Biometric Recognition’s Role in Identity Management

Elisa Bertino

CS Department
CERIAS
Purdue University
bertino@cs.purdue.edu
What is Digital Identity?

**Digital Identity:**
- Digital identity (DI) can be defined as the digital representation of the information known about a specific individual, organization, system, machine and any other identifiable entity.
- It can include things such as name, address, social security and account numbers, biometric data, passwords, transaction data, machine tags, IP address.

**Terminology:**
- A *nym* gives an individual an identity under which to operate when interacting with other parties; example: login names.
  - Nyms can strongly bind to an individual or weakly bind (useful in contexts such as on-line games).
- *Partial identities* encompass a set of an individual’s properties.
  - such properties are referred to as *identity attributes*.
    - Classified as *strong identity attributes* and *weak identity attributes*.
  - each subset of the identity attributes represents a partial identity of the individual.
  - partial identities may or may not be bound to the human identity of one or more actual individuals.
Domains of Interest

- Identity Theft
- Financial
- Border Control
- Virtual Identities
- Law Enforcement
- Telecommunications
- Computing
- Benefits Management
- eGovernment
- Healthcare
- Defense
- Transportation

---

Slide from the presentation “NSTC Activities in Biometrics and Identity Management” by D. Blackburn, June 24 2008
DI Basic Concepts

- **Digital Identity – another definition**: A set of claims made by one digital subject about itself or another digital subject.

- **Claim**: An assertion of the truth of something, typically one which is disputed or in doubt.
  - An identifier
  - Knowledge of a secret
  - Personally identifying information
  - Membership in a given group (e.g. people under 16)

- **Credential**: A set of data providing evidence for claims about parts of or entire identities.
Identities consist of identifiers, credentials, and attributes

Identity as employee
- Identifier
- Credentials
- Attributes
- Employee #: 1080345
- Digital Certificate in a smart card
- Name: Alice Brown
- Job title: Senior manager
- Affiliation: Sales Department
- Office: Chicago

Identity as social network user
- Identifier
- Credentials
- Attributes
- Account name: Ilovemusic
- Password
- Name: Alice Brown
- Gender: Female
- Location: US Midwest
- Favorites: classical music

Which is the role of biometrics in this notion of identities?
Medentity is tied to a subject in a one-to-one manner.
- It is also called true identity.
- True identities came into existence when subjects as natural persons were born.

Ourdentity is an identity that exists by mutual agreements between a subject and a third party.
- Ourdentity is similar to the notion of assigned identity, that is, an identity assigned by a third party.

Theirdentity is an identity that a third party guesses and internally creates without explicit consent from the subject.
- Theirdentities can be generated based on cookies and/or source IP addresses.
- The subjects are not aware of the existence, details, or accuracy of their theirdentities and do not have any control over them.

Ourdentity - example

A user account at an online bookstore is an ourdentity.

- The subject can create, modify, and delete the user account.
- The bookstore may also have some control over the identity based on terms and conditions that the subject and the bookstore agreed upon.
- The bookstore may, for example, record the usage of a subject and recommend him or her books based on the usage record.
Ourdentity - example

A Web search service

- It creates a theirdentity as an internal user model for customized advertisements to the subject
- It sells the usage logs associated with the theirdentity to market analysis specialists.
The Goal of Identity Management

To maintain the integrity of identities through their lifecycles in order to make the identities and their related data (e.g., authentication results) available to services in a secure and privacy-protected manner.

Functions:

- adding or removing (“provisioning”) digital identity information
- managing policies for digital identity authentication and associated access rights to information (i.e., authentication & access control policies)
- enforcing authentication and access control policies to systems, data and applications (access management)
Three key players in DI management

Subject

Provide identity data
Authenticate

Investigate

Provide service

Audit & investigate

Control Party

Identity Provider

Provide identity data
(e.g., authentication results)

Relying Party

Elisa Bertino
Digital Identity
Ownership, Validity and Authentication

**Owner of an identifier:**
- the individual to whom an identifier is issued to by a trusted authority or an individual who is authoritative with respect to the claiming of the identifier

**Validity of an identity attribute:**
- it refers to making sure that an identity attribute is true with respect to some real world (for example, that the age of Bob is 24)

**Authentication:**
- It deals with verifying that identifiers claimed by an individual are owned by that individual
- It deals with verifying that the values of identity attributes are valid
Authentication

- Something You Have + Something You Know + Something You Are
- Something You Have + Something You Are
- Something You Have + Something You Know
- Something You Have
- Something You Know
- PIN, Password
- Key or Card
- Relative Security Level
- Solutions
### Assurance Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Implementation example</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Little or no confidence in the asserted identity’s ownership</td>
<td>Personal identification numbers (PINs)</td>
<td>Online registration to a news website</td>
</tr>
<tr>
<td>2</td>
<td>Some confidence in the asserted identity's ownership</td>
<td>Single-factor remote authentication (e.g., usernames and passwords through encrypted communication channels)</td>
<td>Change of address by beneficiary</td>
</tr>
<tr>
<td>3</td>
<td>High confidence in the asserted identity's ownership</td>
<td>Multi-factor remote authentication with software-based tokens (e.g., a combination of PINs and electronic certificates stored in web browsers)</td>
<td>Online access to a brokerage account</td>
</tr>
<tr>
<td>4</td>
<td>Very high confidence in the asserted identity's ownership</td>
<td>Multi-factor remote authentication with hardware-based tokens (e.g., smart cards with protected by finger print authentication)</td>
<td>Distribution of controlled drugs</td>
</tr>
</tbody>
</table>
Identity Theft

IDENTITY THEFT is the use of personally identifying information belonging to one individual by another individual for financial or personal gain.
## Threat of Identity Theft: Attack Vectors

<table>
<thead>
<tr>
<th>Technical</th>
<th>Pharming, Network Sniffing, Database Attacks, Password Cracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Dumpster Diving, Trusted Insiders, Theft and Loss</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Phishing, Legal Identity Sources</td>
</tr>
</tbody>
</table>
## Objective – Obtain Individual Identity

<table>
<thead>
<tr>
<th>Type</th>
<th>Attack</th>
<th>Description</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Trojan/Keystroke Logging</td>
<td>Spyware/malware placed via hacking, as payload in a virus, or downloaded from an attacker's Web site</td>
<td>1, 3, 4</td>
</tr>
<tr>
<td></td>
<td>Wireless Intercept</td>
<td>Open access points, AirSnarfing, &quot;Evil Twin&quot;</td>
<td>5, 6</td>
</tr>
<tr>
<td></td>
<td>Pharming</td>
<td>DNS spoofing, DNS cache poisoning, proxy attacks</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Scrape Web Site</td>
<td>Gather personal data from Web sites to use as verifiers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Sniffing</td>
<td>Collect targeted network packets</td>
<td>7, 23</td>
</tr>
<tr>
<td>Physical</td>
<td>Theft</td>
<td>Stolen mail, wallets/purses, laptops</td>
<td>2, 5, 6</td>
</tr>
<tr>
<td></td>
<td>Shoulder Surfing</td>
<td>Direct observation of personal, confidential information</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Dumpster Diving</td>
<td>Gather discarded documents or hardware (disks)</td>
<td>2, 8</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Identity information misused by individuals with access</td>
<td>5, 9, 10</td>
</tr>
<tr>
<td>Social</td>
<td>Phishing</td>
<td>Luring individuals to reveal confidential information</td>
<td>1, 20</td>
</tr>
<tr>
<td>Engineering</td>
<td>Family Members</td>
<td>Identity information misused by family members</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Legal Identity Sources</td>
<td>Obtain identity information fraudulently from credit bureaus, government agencies, etc.</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td>&quot;419&quot; Scams</td>
<td>Obtain money and/or account information</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Obtain identity information from service providers (doctors, dentists, lawyers, etc.)</td>
<td>1, 2, 21, 22</td>
</tr>
</tbody>
</table>
Objective – Obtain Multiple Identities

<table>
<thead>
<tr>
<th>Type</th>
<th>Attack</th>
<th>Description</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Hacking</td>
<td>Gain privileged access for further attacks and/or data harvesting</td>
<td>10, 12, 13, 14, 15, 16, 17</td>
</tr>
<tr>
<td></td>
<td>Data Attacks</td>
<td>SQL injection, XSS attacks</td>
<td>7, 18, 19</td>
</tr>
<tr>
<td></td>
<td>Database Attacks</td>
<td>Login attacks, inference attacks, SQL scanners</td>
<td>1, 5, 15</td>
</tr>
<tr>
<td></td>
<td>Password Cracking</td>
<td>Acquire admin passwords to servers</td>
<td>1, 15</td>
</tr>
<tr>
<td>Physical</td>
<td>Theft and Loss</td>
<td>Backup data, tapes, disks, laptops, etc.</td>
<td>5, 7, 11</td>
</tr>
<tr>
<td></td>
<td>Firewall Breaches</td>
<td>Connect and map internal network(s)</td>
<td>15, 16</td>
</tr>
<tr>
<td></td>
<td>Dumpster Diving</td>
<td>Obtain discarded documents, disks, systems, etc.</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Access individuals take data with removable media, e-mail</td>
<td>1, 2, 21, 22</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Gain Physical Access</td>
<td>Computer rooms, server farms, wiring closets, switches, routers</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>DBAs, employees, contractors, individuals with access</td>
<td>1, 2, 21, 22</td>
</tr>
<tr>
<td></td>
<td>Phone Requests</td>
<td>Obtain confidential information to facilitate attacks</td>
<td>2</td>
</tr>
</tbody>
</table>
Mitigations and Compensating Controls

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Multi-factor authentication</td>
</tr>
<tr>
<td>2.</td>
<td>User education</td>
</tr>
<tr>
<td>3.</td>
<td>Anti-virus package(s)</td>
</tr>
<tr>
<td>4.</td>
<td>Anti-spyware package(s)</td>
</tr>
<tr>
<td>5.</td>
<td>Encryption</td>
</tr>
<tr>
<td>6.</td>
<td>Secure configuration</td>
</tr>
<tr>
<td>7.</td>
<td>Encrypted payload</td>
</tr>
<tr>
<td>8.</td>
<td>Shredding</td>
</tr>
<tr>
<td>9.</td>
<td>Enforce need-to-know</td>
</tr>
<tr>
<td>10.</td>
<td>Access controls and user privileges</td>
</tr>
<tr>
<td>11.</td>
<td>Policy and enforcement</td>
</tr>
<tr>
<td>12.</td>
<td>n-tier architecture</td>
</tr>
<tr>
<td>13.</td>
<td>Real-time monitoring</td>
</tr>
<tr>
<td>14.</td>
<td>Honey pots/honey nets</td>
</tr>
<tr>
<td>15.</td>
<td>HIPS (Host Intrusion Protection Systems)</td>
</tr>
<tr>
<td>16.</td>
<td>NIDS (Network Intrusion Detection Systems)</td>
</tr>
<tr>
<td>17.</td>
<td>Well-configured firewall(s)</td>
</tr>
<tr>
<td>18.</td>
<td>Server-side validation</td>
</tr>
<tr>
<td>19.</td>
<td>Secure coding techniques</td>
</tr>
<tr>
<td>20.</td>
<td>Browser toolbars</td>
</tr>
<tr>
<td>21.</td>
<td>Separation of duties</td>
</tr>
<tr>
<td>22.</td>
<td>Audit controls</td>
</tr>
<tr>
<td>23.</td>
<td>SSL/TLS</td>
</tr>
</tbody>
</table>
The VeryIDX project

- To investigate strong and privacy preserving verification of identity attributes
- To investigate the use of biometric identity attributes
- To investigate policy systems for the management if identity attributes
- To investigate the notion of identity attribute quality, provenance and consistency
**Multi-Factor Authentication**

Require additional identity information (like SSN) as proof to qualify to be the owner of the identifier being used (like credit card number)

**Example Real Life Scenario:** Requirement for additional proofs of identity

I will use my credit card to pay

To use your credit card please show your driver license and an additional photo id for verification of your identity
Multi-Factor Authentication without Privacy Loss

- **Zero knowledge proof (ZKP)** is an interactive method to prove the possession of a secret without actually revealing it.

- Our **aggregated ZKP scheme** is used to prove the knowledge of multiple strong identifiers efficiently and reliably without the need to provide them in clear.

- Based on well-known cryptographic techniques:
  - Pedersen Commitments
  - Aggregated Signatures
Pedersen Commitment – ZK
Proving to know how to open

- Public commitment $c = g^x h^r \pmod{p}$
- Private knowledge $x, r$
- Protocol:
  1. $P$ (prover): randomly picks $y, s$ in $[1..q]$, sends $d = g^y h^s \pmod{p}$
  1. $V$ (verifier): sends random challenge $e$ in $[1..q]$
  2. $P$: sends $u = y + ex$, $v = s + er \pmod{q}$
  3. $V$: accepts if $g^u h^v = d c^e \pmod{p}$
Functional View of VeryIDX

- Policy
- Registration
- Identity Records Storage
- Usage
- Audit Log
- Policy
Identity Record (IdR)

- An identity record is a set of identity tuples
- An identity tuple stores the following information about a strong identifier $m$:
  - A tag for $m$ (example: CCN, SSN)
  - $M = g^m h^r$, Pedersen commitment of $m$
  - $\sigma$, registrar signature on $M$
  - Validity assurance
  - Ownership assurance
  - A set of weak identifiers

<table>
<thead>
<tr>
<th>Strong IdTag</th>
<th>Signature [\sigma]</th>
<th>Commitment [M]</th>
<th>Valid-assure</th>
<th>Owner-assure</th>
<th>WeakID(set)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCN</td>
<td>74387264 87979976 66876989</td>
<td>3298397 9798749 3827983</td>
<td>A</td>
<td>B</td>
<td>value tag</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bob</td>
<td>Mars</td>
<td>name</td>
</tr>
<tr>
<td>SSN</td>
<td>88874724 72323098 40923610</td>
<td>3987239 8747973 8294991</td>
<td>U</td>
<td>A</td>
<td>value tag</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bob</td>
<td>Mars</td>
<td>name</td>
</tr>
</tbody>
</table>
Integration with Biometrics

The biometric image hashing is used to generate hash vectors which are bit vector representation of the biometric. The same biometric would be hashed into vectors which are similar (as evaluated in Phase 2).
## Security Analysis

<table>
<thead>
<tr>
<th>Biometric Image</th>
<th>Hashing Secrets</th>
<th>SVM Model</th>
<th>Biometric Key</th>
<th>Commitment Secret</th>
</tr>
</thead>
</table>

Elisa Bertino
Biometrics and Identity

- History of biometrics comes from physical world
  - Law enforcement
  - Supervised applications
  - Trained operators
  - Obligated participation
  - Existing infrastructure

- Today: a crossover between physical and digital world
  - Dramatic change in function and management
  - Service oriented
  - Unexperienced operators (quality of enrolment!)
  - Non-supervised
  - New infrastructure

- Different risk profiles (stealing, spoofing, manipulating):
  - Physical risk is limited and manageable (1:1 interaction)
  - Digital risk is hard to manage (e-distribution, non-supervised)

Based on presentation “Biometrics and (e-) Identity -How and where to increase the efficacy of the dialogue” by Max Snijder (European Biometrics Forum)
What do Biometrics say about Identity?

- Answer:
  - as much as you want
  - as less as you want
- Depends on what identifiers and identity attributes are linked to the biometric information
- If no identifiers or identity attributes are linked, biometrics are ‘anonymous’ and can be disconnected from identity
  - case: anonymous clinical trials
Integrating Biometrics and DI Management

Challenges

- Interoperability
- User mobility – use of mobile smart devices, NFC
- Protection of the biometric infrastructures
- Scalability
- Federated identity management
- Authentication policies
Thank You!

Questions?

Elisa Bertino
bertino@cs.purdue.edu
References
