Trennungen sind schwer:
Sicherheitsprobleme von Smart Cards

Deutsche Übersetzung von Philipp Gühring (pg@futureware.at) aus dem Englischen

Englisches Original: http://www.counterpane.com/smart-card-threats.html
Übersetzung: http://www.futureware.at/smartcard

Bruce Schneier
Counterpane Systems
schneier@counterpane.com

Adam Shostack
Netect, Inc.
adam@netect.com

Original: 19. Oktober 1999
Übersetzung: 6. August 2001

Zusammenfassung

Smart Card Systeme unterscheiden sich von konventionellen Computersystemen dadurch, daß verschiedene Teile der Systeme nicht unter der selben Kontrolle sind. Der Prozessor, die Daten, die Programme und das Netzwerk werden von verschiedenen Parteien kontrolliert. Wir diskutieren die Sicherheitsproblematik dieser Vertrauenstrennungen, und zeigen, daß diese fundamental wichtig für das Verständnis der Sicherheit eines Smart Card Systems sind.

1. Einleitung

Smart Cards, Kreditkarten-große Geräte mit einem einzelnen Embedded Chip - Prozessor mit RAM und ROM - werden von manchen als die eierlegende Wollmilchsau der Computersicherheit gesehen. Sie werden für Zugangskontrollen, E-Commerce, Authentifizierung, die Sicherung der Privatsphäre, ... empfohlen und verwendet. Leider gibt es nur wenige Analysen der Sicherheitsrisiken, die SmartCards im speziellen haben, und die einmalige Angriffsumgebung, der sie ausgesetzt sind.

In diesem Artikel diskutieren wir das Sicherheitsmodell eines SmartCard Systems unabhängig von der Anwendung. Wir untersuchen die grundsätzlichen Eigenschaften einer SmartCard, ein Prozessor und ein Speichermedium, das keine Möglichkeit hat mit der Außenwelt zu kommunizieren, und zeigen daß diese Eigenschaften das System unsicherer machen als Systeme, die in sich einen kompletteren Computer enthalten. Ein einfaches Beispiel ist eine Person, die eine SmartCard trägt, dessen Computer unter der Kontrolle jemand anderes ist. Dies ist eine unübliche Situation für einen typischen Computer, aber eine übliche Situation für eine SmartCard. Wir zeigen, daß bei vielen Anwendungen "eine SmartCard sicher zu verwenden" heißt, daß die SmartCard ein Datenspeicher mit begrenzter Rechenleistung ist.

1.1. Von Computern zu SmartCards

Der beste Weg, die Gefahren zu verstehen, die eine SmartCard bringt, ist mit den Gefahren eines konventionellen Computers anzufangen. Wir glauben, daß der wichtigste Sicherheitsaspekt von SmartCard Systemen, wie die Teilnehmer bei Protokollen, die Art ist, wie SmartCards sich von herkömmlichen Computern unterscheiden. Indem wir bei einem Allzweck-Computer anfangen, und die einzelnen

Funktionen davon trennen, bis wir bei denen eines SmartCard Systems und seiner Umgebung sind, können wir bei jeder Änderung beobachten, wie es die Sicherheit beeinträchtigt. Jede dieser Trennungen gibt Angreifern weitere Möglichkeiten, zu attackieren. Denken Sie an ein Beispiel, bei dem der Eigentümer einer Karte die Daten, die in der Karte gespeichert sind nicht kontrollieren kann. Dies führt zu der Attacke der Person, der die Karte gehört, gegen die Daten, die in der Karte gespeichert sind. Diese Attacke ist grundsätzlich nicht möglich, wenn es diese Trennung nicht gibt.

Unser Modell eines Allzweck-Computers besteht aus einem Prozessor, einem Speicher, Eingabegeräten, Ausgabegeräten und einer Stromversorgung. Die CPU ist der primäre Prozessor des Computers, und zuständig dafür, Berechnungen durchzuführen. In einem normalen Computer, ist die CPU eng mit dem Speicher, wie RAM, Festplatten, Laufwerken, sowie Eingabe/Ausgabegeräten wie Tastaturen, Mäusen, Bildschirmen, Druckern, und einigen digitalen Kommunikationsschnittstellen, wie Serielle Ports, Netzwerk-Karten, ... verbunden. In dieser Konfiguration kann der Computer als eine einzige Einheit für die meisten Gefahrenschemen gesehen werden.

Wir beginnen nun, den Computer zu verkleinern. Nehmen wir einen Computer wie den REX Organizer. Diese PC-Card hat einen kleinen Bildschirm, eine PC-Card Schnittstelle, um mit anderen Computern zu kommunizieren, und ein paar Tasten für Eingaben. Wir werden nun den REX in eine SmartCard verwandeln, und zeigen, wie jeder Schritt der Verwandlung zu neuen Sicherheitsproblemen führt.

Nehmen wir die Eingabe/Ausgabe Schnittstellen, und ersetzen sie mit einem sehr langsamen seriellen Port. Das System, an das sich die Karte verbindet hat wenig Möglichkeiten, Sie zu attackieren, weil die Karte wahrscheinlich nur mit dem Computer des Eigentümers verbunden wird, oder vielleicht für kurze Zeit an einen anderen, um Kontakt-Informationen auszutauschen. Die Karte hat die Möglichkeit, Informationen über den Bildschirm und die Tasten zu senden und zu empfangen. Es wäre nicht schwierig, einen Computer wie den REX in ein sicheres elektronisches Scheckheft zu verwandeln. (Es gibt andere Herausforderungen für Ingenieure, aber es ist grundsätzlich leichter als das selbe System mit einer SmartCard zu machen)

Nehmen wir nun den Eingabemechanismus weg, so daß der Benutzer eine Tastatur, die am Lesegerät angehängt ist, verwenden muß. Es ist offensichtlich, daß sich die Tastatur den PIN und die Karten Information für eine spätere Attacke merken kann. Wenn wir zuletzt den Bildschirm trennen, so daß die Karte keine Möglichkeit mehr hat, mit ihrem Anwender zu kommunizieren, außer über einen Bildschirm, dem man nicht unbedingt vertrauen kann.

Die Charakteristik einer SmartCard ist, daß die Funktionalität getrennt ist, auf eine Art und Weise, die für einen Computer sehr unüblich ist. Diese Trennung bedeutet, daß die SmartCard behindert ist, worunter wir verstehen, daß sie "nicht die Möglichkeit hat, mit der Außenwelt zu kommunizieren, außer über fremde Geräte". Das ist die Natur von SmartCards: eine, die sie von portablen Computern wie Palm Pilot unterscheidet, und das definiert das Vertrauensmodell in dem sie gezwungen sind zu arbeiten. Andere Trennungen können und werden gemacht, aber die grundlegende Trennung ist die der Ein/Ausgabegeräte.

Die SmartCard Funktionalität ist auf mehrere Arten getrennt. Der Karteninhaber hat möglicherweise keine Kontrolle über die Software, die auf der Karte läuft. Im Falle der Multifunktionskarten, hat der Kartenaussteller möglicherweise auch keine Kontrolle. Der Eigentümer der Daten in der Karte muß nicht unbedingt der Inhaber der Karte sein, und der Daten-Eigentümer kann verlangen, daß der Karteninhaber keine Möglichkeit hat, die Daten auf der Karte zu verändern, oder gar die Daten zu lesen.

In den folgenden Abschnitten untersuchen wir die Auswirkungen der oben beschriebenen Trennungen, so wie andere in SmartCard Systemen oft gefundene Auswirkungen. Unsere Modelle beinhalten oft 5 bis 6 beteiligte Parteien. Wir untersuchen genau, wie die beteiligten Parteien, wenn das System getrennt ist,

möglicherweise einander attackieren. Wir untersuchen auch die Motivationen, die Angreifer dazu bewegen, Missbrauch zu treiben, der durch die Rollentrennung möglich wird. Und schlussendlich werden wir verschiedene Abwehr-Modelle besprechen.

2. Vertrauensmodell der Umgebung einer SmartCard

Es gibt viele potentiell beteiligte Parteien an einem SmartCard basierenden System. Üblicherweise, gibt es zumindest 5 oder 6, inklusive dem Karteninhaber, dem Terminal, dem Daten-Eigentümer, dem Karten-Aussteller, dem Karten-Erzeuger, und dem Software Entwickler.

- Der Karteninhaber ist die Partei, die Tag für Tag mit der SmartCard arbeitet. Die SmartCard is meistens in der Brieftasche; er entscheidet, ob und wann er die SmartCard verwendet. Er ist die Person an den die Karte ausgestellt wurde. Er kann Kontrolle über die Daten auf der Karte haben, abhängig vom System, aber es ist sehr unwahrscheinlich, daß er Kontrolle über die Protokolle, die Software, oder die Hardware Entscheidungen, die getroffen wurden, als das System gebaut wurde, hat. Beachten Sie, daß das im Kontrast zu vielen PC basierten Systemen steht, wo der Eigentümer und der Anwender üblicherweise einen gewissen Einfluss auf das System hat, das er benutzt.

- Der Eigentümer der Daten ist die Partei, die die Kontrolle über die Daten in der Karte hat. In Fällen, wo die Karte als Speichermedium für digitale Zertifikate verwendet werden, ist der Karten Eigentümer meist auch der Daten-Eigentümer. Aber bei einem E-Cash System ist der Daten-Eigentümer der Aussteller des Geldes, und dies öffnet die Möglichkeit eines Angriffs.

- Das Terminal ist das Gerät, das der SmartCard die Möglichkeit der Interaktion zur Welt öffnet. Das Terminal kontrolliert alle Ein/Ausgaben zu und von der SmartCard: Die Tastatur mit der Daten eingegeben werden in die SmartCard, der Bildschirm, auf dem Daten aus der SmartCard angezeigt werden. Wenn die Karte als Telefon-SIM-Karte verwendet wird, ist es der Eigentümer der des Handys. Wenn die Karte als ATM Identifikationskarte verwendet wird, gehört das Terminal dem ATM Service Provider. Wenn die Karte eine Pay-TV Mitgliedskarte ist, ist das Terminal die Set-Top Box.

  (Die letzten beiden Beispiele - ATM Identifikationskarte und Pay-TV Mitgliedskarte - zeigen, daß das Terminal sowie die SmartCard in mehrere Teile aufgebrochen werden können. Im Falle des ATM ist die Verwendung eines ATM Netzwerkes einer anderen Bank üblich, was bedeutet, daß die Bank nicht auf die freundlichkeit des Terminals vertrauen kann. Im Falle des Pay-TV Systems, ist das Terminal im langfristigen Besitz des Anwenders, und kann in der Sicherheit und des Komforts daheim angegriffen werden. In Situationen, bei denen der Eigentümer des Terminals, der Programmierung oder andere Funktionen getrennt sind, muß eine gesamte Analyse gemacht werden, um sicherzustellen, daß die Sicherheitsprobleme der Trennungen auch wirklich verstanden werden.)

- Der Kartenaussteller ist die Partei, die SmartCards ausstellt. Diese Partei kontrolliert das Betriebssystem, das auf der SmartCard läuft, und alle Daten, die auf der Karte am Anfang gespeichert sind. Wenn die Karte eine Telefon-Wertkarte ist, ist der Aussteller die Telefonfirma. Wenn die Karte eine Mitarbeiterkarte ist, ist der Arbeitgeber der Aussteller. Manchmal stellt der Aussteller nur die Karte aus, und verschwindet dann aus dem System, manchmal ist er im ganzen System involviert. In manchen Multi-Funktionskarten hat der Karten Aussteller nichts mit den Applikationen, die auf der Karte laufen zu tun, und kontrolliert nur das Betriebssystem. In anderen Multifunktions-Systemen kontrolliert derselbe Aussteller alle Applikationen, die auf der Karte laufen.

Vom Standpunkt der Sicherheitsanalyse her ist es oft am einfachsten, wenn man den Kartenaussteller, den Kartenhersteller und den Software Ingenieur als dieselbe Partei betrachtet. Trotzdem sind sie es meistens nicht. Dadurch:

- Der Karten Hersteller ist die Partei, die die SmartCard produziert. Beachten Sie, daß das eine Vereinfachung ist. Der Hersteller kann, muß aber nicht Eigentümer der Herstellerfabrik sein, in der die Chips tatsächlich hergestellt werden. Die könnten auch weitervergeben sein. Design Funktionen, Tools von Drittanbietern wie zum Beispiel VHDL Compiler. Trotzdem sehen wir alle diese als den Kartenhersteller an. Möglichkeiten, die Herstellung einer Karte negativ zu beeinflussen gibt es an vielen Stellen, für viele daran beteiligte Personen.

- Der Software Hersteller ist die Partei, die die Software produziert, die auf der SmartCard läuft. Dies ist auch wieder eine Vereinfachung eines wahrscheinlich komplexen Zusammenspiels von Compilern, Tools, ... Problem dem Vertrauen zu vertrauen[Tho84] entstehen hier in derselben Art, wie bei den Kartenherstellern.

3. Beispiele von getrennten SmartCard Systemen

Es folgen eine Liste repräsentativer SmartCard basierter Systeme, mit einer Beschreibung, welche Parteien die verschiedenen Aspekte der Systeme kontrollieren. Diese Liste erhebt keinen Anspruch auf Vollständigkeit, und nicht alle Beispiele von Trennungen sind hier beschrieben.

- Digitale Wertkarte
  Diese sind Zahlungskarten als Ersatz für Bargeld. Mondex und Visa Cash sind Beispiele dieser Systemart. Der Karteneigentümer ist der Kunde. Der Terminal Eigentümer ist der Verkäufer. Der Dateneigentümer und der Kartenaussteller sind beides die Finanz-Institution, die das System supported.

- Digitale Scheckkarte
  Dieses System ist ähnlich der digitalen Wertkarte, mit dem Unterschied, daß der Karteneigentümer der Dateneigentümer ist.

- Prepaid Telefonkarten
  Diese sind einfach eine spezielle Anwendung der Wertkarten. Der Karten Eigentümer ist der Kunde. Der Terminal Eigentümer, der Dateneigentümer und der Kartenaussteller sind der Telefonanbieter.

- Konto-basierte Telefonkarte
  Bei diesem System speichert die SmartCard nicht den Kontostand, sondern nur die Kontonummer, die eine Verknüpfung in die Hintergrunddatenbank ist. Der Karteneigentümer und der Dateneigentümer sind der Kunde, der Terminaleigentümer und der Kartenaussteller sind die Telefonfirma.

- Zugangstoken
  In dieser Anwendung speichert die SmartCard einen Schlüssel, mit dem man sich einloggen oder authentifizieren kann. Im Unternehmensumfeld ist der Karteninhaber der Angestellte, der Dateneigentümer, der Terminaleigentümer und der Kartenaussteller ist die Firma. Im Falle einer Multifunktionskarte, können der Karteninhaber und der Dateneigentümer dieselbe Person sein, wobei der Terminaleigentümer ein Verkäufer sein kann, und der Dateneigentümer ein Finanzinstitut.

- WebBrowserkarte
  Bei dieser Anwendung kann ein Kunde mit seiner Karte und seinem eigenen PC Dinge im Internet

einkaufen. Dies ist ein Beispiel einer Wertkarte. Der Unterschied ist, daß der Karteninhaber und der Terminaleigentümer beide der Kunde sind (der Eigentümer des PC's). Der Dateneigentümer und der Kartenaussteller sind beides das Finanzinstitut.

•Digitale Berechtigungs-Karte
Bei dieser Anwendung speichert die SmartCard digitale Zertifikate oder andere Berechtigungen, um Sie einer anderen Partei vorzuweisen. Hier sind der Karteneigentümer und der Dateneigentümer derselbe. Der Terminaleigentümer ist eine andere Partei (in einem Geschäft zum Beispiel) oder der Karteninhaber (der im Internet surft). Der Kartenaussteller ist die CA, die die Berechtigungen ausgestellt hat, oder eine andere Partei, die die Berechtigungen verwaltet.

•Schlüssel-Speicherkarte
In dieser Anwendung speichert der Benutzer verschiedene (möglicherweise verifizierte) öffentliche Schlüssel in einer SmartCard, um sie da aufzubewahren, weil der PC weniger sicher ist. Hier ist der Karteninhaber, der Dateneigentümer und der Terminaleigentümer derselbe.

•Multifunktionskarten
Diese Karte ist die komplizierteste. Der Kartenhersteller und der Kartenaussteller sind verschiedene Parteien, sowie die verschiedenen Softwarehersteller. Der Dateneigentümer kann bei manchen Applikationen der Karteneigentümer sein, und jemand anderer bei anderen Applikationen auf derselben Karte. Es gibt mehrere Terminal-Eigentümer, abhängig davon, welche Applikationen auf der SmartCard sind.

4. SmartCard Gefahrensmodelle

Ein Angriff ist definiert as ein Versuch einer oder mehrerer Parteien, die an einer SmartCard Transaktion beteiligt sind, zu schummeln. Wir unterscheiden zwei Klassen von Angreifern, die die als Partei am System beteiligt sind, und die Eindringlinge. Angriffe von Beteiligten könnten durchen einen Karteninhaber passieren, der versucht einen Terminaleigentümer zu betrügen, oder ein Kartenaussteller, der versucht, einen Karteninhaber zu betrügen, etc. Außenseiter Angriffe könnten durch gestohlene Karten passieren: Ein kurzfristiger Karteninhaber, der eine Karte von einem legitimen Karteninhaber stiehlt, oder ausgetauschte Terminalsoftware oder Hardware. Angriffe von Außenseitern sind meist ähnlich wie Angriffe gegen Protokolle, bei denen herkömmliche Computer beteiligt sind; trotzdem können Sie einen Vorteil durch die Eigenschaften des Systems durch die Trennung der Rollen erhalten.

Motive für Angriffe fallen in ein paar breite Kategorieren [Sch97]. Zuerst und am offensichtlichsten sind finanzielle Diebstähle, inklusive Diebstahl von Geld oder Gutschrift oder Diebstahl von öffentlichen Dienstleistungen wie Telefonkarten. Es gibt aber auch Nachahmungs-Angriffe, bei denen das Kartensystem nur ein Zwischenschritt ist, um Zugang zu Computer oder anderen Sicherheits-Systemen zu erhalten. Diese unterscheiden sich vom Diebstahl dadurch, daß der Dieb nicht die Möglichkeit hätte, sich den Service legitim zu kaufen. Zum Beispiel das Benutzen eines Computers. Die Benutzung von Computern ist öffentlich verfügbar, aber der Zugriff auf einen bestimmten Computer ist das Ziel des Angreifers. Es gibt Angriffe auf die Privatsphäre, wo eine Partei mehr Informationen haben will, als ihr laut Protokoll zustünde. Zuletzt gibt es öffentliche Angriffe, wo es Angreifer nicht auf finanzielle Vorteile abgesehen hat, sondern auf Bekanntheit.

5. Angriffsklassen

Wegen der großen Anzahl an beteiligten Parteien bei jedem SmartCard System gibt es viele Angriffsmöglichkeiten, die man bedenken muß. Unser Ziel ist es hier, diese nach den Funktionstrennungen

zu kategorisieren. Wir untersuchen die Angriffe der am System beteiligten gegeneinander. Die meisten dieser Angriffe wären nicht möglich in konventionellen Computersystemen, weil Sie sich innerhalb der Grenzen eines traditionellen Computer-Sicherheits stattfinden würden. Aber in der SmartCard Welt sind diese möglich.

5.1. Angriffe des Terminals gegen den Karteneigentümer oder den Dateneigentümer

Diese sind die am einfachsten zu verstehenden Angriffe. Wenn ein Karteninhaber seine Karte in das Terminal steckt, vertraut er dem Terminal, daß es alle Ein- und Ausgaben der Karte richtig weiterleitet. Wenn zum Beispiel ein Benutzer eine Wertkarte in einen Automaten steckt, und einen Einkauf über 1$ macht, dann vertraut er dem Terminal, daß das Terminal die Meldung "Ziehe 1$ ab" an die Karte schickt, und nicht "Ziehe 10$ ab." Wenn eine Karte die Nachricht "Guthaben: 1$" an den Karteninhaber schickt, dann erwartet der Karteninhaber, daß der Bildschirm des Terminals die Nachricht richtig anzeigt. Die Möglichkeit eines manipulierten Terminals, in der Umgebung Schaden anzurichten ist signifikant, und es ist unmöglich für den Karteninhaber, diese Art der Schädigung im Kontext eines einzigen Terminals festzustellen. Diese Art von Diebstahl wurde bereits mit gefälschten ATM Maschinen versucht.[?]

Vorbeugende Maßnahmen in den meisten SmartCard Systemen zielen auf das Faktum ab, daß das Terminal nur für kurze Zeit Zugriff auf die SmartCard hat. Software auf der Karte könnte die Schadensmenge begrenzen, die ein manipuliertes Terminal ausrichten kann. Eine Wertkarte könnte zum Beispiel dem Terminal maximal 1$ pro Transaktion, und maximal eine Transaktion pro Minute erlauben. [KS99] Trotzdem gibt es vorbeugende Maßnahmen, die mit einbeziehen, daß dem Benutzer das Terminal gehört, wie eines, das mit einem PC verbunden ist. Die echten Vorbeugemaßnahmen haben nichts mit dem SmartCard/Terminal Datenaustausch zu tun, sie sind die Hintergrund-Verarbeitungssysteme die die Karten und Terminals überwachen und auffälliges Verhalten alarmieren.

5.2. Angriffe des Karteninhabers gegen das Terminal

Subtilere Angriffe sind die des Karteninhabers gegen das Terminal. Diese enhalten gefälschte oder modifizierte Karten, die manipulierte Software enthalten, mit der Absicht, das Protokoll zwischen der Karte und dem Terminal zu stören. Beispiele sind bei [McC96] zu finden.

Gutes Protokoll-Design mildert das Risiko dieser Art von Angriffen durch schwer fälschbare physische Eigenschaften der Karte (z.B. Hologramme von Visa und MasterCard Katen), die durch den Terminaleigentümer manuell geprüft werden können. Beachten Sie hier, daß digitale Signaturen in der Software nicht effektiv sind, weil manipulierte Karten immer über ihre Signaturen lügen können, und es für das Terminal keine Möglichkeit gibt, in die Karten hinein zu schauen. Sich gegen diese Art von Angriffen zu verteidigen benötigt eine weitere Trennung der Funktionen: Der Karteninhaber darf nicht die Möglichkeit haben, die Daten in der Karte zu manipulieren.

5.3. Angriffe des Karteninhabers gegen den Dateneigentümer

In vielen SmartCard basierten Geschäfts-systemen müssen die Daten, die in der Karte sind, gegen den Karteninhaber geschützt werden. In manchen Fällen ist es dem Karteninhaber nicht erlaubt, die Daten überhaupt zu kennen. Eine Zugangskarte zu einem Gebäude zum Beispiel kann geheime Werte in der Karte haben. Das Wissen dieser Werte könnte dem Karteninhaber erlauben, Kopien der Karten anzufertigen. Das Wissen eines geheimen Schlüssels in einer E-Commerce Karte könnte dem Karteninhaber erlauben, gefälschte Transaktionen durchzuführen.
In anderen Situationen darf der Karteninhaber die Werte in der Karte kennen, darf sie aber nicht ändern. Wenn die Karte eine Wertkarte ist, kann der Karteninhaber durch verändern des Wertes Geld erzeugen.

Es gibt zwei essentielle Charakteristiken dieser Angriffe. Die eine ist, daß sich die Karte als sichere

Umgebung verhalten muß, und die Kartendaten vor dem Zugriff durch den Karteninhaber schützen muß. In diesem Kontext muß die Karte ziemlich sicher sein, daß sie Angriffe mit einem Minimum an Kontrolle über ihre Umgebung erkennen und beantworten können muß. Und zweitens hat der Angreifer Zugriff auf die Karte und ihre Umgebung. Ihm ist erlaubt, daß er die Karte in sein eigenes Labor mitnehmen kann, und dort jedes Experiment damit machen kann, das er will. Ihm ist erlaubt die Karten zu zerstören, um zu lernen, wie sie funktionieren.

Es gibt zahlreiche Angriffe gegen die Daten in einer Karte. Diese Angriffe beinhalten Reverse-Engineering und das Überwinden von Einbruchs-sicherungen [AK96], Fehleranalyse [BS97,BDL97] und Verborgene Kanal-Angriffe wie Stromversorgung und Zeitanalysen [Koc96, Koc98b, KSWH98b, DLK+99]. Diese Angriffe waren im speziellen sehr effektiv gegen Pay-TV Zugangskarten [McC98, Row97], und wurden gegen Handy SIM Karten [BGW98] verwendet. Sie werden auch gegen Wertkarten im E-Commerce verwendet. [Row97].

5.4. Angriffe gegen den Karteninhaber durch den Kartenaussteller

Es gibt viele finanzielle Angriffe, die vorgeben, den Aussteller anzugreifen, aber das ist illusorisch. In Wirklichkeit sind es Angriffe gegen die Integrität und Authentizität der Daten oder Programme, die in der Karte gespeichert sind. Diese Angriffe werden möglich gemacht, durch die Entscheidung des Ausstellers, SmartCards zu verwenden, bei einem System, bei dem der Karteninhaber die Daten für den Aussteller oder eine andere Partei hält. Nehmen wir als Beispiel die Telefone. Wenn das Telefon ein Konto-basiertes System verwendet, wo eine SmartCard eine sehr lange Kontonummer speichert, die bei der Telefongesellschaft verwendet wird, um auf das Konto in einem Back-End System zu dereferenziern, dann gibt es die Möglichkeit, Kontonummern zu erraten, und Diebstahl basierend auf der Nummer. Dieses System kann durch Challenge/Response Systeme oder invertierte Hash Ketten Mechanismen um Wiederholungs-resistente Passwörter zu generieren erweitert werden. Die Idee dabei ist es, ein einfaches SmartCard System in Verbindung mit einem Back-Office verwalteten Authentifizierungs-Schema, um Diebstahl zu verhindern. Wenn der Kartenaussteller sich dazu entscheidet, Bits in die Karte zu geben, die das System authorisieren, dann darf er sich nicht wundern, wenn diese Bits angegriffen werden. Diese Bits können "authentifizierte" Kontonummern sein, oder könnten ein System mit einem Schlüssel in der Karte sein, basierend auf der Vermutung, daß man den Schlüssel nicht extrahieren kann, und die richtige Verwendung des Protokolls zeigt, daß die Karte nicht verändert worden ist. Diese Systeme basieren alle auf der fragwürdigen Annahme, daß das Sicherheitsumfeld einer SmartCard ausreicht für diese Anforderungen.

5.5. Angriffe des Karteninhabers gegen den SoftwareHersteller

Grundsätzlich besteht die Annahme, daß eine Karte, die an einen wahrscheinlich feindlichen Anwender ausgestellt wird, nicht mit neuer Software geladen wird. Dies wird durch verschiedene Stufen von Einweg-Transformationen vom Kartenhersteller vor der Ausgabe der Karte sichergestellt. Die darunterliegende Annahme kann sein, daß die Trennung zwischen Karteneigentümer und Softwareeigentümer unangreifbar ist, und man sich auf eine starke Trennung verlassen kann. Trotzdem haben Angreifer eine bemerkenswerte Fähigkeit gezeigt, daß Ihnen die dafür notwendige Hardware zugeschickt wird, meistens gratis, um Ihnen beim Ausführen eines Angriffs zu helfen.

5.6. Angriffe des Terminaleigentümers gegen den Aussteller

In einem System, das geschlossen gegenüber Aussenstehenden ist, wie zum Beispiel manche Prepaid Telefon-Wertkarten, ist der Terminaleigentümer auch der Kartenaussteller. In manchen offeneren Systemen aber, wie Mondex, ist der Terminaleigentümer der Verkäufer und der Kartenaussteller ist Mondex. Diese Trennung öffnet neue Möglichkeiten von Angriffen.

Das Terminal kontrolliert alle Kommunikationen zwischen der Karte und dem Kartenaussteller

(üblicherweise das Back-End des Systems). In diesem System kann das Terminal immer Datensätze fälschen, die nichts mit der SmartCard zu tun haben, die Aufzeichnung von Transaktionen ablehnen, ...
Tas Terminal kann also einen oder mehrere Schritte einer Transaktion auslassen, oder Kundenservice Probleme für den Aussteller bringen. Durch das nicht-abschließen einer Transaktion kann das Terminal den Aussteller betrügen, oder beim Durchführen der Transaktion, aber nicht-Auslieferung des Dienstes kann es zu einem Service Albtraum werden.

Diese Angriffe sind nicht durch die Natur von SmartCards bedingt, sondern sind einfache Angriffe gegen die Beziehung des Terminaleigentümers und dem Kartenaussteller. Manche Systeme versuchen diese Gefahren zu mildern, indem sie eine Sichere Verbindung zwischen der Karte und dem Computersystem des Ausstellers über das Terminal hinweg aufbauen. Viele Systeme verwenden Monitoring beim Backend, um die Effektivität dieser Angriffe zu reduzieren.

5.7. Angriffe des Ausstellers gegen den Karteninhaber

Im Allgemeinen gehen die meisten Systeme davon aus, daß der Kartenaussteller im Interesse des Karteninhabers agiert. Dies muß nicht unbedingt der Fall sein, und ein böser Aussteller kann verschiedene Angriffe gegen den Karteninhaber verwenden.
Diese Angriffe sind üblicherweise Eingriffe in die Privatsphäre auf die eine oder andere Art. SmartCard Systeme, die als Ersatz für Bargeld dienen müssen sehr vorsichtig designet werden, um die Anonymität und Unverknüpfbarkeit zu erhalten, die eine Eigenschaft von Bargeld sind. Angriffe oder Designfehler können die Privatspähre grundlegend reduzieren. Andererseits kann ein System als privater verkauft werden, als es ist, und dadurch dem Aussteller erlauben, Daten über den Karteninhaber zu sammeln.

Zusätzliche Features, die in die Karten hinzugefügt werden, können die anfängliche Charakteristik der Privatsphäre des Systems grundsätzlich verändern. Dies zählt als Angriff des Ausstellers, weil der Karteninhaber kaum gefragt wird, oder die dadurch entstehenden Sicherheitsprobleme wahrnehmen kann. Diese Änderungen sind oft nicht optional vom Standpunkt des Kunden. Die einzigste Auswahlmöglichkeit ist es entweder die Änderung zu akzeptieren, oder das System nicht mehr zu verwenden. Und schließlich kann dieser Angriff vom Aussteller, oder dem Hardware oder Software Hersteller in Zusammenarbeit mit dem Terminal gemacht werden, ohne dem Wissen oder der Zustimmung des Ausstellers.

5.8. Angriffe des Herstellers gegen den Dateneigentümer

Spezielle Designs von Herstellern können substantielle und schädliche Effekte auf den Dateneigentümer eines Systems haben. Das Design von sicheren Multi-User Computern ist eine Herausforderungen, und das Sicherheitsmodell, das man verwenden muß, um einen sicheren Kernel, der Prozessen Absicherung gegeneinander bietet, ist es noch nicht gelöstes Problem. Indem man ein Betriebsystem anbietet, das es erlaubt oder gar empfiehlt, verschiedenen Anwendern verschiedene Programme auf derselben Karte laufen zu lassen, öffnet man eine noch größere Zahl weiterer Sicherheitsprobleme.

Das erste, und am offensichtlichsten ist die Subversion des Betriebssystems und im folgenden der anderen Programme. Dies ist ein Bereich, wo die wichtigsten Betriebssystem-Hersteller es die letzten 30 Jahre nicht geschafft haben, adäquate Sicherungsmechanismen anzubieten. Die Hersteller, die in letzter Zeit SmartCard Betriebssysteme veröffentlicht haben, haben keine beneidenswerte Geschichte. Trotzdem, selbst wenn das SmartCard Betriebssystem sicher gemacht werden könnte, bleiben die Probleme der Benutzer-Schnittstelle, und werden durch die Nachteile der SmartCards nur noch verschlimmert. Woher weiß der Benutzer (oder Designer), welche Programme auf der Karte laufen werden, wenn sie in ein Terminal gesteckt wird? Wie wird sichergestellt, daß das Programm direkt mit dem Terminal reden kann, und nicht durch ein anderes Programm? Wie kann ein Programm, das glaubt, kompromittiert zu sein, sich selbst sicher beenden, und ein Signal an die Außenwelt schicken das dieses Sicherheitsproblem jemandem mitteilt? Oder sollte das möglich sein: Welche interessanten Angriffe werden möglich, wenn eine Karte ihren Selbstmord bekanntgibt? Kann die Karte garantieren, daß sobald eine entsprechende Nachricht

geschickt wurde, daß die Zerstörung des Speichers auch wirklich komplett ist, im Falle einer manipulierten Stromversorgung?

Weniger offensichtlich wären die absichtliche Verwendung schlechter Zufallszahlengeneratoren [KSWH98a], oder anderer Aspekte der Kryptografischen Implementierung, welche geheimnisvoll und schwer zu testen sind [Sch97, Sch98a, Koc98a, Sch98b]. Der Hersteller ist in einer erstaunlichen Position, um kleptographische Angriffe zu machen. [YY96, YY97a, YY97b]. Von den großen SmartCard Herstellern hat keiner eine bemerkenswerte Vergangenheit darin, Betriebssysteme herzustellen, die frei von ausnutzbaren Schwachstellen waren. Zusätzlich kann der Hersteller durch die Unterstützung mehrerer Implementationen unterschiedlicher Protokolle sich die Möglichkeit geben, an die Schlüssel der Anwendungen zu kommen, indem einer von vielen verdeckten Kanälen verwendet wird. [Sim84, Sim85, Sim86, Sim94].

Und schließlich ist es möglich für eine Anwendung einer SmartCard eine andere Anwendung, die auf der SmartCard läuft, zu manipulieren. Es wurde gezeigt, daß wenn man ein sicheres Protokoll nimmt, und ein anderes, auch sicheres, Protokoll entwicklet, daß das zweite Protokoll die Sicherheit des ersten Protokolls brechen kann, wenn beide auf demselben Gerät mit denselben Schlüsseln arbeiten. [KSW96].

6. Veränderungs oder Nachahmungsangriffe

Es gibt eine Klasse von Angriffen, die auf der Trennung oder Veränderung der Rollen, die von den verschiedenen Parteien gespielt werden, basiert. Wenn zum Beispiel die Rolle des Karteninhabers verändert wird, weil die Karte gestohlen wurde, kann der Angreifer Zugang zu Daten, die der Karteninhaber gespeichert hat, bekommen. Oder der Angreifer kann die Möglichkeiten des Terminaleigentümers bekommen, indem er ein spezielles ActiveX Control verwendet, daß es einem Angreifer erlaubt, der Terminaleigentümer zu werden.

Der essentielle Charakter eines Veränderungsangriffs ist, daß eine Partei verändert wird, was zu einer unerwarteten Veränderung der Motivation dieser Partei wird. Wenn eine Karte gestohlen wird, hat der neue Karteninhaber (z.B. der Dieb) alles Interesse verloren, die Sicherheit des Kontos, und möglicherweise die physische Integrität der Karte zu schützen. Wenn ein Terminal manipuliert wird, ist sein Wunsch nach der Teilnahme an dem Protokoll auf faire Art und Weise durch den Wunsch, das Protokoll zu umgehen getauscht. (Warum sonst sollte das Terminal manipuliert werden?). Wenn ein System davon ausgeht, daß die Daten auf einer Karte sicher sind, weil es im Interesse des Karteninhabers und Ausstellers liegt, wird das System gegenüber Diebstahl der Karte verwundbar.

Alternativ untersuchen wir ein System mit einem SmartCard Leser, der an einen PC angeschlossen wird, wobei der PC als Teil des Terminals agiert. Das Terminal wird als freundlich gegenüber seinem Eigentümer angenommen, vielleicht wird es verwendet, um Web-Zertifikate von zuhause in die Arbeit mitzunehmen. Leider kann das Terminal verändert werden, indem man ActiveX Controls einführt, die die Lesesoftware verändern. Dieser Angriff, durch die Veränderung des erwarteten Verhaltens, kann die Sicherheit eines Protokolls umgestalten. Die Verhaltensänderung kann hier aktiv sein, im Falle einer veränderten Anfrage und einem verbundenen Display, oder passive, im Falle eines Überwachungs-angriffs. Überwachungsangriffe können die Privatsphäre einer Transaktion, oder die Geheimhaltung eines PINs oder anderer Daten angreifen. Letzteres ist wahrscheinlich die Vorbereitung auf einen aktiven Angriff, nicht unbedingt gegen das SmartCard Protokoll. Bedenken Sie, daß PINs oft in mehr als einem System verwendet werden, und daß eine aktiver Angriff nicht das SmartCard System angfreifen muß.

6.1. Angriffe von Dritten durch gestohlene Karten

Es gibt zwei Unterschiede zwischen diesem Angriff und einem Angriff des Karteninhabers. Zum einen hat

der Dieb keinen Zugang zu geheimen Informationen, die er benötigt, um die Karte zu aktivieren. Zum Zweiten hat der Dieb nur begrenzt Zeit, seinen Angriff zu tätigen, bevor der Karteninhaber den Diebstahl bemerkt.

Dadurch sind alle Angriffe des Karteninhabers möglich, mit folgenden Zusätzen: Der Dieb hat kein Interesse an Langzeit Auswirkungen gegen den legitimen Karteninhaber. Zum Beispiel, eine Kleinbetrags-Wertkarte kann Aufzeichnungen aller Transaktionen führen, um gegen Karteninhaber-Betrug abzusichern, und alle Diskrepanzen dann dem Karteninhaber verrechnen. Ein Dieb, der eine Karte stiehlt würde sich durch diese Abwehrmaßnahme nicht abhalten lassen.

Es ist möglich, Abwehrmaßnahmen in das System einzubauen, entweder in der Karte, oder beim Aussteller. In der Karte sind Peripherie und Anomalie Verteidigungen verfügbar. Die Peripherie Abwehr ist, daß die Karte mehrere falsche Eingaben einer PIN als Angriffsversuch werten kann. (Beachten Sie, daß dies die Möglichkeit eines Denial of Service ermöglicht) Die Anomalie Erkennung würde bei einer Karte die gesamte Historie abspeichern und eine Musteränderung erkennen. Dies ist eine aggressive Anforderung, aber in den Fällen, wo eine Karte offline verwendet wird, könnte es Sinn machen, einen Kontakt mit dem Aussteller zu erfordern, bevor die Karte weiter verwendet werden kann, um dem Backend System eine Chance zu geben, eine Auswertung und eine anspruchsvollere Entscheidung zu ermöglichen, oder einfach das System gegen Kopien von SmartCards abzusichern.

6.2. Eva und der Holzhammer

Wenn wir annehmen, daß es die Anwendung einer SmartCard ist, Protokoll Interaktionen zu erlauben zwischen sich gegenseitig mißtrauenden Parteien, oder zumindest Parteien, deren Interessen divergieren, dann muß das Protokoll denselben Angriffen widerstehen können, die möglich wären, wenn es auf einem ganz normalen Computer implementiert wäre. Dadurch können die meisten Angriffe, die auf dem Abhören oder böswilligen Protokollmanipulationen basieren, als Fälle modelliert werden, bei denen eine Partei eine andere angreift. Wenn man annimmt, daß das Protokoll richtig designet ist, wird es diesen Angriffen genauso widerstehen, egal ob der Angreifer intern oder extern ist.

6.3. Gemeinsame Angriffe

Systeme, die darauf vertrauen, daß die Trennung zwischen verschiedenen Komponenten als eine feindselige Grenze ohne Kooperation beibehalten wird, könnten überrascht sein, wenn Rollen, die als getrennt wurden zusammengebracht werden. Die SmartCard und SetTop Box, die eigentlich verschiedene Interessen haben, können zur Kollaboration dem Eigentümer helfen, nicht authorisierte Services zu empfangen. Genauso könnte der Terminaleigentümer überrascht sein, wenn er feststellt, daß die Karte und das Terminal von derselben Firma programmiert und hergestellt worden sind, und einige undokumentierte Features hat. Die Zahl der möglichen Kollaborationen und interessanten Modelle der Angriffe wächst mit der Anzahl der beteiligten Parteien des Systems. Die, die vergessen, daß die meisten Angriffe von Insidern ausgeführt werden, werden wahrscheinlich daran erinnert (wenn man davon ausgeht, daß deren Betrugserkennung gut genug funktioniert.)

7. Abwehrmodelle

Es gibt grundsätzlich zwei Modelle, einen Angriff gegen SmartCard Systeme abzuwehren. Das eine ist, spezifische Angriffe zu erschweren: Verwende starke kryptographische Protokolle, erhöhe Abhörsicherheit, ... Wir diskutieren diese Methoden nicht im Detail, wir glauben, daß diese weniger effektiv sind, und mehr DesignFehler verursachen können als die zweiten, die ganze Angriffsklassen ineffektiv machen. Dies kann durch effektives reduzieren der beteiligten Parteien gemacht werden, oder dem Erhöhen der Transparenz der Rolle einer Partei zu dem Punkt, an dem ein Angriff sehr schwer möglich wird.
Der einfachste Weg um die Anzahl der beteiligten Parteien zu reduzieren ist es, die Rollen zu kombinieren,

so daß es weniger Hüte zu tragen gibt. Wenn der Karteninhaber auch der Dateninhaber ist, dann sind alle Angriffe des Karteninhabers gegen den Dateninhaber irrelevant. Oder wenn der Terminal Eigentümer auch der Aussteller ist, dann sind Angriffe des Terminaleigentümers gegen den Aussteller nur mehr nach einer Veränderung der Rollen möglich, wenn der Angreifer die Kontrolle über das Terminal übernimmt.

7.1. Weniger Trennungen

Jedesmal, wenn bei einem System die Design-Rollen von zwei oder mehreren Parteien zu einer verbunden werden, verschwinden die Angriffsmöglichkeiten der Rollen gegeneinander. Zum Beispiel, wenn der Karteninhaber und das Terminal verbunden werden, und ein Bildschirm und ein Dateneingabegerät an die Karte angeschlossen wird, dann verschwinden die Möglichkeiten des Lauschens und vertrauensunwürdigen Anzeigen, ...
Auf der anderen Seite entstehen neue Probleme die man beachten muß, wenn weitere Parteien zum System hinzukommen. Die Trennung des Terminals von der Karte läßt eine Situation entstehen, die Man-In-The-Middle Angriffe möglich macht. Die Kombination der physischen Verpackung der Karte, und der Kontrolle des Terminals über die Benutzerschnittstelle und das Netzwerk erlaubt viele Angriffe der beschriebenen Angriffe, wenn das Protokoll nicht dafür designt wurde, diesen Angriffen zu widerstehen. Die Erfahrung hat gezeigt, daß trotzdem viele Sicherheitsprodukte angeboten werden, ohne MITM, Wiederholungs und Reflektionsangriffe zu bedenken.[Sho96, Sho97]. Selbst wenn diese Angriffe bedacht werden, macht die Erweiterung um weitere Parteien bei den Transaktionen die Verwaltung von Schlüsseln, Sequenznummern und anderer Verteidigungsmaßnahmen alles wesentlich komplizierter.

Wenn man die Unfähigkeit der SmartCard mit der Außenwelt zu kommunizieren bedenkt, wäre die einfachste Trennungs-Reduktion, sicherzustellen, daß der Karteninhaber und der Dateneigentümer derselbe sind. Dies eliminiert Angriffe des Karteninhabers gegen die Daten, die derzeit die größte Plage der existierenden Systeme darstellt. Eine andere extrem effektive Änderung wäre einen Bildschirm und Eingabegeräte den Karten zur Verfügung zu stellen, was eine starke Kostenerhöhung bringen würde.

7.2. Mehr Transparenz

Es hat sich in der Sicherheits-Community herumgesprochen, daß der beste Weg, die Sicherheit eines Systems zu garantieren ist, der Öffentlichkeit die Möglichkeit zu geben, das System zu kontrollieren. Es hat sich immer wieder gezeigt, daß interessierte Angreifer an die nötigen Spezifikationen kommen, oder ein System auch ohne ihnen erfolgreich angreifen können. [Sho96, Bla94], und daß offene Publikationen zu mehr Kontrollen und Analysen führen. (Beispiele sind IPSec, PGP und S/MIME.) Wenn man die Mechanismen von Einfachkeit und Offenheit verbindet, vereinfacht sich die Aufgabe der Prüfer, die ein System kontrollieren. Eine Reduktion der Anzahl der beteiligten Parteien eliminiert nicht nur eine ganze Klasse von Angriffen, sondern macht auch die Aufgabe der Analyse des Systems einfacher. Die Einfachkeit der Sicherheitsanalyse wird die Analyse erleichtern und auch die Erfolgsaussicht verbessern.

Die Transparenz-Verteidigung involviert klar getrennte Rollen so daß Angriffe schwerer durchzuführen sind. Zum Beispiel das Mondex System enhält eine Reihe von Terminal Arten (manche davon portabel) die dem Benutzer erlauben, verschiedene Parameter zu kontrollieren, unabhängig vom Terminal eines Verkäufers. Dies erlaubt eine Klasse von Angriffen gegen den Karteninhaber oder wird wesentlich schneller aufgedeckt. Zugang zu allen von Mondex gespeicherten Parametern (z.B. die Daten des Dateneigentümers) würden wahrscheinlich das System wesentlich sicherer machen, weil die Kontrollierbarkeit des Systems steigt. Ähnlich dazu ist ein Angriff des Softwareherstellers viel schwerer, wenn eine starke und klare Spezifikation vorliegt, und/oder OpenSource Implementierungen vorliegen.

7.3. Design für Sicherheit

Dieses Abwehrmodell ist darauf fokussiert, daß das Systemdesign von der Architektur weg sicher ist. [SSS+98]. Es hat sich gezeigt, daß das Hinzufügen von Sicherheit zu einem System nach der Designphase

sehr schwierig, teuer und fehleranfällig ist. Daher bieten wir ein Modell an, bei dem gründliches Design von Anfang an den Aufwand für kostenspielige und komplexe Versuche, die Sicherheit im Nachhinein wieder hinzubiegen, eliminiert. Das Reduktionsmodell vereinfacht nicht nur den Designprozess und die Implementierung, sondern ist auch schwer falsch zu machen.Wir haben gesehen, daß Implementationsfehler meistens der Grund sind für die Fehler von Kryptosystemen. [And94, Sch97, Sch98a, Koc98a, Sch98b].

Eine andere Facette zur Transparenzverteidigung ist es, Komplexitäten und Risiken von Multi-Anwendungs SmartCards zu vermeiden. Multi-Anwendungs SmartCards nicht zu verwenden reduziert die Anzahl der beteiligten Parteien und erzeugt ein einfacheres Betriebssystem mit weniger Komplexität und weniger Potential für Fehler. Die Reduktion der Anzahl der beteiligten Parteien, die die Karte verwenden (von N zu 2) bedeutet, daß die Probleme von Betriebssystem-Manipulation und gegenseitigen Anwendungs-Angriffen praktisch eliminiert sind.

8. Zusammenfassung

Wir haben gezeigt, daß die Trennung von Sicherheitsgrenzen eine schwierige Aufgabe ist. Im besonderen, ein Benutzer, der einen Computer trägt mit Daten eines anderen Dateneigentümers, den der Karteneigentümer angreifen will, ist eine sehr riskante Situation für den Dateneigentümer. Wir haben auch gezeigt, daß das Handicap der Karten, nicht kommunizieren zu können es sehr anfällig für Angriffe des Terminals macht. Diese Verletzbarkeiten sind Teil eines SmartCard Systems durch das Design, und benötigen viel Aufwand, bekämpft zu werden.

Wir haben ein paar fundamentale Verteidigungsmethoden für Karten gezeigt die auf der Systemdesign Ebene ansetzen, und dem Systemdesigner ein neues Modell angeboten, mit dem Systeme evaluiert werden können. Dieses Modell empfiehlt, Sicherheit von Anfang an beim Systemdesign schon zu entwickeln. Wir empfehlen, die Benutzerschnittstelle unter die Kontrolle des Benutzers zu geben. Systemdesign, das die Rollen wieder kombiniert in bessere Systeme wird in einer Investition durch weniger Schwachpunkte resultieren.

Referenzen

Die Referenzen entnehmen Sie bitte dem Originaldokument
http://www.counterpane.com/smart-card-threats.html