Its is time to standardize BTP

Biometric Template Protection

- alias {Helper Data Scheme, biotoken, biotypes, Pseudo Identities, Pseudonymous Identifier, Fuzzy commitment, Cancelable Biometrics, Biometric encryption, Biohasing, Fuzzy Vault, Shielding functions, Fuzzy extractors, Extended PIR, BIOCRYPTICS,}
- All of them can be represented in a unified architecture
  - see Brebaart et al. „A Reference Architecture for Biometric Template Protection based on Pseudo Identities“, GI-LNI: BIOSIG 2008

- Vendors:
  - IBM
  - Philips
  - priv-ID
  - GenKey
  - Mitsubishi
  - Hitachi
  - Sagem Securite
  - securis
  - secunet
Standardization on Template Protection

Biometric Standardisation

International Organization for Standardisation

Joint Technical Committee One

International Electrotechnical Commission

International Civil Aviation Organization

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

SC 37 Formal Liaisons
The Process

International Standard
- Working Draft (WD)
- Committee Draft (CD)
- Final Committee Draft (FCD)
- Final Draft International Standard (FDIS)
- International Standard (IS)

Issues to consider:
- Commenting periods
- Potentially multiple loops at one level
- Need for mature technology (has been argued for Template Protection...)
- Decisions are made on consensus
- Need to progress
- Five year revision cycle

Biometric Standardisation

Onion Layers
- Layer 1: BDB
  - Digital representations of biometric characteristics
- Layer 2: LDS
  - CBEFF Meta-data
- Layer 3+4: System properties
  - Security
  - Performance
- Layer 5: BioAPI, BIP
  - System Integration
Biometric Template Protection

- October 2006
  - M.G. Chun and Mr. P.J. Lee were appointed as new Co-editors
  - 3rd WD had not been created
- October 2007: Lucerne meeting
  - Discussion on refocusing the standard
- April 2008: Kyoto meeting
  - NB commented on N6314 and accepted to continue with original scope (N3928rev1, 2004)
  - ".... project under its original scope"
- October 2008: Cyprus meeting
  - Inclusion of renewability and diversification
- November 2009: Redmond meeting
  - 2nd CD

Biometric Template Protection

- Dependency to other projects

ISO/TC 68-Finacial Services
Biometrics Security Framework 19092
19092:2007

SC27 WG5
IdM
Privacy
Framework/Arch.
E.A. Assurance

SC37 WG2
Biometrics
CBEFF-Part 4
Security Block Format Spec. 19785-4

SC37 WG6
Biometrics
Jurisdictional and Societal Considerations 24714-1 for Commercial
Content of 2nd CD ISO 24745

6.1 Security requirements for biometric systems

- 6.1.1 Confidentiality
- 6.1.2 Integrity
- 6.1.3 Availability
- 6.1.4 Renewability and revocability

...

8.2 Biometric information privacy requirements

- 8.2.1 Irreversibility
- 8.2.2 Unlinkability
- 8.2.3 Confidentiality
- 8.2.4 Data minimization

Threats and Countermeasures

Against biometric system components

- Data capture: T sensor spoofing -
  ‣ liveness detection / multimodal biometric, challenge response
- Signal processing: T insertion of imposter data
  ‣ use approved algorithm
- Comparison: T manipulation of comparison scores
  ‣ secure server and/or client, trusted COC
- Storage: T database compromise
  ‣ diversification to allow renewability of biometric references
  ‣ data separation
  ‣ database access control
- Decision: T hill climbing, T threshold manipulation
  ‣ secure channel, access control
Threats and Countermeasures

During transmission

• Data Capture - Signal Processing:
  ‣ T Eavesdropping
  ‣ T Replay

• Signal Processing-Comparison
  ‣ T Brute Force

• Storage-Comparison
  ‣ T Eavesdropping
  ‣ T Replay
  ‣ T Man in the middel
  ‣ T Hill climbing

• Comparison-Decision
  ‣ T: Comparison score manipulation

Security in Application Models

Classification of system regarding storage of biometric references and comparison

• Clause 7.2
  ‣ Model A – Store on server and compare on server
  ‣ Model B – Store on token and compare on server
  ‣ Model C – Store on server and compare on client
  ‣ Model D – Store on client and compare on client
  ‣ Model E – Store on token and compare on client
  ‣ Model F – Store on token and compare on token
  ‣ Model G – Store distributed on token and server, compare on server
  ‣ Model H – Store distributed on token and client, compare on client
Consensus at Oct 2008 meeting

Biometric Template Protection should include Pseudonymous Identifiers

- Now a mature technology with various products
  - Significant progress over 1st ad 2nd WD
- Allows renewability/revocability
  - Create new Pseudonymous Identifiers from same biometric sample
- Prevents collisions and associated security / privacy risks
- Allows a data separation principle
  - PI and AD stored in different places to
    - Enhance security
    - Puts both data subject and service provider in control of comparison process and revocation

Renewable Biometric References

Elements in the architecture

- auxiliary data AD
  - subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general
- pseudonymous identifier PI
  - part of a renewable biometric reference that represents an individual or data subject within a certain context by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any)
- supplementary data SD
  - data intended for security amplification of renewable biometric references by means of possession, knowledge or application-based secrets that are both required during enrolment and verification and are not stored with biometric references nor dependent on biometric characteristics, that are either provided by the data subject or the identity management system
PI Framework

- Architecture for renewable biometric references

Protected Template Structure

Protected Template
- Pseudonymous Identifier
- Auxiliary Data
  - Diversification Data
  - Other data elements
## Example Methods Generating PIs

### Table C.1 maps existing methods to ISO 24745

<table>
<thead>
<tr>
<th>Method</th>
<th>Reference</th>
<th>Pseudonymous identifier (Pi)</th>
<th>Auxiliary data (AD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helper data systems</td>
<td>[23]</td>
<td>Hash of secret string</td>
<td>Helper data</td>
</tr>
<tr>
<td>Fuzzy commitment</td>
<td>[24]</td>
<td>Hash of secret string</td>
<td>Offset</td>
</tr>
<tr>
<td>Biometric encryption</td>
<td>[25]</td>
<td>Cryptographic key</td>
<td>Filter and key link</td>
</tr>
<tr>
<td>Fuzzy vault</td>
<td>[26]</td>
<td>Hash of secret string</td>
<td>Point set P</td>
</tr>
<tr>
<td>Shielding functions</td>
<td>[27]</td>
<td>Hash of secret string</td>
<td>Authentication challenge W</td>
</tr>
<tr>
<td>Fuzzy extractors</td>
<td>[28]</td>
<td>Hash of secret string</td>
<td>Public string P</td>
</tr>
<tr>
<td>Extended PIR</td>
<td>[29]</td>
<td>Encrypted template</td>
<td>n/a</td>
</tr>
<tr>
<td>2D hexagonal quantization index modulation</td>
<td>[30]</td>
<td>Hash of a secret string</td>
<td>Quantization errors</td>
</tr>
<tr>
<td>Cancellable biometrics</td>
<td>[32]</td>
<td>Transformed template</td>
<td>Transform parameters</td>
</tr>
</tbody>
</table>

---

**References:**


Table C.1  Suggested add-ons to examples

<table>
<thead>
<tr>
<th>Method</th>
<th>Reference</th>
<th>PI</th>
<th>AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Robust Hashing</td>
<td>[1]</td>
<td>Hash of a robust binary string</td>
<td>One-way transformation</td>
</tr>
<tr>
<td>Short-lived cryptokey</td>
<td>[3]</td>
<td>Crypto-key</td>
<td>System parameters</td>
</tr>
<tr>
<td>Secure sketch</td>
<td>[5]</td>
<td>Quantization residue</td>
<td>Quantizer</td>
</tr>
<tr>
<td>Robust Minutiae Hash</td>
<td>[6]</td>
<td>Robust binary string for each minutia</td>
<td>Random diversification table</td>
</tr>
</tbody>
</table>

References

Current Status
- SC27 WG5 Redmond meeting addressed numerous comments - also from SC37
- Latest 2nd CD 24745
- Comments are due: April 8, 2010
Contact

Christoph Busch, Dr.-Ing.
Professor

P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no