Stand-by Attacks on E-ID Password Authentication

Lucjan Hanzlik, Przemysław Kubiak, Mirosław Kutyłowski

Wrocław University of Technology, Poland

INSCRYPT 2014, Beijing

Quality Control of Cryptographic Products

Security of cryptographic products
academia

Common approach – academic point of view

Usual steps:

1. good algorithm
2. formal security proof in an abstract model
3. careful implementation
4. checking that the implemented product executed the secure algorithm

Security of cryptographic products
academia

Common approach – academic point of view

1. **good algorithm**
2. **formal security proof in an abstract model**
3. careful implementation
4. checking that the implemented product executed the secure algorithm

not much interest for points 3 and 4

Security of cryptographic products
industry

Common Criteria - industrial point of view - ISO 15408

1. *Protection Profile* concerning security targets
2. evaluation of conformance with PP

Security of cryptographic products
industry

Common Criteria - industrial point of view - ISO 15408

1. *Protection Profile* concerning security targets
2. evaluation of conformance with PP

Mechanism:

- common platform enabling comparison of products
- risk analysis $\Rightarrow$ security targets $\Leftarrow$ requirements (PP)
- for a product: check only conformance with PP
- based on the trust to a certification body

Security of cryptographic products
industry

Common Criteria - industrial point of view - ISO 15408

1. *Protection Profile* concerning security targets
2. evaluation of conformance with PP

Mechanism:

- common platform enabling comparison of products
- risk analysis $\Rightarrow$ security targets $\Leftarrow$ requirements (PP)
- for a product: check only conformance with PP
- based on the trust to a certification body

Advantages:

- reusing the risk analysis, formulating the requirements and evaluation process
- process transparency

Situation

Academic designs

- nice papers
- unrealistic models
- unrealistic assumptions

Main objective: publish

Situation

Academic designs

- nice papers
- unrealistic models
- unrealistic assumptions

Main objective: publish

Industrial designs

- product propaganda
- black box
- strong assumptions
- trust based

Main objective: sell products

Objective: make the customer believe that he is secure, then steal his data ...

Situation

Academic designs

- nice papers
- unrealistic models
- unrealistic assumptions

Main objective: publish

Industrial designs

- product propaganda
- black box
- strong assumptions
- trust based

Main objective: sell products

Objective: make the customer believe that he is secure, then steal his data ...

Hidden Penetration Attacks

Attack detection

Assumptions

attack mechanism an attacker breaks into the system and changes the implementation (installs a bug) the system no longer complies with the security specification

defense typical approach:

- protect against breaking in
- check system integrity

Why this approach fails

Sources of threats

- there is no fully secure storage for secret keys
- there is no fully secure operating system
- no party should be unconditionally trusted
- ...

Reality

- e.g. cryptographic smart cards: a continuous game between sophisticated attack techniques and sophisticated protection methods
- software: bugs, bug, bugs ...
- e.g.: alleged eavesdropping Greek, German, ... top politicians by US agencies

Hidden penetration attack model

Attack scenario

1. gain a temporary access to the systems
2. learn some confidential data
3. leave the system, do not change anything
4. use the knowledge and the publicly available knowledge

Hidden penetration attack model
ineffectiveness of security screening

Sources of problems

1. a very short access to the system might be enough for the adversary
2. it is impossible to monitor/audit the system all the time
3. each audit is itself a threat – doors must be in some sense open for an external access
4. the attack may occur during manufacturing/delivery/configuration of the product

Hidden penetration attack model

Fundamental source of problems

The cryptographers tend to

- believe that there are secure devices implementing secret keys
- hidden penetration attacks should be deferred by non-cryptographic means

We believe that this is wrong and that cryptographic protection means may help very much.

Privacy and Tracing Threats

Privacy concepts

Necessity of privacy protection

- gaining private data (even seemingly worthless) may be very useful for mounting further attacks
- data can be very useful for criminals, terrorists, ...
- it is not only protecting (encrypted) data, **the fact of interaction with a certain system is a sensitive information**

Contactless electronic ID documents

Contactless communication

- necessary to make an e-ID card durable
- convenient
- the communication can be eavesdropped
  (the range might be limited but . . .)

Examples

- biometric passport
- personal ID cards in some countries

Privacy requirements for eID wireless communication

Requirement 1

The eavesdropper should not learn the identity of an eID by eavesdropping the wireless communication.

Privacy requirements for eID wireless communication

Requirement 1

The eavesdropper should not learn the identity of an eID by eavesdropping the wireless communication.

Requirement 2

The attacker should not be able to activate an eID so that it betrays its identity.

Privacy requirements for eID wireless communication

Requirement 1

The eavesdropper should not learn the identity of an eID by eavesdropping the wireless communication.

Requirement 2

The attacker should not be able to activate an eID so that it betrays its identity.

Requirement 3

A legitimate terminal should not be able to collect undeniable proofs of presence of an eID unless explicitly admitted by a system specification.

Design Rules

Identity via a secure channel

The identity of the eID is not shown until a secure channel is created.

Design Rules

Identity via a secure channel

The identity of the eID is not shown until a secure channel is created.

Password/CAN protection

The communication cannot be established by the eID until it becomes sure that the reader (terminal) knows the password or a card access number (CAN)

Design Rules

Identity via a secure channel

The identity of the eID is not shown until a secure channel is created.

Password/CAN protection

The communication cannot be established by the eID until it becomes sure that the reader (terminal) knows the password or a card access number (CAN)

Simultability

ZKP concept: A reader can create fake transcripts of interaction with an eID.
Therefore a transcript of a real interaction has no proof value for a third party.

Password Authentication – PACE

PACE
main points

Password Authenticated Connection Establishment

1. establishes an authenticated encrypted channel if correct password given
2. main purpose was to secure wireless connections
3. password guessing as hard as possible:
   — a reader interacting with a chip may try one password per session
4. ICAO de facto standard
5. implemented in German personal ID cards
6. in the future obligatory for biometric passports in the EU
7. developed by German security authorities, later French modifications

PACE
parameters

Card	Reader
holds: π - password x_A - private key $X_A = g^{x_A}$ - public key $cert_A$ - certificate for X_A $\mathcal{G} = (a, b, p, q, g, k)$ - parameters	holds: π - password, input from owner

PACE
password dependent data

Card		Reader
π x_A, $X_A = g^{x_A}$		π
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$		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 $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := Y'^{y_A}_B$		$K := Y'^{y_B}_A$
$K_{\ldots} := H(\ldots\|\|K)$		$K_{\ldots} := H(\ldots\|\|K)$

PACE

first DH key exchange - base establishment

Card		Reader
π x_A, $X_A = g^{x_A}$		π
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
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 $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := Y'^{y'_A}_B$		$K := Y'^{y'_B}_A$
$K_{...} := H(...\|\|K)$		$K_{...} := H(...\|\|K)$

PACE

first DH key exchange - base establishment

Card		Reader
...		...
choose $s \leftarrow \mathbb{Z}_q$ $z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect $s := DEC(K_\pi, z)$
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 $Y_A \notin \langle g \rangle \backslash \{1\}$
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
...		...

- definition of $\hat{g}$ is so called **Generic Mapping** - PACE v1 Generic Mapping (PACE-GM). according to *ISO/IEC JTC1 SC17 WG3/TF5 for the International Civil Aviation Organization: Supple- mental access control for machine readable travel documents (2011)*
- Integrated Mapping (PACE-IM) from the same standard – specific operations for ECC, partially patented.

PACE

the second Diffie-Hellman for key establishment

Card		Reader
π x_A, $X_A = g^{x_A}$		π
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	
		abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
	$\xrightarrow{Y_A}$	
abort if $Y_B \notin \langle g \rangle \backslash \{1\}$		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 $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{...} := H(...\|\|K)$		$K_{...} := H(...\|\|K)$

PACE

final phase - proof of possession and deriving keys

Card		Reader
...		...
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{ENC} := H(1\|\|K)$		$K_{ENC} := H(1\|\|K)$
$K_{MAC} := H(2\|\|K)$		$K_{MAC} := H(2\|\|K)$
$K'_{MAC} := H(3\|\|K)$		$K'_{MAC} := H(3\|\|K)$
$T_A :=$		$T_B :=$
$MAC(K'_{MAC}, (Y'_B, \mathcal{G}))$		$MAC(K'_{MAC}, (Y'_A, \mathcal{G}))$
	$\xleftarrow{T_B}$	
abort if T_B invalid		
	$\xrightarrow{T_A}$	
		abort if T_A invalid

- chip interrupt if it discovers that the tag of the reader is wrong,
- until this moment **all data sent to the reader by the chip have uniform probability distribution for every password** ...
- ... and for **every choice of the reader**

PACE

final phase - proof of possession and deriving keys

Card		Reader
$\ldots$		$\ldots$
$K := {Y'_B}^{y'_A}$		$K := {Y'_A}^{y'_B}$
$K_{ENC} := H(1\|\|K)$		$K_{ENC} := H(1\|\|K)$
$K_{MAC} := H(2\|\|K)$		$K_{MAC} := H(2\|\|K)$
$K'_{MAC} := H(3\|\|K)$		$K'_{MAC} := H(3\|\|K)$
$T_A :=$ $MAC(K'_{MAC}, (Y'_B, \mathcal{G}))$		$T_B :=$ $MAC(K'_{MAC}, (Y'_A, \mathcal{G}))$
	$\xleftarrow{T_B}$	
abort if T_B invalid		
	$\xrightarrow{T_A}$	
		abort if T_A invalid

- reader interrupt if it discovers that the tag of the chip is wrong (maybe the communication was hijacked by another device?)
- until this moment **the reader sent one message that depends on password**
  security is a more subtle issue

Randomness and Hidden Penetration Attacks

Physical random sources

Advantages

- real random numbers are unpredictable
- they correspond to assumptions of cryptographers

Disadvantages

- aging
- unpredictable errors
- impossibility to test
  (unless heavy deviations from uniform distribution)
- hard to manufacture

Pseudorandom number generators

Advantages

- simple and cheap
- provable/well studied properties
- no aging effects

Disadvantages

- security depends on confidentiality of the seed and/or internal state

Hidden Penetration Attacks
Breaking Privacy of PACE GM

this is just an example: other protocols of this kind fail too, including PACE IM

General attack scenario

General scenario

reader architecture: the readers are white boxes, except for PRNG which are black boxes

attack target: hidden penetration attack on all readers produced, getting the seeds installed in PRNG

shadow readers: the attacker installs a passive device recording communication between the readers and the identification documents

- the attacker has no control over deployment of readers
- shadow readers can be installed
- data analysis is offline

Attack targets

Target

learn the passwords and identity of documents

Offline analysis - Step 1

Finding ID of the reader

- first the reader sends $Y_B = g^{y_B}$, where y_B comes from the PRNG installed in the reader,
  Y_B does not depend on the eID!
- search over all seeds and a realistic number of steps

Card		Reader
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
choose $y_A \leftarrow \mathbb{Z}_q^*$		choose $y_B \leftarrow \mathbb{Z}_q^*$
$Y_A := g^{y_A}$		$Y_B := g^{y_B}$
	$\xleftarrow{Y_B}$	
...	...	...

Step 2: finding h

As $h = Y_A^{y_B}$, h can be derived with y_B from Step 1 and from Y_A known from the communication transcript.

Card		Reader
$K_\pi := H(0\|\|\pi)$		$K_\pi := H(0\|\|\pi)$
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
	$\xrightarrow{\mathcal{G}, z}$	
		abort if $\mathcal{G}$ incorrect
		$s := DEC(K_\pi, z)$
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 $Y_B \notin \langle g \rangle \backslash \{1\}$		abort if $Y_A \notin \langle g \rangle \backslash \{1\}$
	$\xrightarrow{Y_A}$	
...	...	...
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		
		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
...	...	...

Step 3: Reconstruction of K

- compute y'_B as the next output of PRNG
- $K := Y'^{y'_B}_A$
- follow the steps of the reader to get the session keys

Card		Reader
$\dots$	$\dots$	$\dots$
$h := Y_B^{y_A}, \hat{g} := h \cdot g^s$		$h := Y_A^{y_B}, \hat{g} := h \cdot g^s$
$\dots$	$\dots$	$\dots$
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 $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
	$\xrightarrow{Y'_A}$	
$K := Y'^{y'_A}_B$		
		$K := Y'^{y'_B}_A$
$K_{\dots} := H(\dots \| K)$		$K_{\dots} := H(\dots \| K)$

Step 4: Reconstruction of $\hat{g}$ and g^s

- compute $\hat{g}$ as $(Y'_B)^{(y'_B)^{-1} \bmod q}$
- $S := \hat{g}/h$ (note that $S = g^s$)

Card		Reader
...	...	...
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
...	...	...
choose $y'_A \leftarrow \mathbb{Z}_q^*$		choose $y'_B \leftarrow \mathbb{Z}_q^*$
$Y'_A := \hat{g}^{y'_A}$		$Y'_B := \hat{g}^{y'_B}$
	$\xleftarrow{Y'_B}$	
	$\xrightarrow{Y'_A}$	
check $Y'_B \neq Y_B$		check $Y'_A \neq Y_A$
...	...	...

Step 5: Deriving the password

- For each password π, compute $s_\pi := \mathrm{DEC}(\mathrm{Hash}(0||\pi), z)$
- if $S = g^{s_\pi}$, then the real password is π

Card		Reader
		$K_\pi := H(0\|\|\pi)$
$K_\pi := H(0\|\|\pi)$		
choose $s \leftarrow \mathbb{Z}_q$		
$z := ENC(K_\pi, s)$		
		abort if $\mathcal{G}$ incorrect
	$\xrightarrow{\mathcal{G}, z}$	
...	...	...
$h := Y_B^{y_A}$, $\hat{g} := h \cdot g^s$		$h := Y_A^{y_B}$, $\hat{g} := h \cdot g^s$
...	...	...

Complexity

- Step 1 is a brute force search, but only for a limited number of possibilities due to the limited number of readers.
- Step 5 is a brute force search, but only for a limited number of possibilities due to the low entropy of the passwords.
- The rest is easy.

Defense Methods

Defense techniques

Exponentiation unit with DH

- instead of $Y_B := g^{y_B}$ take

$$Y_B := (g^{y_B})^x$$

where x is a secret key in a separate black box

- compute

$$(Y_A)^{y_B \cdot x}$$

as

$$(Y_A^{y_B})^x$$

exponentiation to the power x done by a separate *exponentiation unit*

the same trick with the second DH key agreement

Defense mechanism

Exponentiation unit -randomization

- x can be set and/or randomized by the owner of the device at any time
- randomization: choose r at random and put $x := x \cdot r$
- the modified public key of the exponentiation unit: $X := X^r$

Why attacks fails now?

DDH result cannot be reconstructed anymore.

Defense mechanism
testing

Test

in the test modus one can check that the exponentiation unit is performing honestly:

1. choose t at random, $u := g^t$,
2. give u to the exponentiation unit,
3. receive v from the exponentiation unit
4. check that $v = X^t$, where X is the (current) public key of the exponentiation unit

note that the PRNG cannot be checked in a similar way

Security

- extra exponentiation does not change security of the original scheme
- fluctuations of the exponent force the adversary to penetrate the reader continuously

Conclusion:

a dishonest manufacturer not that dangerous anymore

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.edu.pl
2. http://kutylowski.im.pwr.edu.pl