Biometrische Ausweise

Technische Funktionsweise, Probleme und Angriffe

Andreas Müller

Chaostreff Zürich vom 11.03.2009

Was ist Biometrie?

Wikipedia:

Die Biometrie beschäftigt sich mit Messungen an Lebewesen und den dazu erforderlichen Mess- und Auswerteverfahren.
[..]
Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika.

Merkmale:

Unterschrift, Fingerabdrücke, Sprache, Gang, DNA, Körpergeruch, Gesicht, ...

Was ist RFID?

RFID

- Radio Frequency Identification: Identifizierung (von Menschen, Tieren oder Produkten) mit Hilfe eines Funkchips.
- Ursprünglich nur Speicherung einer ID, heute ganze Computer mit OS, Crypto-Coprozossor, RAM, etc.
- Meist passiv (Leser versorgt Tag mit Energie), für grössere Reichweiten auch aktiv (Tag mit Batterie)
- Einsatzgebiete: Bezahlsysteme, Tickets, Hunde, Diebstahlsicherung, Müllentsorgung, ...
- Relevante Spezifikationen
  - ISO 10536 (Close Coupling) (ca 1cm)
  - ISO 14443 (Proximity Coupling) (10-15cm)
  - ISO 15693 (Vicinity Coupling) (bis 1.5m)

ISO 14443 (z.B. E-Pässe)

ISO 14443

- Träger: 13.56 MHz
- ASK (Amplitudenumtastung)
- Lastmodulation: Seitenbänder: 13.56MHz$\pm$847kHz
- Anticollision

E-Pässe

- Spezifiziert von der ICAO (International Civil Aviation Organisation; eine Unterorganisation der UN)
- Implementierung variiert von Land zu Land; einzelne Teile der Spezifikation sind optional

Auslesedistanz bei RFID nach ISO 14443 – Aktiv

Konfusion

Aktives Auslesen $\leftrightarrow$ Passives Mithören

Aktives Auslesen

- Leser muss Tag mit Energie versorgen
- Linear grösserer Abstand $\rightarrow$ polynomial grössere Fläche der Antenne oder Energie
  - skaliert nur begrenzt
- Maximale Distanz:
  - Spezifikation: ca 10 cm
  - Hancke[2]: 15 cm
  - Kirschenbaum/Wool [4]: 25cm
  - Kfir/Wool [3]: 40-50cm (Simulationen)
  - Fragwürdige Medienberichte: mehrere Meter $\rightarrow$ oft anderer Frequenzbereich (z.B. UHF) oder passives Mithören gemeint

Auslesedistanz bei RFID nach ISO 14443 – Passiv

Passives Mithören

- Reader → Tag:
  - sehr starkes Feld, da auch Energieversorgung
    [Demo mit RFID Armband und Kurzwellen-Radio]
  - Mithören auch aus grösseren Distanzen kein Problem
- Beide Richtungen:
  - Problematisch ist Tag → Reader
  - Seitenträger rund 60-80dB schwächer als Träger → gute Filter im Empfänger nötig
  - Distanz:
    - BSI [1]: 2m ohne Probleme, ab 3m nur mit mehreren Messungen
    - Hancke [2]: 4m

MRTD und E-Pass

Maschinenlesbar vs elektronisch

- MRTD: Machine Readable Travel Document – ein maschinenlesbares Reisedokument mit MRZ; dieses muss nicht zwingend auch einen RFID Chip enthalten
- MRZ: Maschine Readable Zone – Text in einer speziellen Schrift, der auch von einem Computer mittels Scanner und OCR gelesen werden kann

Identitätskarte

Identitätskarte

- Aktuell nur MRZ
- “Ob und wann es eine Identitätskarte geben wird, in der Daten zur Person elektronisch gespeichert sind, ist noch nicht entschieden.“ (Informationsseite des Bundes)
- Ausweisgesetz ist allgemein gehalten

→ Bundesrat entscheidet das Vorgehen und passt ggf. die Ausweisverordnung an

- .de: Elektronischer Personalausweis auch als Dienstleistung für die Wirtschaft (elektronischer Identitätsnachweis und Signatur)

Pässe

Pässe

- Pass 85
  - veraltet
- Pass 03
  - maschinenlesbar aber kein RFID Chip
  - hoher Sicherheitsgrad
- **Pass 06**
  - maschinenlesbar und RFID Chip mit den gleichen Daten wie der Pass (inkl. Photo)
  - zeitlich befristetes Pilotprojekt
- **Pass 10**
  - maschinenlesbar und RFID Chip mit zusätzlichen Daten (Fingerabdrücke beider Zeigfinger)

Passive Authentication (Pass 06: Ja; Pass 10: Ja)

Verfahren

- Signatur mit Länderzertifikat
- CH: DSA mit SHA1 [9], sonst oft RSA
- Länderzertifikate im Internet verfügbar

Probleme

- Schützt explizit nicht gegen 1:1 Klonen
- Seite mit Schweizer Länderzertifikat (www.bit.admin.ch) war bis vor kurzem selbst durch ein abgelaufenes, selbst-signiertes und ungültiges Zertifikat geschützt :-)
  - inzwischen überhaupt kein gesicherter Zugang (https) mehr

Basic Access Control (Pass 06: Ja; Pass 10: Ja)

BAC: Verfahren

- Art. 14b Ausweisverordnung: “Damit auf den Inhalt des Datenchips zugegriffen werden kann, muss die maschinenlesbare Zone des biometrischen Passes auf ein dazu bestimmtes Lesegerät platziert werden.”
- Key aus Passnummer, Geburtsdatum, Ablaufdatum
- 3DES, CBC-MAC – “as if we were still in the 1980s“ [8]

BAC: Probleme

- Daten sind leicht herauszufinden oder zu erraten
- Max 56 Bit Entropie [7]
- Offline Brute Force [8]
- Brute Force “in ein paar Stunden“ [9]

Active Authentication (Pass 06: Nein; Pass 10: Ja)

Verfahren

- RSA
- Privater Key im Pass kann nicht ausgelesen werden
- Public Key auf dem Pass (mit Zertifikat signiert)
- Challenge wird vom Pass mit Private Key signiert
- Soll Klonen des Passes verhindern

Probleme

- ?
- Sicherheit hängt auch von der Sicherheit der Passive Authentication ab

Extended Access Control (Pass 06: Nein; Pass 10: Ja)

Verfahren

- Leser muss sich gegenüber dem Pass authentifizieren, um besonders geschützte Daten (atm: Fingerabdrücke) auslesen zu dürfen
- Challenge-Response Verfahren mit RSA
- RSA ist offen, verbreitet und i.A. zuverlässig

Extended Access Control (Pass 06: Nein; Pass 10: Ja)

Probleme

- “Damit ein anderes Land die Fingerabdrücke überhaupt lesen kann, muss es über die Berechtigung der Schweiz verfügen. Der Bundesrat erteilt diese nur jenen Ländern, deren Datenschutzniveau dem schweizerischen gleichwertig ist. Er kann die Berechtigung auch anderen Stellen (z.B. Fluggesellschaften) erteilen, die im öffentlichen Interesse die Identität von Personen prüfen müssen.“ (FAQ des Bundes [5])

→ Die wenigsten Länder verfügen über einen gleichwertigen Datenschutz (z.B. USA? WTF?!?)

→ Was wollen Fluggesellschaften mit meinen Fingerabdrücken?

Extended Access Control (Pass 06: Nein; Pass 10: Ja)

Probleme

- Zertifikate haben begrenzte zeitliche Gültigkeit (macht Sinn)

→ Aber: woher weiss der Pass das Datum (ohne Leser komplett deaktiviert)?

→ Leser kann dem Pass das aktuelle Datum mitteilen

→ EAC eines Passes, der 2 Jahre nicht mehr ausgelesen wurde kann mit Zertifikat, dass 1.5 Jahre abgelaufen ist umgangen werden

→ Sind alle Computer der Fluggesellschaften sicher und alle Angestellten unbestechlich?

Random ID (Pass 06: Nein; Pass 10: Ja)

Random ID

- Anticollision Verfahren benötigt ID
- Dadurch ist eine Identifizierung auch ohne auslesen von Daten möglich
- Lösung: Zufällige ID

Probleme:

- Unterschiedliche Implementierungen (z.B. erste 2 Ziffern fix vs alles zufällig)

$\rightarrow$ Fingerprinting

Fingerprinting

Fingerprinting

- Durch Beobachtung von “Umweltfaktoren“ können Rückschlüsse auf des Land, möglicherweise auch auf den spezifischen Pass gezogen werden
- Keine Überwindung der Sicherheitsmechanismen nötig
- z.B. verschiedene Chiphersteller $\rightarrow$ verschiedene ATR, unterschiedliche Reaktionszeit, etc.
- z.B. unterschiedliche Gesichter $\rightarrow$ verschieden starke Komprimierung $\rightarrow$ verschieden lange Auslesedauer
- Allerdings: Tracking geht mit Mobiltelefonen auch einfacher

Weitere Angriffspunkte

Nicht vergessen:

Auch wenn die eigentlichen Sicherheitsverfahren verhalten, sind Angriffe auf anderen Ebenen möglich.

Beispiele

- Implementationsprobleme (z.B. schwache Zufallszahlen)
- Angriffe auf die darunterliegende Infrastruktur (z.B. Trojaner in einem Computer eines Ausstellungszentrums)
- Side-channel attacks
- Relay Attacken
- Denial of Service Attacken (z.B. RFID Zapper)
- Der menschliche Faktor (z.B. Bestechung, um an ein Auslesezertifikat zu kommen)

Was sonst noch zu sagen wäre . . .

Zentrale Datenbank

- Kann zu unbeabsichtigten Datenverlusten tendieren
- Technisch und politisch unnötig
- Um Missbrauch nach Diebstahl zu verhindern würde eine Datenbank gestohlener Pässe genügen

Fingerabdrücke

- Können sehr leicht gefälscht werden (siehe z.B. CCC[6])

→ Falsches Vertrauen auf sichere Identifizierung senkt die Sicherheit

- Problem mit false Negatives führt zu grosser Toleranzschwelle → darum kaum zusätzliche Sicherheit (gleiches Problem bei Gesichtserkennung)
- Film vom CCC (2min)

Zusammenfassung

Zusammenfassung

- Mehr Technologie bringt auch eine breitere Angrifsfläche
- Komplexe Technologie, die unter Zeitdruck eingeführt wird
  - → wer versteht die ganze Technik dahinter? (ich jedenfalls nicht :)
- Kontaktbasierte statt kontaktlose Lösung hätte einige Probleme verhindert
  - wohl politisch nicht möglich
- Fingerabdruck als Sicherheitsmerkmal: Schlechte Idee
- Datenbank bringt keinen Sicherheitsgewinn, schafft aber Begehrlichkeiten
- Langsame Verlagerung der Kontrollaufgabe von Sicherheitspersonal zu Computern?

Fragen?

Weitere Infos:

Unsere sich im Aufbau befindliche Website:

⇒ `http://biometrische-ausweise.ch`

Dank geht an . . .

- alle Zuhörer für die Aufmerksamkeit
- den CCCZH für die Organisation des Talks
- die Leute, die mir ihre Pässe zum Testen anvertraut haben
- Adam Laurie, THC, etc. für Open Source MRTD Tools

Referenzen I

[1] Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems
`http://www.bsi.de/fachthem/rfid/whitepaper.htm`

[2] G.P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In 2006 IEEE Symposium on Security and Privacy (S&P'06), Berkeley, CA, USA, pp. 328-333, IEEE, 2006.

[3] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In Proc. 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), pages 47-58, Athens, Greece, September 2005. IEEE.

Referenzen II

[4] How to Build a Low-Cost, Extended-Range RFID Skimmer
http://www.eng.tau.ac.il/ yash/kw-usenix06/index.html

[5] Informationsseite des Bundes
http://www.schweizerpass.admin.ch/

[6] Der CCC erklärt, wie ein Fingerabdruck kopiert werden kann
http://www.ccc.de/biometrie/fingerabdruck_kopieren

[7] A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Washington, DC, USA, pp. 74-88, IEEE, 2005.

Referenzen III

[8] E-Passport Threats – Vaudenay, Serge
http://infoscience.epfl.ch/record/115087

[9] About Machine-Readable Travel Documents – Vaudenay, Serge ; Vuagnoux, Martin
http://infoscience.epfl.ch/record/110699