Sicherheitsanalyse ubiquitärer drahtloser Anwendungen - Physikalische und Protokoll-Angriffe in der Praxis

Portable drahtlose Geräte sind ein allgegenwärtiger Bestandteil des täglichen Lebens. Diese Dissertation untersucht Schwachstellen der Sicherheit verschiedener kommerzieller Produkte im Hinblick auf Protokollangriffe und physikalische Attacken, insbesondere so genannter Seitenkanalanalysen.

Dazu wird zunächst spezielle, kostengünstige Hardware zur Schwachstellenanalyse von RFID (Radio Frequenz Identifikation) Geräten entwickelt, einschließlich eines elektronischen Emulators für kontaktlose Smartkarten. Mit Hilfe dieser Hardware wird ein weit verbreitetes kontaktloses Bezahlsystem untersucht, das auf schwachen Mifare-Classic Karten basiert. Dabei werden eklatante Sicherheitsmängel festgestellt: Das Extrahieren der kryptografischen Schlüssel aus einer dieser Bezahlkarten (mit der entwickelten Hardware) ermöglicht das Modifizieren von Geldbeträgen beliebiger Karten im System, da fatalerweise alle Karten denselben geheimen Schlüssel benutzen. Dies ermöglicht eine Reihe praktischer Angriffe. Beispielsweise ist das Bezahlen mit modifizierten Bezahlkarten bzw. dem Emulator ebenso problemlos möglich wie das Umwandeln von gefälschten digitalen Geldbeträgen in echtes Bargeld.

Eine naheliegende Aufrüstung des Bezahlsystems auf modernere Mifare DESfire Karten bringt ohne Änderungen der weiteren Systemparameter keine spürbare Verbesserung. Diese Arbeit demonstriert, wie die Sicherheit dieser kontaktlosen Karten durch Auswertung der während der kryptografischen Berechnungen entstehenden elektromagnetischen Abstrahlung ausgehebelt werden kann: Mittels spezieller RFID-Seitenkanalanalyse wird der 112-bit Schlüssel der zur Authentifizierung und Verschlüsselung in DESfire Karten eingesetzten Triple-DES Chiffre exakt bestimmt. Mit dem Angriff können sämtliche Schlüssel einer DESfire Karte extrahiert und infolgedessen der Inhalt der Karte beliebig ausgelesen und modifiziert werden.

Im Gegensatz zu den passiven, kontaktlosen Karten verfügen aktive Handsender über eine eigene Energiequelle in Form einer Batterie. Die entsprechend größere verfügbare Rechenleistung würde den Einsatz starker Kryptografie ermöglichen, was jedoch in der Praxis häufig nicht umgesetzt wird. Anhand der weltweit eingesetzten „KeeLoq“ Funktüröffner wird demonstriert, wie die Sicherheit dieses aktiven Systems vollständig umgangen werden kann. Durch Auswertung des Leistungsverbrauchs der Handsender können in deren Hardware gespeicherte geheime Schlüssel in wenigen Minuten aus ca. 10-30 Messungen ermittelt werden. Eine optimierte Seitenkanalanalyse der Software eines Empfängers offenbart nach nur einer einzigen Stromkurvenmessung den kryptografischen Hauptschlüssel des Funktüröffnersystems. Mit Kenntnis des Hauptschlüssels wird ein verheerender Lauschangriff möglich, der aus nur einem abgefangenen Funkcode alle weiteren gültigen Codes zu berechnen erlaubt. Ein Angreifer kann somit aus der Entfernung mit KeeLoq gesicherte Objekte u. A. beliebig öffnen und schließen. Für einen weiteren Angriff durch erschöpfende Schlüsselsuche dient eine Implementierung auf kryptanalytischer Hardware. Als eine mögliche Alternative zu KeeLoq wird eine neu entwickelte, seitenkanalresistente Implementierung eines Funktüröffnersystems vorgestellt.

Der letzte Teil der Dissertation beschäftigt sich mit dem elektronischen Reisepass (ePass). Das per RFID auslesbare Ausweisdokument sichert die privaten Daten des Inhabers u. A. durch das Basic Access Control (BAC) Protokoll ab. BAC verhindert ein unbefugtes Auslesen des Passes, indem es den Zugriff auf die im Pass gespeicherten Informationen nur authentifizierten Lesegeräten (z.B. Grenzkontrolle) gestattet. Die anschließende drahtlose Kommunikation wird zusätzlich verschlüsselt, um die Vertraulichkeit der Daten zu gewährleisten. Jedoch ist auch das BAC Verfahren wegen einer schwachen Ableitung der kryptografischen Schlüssel angreifbar: Zwei Implementierungen auf der kryptanalytischen Hardware COPACOBANA erlauben in praktischen Angriffsszenarien, aus mitgeschnittener bzw. abgehörter verschlüsselter Kommunikation mit dem ePass in Sekunden die kryptografischen Schlüssel des BAC zu bestimmen. Mit Kenntnis der Schlüssel können die abgehörten privaten Informationen entschlüsselt, Bewegungsmuster von Individuen erstellt oder ein Alarm bei Detektierung eines bestimmten ePasses ausgelöst werden.

Die Ergebnisse dieser Arbeit verdeutlichen, dass die Sicherheitsmechanismen kommerzieller drahtloser Systeme häufig nicht dem Stand der Wissenschaft entsprechen. Besonders beim Schutz gegen Seitenkanalangriffe, doch auch bei der Umsetzung des Gesamtsystems , besteht erheblicher Nachbesserungsbedarf in vielen Produkten.