizierungs-, Authorisierungs- und Aktionsmechanismen erweitern werden kann.

Als Embedded-Plattform wurde ein PC/104 Computer verwendet, der über die Parallelschnittstelle und ein Relais das Schloss ansteuert. Das Linux wurde so konfiguriert, dass es nur die absolut notwendigen Teile beinhaltet und dadurch sehr wenig Speicherplatz benötigt.