Recent Advances in Network Security

IDEMIX: Pseudonomity for e-Transaction

January 19th, 2004

Presenter: Michael Nordhoff
Overview

1. Introduction
2. Ordinary certificates
3. Privacy – meaning / significance
4. Anonymity / Pseudonymity
5. Certificates Lifecycle / Role of CAs
6. IDEMIX
   • Project and Features
   • Example Scenarios
7. Problems
8. Resume
Introduction

• e-transaction & e-commerce more and more important
• without security: lack of acceptance
• solution: certificates with private/public key algorithms
• NOT solved: personal data protection
• keeping privacy with pseudonymous / anonymous certificates
Introduction (2)

usual purchase in a shop

- money (cash)
- goods
- no exchange of information
- => full privacy

e-shopping via internet

- sends lots of private information:
  - credit card data (name, no, …)
  - delivery address
  - email address, phone number
  - …
User Concerns regarding Privacy on the Internet

• being extremely/very **concerned** about divulging personal information online
  - 67% - 74%

• have **left websites** that required registration information
  - 41%

• having entered **fake registration** information
  - 32% - 40%

• having **refrained from shopping** online due to privacy concerns
  - 24% - 64%

[KOSCH03]
Different Primary Interests:

User / Customer
- wants to have control on use of own personal data
- wants to keep privacy/anonymity

E-Commerce Provider / Seller
- wants to get the money
- wants to know the personal data of the liable person

Interests compatible or incompatible?
Satisfying Sellers Interests:

Ordinary Certificates

• “A digital certificate is simply a statement signed by an independent and trusted third party. “[THAW]"

• first standardized by ITU

• later modified by IETF (RFC 2459)
Ordinary digit. Certificates

• contents
  – subject name & other identity details
    (i.e. personal ID, email address, web site URL)
  – public key of identity
  – issuer (Certification Authority - CA)
  – validity period
  – attributes

• signed by the CA
Example: Certificate

Version: 0 (0x0)

Serial Number: 0 (0x0)

Signature Algorithm: md5withRSAEncryption

Issuer: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
       OU=Certification Services, CN=www.thawte.com,
       Email=webmaster@thawte.com

Validity
   Not Before: Nov 14 17:15:25 1996 GMT
   Not After: Dec 14 17:15:25 1996 GMT

Subject: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
         OU=Certification Services, CN=www.thawte.com,
         Email=webmaster@thawte.com

Subject Public Key Info:
   Public Key Algorithm: rsaEncryption

   Modulus:
       ...
       a5:94:ac:8a:67
   Exponent: 65537 (0x10001)

Signature Algorithm: md5withRSAEncryption

   ...
   ee:bc:0e:fe:fc:f8:9b:9d:70:e3

IDEMIX: Pseudonymity for e-Transaction
Satisfying Customers Interests: Privacy - Meaning

• in general: “the right to select what personal information about me is known to what people” [WES67]
• non-material value
• e-transaction privacy more or less protected by law in different countries
• **but:** you cannot check secrecy of service providing organizations
Problem: Non-Privacy

• organizations get information…
  – they do not need for the purpose of this interaction
  – they should not get because it is private

• organizations can intrude into privacy by…
  – linking data of different certificates sent by the same user
  – pooling data with other organizations

• organizations use private information for other purposes
Unauthorized privacy revealing

Doctor/Hospital

unauthorized information exchange

discriminatory treatment

Employee/Patient

raise charge

Insurance Company

knows:
• name
• social security number (ssn)
• health status, e.g.:
  • high cancer risk
  • wants to get a baby
• ...

Employee

withholds insurance amount, knows:
• name
• ssn
• salary
• ...

Fire

unauth. info. exch.

unauth. info. exch.

unauth. info. exch.

2004/01/19 Michael Nordhoff
Identity spectrum must be balanced

• Levels of anonymity:
  – Anonymity
  – Pseudonymous Identification
  – Latent Identification
  – Identification
  – Superidentification

Try to satisfy both sides’ interests
Anonymity - Meaning

- “Anonymity is the state of being not identifiable within a set of subjects” [PF00]
- “[Anonymity] ensures that a user may use a resource or service without disclosing the user’s identity” [ISO99]
Pseudonyms/Pseudonymity

- Pseudonyms are identifies of subjects
- Pseudonymity is the use of pseudonyms as IDs [PF00]
- digital pseudonym:
  - bit string, unique as ID
  - used to authenticate the holder
Pseudonyms

- **dimensions**
  - public pseudonym
  - non-public pseudonym
  - unlinkable pseudonym

- **context**
  - personal pseudonym
  - role pseudonym
  - relationship pseudonym
  - role-relationship pseudonym
  - transaction pseudonym
Pseudonyms (context)

- Person pseudonym
- Role pseudonym
- Relationship pseudonym
- Role-relationship pseudonym
- Transaction pseudonym

Increasing unlinkability of transactions → increasing available anonymity

Unlinkable

Linkable

[PF00]
Pseudonymous Certificate

- does NOT content the real subject (user) name
- pseudonym substitutes the real name
  - randomly chosen, artificial
  - keeps anonymity towards outsiders
  - can keep anonymity towards communication partners
- also standardized by ITU / IETF
Insufficiency of **linkable** pseudonymous Certificate

- service provider can still link users’ information of several transactions / make users’ profiles
- involuntary de-anonymization by monitoring usage of services
- possibility of pooling data with other organizations to get out users’ information and identity
Solution: **Transaction**

Pseudonymous Credentials

- each transaction with different pseudonym
- no linkability between two transactions
- no transmit of certificate, just proof of possession
Certificates: Lifecycle

- Key Pair Generated
- Certificate Issued
- Certificate valid and in use
- Certificate Expires
- Keypair Expired
- Recertify
- Private Key compromised
- Certificate Revoked

[APN]
Role of CA / Pseudonymous-CA (PCA)

**tasks of CA**
- issuing signatures
- certifying validity and ID of dig. signature’s/public key’s owner
- revoking signature when private key compromised
- maintain pki-infrastructure

**additional tasks of PCA**
+ registering nym
+ verifying credential
+ de-anonymization decision
+ global / local de-anonymization
IDEMIX („IDENTity MIX“)

- project of engineers at IBM’s Zurich Research Laboratory, Switzerland
- prototype system to guarantee ‘anonymity’ in the Internet
- implementation of
  - cryptographic protocols
  - ‘pseudonym authority’ (credentials’ issuer)
  - web servers using anonymous access
- protocols also used in other projects / software
IDEMIX Features (1)

- organization knows users just by pseudonyms ("nyms")
- different nyms of same user cannot be linked
- user of a credential can prove possession of it without revealing the credential itself
- encoding of attributes: user can choose which attributes he reveals to the service provider
Necessary Information/Attributes

Example: Car rental system

- reducing given information to prevent linkability / data pooling

<table>
<thead>
<tr>
<th>information usually given</th>
<th>information actually needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>• birthday: 11/23/1973</td>
<td>• age: 18 or over</td>
</tr>
<tr>
<td>• account balance: $ 16,357</td>
<td>• account balance &gt; $ 5000</td>
</tr>
<tr>
<td>• all passport information</td>
<td>• nationality</td>
</tr>
<tr>
<td>• all driver’s license information</td>
<td>• possession of driver’s license</td>
</tr>
<tr>
<td>• dig. credential with attributes and personal information</td>
<td>• possession of a credential (i.e. an allowance to …)</td>
</tr>
<tr>
<td>• user’s name</td>
<td>• (pseudonym)</td>
</tr>
</tbody>
</table>
IDEMIX Features (2)

• different users cannot pool/share their credentials
• anonymity revocation by trusted third party in case conditions of foregoing agreement apply
• mechanisms to revocate credentials
• one-show credentials
Example Scenario: Issuing/Verifying

IDEMIX: Pseudonymity for e-Transaction

User

Certificate (i.e. digit. drivers license)

PCA (i.e. traffic department)

Proof of license possession without revealing itself (transaction pseudonymous)

Knowing the responsible PCA / checking de-anonymization policy

Granting the digit. key for the car

Car Rental Agency
Example Scenario: Payment

User discloses all credit card details

service provider gets real name, etc...

User pays in

holds account

certifies several amounts

proves possession of amount / issues pseudonymous debit order

withdraws the money with the debit order

‘Payment PCA’ / Bank

User

Car Rental Agency

Car Rental Agency
Example Scenario: Revealing ("global")

User
doesn't bring car back

PCA (traffic department)
checks the de-anonymization case and the user-related policy

Car Rental Agency
notices the situation / requires user’s name and address

Police
notifies

reveals user’s identity/name/address …
Idemix Protocol: a small extract

- **U** (user)
- **O_i** (issuing organization)
- **O_v** (verifying organization)
- **N** (pseudonym)
- **attr** (credential's attributes)
- **S_u** (user's master secret)
- **PK/SK** (public/secret encryption key)

**Diagram:**
- **U (S_u)**
  - cred(N, O_i, attr)
  - show(O_i, attr', O_v (PK_v, SK_v))
- **O_v (PK_v, SK_v)**
  - show(O_i, attr', EV_D(N))
- **O_D (PK_D, SK_D)**
  - de-anonymize(transcript)
  - N

**Notations:**
- **OD** (de-anonymizing organization)
- **EV_D(N)** (with PK_D encrypted N, verifiable)
Problems:

- general danger of misuse of a pseudonym credential without attention
- you still need 3rd party organizations you and your transaction partner have to trust and give it your identity information
- no development of provider-customer relationship
- no marketing analysis possible
Resume:

- idemix solves problems which weren’t solved before
- practical in use
- but: system must become accepted by the users and especially by the service providers
- service providers may just see the disadvantages for them (information needed for marketing, expenses of system, i.e.)
• Questions? Please, feel free to ask.

• What do you think?
  – Is there a chance for anonymous credential systems like IDEMIX?
References: