Restricted Identification Scheme and Diffie-Hellman Linking Problem

Michał Koza, Łukasz Krzywiecki, Przemysław Kubiak, Mirosław Kutyłowski

Wrocław University of Technology

INTRUST 2011, Beijing

Identification

classical approach

Standard procedure

1. user identity proved
2. rights of the user determined
3. appropriate access granted

Prove your identity, then I grant you access to resources.

Identification
classical approach - problems

Problems

- in most cases full disclosure of identity is unnecessary
- **unnecessary data is a security threat**, especially if confirmed by strong cryptographic mechanisms
- $\Rightarrow$ consequences **for personal data protection**:
  - high costs of protecting personal data
  - high legal risk of protection violation

Restricted Identification
idea

The main idea of restricted identification

- concentrate on rights of a user
- hide identity of the user ...
- but bind the user with a physical person

Related techniques
pseudonyms

Pseudonyms?

are not enough:

Sybil attacks: one person may acquire many pseudonyms for interaction with the same system

identity transfer: pseudonym (and authentication data) may be sold to a third person

Related techniques

anonymous credentials

Anonymous credentials?

are not enough when **actions of the same person are to be linked within** some area of activity:

Sybil attacks: one person may get new credentials and restart with a new identity – no consequence of a bad reputation

Austrian Concept of Sectors

Idea of sectors

1. activity areas divided into independent sectors
2. strict data separation between sectors, interaction only if explicitly defined
3. for each sector different authentication

Austrian Concept of Sectors

Idea of sectors

1. activity areas divided into independent sectors
2. strict data separation between sectors, interaction only if explicitly defined
3. for each sector different authentication

Sector examples

health care system: a patient should be always recognized as the same person,

health insurance: there must be no possibility for insurance companies to link a person with medical records
stolen database with medical records must be of no use for an insurance company

Properties of restricted identification

- one person – one identity per sector
- activities of the same person in different sectors are unlinkable
- preferably one secret key per person to be used for all sectors
- *implementation on a personal identity card?*

German Restricted Identification

Preliminaries

Static Diffie-Hellman authentication

all computations in a group with hard DL problem
e-ID card holds a secret x and a certificate for public key $y = g^x$

e-ID card		card reader
		generate a at random compute $z = g^a$
	$\xleftarrow{z}$	
compute $K := F(z^x)$		compute $K := F(y^a)$
communicate via a channel encrypted with K		communicate via a channel encrypted with K

Static DH authentication

Zero-knowledge properties

1. in order to compute the session key K, the e-ID card has to know the secret key x
2. it is quite easy to create the transcript of a session – it suffices to write the responses of the e-ID card by himself!

Procedure

login in a sector:

1. e-ID card computes a unique password for each sector
2. the terminal of service provider:
   a) checks that it is talking with an e-ID card
   b) receives a password
   c) checks the password against the blacklist of this sector

Phase 1

1. activating the card:
   PACE (password ...) - a DH based protocol in which the reader shows that it knows the owner's password
   - immune against replay attacks
   - as good as it can be regarding small entropy of the password
2. Terminal Authentication:
   a protocol showing that the terminal is trustworthy,
   - based on certificates (CVCA)
3. Chip Authentication:
   ...

Phase 1

1. activating the card:

   . . .

2. Terminal Authentication:

   . . .

3. Chip Authentication:
   - **a challenge: the card cannot show any identification information,**
   - current implementation based on a *group key* shared by a large group of e-ID cards

German Restricted Identification

computing a password

Phase 2

e-ID card with secret x		sector terminal with public key y
	$\xleftarrow{y}$	
compute $u = H(y^x)$		
	$\xrightarrow{u}$	
		if u is on a blacklist, then refuse service
		else accept

Assumptions and features

- since the chip of the e-ID is assumed to be secure, we believe that the card really sends $H(y^x)$ where x is the key for RI
- *a malicious e-ID might cheat by sending some junk – it would not be found on the black list whp*

German Restricted Identification
blacklisting

Blacklist

a list of values $H(y^{x_i})$, where x_i belongs to a banned person

Excluding a user from a sector

- the password of a user in the sector computed in a two-party protocol by e-ID Authority issuing personal identity cards and a sector.
- a simple protocol based on DH mechanism

Alternative Approach for Restricted Identification

Alternative Approach for RI

Our approach

a modification of a German scheme such that

1. management of users in a sector with
   - white-lists (list legitimate users) and/or . . .
   - . . . blacklists (list of excluded users)
2. each time a different password –
   the terminals need not to be trusted
3. but still a single private key on a e-ID card for RI in all sectors

Alternative Approach for RI

Keys in a sector

1. an e-ID card C_i holds a single secret key x_i for authentication in all sectors, and a corresponding parameter $y_i = g^{x_i}$,
2. a sector S holds a base key g^r, for $r = r_S + R_S$, where r_S is a secret of ID Authority, R_S is a secret of S
3. the public keys of users in the sector with the base key g^r are

$$y_1^r, y_2^r, y_3^r, \ldots$$

Alternative Approach for RI

computing user's public keys

Computing by a user

e-ID card i, private key x_i		ID Authority
		public key Y_S of a sector S, certificate C_S for S
	$\xleftarrow{Y_S, C_S}$	
check certificate C_S $y_i := Y_S^{x_i}$		

Usage

issuing a certificate/a ticket for a user to be served by a sector

Alternative Approach for RI

computing user's public keys

Computing public key of a user for a sector

ID Authority	sector, public key $Y = g^{R_S + r_S}$
private key r_S for sector S	private key R_S

public key y of a user retrieved

$y' := y^{r_S}$

$\xrightarrow{y'}$

$y'' := y'^{R_S}$

Usage

procedure for blacklisting or whitelisting a user

Alternative Approach for RI

authentication

Simplified version of authentication protocol

e-ID card with secret x		sector terminal with public key $Y = g^r$
	$\xleftarrow{Y}$	
$y_i := Y^{x_i}$	$\xrightarrow{y_i}$	
		abort if $y_i \in$blacklist or $y_i \notin$whitelist choose t at random, $c := Y^t$
	$\xleftarrow{c}$	
$k := G(c^x)$		$k := G((y_i)^t)$

the terminal and e-ID card talk over a connection encrypted with k, implicit authentication by knowledge of k

Alternative Approach for RI

Omitted details

Some additional mechanisms is the protocol:

1. the e-ID card must know that it talks with a terminal of a given sector
2. some additional mechanisms to allow a full equivalence between impersonation and computational DHP

Unlinkability Issues

Linkability Problem

Problem

- each list of public keys $y_1^r, y_2^r, y_3^r \ldots$ and $y_1^{r'}, y_2^{r'}, y_3^{r'} \ldots$ is available in a mixed (or sorted) form
- nevertheless, two sectors may analyze their whitelists (or blacklists) and try to link corresponding entries

$$y_i^r \text{ and } y_i^{r'}$$

corresponding to the same person
- **the linking threat concerns both alternative RI as well as German RI**

LDH

Linking DH Problem

unlinkability question reduces to *Linking Diffie-Hellman Problem*:
given g^r, (g^a, g^b) and g^{z_1}, g^{z_2} where $\{g^{z_1}, g^{z_2}\} = \{g^{ra}, g^{rb}\}$
find i such that $g^{ra} = g^{z_i}$.

DDH and LDH

- for DDH the input triples may have the form (g^a, g^b, g^c) or (g^a, g^b, g^{ab}) for random c
- for LDH there is a subtle advantage for the adversary who knows that none of the input components has the form g^c, for c random
- **LDH is *only* to find an ordering (under assumption that input data have proper form)**

LDH Results

Results

reduction it can be formally proved that

Linking Diffie-Hellman Problem can be broken
iff
Decisional Diffie-Hellman Problem can be broken

corollary the construction does not introduce any new threat.

Proof

security games framework

Conclusions

It turns out that hashing blacklist for RI in Germany is not really necessary, unlinkability is achieved in the standard model.

Acknowledgment

Partially supported by

- Polish Ministry of Science and Education,
- Foundation for Polish Science, Programme “Mistrz”

FNP

Fundacja na rzecz Nauki Polskiej

We are thankful for exchange of ideas with German authority BSI.
We especially thank Dennis Kügler and Jens Bender for cooperation.

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl, Przemyslaw.Kubiak@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, +48 71 3202105
   fax: +48 71 3202105