HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Diplomarbeit

Abteilung	**Informatik**
Name der Diplomandin / des Diplomanden	**Flavio Grisch** **Fernando Garcia**
Diplomjahr	**2003**
Titel der Diplomarbeit	**Dezentraler Druck und Kontrolle fälschungssicherer Parkkarten**
Examinator / Experte	**Prof. Dr. P. Heinzmann / Dr. Th. Siegenthaler, CSI**
Industriepartner	**OIZ Organisation und Informatik der Stadt Zürich, A. Fähndrich**

Im Rahmen dieser Diplomarbeit, durchgeführt für den Auftraggeber Stadtpolizei Zürich, wird ein Teilsystem zu einer e-Government Lösung realisiert, mit welcher Parkkarten über das Internet bestellt, bezahlt und ausgedruckt werden können. Das Parkkarten-System soll sowohl Privaten als auch Angestellten der Kreisämter und Bewilligungsstellen der Stadt Zürich zu Verfügung stehen. Eine ausgedruckte Parkkarte wird hinter die Windschutzscheibe des Fahrzeugs gelegt, damit diese von einer Kontrollpersonen der Stadtpolizei mit Hilfe eines mobilen Datenerfassungsgerätes (MDE) verifiziert werden kann. Das System ist sicher, wenn gültige Parkkarten nicht ohne Bezahlung produziert werden können, d.h. wenn die ausgedruckten Parkkarten bei der Verifikation durch das Kontrollpersonal nur dann als gültig erklärt werden, wenn sie für die entsprechende Parkdauer gekauft wurden. Für die Diplomarbeit wurde ein Lösungsansatz mit kryptographischer Prüfsummenbildung vorgegeben.

In der Systemanalyse wurde der vorgegebene Lösungsansatz anhand des Vergleichs mit ähnlichen Systemen optimiert. In einer Sicherheitsanalyse wurden verschiedene Fälschungsmöglichkeiten aufzeigt und bewertet. Die Sicherheit des Parkkartensystems bedingt einerseits bestimmte Vorgaben im Parkkarten-Beschaffungs- und Kontroll-Prozess, andererseits ist die Sicherheit der kryptographischen Prüfsummenbildung von Bedeutung. Bei der Analyse zur Sicherheit des Systems wurden daher einerseits mögliche Risiken, deren Folgen und Gegenmassnahmen auf breiter Basis aufgezeigt, andererseits wurden die in Frage kommenden kryptographischen Algorithmen detailliert untersucht.

Im realisierten Prototypen-System wird die Fälschungssicherheit der Parkkarten mittels Message Authentication Code (MAC) PMAC mit AES realisiert. Der realisierte Prototyp umfasst eine Webapplikationen und ein Software-Modul für das mobile Datenerfassungsgerät (MDE). Die kundenseitige Anwendung zum bestellen und ausdrucken von Parkkarten basiert auf Java Servlets. Sie kann somit von jedem Internet-Browser aus bedient werden. Die Server-Applikation, welche von der Stadtpolizei dazu benutzt wird, um die Schlüssel für den Algorithmus zu verwalten, ist ebenfalls mit Java Servlets implementiert.

Die Anwendung zur Überprüfung des auf einer Parkkarte aufgedruckten Prüfcodes mit Hilfe des mobilen Datenerfassungsgeräts (MDE) wurde in C realisiert. Sie berechnet aus den eingegebenen Parkdaten (Postleitzahl des Parkbezirkes, Fahrzeugkennzeichen und Gültigkeitsdatum der Parkkarte) einen Prüfcode. Dieser wird zur Verifikation der Parkkarte durch das Kontrollpersonal mit dem auf der Parkkarte aufgedruckten Code verglichen. Stimmen die beiden Werte überein, so kann davon ausgegangen werden, dass die Parkkarte gültig ist.