COMP 3410 – I.T. in Electronic Commerce

eSecurity

Identity in Marketspaces

Roger Clarke

Xamax Consultancy, Canberra

Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...

ETS3 {.html, .ppt}

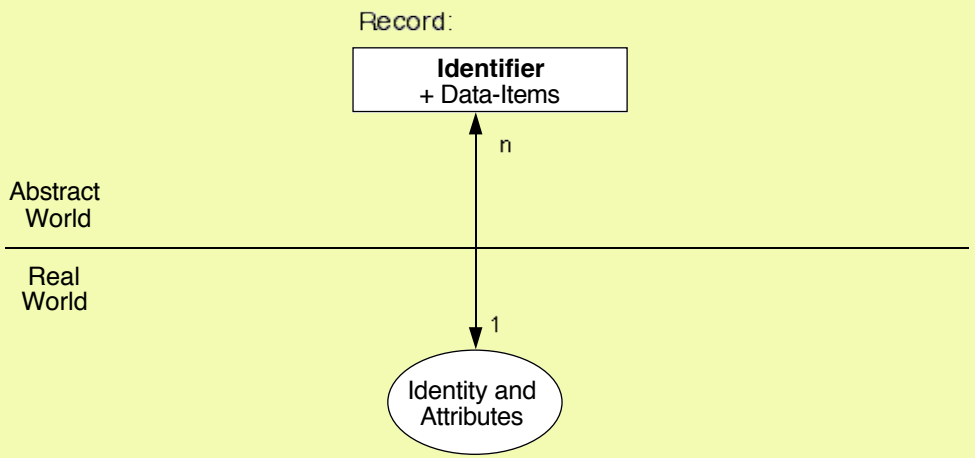
ANU RSCS, 16 October 2012

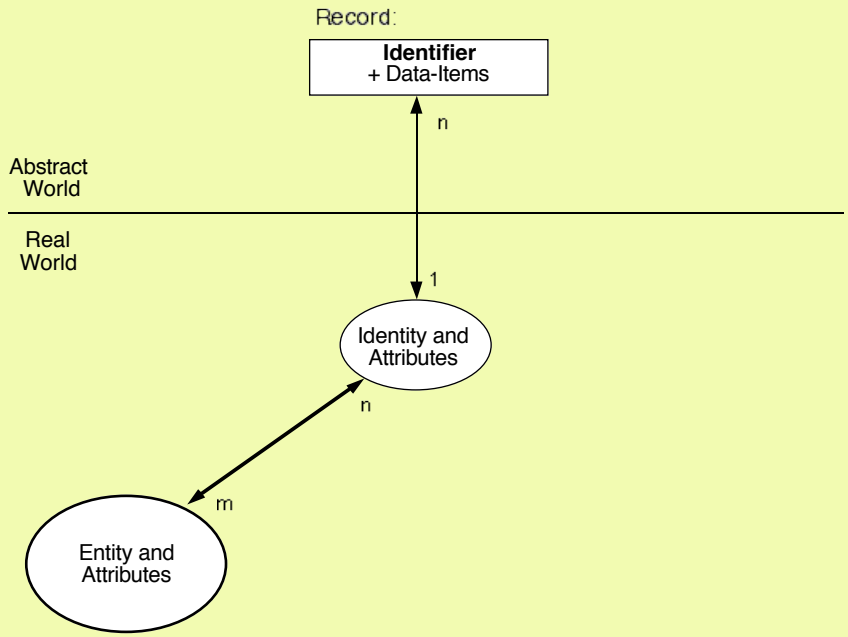
(Id)entification

The process of associating data with a particular (id)entity

(Id)entifier

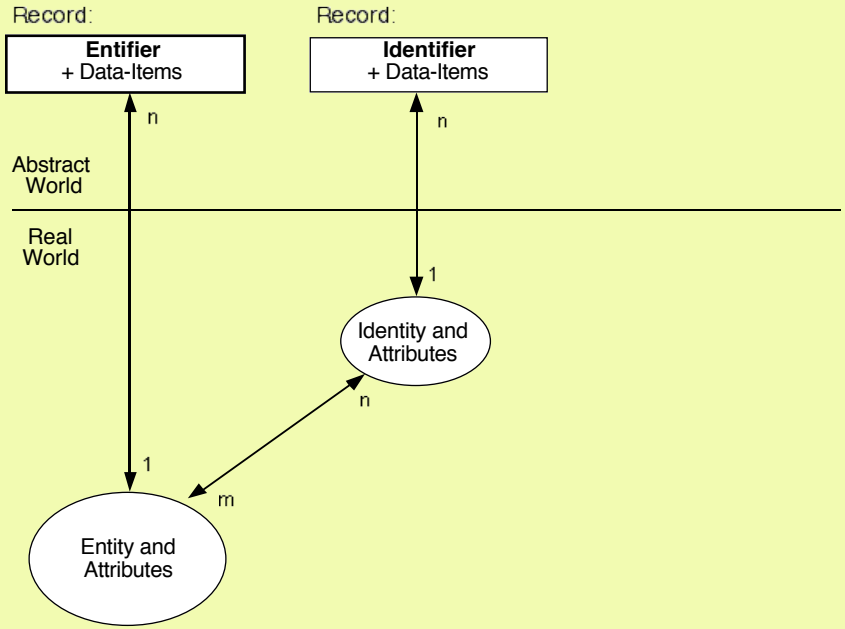
A particular attribute of an (id)entity
that is sufficient
to distinguish it
from other instances of its class
(cf. a 'candidate key')

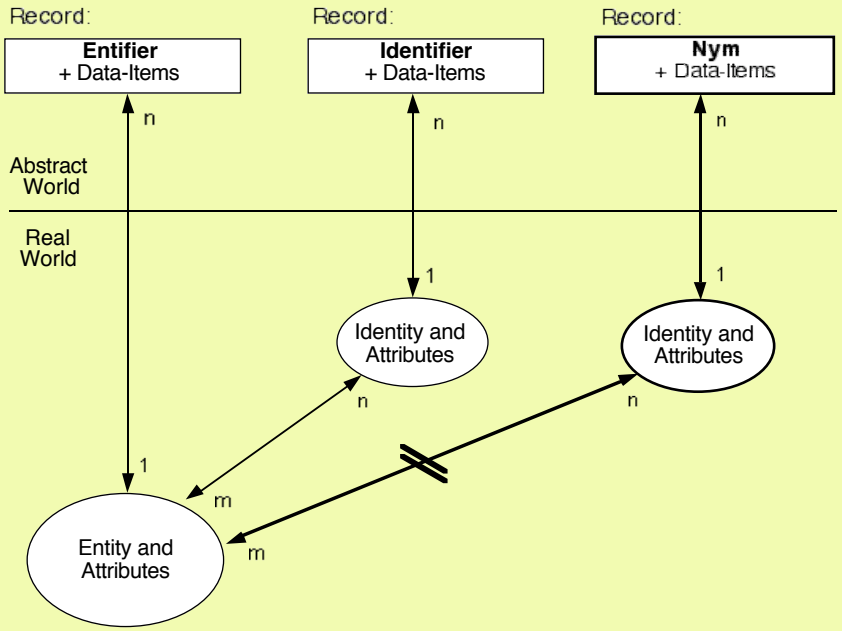




Identities and Entities

- A User
- A Role (shift supervisor, delegate/rep, first-aider)
- Me-at-home, Me-at-work, Me-at-play
- A Guide-Dog, a Pet
- The Car the Pope's in
- A Physical Person (or an imposter)
- Different Physical People at various times
- A Physical Person in different contexts (or an imposter)
- A Dog, allowed / not allowed in an aeroplane
- Various physical cars





(Id)entified Transaction

A Transaction in which the data can be associated with one or more (id)entities

Examples

Order paid with an identified credit card

Order for delivery to a person at an address

Anonymous Transaction

A Transaction in which the data
cannot be associated with an entity
(whether from the transaction alone,
or by combining it with other data)

Examples
Calls from a public phone – ?
Bus-rides – ?
Cups of coffee – ?
Drives along public roads ?

Pseudonymous Transaction

One in which the data **cannot,
in the normal course of events,
be associated with a particular entity**

The data may, however, be indirectly associated with the entity, if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index

Pseudonymous Transaction

One in which the data **cannot,
in the normal course of events,
be associated with a particular entity**

The data may, however, be indirectly associated with the entity, if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index

Examples: HIV / AIDS research, share-trading, phone-calls with CLI, all Internet transactions

2. Authentication

The process of confirming an assertion

- **'(Id)entity Authentication'**
  that data is associated with the correct (id)entity

Authentication

The process of confirming an assertion

- **'Data Authentication'**
  that data accurately reflects reality
- **'(Id)entity Authentication'**
  that data is associated with the correct (id)entity
- **'Attribute Authentication'**
  that an entity has a particular attribute, especially:
  - eligibility for a subsidy, concession or tariff, or to purchase age-restricted goods or services
  - the power to perform acts on behalf of another entity
- **'Value Authentication'**
  that liquid assets are of appropriate quality and quantity

Human (Id)entifiers

- Appearance — How the person looks
- Social Behaviour — How the person interacts with others

Human (Id)entifiers

- Appearance — How the person looks
- Social Behaviour — How the person interacts with others

- Name — What the person is called by other people
- Code — What the person is called by an organisation

Human (Id)entifiers

- Appearance — How the person looks
- Social Behaviour — How the person interacts with others

- Name — What the person is called by other people
- Code — What the person is called by an organisation

- Bio-dynamics — What the person does
- Natural Physiography — What the person is
- Imposed Physical Characteristics — What the person is now

Human (Id)entity Authenticators

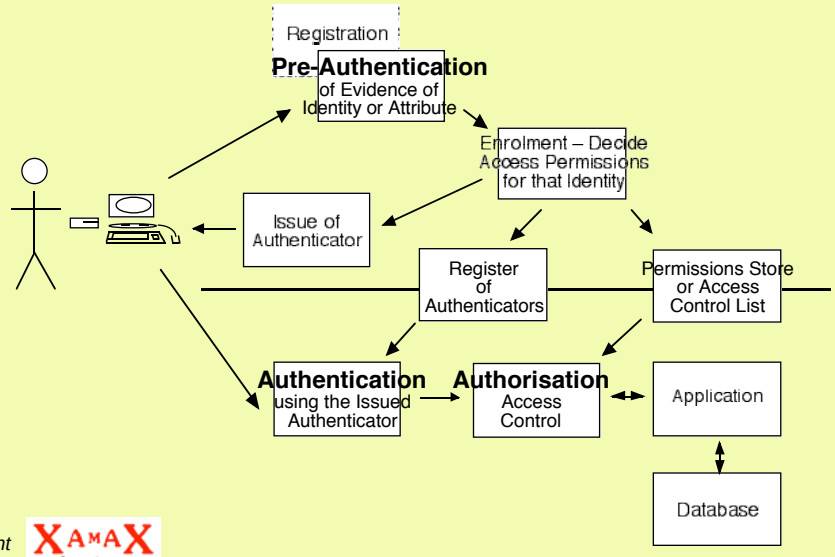
- **What the Person Knows**
  e.g. mother's maiden name, **Password, PIN**
- **What the Person Has**
  esp. a Token, e.g. a Ticket, Document, Card, or maybe a Digital Signature consistent with the Public Key attested to by a Digital Certificate
- **What the Person Does** (signing, keying)

- **What the Person Is** (biometrics)
- **What the Person Is Now** (imposed biometrics)

Human Identity Authentication Current Activities

- The Passports-originated **100-point Check**, based on documents, continues to proliferate
- It is very weak, and it invites identity fraud by scattering insecure copies of key documents
- Organisations such as the new **Online Banks are increasingly accessing 'public' records** to cross-check data provided by the applicant
  e.g. Australia Post's register of names and addresses, the Electoral Roll, the White Pages, ...
  http://www.edentiti.com/
  http://www.greenid.com.au/greenid/howitworks/

Identity Authentication and Authorisation Its Application to Access Control



3. 'Identity Management' aka Single Signon Across Organisations

Industry Associations and Standards Initiatives

Existing Associations

- Identrus
- **Internet2 Shibboleth**
- OASIS SAML
- The Open Group

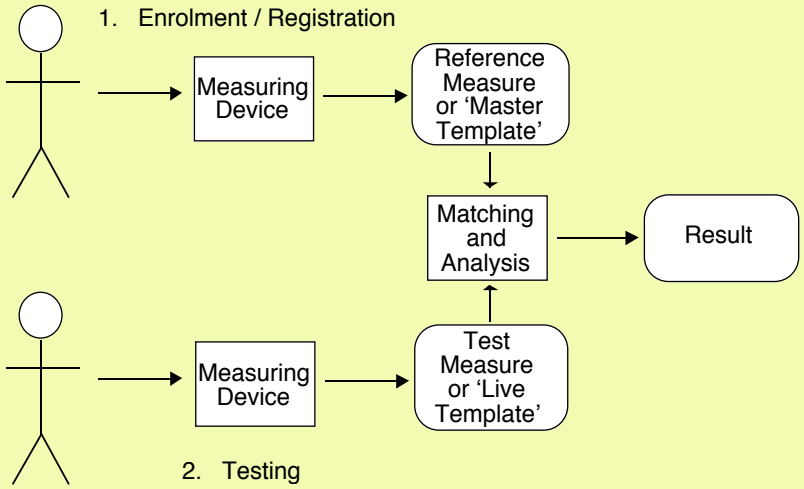
New Associations

- **Liberty Alliance**
- **OpenID** http://openid.net/
- OpenSAML
- PingId
- SourceID
- **Web Services Federation**
- XNS

4. Biometrics

- **Appearance**
  height, weight, colour of skin, hair and eyes, visible physical markings, gender?, race??, facial hair??, wearing of glasses??, **facial appearance??**
- **Social Behaviour**
  habituated body-signals, general voice characteristics, style of speech, visible handicaps
- **Bio-Dynamics**
  manner of writing one's signature, **voice characteristics**, keystroke dynamics, esp. of login-id, password
- **Natural Physiography**
  skull measurements??, teeth and skeletal injuries?, **thumbprint**, **fingerprint sets**, handprints, retinal scans, **iris scans**, capillary patterns (e.g. in earlobes), **hand and digit geometry**, DNA-patterns
- **Imposed Features**
  dog-tags, collars, bracelets and anklets, bar-codes and other kinds of brands, **embedded micro-chips / RFID tags** and transponders

The Biometric Process



Uses of Biometrics

1. For (Id)entification

A process to find 1-among-many, in order to help answer the question '**Who is it?**'

Uses of Biometrics

1. For (Id)entification

A process to find 1-among-many, in order to help answer the question '**Who is it?**'

2. For (Id)entity Authentication

A process to test 1-to-1, in order to help answer the question '**Is this the person who you think it is?**'

Uses of Biometrics

1. For (Id)entification

A process to find 1-among-many, in order to answer the question '**Who is it?**'

2. For (Id)entity Authentication

A process to test 1-to-1, in order to help answer the question '**Is this the person who you think it is?**'

3. For Attribute Authentication w/- (Id)entity

A process to help answer the question
'**Does this person (whoever they are) have the attribute they purport to have?**'

The Huge Quality Problems with Biometric Applications

Dimensions of Quality

- Reference-Measure
- Association
- Test-Measure
- Comparison
- Result-Computation

Other Aspects of Quality

- Vulnerabilities
- Quality Measures
- Counter-Measures
- Spiralling Complexity

Consequences of the Quality Problems

- There is never 'a perfect match'; it's fuzzy
- A Tolerance Range has to be allowed
- 'False Positives' / 'False Acceptances' arise
- 'False Negatives' / 'False Rejections' arise
- Tighter Tolerances (to reduce False Negatives) increase the rate of False Positives; and vice versa
- The Scheme Sponsor sets (and re-sets) the Tolerances
- Frequent exceptions are mostly processed cursorily
- Occasional 'scares' slow everything, annoy everyone

Threats to Biometric Applications

- Live Biometric capture, theft
- Live Biometric simulation
- Live Biometric substitution
- Reference Biometric substitution
- Reference Biometric forgery
- Message interception, modification, insertion
- Stored Biometric capture, theft, change, substitution
- Threshhold manipulation
- Device tampering
- Environmental tampering (e.g. lighting, jamming)
- Infrastructure manipulation (e.g. power-outage)
- Device or System override / backdoor / trojan utilisation
- Exception-Handling Procedures manipulation
- Fallback procedures for the Unenrollable subversion
- Insider collusion

5. Identity-Related Crimes

Use of an identifier and/or authenticators ...

- **Identity Fraud**
  ... to financially advantage or disadvantage someone
- **Identity Theft**
  ... to such an extent, or with such a negative impact, that further use by the person they were originally associated with is effectively precluded
- **Identity-Facilitated Criminal Acts**
  Proceeds of crime laundering, tax avoidance, trafficking ...

The identity that is compromised
may be someone else's, 'fictional',
or even the person's own

I.T. and Dataveillance

- **Privacy-Invasive Technologies (the PITs)**
  - Data-Trail Intensification (id'd phones, SVCs, ITS)
  - Data Warehousing and Data Mining
  - Person-Location and Person-Tracking
  - Stored Biometrics
  - Imposed Biometrics

I.T. and Dataveillance

- **Privacy-Invasive Technologies (the PITs)**
  - Data-Trail Intensification (id'd phones, SVCs, ITS)
  - Data Warehousing and Data Mining
  - Person-Location and Person-Tracking
  - Stored Biometrics
  - Imposed Biometrics
- **Privacy-Enhancing Technologies (PETs)**
  - Countermeasures against the PITs
  - Tools for Data Protection
  - Tools for Client-Side Device Security
  - Tools for Anonymity and Pseudonymity

6. PETS
PIT Countermeasures

- Cookie-Cutters
- Cookie-Managers
- Personal Data Managers (e.g. P3P implementations)
- Personal Intermediaries / Proxies
- Data Protection Tools
- Client-Side Security Tools
- Channel, Server and Proxy/Firewall Security Tools

Savage PETs

Deny identity
Provide anonymity

Genuinely anonymous ('Mixmaster') remailers, web-surfing tools, ePayment mechanisms, value authentication, attribute authentication

Gentle PETs

Balance nymity and accountability through Protected Pseudonymity

Intermediary Tools and Proxies, Client-Side Agents, Pseudonymous Connection, Remailers, Web-Surfers

7. Digital Signatures and ...

A string of characters that the Sender adds to a message

The Theory: **Only the entity that has access to the relevant Private Key can have possibly sent the message**

... Public Key Infrastructure (PKI)

A substantial set of equipment, software, procedures and organisations necessary to generate and protect key-pairs, generate signatures, publish public keys and revocations, pre-authenticate signors, authenticate signatures, assure quality, insure participants, prosecute the guilty

What a Digital Signature Actually Means

A Digital Signature attests **only** that:

the message was signed by a device
that had access to the private key
that matches the public key

Conventional, X.509-Based PKI Doesn't Work

- A DigSig does not confirm sender identity unless a long list of conditions is fulfilled
- Fulfilment of those conditions depends upon a substantial infrastructure, which is highly intrusive, and which has never been deployed
- Conventional, X.509-based PKI doesn't fulfil those conditions, and it never will

Alternative PKI
Trust without Authenticated Identity

- Pretty Good Privacy (PGP)
  Intro: http://web.bham.ac.uk/N.M.Queen/pgp/pgp.html
- Simple Public Key Infrastructure (SPKI)
  http://www.ietf.org/html.charters/spki-charter.html
- Simple Distributed Security Infrastructure (SDSI)
  http://theory.lcs.mit.edu/~cis/sdsi.html
- Stefan Brands / Credentica/MS UProve
  Bought by Microsoft, but now there's an open source SDK: http://code.msdn.microsoft.com/uprovesdkcsharp

E-Trading
Identity in Marketspaces
Agenda

1. (Id)entification and Nymity
2. Authentication
3. 'Identity Management'
4. Biometrics
5. Identity-Related Crimes
6. PITs and PETs
7. Digital Signatures and PKI

COMP 3410 – I.T. in Electronic Commerce

eSecurity
Identity in Marketspaces

Roger Clarke
Xamax Consultancy, Canberra
Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/EC/ ...
ETS3 {.html, .ppt}

ANU RSCS, 16 October 2012

A Digital Signature

A string of characters that the Sender adds to a message

The string is a concise representation of the whole message (called **a 'Message Digest'**)

In practice, a **hashing algorithm** is used

The Digest is **encrypted** with the Sender's Private Key

The Receiver:

- decrypts the signature using the Sender's Public Key
- regenerates the Message Digest from the message
- checks that the two are the same

The Theory: **Only the entity that has access to the relevant Private Key can have possibly sent the message**

Public Key Infrastructure (PKI)

- **Signer-Side**
  - Means to generate a key-pair
  - Security for the private key in use and storage
  - Means to apply for a certificate
  - Means to generate digital signatures
  - Means to revoke a certificate
- **Service-Provider Side**
  - Authentication of certificate applicants
  - Issue of certificates
- **Relier-Side**
  - Means to acquire certs
  - Means to check:
    - their value
    - their currency
  - Means to check dig sigs
  - Means to sue service-providers

Conventional, X.509-Based PKI Doesn't Work

- A DigSig does not confirm sender identity unless a long list of conditions is fulfilled
- Fulfilment of those conditions depends upon a substantial infrastructure, which is highly intrusive, and which has never been deployed
- Conventional, X.509-based PKI doesn't fulfil those conditions, and it never will

What a Digital Signature Actually Means

A Digital Signature attests **only** that:

the message was signed by a device
that had access to the private key
that matches the public key

Public Key Infrastructure Security and Privacy Issues

- **Generation of Key-Pairs**
  In some schemes, someone else sees the Private Key
- **Security of the Private Key**
  It's vulnerable to malware when in use
  It's generally vulnerable in storage as well
- **Onerous and Intrusive Authentication Processes**
- **Information Privacy Risks**
  Directory of keyholder details, Trail of sites visited
- **Consequential Privacy Implications**
  e.g. increased expectation of identity disclosure

The SSL / https Process

Sender Actions:

Message-in-Clear-Text * Hash-Function => Hash-Value
Hash-Value * **Sender's-DigSig-Private-Key** => **Dig. Signature**
Message-in-Clear-Text | | Signature => Signed-Text
Signed-Text * Secret-Encryption-Key => Encrypted-Signed-Text

Recipient Actions:

Encrypted-Signed-Text / Secret-Encryption-Key
=> Message-in-Clear-Text | | Signature
Message-in-Clear-Text * Hash-Function => Hash-Value
Signature / **Sender's-DigSig-Public-Key** => Hash-Value
If the Hash-Values match, then Sender ID is Authenticated

SSL / TLS in Practice

- **Channel-Encryption: Effective and Valuable**
- **Authentication:**
  - of Workstations / Browsers / Users
    - **Almost Nil**
  - of Hosts / Servers / Organisations
    - **Very Low-Grade**
    - Upgrades, e.g. 'Extended Validation' (EV), keep failing, because they're:
      - expensive
      - incomprehensible to consumers
      - unable to handle key revocation, expiry
      - not supported by warranties
      - little-implemented

Alternative PKI

Trust without Authenticated Identity

- Pretty Good Privacy (**PGP**)
  Intro: http://web.bham.ac.uk/N.M.Queen/pgp/pgp.html
- Simple Public Key Infrastructure (**SPKI**)
  http://www.ietf.org/html.charters/spki-charter.html
- Simple Distributed Security Infrastructure (**SDSI**)
  http://theory.lcs.mit.edu/~cis/sdsi.html
- **Stefan Brands / Credentica/MS UProve**
  Bought by Microsoft, but now there's an open source SDK: http://code.msdn.microsoft.com/uprovesdkcsharp