„Die gesamte Technik ist sicher“
Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis

Frank Morgner und Dominik Oepen
{morgner|oepen}@informatik.hu-berlin.de
Humboldt-Universität zu Berlin
Institut für Informatik, Lehrstuhl für Systemarchitektur
Unter den Linden 6, 10099 Berlin

***Zusammenfassung*—Die Authentisierung mit dem neuen Personalausweis basiert auf dem Prinzip der Zweifaktorauthentisierung durch Besitz und Wissen. Notwendig sind der Besitz des Ausweises und die Kenntnis einer PIN. Mögliche Angriffe auf diese Faktoren wurden bereits vor der Einführung des neuen Personalausweises vorgestellt und als unrealistisch oder unvollständig zurückgewiesen. Wir untersuchen hier die Machbarkeit und Auswirkung von Relay-Angriffen in Hinblick auf die verschiedenen Lesegeräteklassen und Anwendungsszenarien des neuen Personalausweises. Nach dem derzeitigen Stand der Spezifikationen lassen sich solche Angriffe kaum verhindern. Einige der Probleme erweisen sich als unlösbar, für andere existieren Lösungsansätze, welche von simpel, aber unzureichend bis komplex, aber kaum umsetzbar reichen.**

I. Überblick

Der am 1. November in Deutschland eingeführte neue Personalausweis (nPA) beinhaltet einen Chip, welcher über eine drahtlose Schnittstelle kommuniziert und drei verschiedene Funktionen zur Verfügung stellt. Neben der hoheitlichen Identifikation stehen eine über das Internet nutzbare Authentisierungsfunktion und die Möglichkeit der Erstellung qualifizierter elektronischer Signaturen (QES) durch die eID- bzw. eSign-Funktion des Ausweises zur Verfügung.

Zur Nutzung dieser Funktionen sind prinzipiell zwei Faktoren notwendig: Besitz des Ausweises und Kenntnis (mindestens) eines Geheimnisses. Wir untersuchen die Möglichkeiten eines Angreifers, Zugriff auf diese beiden Faktoren zu erhalten und betrachten die sich daraus ergebenden Konsequenzen für die eID- und eSign-Funktion.

Zur Verwendung des nPA ist ein Lesegerät notwendig. Dieses realisiert im einfachsten Fall lediglich den Datenaustausch mit dem Ausweis mittels einer ISO-14443 konformen Funkschnittstelle, kann aber auch noch weitere Funktionen anbieten. Es existieren drei verschiedene Kategorien von Lesegeräten: Basis-, Standard- und Komfortleser. Tabelle I listet einige Merkmale der verschiedenen Klassen auf.

Diese Aufteilung entspricht weitgehend der bisher üblichen Einteilung von kontaktbehafteten Lesegeräten in die Geräteklassen eins bis drei. Die wesentlichen Unterschiede bestehen in der kontaktlosen Schnittstelle, in der Notwendigkeit eines Sicherheitsmoduls zur Speicherung des privaten TA-Schlüssels im Komfortleser und in der Fähigkeit von Standard- und Komfortleser einen verschlüsselten Kanal zum Ausweis aufzubauen.

Im Rahmen dieser Arbeit wollen wir uns auf zwei Anwendungsfälle konzentrieren: die Verwendung der eID-Funktion über das Internet und die lokale Nutzung der eSign-Funktion. In beiden Fällen liegt der Personalausweis auf einem Lesegerät, welches wiederum an einen Computer angeschlossen wird. Bei Verwendung der eID-Funktion kommuniziert dieser Computer mit dem eigentlichen Dienstanbieter über die Schnittstellen der eCard-API. Dazu benötigt der Dienstanbieter ein Terminalzertifikat (und den zugehörigen privaten Schlüssel) und stellt somit das eigentliche Authentisierungsterminal zur Verfügung. Der am PC des Nutzers angeschlossene Reader übernimmt als lokales Terminal lediglich die RFID-Kommunikation.

Bei Verwendung der eSign-Funktion ist hingegen das Signaturterminalzertifikat inklusive des privaten Schlüssels im Lesegerät selbst gespeichert. Das Lesegerät stellt in diesem Fall als integriertes Terminal den Endpunkt der Kommunikation mit dem Personalausweis dar.

Zur Absicherung der Datenübertragung kommen die Protokolle der Extended Access Control (EAC) [1] zum Einsatz. PACE etabliert dabei einen gesicherten Kanal zwischen dem Ausweis und dem Ort der PIN-Eingabe, die Terminal Authentication authentisiert und autorisiert den Dienstanbieter, der auf den nPA zugreifen möchte und die Chip Authentication (CA) dient dem Nachweis der Authentizität des nPA. Nach der CA ist ein Ende-zu-Ende verschlüsselter Kanal zwischen Dienstanbieter und Ausweis etabliert, über den die gesamte weitere Kommunikation erfolgt.

Zur Durchführung von PACE ist die Kenntnis eines Geheimnisses (zumeist eID-PIN oder CAN) notwendig, es wird also der Authentisierungsfaktor „Wissen“ überprüft. Um die

Tabelle I
Unterschiedliche optionale (O) oder obligatorische (X) Module der Lesegeräteklassen

	Basisleser	Standardleser	Komfortleser
RFID	X	X	X
Tastatur	O	X	X
PACE	O	X	X
Firmware-Update	O	X	X
Display	O	O	X
QES (nPA)	O	O	X

CA durchzuführen, wird der im Personalausweis gespeicherte private CA-Schlüssel benötigt. Unter der Annahme, dass es nicht möglich ist, diesen Schlüssel aus dem Ausweis zu extrahieren, soll die CA also unter anderem den Besitz eines Personalausweises sicherstellen.

II. Relay-Angriffe

Bereits im Vorfeld der Einführung des nPA gab es erste Kritik an der Sicherheit. Der Chaos Computer Club wies darauf hin, dass ein Angreifer über einen auf dem PC des Opfers installierten Keylogger die eID-PIN des Ausweises abgreifen könnte, falls sie über die Tastatur des PCs eingegeben wird [13]. Später führten Max Moser und Thorsten Schröder einen sogenannten Relay-Angriff auf die Schweizer SuisseID vor [12] und wiesen darauf hin, dass dieser Angriff grundsätzlich auf den nPA mit Basislesegerät übertragbar sei. Ihr Angriff basierte auf der Weiterleitung von USB-Paketen über das Internet. Auch hierfür ist eine Schadsoftware auf dem PC des Opfers notwendig. Bemerkenswert ist dabei vor allem die Einfachheit des Angriffes. Die zum Schutz des Ausweises verwendeten EAC-Protokolle werden komplett ignoriert. Durch einfaches Weiterleiten von Paketen erhält der Angreifer *Zugriff* auf die Chipkarte, ohne ihn selbst zu besitzen.

A. Angriff auf die eID-Anwendung

Die Interaktion zwischen Chipkartenapplikationen und Kartenlesern ist Betriebssystem übergreifend durch den PC/SC-Standard beschrieben. Morgner und Oepen haben im Rahmen der Virtual Smart Card Architecture [11] einen Treiber für die Unix-Implementation des PC/SC-Dienstes erstellt, der für Chipkartenapplikationen wie ein einfacher Smartcardleser erscheint. Tatsächlich ist es aber keine reale Smartcard, mit der dieser Leser kommuniziert, sondern die virtuelle Smartcard. Virtueller Smartcardleser und virtuelle Smartcard tauschen APDUs über das Netzwerk aus. Die virtuelle Smartcard kann nicht nur existierende Smartcards nachbilden[1], sondern die vom virtuellen Smartcardleser erhaltenen Daten auch an eine lokal verfügbare Chipkarte weiterleiten. APDUs fließen in unserem Versuchsaufbau (siehe Abbildung 1) also von der Applikation beim Angreifer über den virtuellen Smartcardleser zur virtuellen Smartcard beim Opfer und von dort zur realen Chipkarte des Opfers und wieder zurück. Die AusweisApp beim Opfer wird nicht verwendet oder modifiziert.

Die beim Angreifer gestartete AusweisApp erkennt den virtuellen Leser als gültigen Smartcardleser[2]. Nachdem sich die virtuelle Smartcard mit dem nPA und dem virtuellen Smartcardleser verbunden hat, initialisiert die AusweisApp den weitergeleiteten Ausweis des Opfers. Der Angreifer kann nun wie gewohnt über den Browser eine Verbindung zum Dienstanbieter aufbauen. Das Browser-Plugin leitet Anfragen weiter an die AusweisApp des Angreifers und diese führt PACE mit dem entfernten nPA durch. Nachdem TA und CA

[1]Unter anderem kann die virtuelle Smartcard einen deutschen Reisepass nachbilden

[2]Zur Erkennung zertifizierter Smartcardleser siehe III.

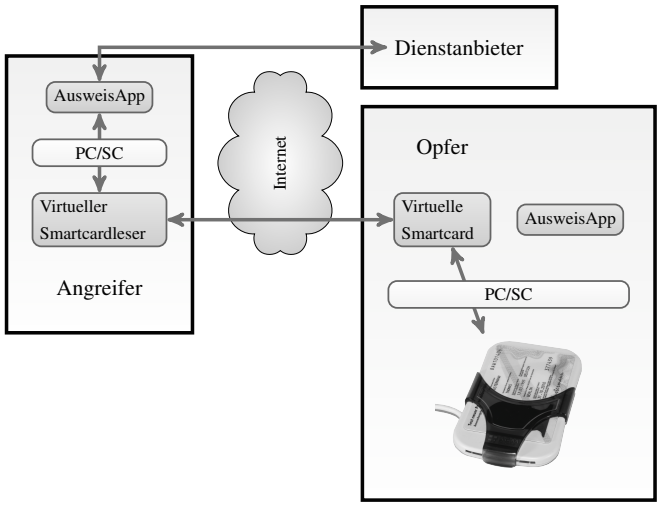

Abbildung 1. Angriff auf die eID-Funktion

erfolgreich abgeschlossen sind, werden die Daten aus dem neuen Personalausweis des Opfers ausgelesen.

Dabei werden hier folgende Annahmen getroffen:

- A1 Ein Lesegerät ist für den Betrieb beim Opfer vorbereitet, der nPA eingelegt.
- A2 Der Angreifer kann beim Opfer die virtuelle Smartcard starten und mit dieser kommunizieren.
- A3 Der Angreifer ist im Besitz der für die Chipkarte benötigten Geheimnisse.

Mit Mitteln aus dem Konjunkturpaket II versucht die Bundesregierung, „eine signifikante Anzahl an Lesegeräten für die Nutzung elektronischer Chipkarten verfügbar“ [5] zu machen. Es werden bereits zahlreiche kostenlose Basisleser verteilt. Die Ausgabe von vergünstigten Standard- oder Komfortlesern ist geplant. Damit ein Angreifer auch den Ausweis in einem betriebsbereiten Lesegerät verwenden kann, muss dieser eingelegt sein. Automatisiert könnte ein Angreifer vor oder nach der regulären Nutzung des nPA einen den elektronischen Identitätsnachweis innerhalb von etwa fünf bis zehn Sekunden durchführen. Annahme A1 ist also durchaus gerechtfertigt.

Für die Nutzung der eID-Funktion ist eine Internetanbindung zwingend erforderlich. Zur Absicherung des verwendeten PCs empfiehlt das BSI daher technische und organisatorische Maßnahmen wie Firewall, Virenscanner und das ständige Einspielen aller System- bzw. Softwareupdates [3]. Es ist jedoch utopisch anzunehmen, dass ein 100-prozentiger Schutz möglich ist. In einem aktuellen Test [9] erreichte selbst das beste der getesteten Virenschutzprogramme bei neuen Schadprogrammen lediglich eine Erkennungsquote von 54,9%. Bei breiter Nutzung des neuen Personalausweises sollte es also einem Angreifer möglich sein, bei entsprechend vielen Opfern ein speziell für den nPA entwickeltes Schadprogramm platzieren und starten zu können. Ein infizierter Computer (A2) ist also kein unrealistisches Szenario.

Die dritte Annahme zielt auf den zweiten Schutzfaktor

ab, das Wissen um die geheime PIN. Bei Verwendung eines Basislesers beim Opfer und ausgehend von einem kompromittierten Computer (A1, A2), wurde gezeigt, dass das Abgreifen der eID-PIN durch einen Keylogger bzw. Trojaner möglich ist [13]. Das Erfassen der PIN beim Opfer könnte ein Standard- oder Komfortleser verhindern. Aber es besteht auch hier erwiesenermaßen die Gefahr, dass die speziell getesteten Chipkartenleser trotz Zertifizierung manipuliert werden können [7]. Generell sollten aber in diesem Fall klassische Betrugsmethoden wie Social Engineering, Phishing oder Skimming für Angreifer leichter umzusetzen sein. Die eID-PIN könnte z. B. ausgespäht oder missbraucht werden, wenn diese im öffentlichen Raum genutzt wird. Weiterhin könnte ein Angreifer auch schlicht versuchen, die eID-PIN zu erraten. Zwar bleiben dafür nur zwei bzw. drei Versuche, aber bei einer besonders breiten und großen Nutzerschicht, ist es wahrscheinlich, dass für die frei wählbare eID- oder eSign-PIN gelegentlich auch beliebte Passworte wie „123456“ oder die aufgedruckte CAN verwendet werden.

Standard- und Komfortleser schützen den Authentisierungsfaktor „Wissen“, indem sie eine gesonderte Eingabemöglichkeit für die PIN bieten. Grundsätzlich ist auch mit einem solchen Lesegerät das Weiterleiten von APDUs an einen Angreifer möglich. Wir stellten dieses Szenario mit einem nicht zertifizierten Testmuster nach. Bei einer bekannten PIN war es uns auch mit diesem Lesegerät möglich, den elektronischen Identitätsnachweis aus der Ferne mit einem nPA durchzuführen.

Die Möglichkeit, auch bei der Verwendung eines höherwertigen Lesegeräts das Geheimnis über die Tastatur des PCs einzugeben, ist in der Technischen Richtlinie 3119 sogar explizit vorgesehen [2, 47f]. Die Chipkartenapplikation kann demnach PIN, PUK oder CAN an den Komfortleser übermitteln, so dass dieser damit selbstständig damit das PACE-Protokoll durchführt. Dieses Verhalten konnten wir ebenfalls mit dem Lesermuster mit PIN-Pad testen.

Für einen Angreifer ist es entscheidend, dass der betriebene Aufwand im Verhältnis zu seinem Nutzen steht. Hier steht der Personalausweis besonders als sichere Signaturerstellungseinheit im Fokus. Dabei ist es in diesem Falle unvorteilhaft, dass die QES mit sehr hohem Schutzbedarf auf derselben Chipkarte vorhanden ist wie die eID-Funktion mit niedrigem bis mittlerem Schutzbedarf.

B. Angriff auf die eSign-Funktion

Bisher wurden für die Erzeugung von einer QES üblicherweise dedizierte kontaktbehaftete Signaturkarten in Kombination mit einem Klasse-3-Lesegerät verwendet. Die Förderung der Verbreitung der QES ist eines der erklärten Ziele der Bundesregierung. Da in absehbarer Zeit nahezu jeder Bundesbürger mit einem neuen Personalausweis ausgestattet sein wird, besitzt damit auch jeder eine sichere Signaturerstellungseinheit (SSEE). Um den neuen Personalausweis für eine QES nutzen zu können, müssen drei Voraussetzungen erfüllt sein:

1. Nachladen der QES und Bereitstellung des qualifizierten Zertifikats durch einen ZDA
2. Kenntnis der eSign-PIN
3. Zugriff auf den nPA: Verifkation der eSign-PIN und Signaturerstellung durch den Ausweis

Da die Bereitstellung der Zertifikate durch private Trust-Center erfolgen soll, müssen sie nach der Ausstellung des Ausweises vom Ausweisinhaber separat beantragt und auf den Ausweis nachgeladen werden. Um den Anforderungen des Signaturgesetzes und der Signaturverordnung Genüge zu leisten, ist dabei die zuverlässige Identifikation des Antragsstellers durch den Zertifizierungsdiensteanbieter (ZDA) zu gewährleisten. Laut TR-03117 [4, S. 31] genügt dafür der elektronische Identitätsnachweis des nPA. Im offenen Anwendungstest des nPA war oft die Rede vom „medienbruchfreien Nachladen“ der QES, also das Nachladen ohne die Verwendung eines weiteren Kommunikationskanals, um die QES an den rechtmäßigen Besitzer zu binden. Auch ein entsprechender Dienst im Rahmen des Anwendungstests des ZDA D-Trust suggerierte, dass ein erfolgreicher eID-Durchlauf die einzige Voraussetzung zur Bereitstellung eines Zertifikats sei.

Mit der Änderung der Signaturverordnung vom 15. November 2010 hat die Bundesregierung eine weitere Anforderung an den ZDA expliziert. Dieser muss nun nicht mehr nur die zuverlässige Identifikation des Antragsstellers durchführen. Der ZDA „hat sich vom Signaturschlüssel-Inhaber den Besitz der sicheren Signaturerstellungseinheit [...] bestätigen zu lassen“. Die Form der Bestätigung kann vom ZDA gewählt werden. In der Signaturverordnung schlägt man unter anderem die Bestätigung in Schriftform vor. Hier könnte sich möglicherweise zeigen, dass die Bestätigung des Besitzes doch von einem Angreifer und nicht nur vom rechtmäßigen Besitzer durchgeführt werden kann. Weil die konkrete Umsetzung durch einen ZDA aber noch fehlt, können wir nicht genau sagen, ob dies für einen Angreifer eine Hürde darstellen wird oder nicht.

Mit dem in Abschnitt II-A beschriebenen Relay-Angriff auf die eID-Funktion ergibt sich für den Angreifer die Möglichkeit, den Ausweis des Opfers auch zum Nachladen eines qualifizierten Zertifikates zu verwenden. Die eSign-PIN kann der Angreifer dabei im Zuge der Aktivierung der eSign-Funktion selbst setzen, solange der Ausweis noch nicht für die QES vorbereitet wurde. Er benötigt dafür die Card Access Number (CAN) des Ausweises[3].

Allerdings werden für das Setzen der eSign-PIN und das eigentliche Signieren Berechtigungen benötigt, wie sie in einem Komfortleser-Zertifikat zu finden sind. Daher ist die in Abbildung 2 dargestellte Modifikation des Angriffes notwendig. Der Angreifer benötigt nun selbst einen Komfortleser. Der Ausweis des Opfers wird dann „virtuell“ in den Leser des Angreifers eingelegt. Dies kann durch das Einspielen der Antwort-APDUs des Ausweises per NFC in den Komfortleser geschehen. Eine weitere Möglichkeit wäre es, einen Komfortleser per Software zu emulieren. Hierzu müsste man den privaten TA-Schlüssel

[3]Weil die CAN nicht durch einen Fehlbedienungszähler geschützt ist, ist ein Brute-Force Angriff auf dieses Geheimnis prinzipiell möglich. Mit Ausweisen aus dem Anwendungstest haben wir dies erfolgreich getestet. Es dauerte durchschnittlich etwa 6 Tage, bis wir die CAN ermittelt hatten.

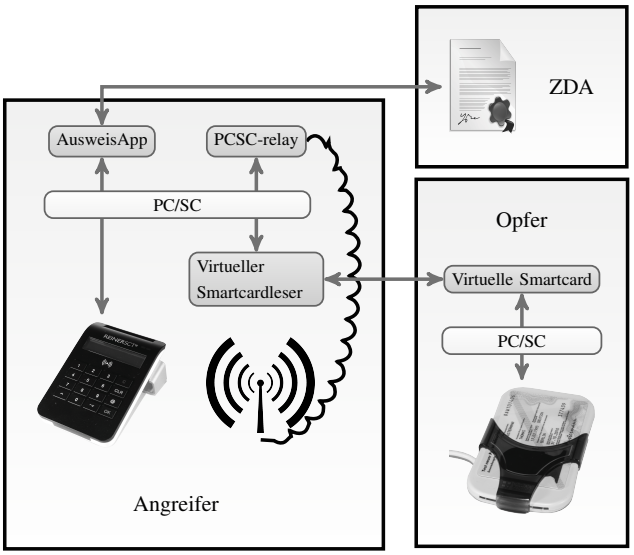

Abbildung 2. Relay-Angriff bei der Beantragung eines qualifizierten Zertifikats

aus einem Komfortleser extrahieren oder das Sicherheitsmodul eines Komfortlesers als Orakel nutzen.

Wir haben exemplarisch das Wiedereinspielen der Antwort-APDUs über die Luftschnittstelle mittels des in den Touchatag integrierten PN532 nachgestellt. Auf dem Computer des Opfers kam dabei wieder die virtuelle Smartcard im Relay-Modus zum Einsatz. Auf der Angreiferseite nahm wiederum der virtuelle Smartcardleser die Pakete entgegen, leitete sie in diesem Fall aber nicht an die AusweisApp, sondern an das Programm PCSC-relay [11] weiter. Letzteres dient der Ansteuerung des PN532. Die AusweisApp und das uns vorliegende Muster eines Lesers mit PIN-Pad hielten die emulierte Chipkarte für einen validen nPA.

Die tatsächliche Beantragung eines qualifizierten Zertifikats und die Erzeugung qualifizierter elektronischer Signaturen aus der Ferne war aber aus Mangel an entsprechenden Dienstanbietern noch nicht möglich. Aber wir konnten durch Durchführung des PACE-Protokolls [10, 11] und Nachstellen der Verifikation der eSign-PIN feststellen, dass keines der von uns getesteten Chipkartenlesermodelle beim Opfer dies verhindern konnte. Das Muster verhielt sich wie ein Basisleser, obwohl dieser die Möglichkeit zur Regulierung der APDUs hätte.

Da es sich bei unserem Komfortleser lediglich um ein Testmodell handelt, haben wir den Relay-Angriff auf der Seite des Opfers auch mit einem zertifizierten Klasse-3-Leser geprüft. Auch dieser zeigte sich verwundbar. Ungehindert konnte auch hier der Angreifer die in ISO-7816 standardisierten Kommandos für die PIN-Behandlung durchführen. Generell scheinen also Chipkartenleser mit PIN-Pad die Eingabe von einem Geheimnis nicht am lokalen PIN-Pad zu erzwingen. Dies ist überraschend, da nach Auskunft des BSI im Rahmen der Zulassung nach Signaturverordnung geprüft wird, dass der Leser zumindest die Verifikation einer PIN ausschließlich am lokalen PIN-Pad zulässt.

Wir haben gezeigt, dass es einem Angreifer möglich ist, einen Signaturschlüssel auf einem fremden Ausweis zu erzeugen. Die eSign-PIN muss er bei einer noch nicht dafür initialisierten Chipkarte nicht erraten oder ausspähen, sondern er kann diese selbst setzen. Weiterhin ist auf der Seite des Opfers der Datenverkehr zur Chipkarte nicht eingeschränkt, sodass das Signieren und Verifizieren der eSign-PIN problemlos möglich ist. Lediglich das Nachladen eines qualifizierten Zertifikats von einem ZDA kann an dieser Stelle noch nicht vollständig geprüft werden, weil noch keine konkreten Umsetzungen der geänderten Signaturverordnung vorliegen. Geht man davon aus, dass dieses Nachladen gelingt, so ist ein Angreifer in der Lage mit einfachen Mitteln in falschem Namen eine QES zu erzeugen.

C. Gegenmaßnahmen

Weil kein konkretes kryptografisches Protokoll gebrochen wurde, ist es schwierig, sich gegen Relay-Angriffe zu wehren. Gegenmaßnahmen sollten sich daher auf den unbemerkten Zugriff und die Kommunikation mit größerer zeitlicher Verzögerung konzentrieren [8, S. 11].

Der Besitzer des neuen Personalausweises könnte Datenverkehr mit der Chipkarte folgendermaßen regulieren:

- G1 Zerstörung des Chips
- G2 Unterbinden der Kommunikation zum nPA
- G3 eID-Funktion deaktivieren
- G4 eSign-PIN setzen

Zwar kann man die Kommunikation zum nPA zuverlässig unterbinden, indem man ihn nicht in die Nähe eines Lesegeräts legt oder ihn gegen RFID-Signale abschirmt (G2). Wie aber schon angesprochen könnte sich für einen Angreifer vor oder nach einer regulären Nutzung der Chipkarte ein Zeitfenster ergeben, in welchem dieser seinerseits Chipkartenoperationen ausführen kann. Die Maßnahmen G3 und G4 verhindern, dass ein Angreifer selbst die eSign-PIN setzt und so in deren Besitz gelangt. Dies hat aber offensichtlich Nebenwirkungen: Der elektronische Identitätsnachweis ist nicht mehr nutzbar bzw. die eSign-PIN könnte bei Nichtbenutzung vergessen werden oder verloren gehen. Bei G1 ist der Chip gar nicht mehr verwendbar.

Hinzu kommen Maßnahmen, die eine Modifikation von Leser oder Chipkarte verlangen:

- G5 Filtern der Authentisierungsprotokolle durch den Chipkartenleser
- G6 Physikalischer Umschalter an der Chipkarte für Kontexte unterschiedlichen Schutzbedarfs
- G7 Einmal-PIN und Visualisierung des Anwendungskontextes durch Chipkartendisplay

Eine mögliche Lösung, die nicht nur Standard- oder Komfortleser, sondern alle Chipkartenleser mit PIN-Pad betrifft, ist das inhaltliche Filtern von APDUs. Man könnte bei diesen Lesern verlangen, dass sie jegliche Authentisierung des Benutzers gegenüber der Chipkarte ausschließlich am eigenen PIN-Pad zulassen (G5). Dies betrifft sowohl in ISO-7816 standardisierte Kommandos für die PIN-Behandlung als auch die PIN-Eingabe im Rahmen von PACE.

Eine stärke Bindung des Chips an den Kartenkörper durch G6 und G7 könnte eine erhöhte Kontrolle der Chipkartenkommunikation erreichen. Ein Umschalter zur Deaktivierung der Chipkarte, aber auch zur Auswahl zwischen Anwendungskontexten mit niedrigem (z. B. Altersverifikation), mittlerem (Identitätsnachweis) und hohem Schutzbedarf (QES), ist denkbar. Der reguläre Besitzer kann so die Kommunikation der Chipkarte „mit den eigenen Händen“ kontrollieren. Ein Kartendisplay kann nicht nur den aktiven Anwendungskontext signalisieren. Hier könnten auch Ziffern angezeigt werden, die der eID-/eSign-PIN bei einer Authentisierung vorangestellt werden. Zugriff auf die Chipkarte und das Wissen des Geheimnisses genügen dann einem Angreifer nicht mehr. Er müsste die Karte sehen können, um die temporären Ziffern auf dem Display zu erfahren. Selbst wenn ein temporäres Geheimnis von einem Angreifer abgefangen würde, ist dieses nur für eine einzige Transaktion nutzbar und das auch nur, während die Chipkarte sich noch im RFID-Feld befindet. Diese beiden Modifikationen kommen wohl aber erst für die nächste Generation von Ausweisen in Frage.

Um über die größere Verzögerung der Daten bei einem Relay-Angriff eine Unregelmäßigkeit festzustellen, sehen wir folgende Möglichkeiten:

G8 Distance-Bounding zwischen Leser und Chipkarte
G9 Messung der Antwortzeiten im PACE-Kanal

Ausgehend von der Annahme, dass sich elektromagnetische Wellen mit Lichtgeschwindigkeit ausbreiten, kann ein Distance-Bounding-Protokoll[4] anhand sehr kleiner Verzögerungen bereits Unregelmäßigkeiten festgestellt werden (G8). Weder bei einem Komfortleser noch beim neuen Personalausweis ist es aber denkbar, dass die dafür notwendigen Rahmenbedingungen realisierbar sind. Aber man könnte in der Firmware eines Standard- oder Komfortlesers die Antwortzeiten der Chipkarte in einem etablierten PACE-Kanal auswerten (G9). Auf dieser Ebene sind Berechnungen wesentlich langsamer und Zeittoleranzen müssten so groß gewählt werden, dass man Weiterleitungen per Internet nur schwer erkennt.

Unter Beibehaltung bestehender Hardware ist ein vollständiger Schutz gegen das Weiterleiten ohne Einschränkung der Funktionalität nur für Besitzer eines Standard-/Komfortlesers möglich (G5). Insbesondere kann ein Basisleser einen Relay-Angriff *prinzipiell* nicht verhindern, sodass deren Besitzer auf unzureichende Gegenmaßnahmen angewiesen sind (G2, G3). Für sie könnte zumindest ein erweiterter Schutz der eSign-Anwendung umgesetzt werden (G4, G9).

III. Der Komfortleser meines Vertrauens

Mit der stetig zunehmenden Verbreitung des neuen Personalausweises könnte die qualifizierte elektronische Signatur eine breitere Anwendung finden. Damit könnten Angriffe speziell gegen Nutzer von Komfortlesern zunehmen. Zum einen ist es denkbar, dass ein Angreifer die Sicherheit von bestehenden Komfortlesern bricht (ähnlich wie in [7]). Zum anderen ist es denkbar, dass ein Angreifer einen bekannten Komfortleser fälscht.

Ein Firmware-Update ist die wahrscheinlichste Ursache für einen kompromittierten Komfortleser. Die Update-Funktion soll die Authentizität, Integrität und Vollständigkeit der Daten sicherstellen [2]. Es ist zu erwarten, dass im Rahmen der Zertifizierung eines Lesers nach prinzipiellen Lücken in dem konkreten Protokoll und Implementierungsfehlern gesucht wird. Daher konzentrieren wir uns hier auf die Frage, wie ein (gefälschter) Komfortleser erkannt werden kann.

Die AusweisApp weist beim Start darauf hin, ob es sich bei den angeschlossenen Lesegeräten um zertifizierte Lesegeräte handelt oder nicht. Diese Prüfung täuscht eine Authentizität vor, die in dieser Form nicht geprüft werden *kann*. Denn es ist lediglich die *Bezeichnung* des Lesers, welche mit der zertifizierter Lesegeräte verglichen wird. Je nach Betriebssystem stammt die verwendete Bezeichnung vom installierten Gerätetreiber oder gar vom Gerät selbst. In jedem Fall ist die Bezeichnung von einem Angreifer potenziell kontrollierbar.

Ein Angreifer könnte das Aussehen und die Funktionalität eines Komfortlesers nachempfinden, sodass ein Opfer hier im Glauben einen validen Leser zu nutzen, die eID- oder eSign-PIN eingibt. Der gefälschte Komfortleser kann diese Geheimnisse und zugleich den Zugriff auf den neuen Personalausweis des Opfers (siehe oben) weiterleiten. Ein Angreifer könnte damit den elektronischen Identitätsnachweis oder das digitale Signieren im Namen des rechtmäßigen Besitzers durchführen. Das Berechtigungszertifikat ist die einzige Komponente des Komfortlesers, die ein Angreifer nicht nachbauen kann. Der Angreifer hat aufgrund der oben gezeigten Relay-Eigenschaften, die Möglichkeit die Daten an einen gültigen Komfortleser weiterzuleiten. Der gefälschte Komfortleser fungiert hier also als klassischer Man-in-the-Middle.[5]

Ohne sich allein auf die Vertrauenswürdigkeit der Bezugsquellen für Komfortleser verlassen zu müssen, hätte man als Nutzer über das Berechtigungszertifikat des Komfortlesers sehr wohl eine Möglichkeit, diesen zu identifizieren. Das Berechtigungszertifikat kann zur Prüfung mittels einer emulierten Smartcard [11] im Rahmen des PACE-Protokolls abgegriffen werden. Sinnvoller wäre es aber, wenn diese Funktion direkt in die Update-Software für die Leser-Firmware integriert wäre. Mit dem extrahierten Zertifikat könnten so Plausibilitätsprüfungen durchgeführt werden[6].

Eine Prüfung des Berechtigungszertifikats vom Komfortleser ist derzeit einzig von der Chipkarte während der Signaturerstellung vorgesehen. Weil der Chipkarte der Zugang zu Revocation-Listen fehlt, gibt es keinen Mechanismus, ein Berechtigungszertifikat zurückzuziehen. Für Berechtigungs-

[4] Für einen Überblick von Distance-Bounding-Protokollen siehe [6]

[5] Alternativ gäbe es für einen Angreifer noch die Möglichkeit von einem echten Komfortleser das Modul mit dem privaten Schlüssel zu extrahieren und dieses in seiner Fälschung zu verbauen. Hier steht jedoch der Aufwand wahrscheinlich nicht im Verhältnis zum erwarteten Gewinn.

[6] Man hätte das Berechtigungszertifikat des Komfortlesers auch zu einem Teil der elektronischen Signatur machen können. Damit hätte man bei der Signaturprüfung auch feststellen können, mit welchem möglicherweise kompromittierten TA-Schlüssel diese erstellt wurde. Derzeit sieht man aber einer Signatur nicht an, mit welchem Berechtigungszertifikat sie erstellt wurde.

zertifikate eines Dienstanbieters ist dies unproblematisch, weil sie nur wenige Tage gültig sind. Das Berechtigungszertifikat eines Lesers soll aber für mehrere Jahre gültig sein. Ein kompromittiertes Berechtigungszertifikat kann also nicht zurückgezogen werden.

Zusammenfassend kann man festhalten, dass die Prüfung der Authentizität eines Komfortlesers durch den Benutzer nicht vorgesehen ist. Darüber hinaus kann die Fälschung eines Komfortlesers einem Angreifer den Zugriff auf den neuen Personalausweis ermöglichen und die eID-/eSign-PIN kompromittieren. Auf ein kompromittiertes Berechtigungszertifikat oder einen missbrauchten Komfortleser kann nicht adäquat reagiert werden.

IV. Lessons learned

Von den zwei Authentisierungsfaktoren, Besitz und Wissen, ist durch den Relay-Angriff der Besitzfaktor erheblich geschwächt. Dies gilt unabhängig vom Anwendungskontext, also sowohl für die eID-Anwendung als auch für die eSign-Anwendung. Wir haben diesen Angriff gegen einen nPA demonstriert, der beim Opfer auf einem Basisleser oder Lesermuster mit PIN-Pad liegt. Weiterhin haben wir beschrieben wie gefälschte Chipkartenleser mit PIN-Pad den Wissensfaktor kompromittieren können. Ist dabei ein aus einem echten Komfortleser extrahierter TA-Schlüssel involviert, gibt es kaum Chancen den Betrug zu erkennen geschweige denn darauf adäquat zu reagieren.

Das größte Problem erwächst aus einem Umstand, der zumeist als Vorteil gesehen wird. Der nPA vereinigt Anwendungen mit hohem, mittlerem und niedrigem Schutzbedarf in einer Chipkarte. Für den Nutzer ist es aber nicht ersichtlich, in welchem dieser Anwendungskontexte der eigene Ausweis kommuniziert. Wir haben Möglichkeiten vorgestellt, um dies greifbarer zu machen. Besonders interessant erscheint uns dabei das Kartendisplay, da es hierfür auch weitere Nutzungsfälle gibt. Weil dies aber höchstens für zukünftige Ausweisgenerationen denkbar ist, muss man überlegen wie man dieses Problem mit der bestehenden Infrastruktur bewältigen kann.

Der Authentisierungsfaktor „Besitz“ wird für den neuen Personalausweis (aber auch für die meisten anderen Chipkarten) reduziert auf die Möglichkeit zum Zugriff auf die Karte. Da ein Basisleser genau dies bereitstellt und nicht mehr, kann dieser einen Relay-Angriff nicht verhindern. Ein Standard- oder Komfortleser hingegen wäre in der Lage, Kommandos zur PIN-Behandlung zu filtern und so eine entfernte Verbindung mit Authentifizierung zum nPA zu verhindern. Diesen Anspruch könnte man auch an andere Lesegeräte nach dem Signaturgesetz und der Signaturverordnung haben.

Lösungsmöglichkeiten für gefälschte Lesegeräte und kompromittierte TA-Schlüssel lassen sich nur schwer in die bestehende Architektur zum neuen Personalausweis integrieren. Für Besitzer eines Komfortlesers könnte man die Möglichkeit schaffen, zumindest das Berechtigungszertifikat des Lesers zu prüfen und mit einer speziellen Revocation-Liste abzugleichen. Dennoch wird es schwierig sein, kompromittierte TA-Schlüssel überhaupt erst zu erkennen und die entsprechenden Zertifikate zurückzuziehen.

Obwohl der neue Personalausweis eine der sichersten Chipkarten der Welt sein mag und auch an Komfortlesegeräte höhere Anforderungen gestellt werden als an existierende Chipkartenleser für Signaturkarten, gibt es im Zusammenspiel der Komponenten Probleme, die mit keinem konkreten Versagen einer Komponente zusammenhängen müssen.

Danksagung

Besonderer Dank gebührt Dr. Wolf Müller für seine zahlreichen Anregungen und stetige Unterstützung. Desweiteren gilt unser Dank den Mitarbeitern von Bundesdruckerei, Bundesministerium der Sicherheit in der Informationstechnik und Bundesministerium des Innern, mit denen wir in konstruktivem Diskurs standen und die uns Lesegeräte und Test-Ausweise zur Verfügung stellten.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik. *Advanced Security Mechanisms for Machine Readable Travel Documents*. TR-03110. 2.05. 2010.

[2] Bundesamt für Sicherheit in der Informationstechnik. *Anforderungen an Chipkartenleser mit ePA Unterstützung*. TR-03119. 1.1. 2009.

[3] Bundesamt für Sicherheit in der Informationstechnik. *BSI weist Sicherheitsbedenken zum neuen Personalausweis erneut zurück*. 2010.

[4] Bundesamt für Sicherheit in der Informationstechnik. *eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit*. TR-03117. 1.0. 2009.

[5] Bundesministerium des Innern. *IT-Sicherheitskit für Bürgerinnen und Bürger*. 2010.

[6] Jolyon Clulow u. a. „So near and yet so far: Distance-bounding attacks in wireless networks“. In: *In Security and Privacy in Ad-hoc and Sensor Networks*. Springer, 2006, S. 83–97.

[7] Colibri. *Smartcard-Reader von Kobil geknackt*. 2010. URL: http://colibri.net63.net/Smartcard-Reader-Hack.htm.

[8] Gerhard P. Hancke. *A Practical Relay Attack on ISO 14443 Proximity Cards*. Techn. Ber. Cambridge: University of Cambridge, 2005.

[9] Gerald Himmelein. „Fensterputzer: Sieben Antivirenprogramme im Vergleich“. In: *c't* 25/2010 (2010).

[10] Frank Morgner und Dominik Oepen. *OpenPACE*. URL: http://sourceforge.net/projects/openpace/.

[11] Frank Morgner und Dominik Oepen. *Virtual Smart Card Architecture*. URL: http://sourceforge.net/projects/vsmartcard/.

[12] Max Moser und Thorsten Schröder. *SuisseID / Smartcard USB Takeover*. 2010. URL: http://www.vimeo.com/15155073.

[13] N. Kohnert und R. Stumpf. *Plusminus*. WDR. Fernsehmagazin, Sendezeit: 24. August 2010 21:50–22:15. 2010.