Advanced Security Mechanisms for Machine Readable Travel Documents

Password Authenticated Connection Establishment (PACE)

Matthias Ohst

Sommerakademie II – La Colle sur Loup (Nizza)
Arbeitsgruppe 4 (Applied Cryptography and Security Engineering)

1. Oktober 2009

Gliederung

Einführung

Sicherheitsanforderungen

Sicherheitsanforderungen

Wichtige Sicherheitsattacken bei kontaktlosen Chipkarten

- Kommunikation zwischen dem Terminal eines Angreifers und der Karte ohne das Wissen des Karteninhabers
- Abhören einer existierenden Funkübertragung

Sicherheitsanforderungen

Wichtige Sicherheitsattacken bei kontaktlosen Chipkarten

- Kommunikation zwischen dem Terminal eines Angreifers und der Karte ohne das Wissen des Karteninhabers
- Abhören einer existierenden Funkübertragung

Sicherheitsanforderungen

- Authentifizierung des Terminals
- Starke Sitzungsschlüsseleinigung zwischen dem authorisierten Terminal und der kontaktlosen Chipkarte
- *Forward Secrecy* der Sitzungsschlüssel

Passwort-basierte kryptographische Protokolle

Passwort-basierte kryptographische Protokolle

Idee: Gemeinsames Geheimnis – Passwort mit geringer Entropie

- Starke Schlüsseleinigung für Sitzungsschlüssel
- Implizite Authentifizierung der Kommunikationspartner

Passwort-basierte kryptographische Protokolle

Idee: Gemeinsames Geheimnis – Passwort mit geringer Entropie

- Starke Schlüsseleinigung für Sitzungsschlüssel
- Implizite Authentifizierung der Kommunikationspartner

Sicherheitsmerkmale: Resistenz gegen

Offline-Wörterbuchangriff Ein passiver Lauscher nimmt ein oder mehrere Protokoll-Durchläufe auf und kann daraus keine Information bezüglich des Passworts erhalten.

Online-Wörterbuchangriff (1) Ein aktiver Gegner kann nicht das Protokoll missbrauchen, um eine signifikante Anzahl an möglichen Passwörtern zu eliminieren.

Online-Wörterbuchangriff (2) Ein aktiver Angreifer kann nur ein Passwort pro Protokoll-Durchlauf testen.

Das PACE-Protokoll

Allgemeines

Allgemeines

Das PACE-Protokoll

- PACE: *Password Authenticated Connection Establishment*
- Passwort-authentifizierte Diffie-Hellman-Schlüsseleinigung
- Sichere Kommunikation und implizite Passwort-basierte Authentifizierung des MRTD-Chips und des Terminals
- Gemeinsames Geheimnis mit niedriger Entropie (Passwort), z. B. geheime PIN oder CAN (*Card Access Number*)

Allgemeines (Forts.)

Das PACE-Protokoll (Forts.)

- Nachfolger von BAC (*Basic Access Control*) im elektronischen Personalausweis
  - Beseitigung festgestellter Schwächen von BAC
  - Insbesondere: Entropie des abgeleiteten Sitzungsschlüssels kleiner als 56 Bit (erste Version) bzw. 73 Bit (zweite Version)
- Benötigt keine Public-Key-Infrastruktur
- Entwickelt vom Bundesamt für Sicherheit in der Informationstechnik (bemüht um Patent-freien Algorithmus)

Das PACE-Protokoll

Das PACE-Protokoll

Bezeichnungen

- π: Gemeinsames Geheimnis
- h: Hashfunktion (SHA-1 im elektronischen Personalausweis)
- m: Blockbreite des Verschlüsselungsalgorithmus
- ENC, DEC: Symmetrische Verschlüsselung
  (AES mit 128 Bit im elektronischen Personalausweis)
- MAC: Berechnung des *Message Authentication Code*

Das PACE-Protokoll

Bezeichnungen

- π: Gemeinsames Geheimnis
- h: Hashfunktion (SHA-1 im elektronischen Personalausweis)
- m: Blockbreite des Verschlüsselungsalgorithmus
- ENC, DEC: Symmetrische Verschlüsselung
  (AES mit 128 Bit im elektronischen Personalausweis)
- MAC: Berechnung des *Message Authentication Code*

Voraussetzungen

- Zuerst Einigung über elliptische Kurve E und Basispunkt G
- Operation in zyklischer Gruppe $\langle G \rangle := \{t \cdot G : t \in \mathbb{Z}\}$
- $n := |\langle G \rangle|$

Das PACE-Protokoll

Das PACE-Protokoll

Chip (PICC)	Terminal (PCD)

Das PACE-Protokoll

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von s $(0 \leq s < 2^m)$		
$k_\pi = h(\pi \mid 1) \mod n$		$k_\pi = h(\pi \mid 1) \mod n$
$z = \mathrm{ENC}(k_\pi, s)$		
	$\xrightarrow{z}$	
		$s = \mathrm{DEC}(k_\pi, z)$

Das PACE-Protokoll

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von s $(0 \leq s < 2^m)$		
$k_\pi = h(\pi \mid 1) \mod n$		$k_\pi = h(\pi \mid 1) \mod n$
$z = \mathrm{ENC}(k_\pi, s)$		
	$\xrightarrow{z}$	
		$s = \mathrm{DEC}(k_\pi, z)$
Zufällige Wahl von $y_1 \in \mathbb{Z}_n^\times$		Zufällige Wahl von $x_1 \in \mathbb{Z}_n^\times$
$Y_1 = y_1 \cdot G$		$X_1 = x_1 \cdot G$
	$\xleftarrow{X_1}$	
	$\xrightarrow{Y_1}$	
$P = y_1 \cdot X_1$		$P = x_1 \cdot Y_1$

Das PACE-Protokoll

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von s $(0 \leq s < 2^m)$		
$k_\pi = h(\pi \mid 1) \mod n$		$k_\pi = h(\pi \mid 1) \mod n$
$z = \mathrm{ENC}(k_\pi, s)$		
	$\xrightarrow{z}$	
		$s = \mathrm{DEC}(k_\pi, z)$
Zufällige Wahl von $y_1 \in \mathbb{Z}_n^\times$		Zufällige Wahl von $x_1 \in \mathbb{Z}_n^\times$
$Y_1 = y_1 \cdot G$		$X_1 = x_1 \cdot G$
	$\xleftarrow{X_1}$	
	$\xrightarrow{Y_1}$	
$P = y_1 \cdot X_1$		$P = x_1 \cdot Y_1$
$G' = s \cdot G + P$		$G' = s \cdot G + P$

Das PACE-Protokoll (Forts.)

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von $y_2 \in \mathbb{Z}_n^\times$		Zufällige Wahl von $x_2 \in \mathbb{Z}_n^\times$
$Y_2 = y_2 \cdot G'$		$X_2 = x_2 \cdot G'$
	$\xleftarrow{X_2}$	
	$\xrightarrow{Y_2}$	
$K = y_2 \cdot X_2$		$K = x_2 \cdot Y_2$

Das PACE-Protokoll (Forts.)

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von $y_2 \in \mathbb{Z}_n^\times$		Zufällige Wahl von $x_2 \in \mathbb{Z}_n^\times$
$Y_2 = y_2 \cdot G'$		$X_2 = x_2 \cdot G'$
	$\xleftarrow{X_2}$	
	$\xrightarrow{Y_2}$	
$K = y_2 \cdot X_2$		$K = x_2 \cdot Y_2$
$k_{\mathrm{ENC}} = h(K_x \mid 1)$		$k_{\mathrm{ENC}} = h(K_x \mid 1)$
$k_{\mathrm{MAC}} = h(K_x \mid 2)$		$k_{\mathrm{MAC}} = h(K_x \mid 2)$

Das PACE-Protokoll (Forts.)

Chip (PICC)		Terminal (PCD)
Zufällige Wahl von $y_2 \in \mathbb{Z}_n^\times$		Zufällige Wahl von $x_2 \in \mathbb{Z}_n^\times$
$Y_2 = y_2 \cdot G'$		$X_2 = x_2 \cdot G'$
	$\xleftarrow{X_2}$	
	$\xrightarrow{Y_2}$	
$K = y_2 \cdot X_2$		$K = x_2 \cdot Y_2$
$k_{\mathrm{ENC}} = h(K_x \mid 1)$		$k_{\mathrm{ENC}} = h(K_x \mid 1)$
$k_{\mathrm{MAC}} = h(K_x \mid 2)$		$k_{\mathrm{MAC}} = h(K_x \mid 2)$
$t_{\mathrm{PICC}} = \mathrm{MAC}(k_{\mathrm{MAC}}, X_{2,x})$		$t_{\mathrm{PCD}} = \mathrm{MAC}(k_{\mathrm{MAC}}, Y_{2,x})$
	$\xleftarrow{t_{\mathrm{PCD}}}$	
	$\xrightarrow{t_{\mathrm{PICC}}}$	
$t'_{PCD} = \mathrm{MAC}(k_{\mathrm{MAC}}, Y_{2,x})$		$t'_{\mathrm{PICC}} = \mathrm{MAC}(k_{\mathrm{MAC}}, X_{2,x})$
Abbruch, falls $t'_{\mathrm{PCD}} \neq t_{\mathrm{PCD}}$		Abbruch, falls $t'_{\mathrm{PICC}} \neq t_{\mathrm{PICC}}$

Aufwand

Aufwand

Aufwand von PACE

- Hashaufrufe: jeweils 2 + 1 (Chip/Terminal)
- Verschlüsselungen: 1 (Chip)
- Entschlüsselungen: 1 (Terminal)
- Skalare Multiplikationen in E: jeweils 5 (Chip/Terminal)

Sicherheit von PACE

Sicherheit von PACE

Grundsätzliches Problem

Die Menge aller möglichen Passwörter π_i ist prinzipiell bekannt (geringe Entropie).

Sicherheit von PACE

Grundsätzliches Problem

Die Menge aller möglichen Passwörter π_i ist prinzipiell bekannt (geringe Entropie).

Folgerung

Die Werte $k_{\pi_i} = h(\pi_i \mid 1)$, $s_i = \mathrm{DEC}(k_{\pi_i}, z)$ können berechnet werden.

Aber: Kenntnis von k_π und s ist keine Hilfe, um π zu berechnen.

Sicherheit von PACE

Grundsätzliches Problem

Die Menge aller möglichen Passwörter π_i ist prinzipiell bekannt (geringe Entropie).

Folgerung

Die Werte $k_{\pi_i} = h(\pi_i \mid 1)$, $s_i = \mathrm{DEC}(k_{\pi_i}, z)$ können berechnet werden.

Aber: Kenntnis von k_π und s ist keine Hilfe, um π zu berechnen.

Sicherheit abhängig von

- Diffie-Hellman-Annahme
- Geheimhaltung des Passworts π

Notwendigkeit der zweiten Diffie-Hellman-Schlüsseleinigung

Notwendigkeit der zweiten Diffie-Hellman-Schlüsseleinigung

Annahmen

- Keine zweite Diffie-Hellman-Schlüsseleinigung
  (d. h. G' wird statt K benutzt)
- Karten-Authentifizierung vor Terminal-Authentifizierung

Notwendigkeit der zweiten Diffie-Hellman-Schlüsseleinigung

Annahmen

- Keine zweite Diffie-Hellman-Schlüsseleinigung (d. h. G' wird statt K benutzt)
- Karten-Authentifizierung vor Terminal-Authentifizierung

Angriff

- Aktiver Angreifer: Prokotoll-Durchlauf bis Kenntnis von P
- Aus Menge aller π_i lassen sich s_i, G'_i, k_{MAC_i} und somit t_{PICC_i} berechnen und mit t_{PICC} vergleichen (Brute-Force-Attacke)
- Daraus Kenntnis von k_{MAC}, G', s und letztlich π

Sicherheitsmerkmale von PACE

Sicherheitsmerkmale von PACE

Authentifierung des Terminals

- Geheimhaltung von π
- Kenntnis von π

Sicherheitsmerkmale von PACE

Authentifierung des Terminals

- Geheimhaltung von π
- Kenntnis von π

Starke Schlüsseleinigung für Sitzungsschlüssel

- Diffie-Hellman-Annahme

Sicherheitsmerkmale von PACE

Authentifierung des Terminals

- Geheimhaltung von π
- Kenntnis von π

Starke Schlüsseleinigung für Sitzungsschlüssel

- Diffie-Hellman-Annahme

Starke *Forward Secrecy*

- P, K werden aus zufälligen Zahlen berechnet
- P, K werden nach jedem PACE-Protokoll-Durchlauf gelöscht

Sicherheitsmerkmale von PACE (Forts.)

Offline-Wörterbuchangriffe

- Menge der Passwörter π_i bekannt
- Damit Berechnung von $k_{\pi_i} = h(\pi_i \mid 1)$, $s_i = \mathrm{DEC}(k_{\pi_i}, z)$ möglich
- Daraus keine Berechnung von π möglich

Sicherheitsmerkmale von PACE (Forts.)

Offline-Wörterbuchangriffe

- Menge der Passwörter π_i bekannt
- Damit Berechnung von $k_{\pi_i} = h(\pi_i \mid 1)$, $s_i = \mathrm{DEC}(k_{\pi_i}, z)$ möglich
- Daraus keine Berechnung von π möglich

Online-Wörterbuchangriffe (1)

- Unmöglich
- Zufällige Wahl von s, $0 \leq s < 2^m$

Sicherheitsmerkmale von PACE (Forts.)

Offline-Wörterbuchangriffe

- Menge der Passwörter π_i bekannt
- Damit Berechnung von $k_{\pi_i} = h(\pi_i \mid 1)$, $s_i = \mathrm{DEC}(k_{\pi_i}, z)$ möglich
- Daraus keine Berechnung von π möglich

Online-Wörterbuchangriffe (1)

- Unmöglich
- Zufällige Wahl von s, $0 \leq s < 2^m$

Online-Wörterbuchangriff (2)

- Möglich
- Technische Gegenmaßnahmen

Sicherheit formal verifiziert

Sicherheit formal verifiziert

Sicherheit formal verifiziert

- Pressemitteilung vom BSI und CASED am 20.08.2009
- Details auf der Information Security Conference 2009 in Pisa

Zusammenfassung

Zusammenfassung

Zusammenfassung

PACE-Protokoll

- Passwort-basiertes Authentifizierungs-Schlüsseleinigungsprotokoll
  - Gegenseitige Authentifizierung
  - Starke Schlüsseleinigung für Sitzungsschlüssel
- Gegen unauthorisierte Kommunikation mit der Karte
- Gegen Lauschen der Datenübertragung zwischen Terminal und Karte
- Geeignet für ellliptische Kurven
- Ersetzt BAC-Protokoll im elektronischen Personalausweis
- Sicherheit formal verifiziert

Literatur

Bundesamt für Sicherheit in der Informationstechnik BSI:
Advanced Security Mechanisms for Machine Readable Travel Documents. Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI).
Technical Guideline BSI-TR 03110, Version 2.01, Mai 2009

Ullmann, Markus; Kügler, Dennis; Neumann, Heike; Stappert, Sebastian; Vögeler, Matthias:
Password Authenticated Key Agreement for Contactless Smart Cards.
Workshop on RFID Security 2008, Budapest, Juli 2008

Nithyanand, Rishab:
The Evolution of Cryptographic Protocols in Electronic Passports.
Cryptology ePrint Archive, Report 2009/200, Mai 2009