Privacy and Security Analysis of PACE GM Protocol

Mirosław Kutyłowski, Przemysław Kubiak

Wrocław University of Science and Technology, Wrocław, Poland

2019, Rotorua

Contactless identity documents - eID

Architecture

1. chip embedded into an eID
   ⇒ secure data storage & executing cryptographic protocols
2. communication & power supply over embedded antenna
   ⇒ more durable than with contacts, but no physical control over activation
3. no other interface
   ⇒ no own keyboard or biometric reader

Features

- ID data cryptographically authenticated by the ID issuer,
- no physical protection against eavesdropping/hijacking communication
- possible attempts to activate the chip without the owner's consent

General problems with identity documents

Frauds

a weakly protected identity document ⇒
fake identity data can be accepted and trusted

Impersonation

an attacker authenticates himself as a victim person

Data theft

authenticated data communicated by an eID can be sold to third parties, ...

Biometry on eID

Biometry as necessity

only biometric check enables to reduce the problems of

- using different identities by the same person (and original eID documents)
- using eID of a similar person (if a (low quality) face image printed on the eID)

Reusing biometric data

- cryptographically authenticated biometric data can be transmitted to third parties and misused there
- solutions based e.g. on issuer's signature over the biometric data create additional threats – signed data have a "quality seal"

Password authentication

Security mechanisms

Password verification

eID’s chip transmits payload data only when the reader proves to know the password

Confidentiality

an external observer monitoring the data exchanged cannot derive any data

- even when knowing the password
- in particular: it must be hidden whether the password has been accepted

PACE protocol

strong privacy protection

Password Authenticated Connection Establishment

1. a protocol developed by German Federal Authority for Information Security (BSI)
2. primary goal: avoiding the patent of David Jablon on SPEKE (expired 2017)
3. later enhanced in France, so PACE v2 consists of two protocols
    - PACE GM - PACE General Mapping (German)
    - PACE IM - PACE Integrated Mapping (French, mapping by Thomas Icart)
4. password guessing hard:
   — a reader interacting with a chip may try only **one password** per session
5. partially patent free

Deployment of PACE

German personal ID: PACE has been developed for *Personalausweis* - German ID card – by the Federal Offices for Information Security

biometric passport: an advanced option to avoid passport scamming adopted by ICAO
sooner or later will replace BAC due to security reasons

EU ID cards: recent EU decision to introduce EU-wide uniform ID cards with biometry following the ICAO standard

PACE-GM (PACE General Mapping)

double DH key exchange, only random values until secure channel

e-ID chip		reader
π		π typed in by the owner
$K_\pi := H(0\Vert\pi)$		$K_\pi := H(0\Vert\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := \mathrm{ENC}(K_\pi, s)$		
	$\xrightarrow{\mathcal{G},z}$	abort if $\mathcal{G}$ incorrect
		$s := \mathrm{DEC}(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
check $Y'_B \neq Y_B$	$\xrightarrow{Y'_A}$	check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$

PAKE

Password Authenticated Key Exchange – simplified

An adversary is given a transcript of password authentication and an alleged resulting session key K.

Then the adversary cannot say whether

- K is a fake one, or
- K is the genuine one.

That is, any feasible cryptanalysis can be only negligibly better than random guessing.

Published proofs

Security Analysis of the PACE Key-Agreement Protocol,
Jens Bender, Marc Fischlin, Dennis Kügler

- ISC 2009, LNCS, Springer-Verlag, 2009
- extended to: IACR ePRINT report: 2009-624

What has been presented:

- PAKE proof
- claimed to concern an active adversary but a key transition in the security games is completely incomprehensible
  $\Rightarrow$ so it must be treated as concerning a passive adversary only
- reduction to two new cryptographic assumptions related to the DH Problem

More properties needed

password derivation

find out the password used by an eID based on a transcript of communication
.. or try to interact with the eID

privacy - tracing

forget deriving the password but for instance find out if two communications correspond to the same password

privacy - deniability

the protocol should not provide any transferable proof that it has been executed by the eID

Situation

- the designers of PACE have been aware of multiple requirements and the protocol has been designed deliberately to meet these requirements,
- however so far no proof has been publicly presented and checked

should it be the situation for a protocol of such a paramount importance?

“dowieriaj no prowieriaj” – “trust but check”

Approach

Standard approach

- define a security model for each requirement
- create a proof for each model

Problems

- a large variety of (somewhat incompatible) models
- for privacy – hard to formulate a model
- likely to redo the same work

Our approach

- derive specific properties of the protocol
- then address specific requirements

Question 1

Is it possible to run the protocol with an active adversary as man-in-the-middle, so that finally

the reader, the eID and the adversary

share the same session key K?

Question 1

Is it possible to run the protocol with an active adversary as man-in-the-middle, so that finally
the reader, the eID and the adversary
share the same session key K?

Note 1: we do not assume that the point of view of the reader and the eID are the same
maybe the attacker can manipulate the communication in a smart way so he learns K but the reader and the eID see different messages
Note 2: we are not addressing the classical MitM attack, where the adversary may share different keys with the reader and the eID

Question 1

Is it possible to run the protocol with an active adversary as man-in-the-middle, so that finally
the reader, the eID and the adversary
share the same session key K?

Security property shown

such a situation cannot occur whp

Consequences

Note 3: *It might be hard to prove/or even false if we change PACE just a little bit.*

Corollary

So if a shared key K is established, then at most one of the following cases may occur:
the key K is shared by

1. the reader & the eID
2. the reader & the adversary
3. the eID & the adversary

Note 4: of course, the situations 2 and 3 may occur if the adversary knows the password

Question 2

session hijacking

Is it possible to run the protocol with an active adversary so that **the correct password is used by an honest reader**, but finally **the adversary shares the session key with (eID or the reader)?**

Question 2

session hijacking

Is it possible to run the protocol with an active adversary so that **the correct password is used by an honest reader**, but finally **the adversary shares the session key with (eID or the reader)?**

Note 1: So far we only know that the adversary can share the key with one party only.
Note 2: This situation would mean a successful attack:

- impersonating a legitimate reader, or
- impersonating the eID (and manipulating the payload data)

Question 2

session hijacking

Is it possible to run the protocol with an active adversary so that **the correct password is used by an honest reader**, but finally
the adversary shares the session key with (eID or the reader)?

Security property shown

such a situation cannot occur whp

Let us take a look at the protocol again

intuitions

e-ID chip		reader
π		π typed in by the owner
$K_\pi := H(0\|\|\pi)$ choose $s \leftarrow \mathbb{Z}_q$ $z := \mathrm{ENC}(K_\pi, s)$		$K_\pi := H(0\|\|\pi)$
	$\xrightarrow{\mathcal{G},z}$	abort if $\mathcal{G}$ incorrect
		$s := \mathrm{DEC}(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$ $Y_A := g^{y_A}$		choose $y_B \leftarrow \mathbb{Z}_q^*$ $Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$	$\xrightarrow{Y_A}$	abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$ choose $y'_A \leftarrow \mathbb{Z}_q^*$ $Y'_A := \hat{g}^{y'_A}$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$ choose $y'_B \leftarrow \mathbb{Z}_q^*$ $Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
check $Y'_B \neq Y_B$	$\xrightarrow{Y'_A}$	check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$

Consequences

Corollary

If the adversary does not know the password, then he cannot learn the session key.

However...

it does not mean that the password is secure and privacy is preserved.

Question 3

Fragility

Can an active adversary manipulate the communication without creating a protocol crash?

Question 3

Fragility

Can an active adversary manipulate the communication without creating a protocol crash?

Note 1: Creating crash or not might turn out to be an oracle enabling to learn something about the password used.

Question 3

Fragility

Can an active adversary manipulate the communication without creating a protocol crash?

Security property shown

there is only one strategy that does not lead to a crash:
before delivering X_A and X_B raise them to the same power k, where k can be chosen arbitrarily

Consequences

Corollary

No manipulation provides any information about the password:
the protocol either crashes or not independently of the password used.

Corollary

So in fact the adversary is limited to a passive attacks.

In the last case showing privacy features follows standard arguments.

Conclusions

- PACE is secure concerning confidentiality and privacy[1]
- the argument can be extended to the protocols like PACE CAM from the ICAO standard (PAKE+ chip authentication)

[1] except for implementations based on a poor/malicious PRNG, but this problem can be fixed too, see our forthcoming journal paper in Fundamenta Informaticae