Biometric Transaction Authentication Protocol (BTAP)

Christoph Busch

Fraunhofer IGD / Gjøvik University College / Hochschule Darmstadt
http://www.christoph-busch.de/

August 26, 2011
Sensitive Messages

Scenario: online banking / financial transactions

- Bilateral communication on a sensitive topic
- Risk to manipulate or replay messages

• The message: Order to transfer volume X from account Y to Z
Objective

Biometric Message Authentication

- **Person** authentication
  - Proof that a registered individual and **only** this subject has initiated a transaction/order

- **Data** authentication
  - the registered individual has viewed and **authorized** the transaction data
Why Biometrics?
Identity authentication can be achieved by:
Identity authentication can be achieved by:

- Something you **know**: Password, PIN, other secret
Why Biometrics?

Identity authentication can be achieved by:

- Something you **know**: Password, PIN, other secret
- Something you **own**: SmartCard, USB-token, key
Identity authentication can be achieved by:

- **Something you know:**
  Password, PIN, other secret

- **Something you own:**
  SmartCard, USB-token, key

- **Something you are**
  Body characteristics
Identity authentication can be achieved by:

- **Something you know:**
  Password, PIN, other secret

- **Something you own:**
  SmartCard, USB-token, key

- **Something you are**
  Body characteristics

Something you know or own, you may loose, forget or forward to someone else, with biometrics this is more difficult.
Identity authentication can be achieved by:

- **Something you know:**
  Password, PIN, other secret

- **Something you own:**
  SmartCard, USB-token, key

- **Something you are**
  Body characteristics

Something you know or own you may **loose, forget or forward** to someone else, with biometrics this is more difficult.

- security policy not violated by delegation
Why Biometrics?

Identity authentication can be achieved by:

- Something you **know**: Password, PIN, other secret
- Something you **own**: SmartCard, USB-token, key
- Something you **are**: Body characteristics

Something you know or own you may **loose, forget or forward** to someone else, with biometrics this is more difficult.

- security policy not violated by delegation
- non-repudiation of transactions
  „This transaction was initiated by Igor Popov, who was mis-using my card“
Risks in Biometric Systems

Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture
Risks in Biometric Systems

Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture
Risks in Biometric Systems

Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture
Risks in Biometric Systems

Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture
Gummi Fingers

S Korean fools finger printing system at Japan airport: reports

THU Jan 1, 2:57 pm ET

TOKYO (AFP) - A South Korean woman barred from entering Japan last year passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine, reports said Thursday.

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan, the Yomiuri Shimbun said.

The woman, who has a deportation record, told investigators that she placed special tapes on her fingers to pass through a fingerprint reader, according to Kyodo News.

Japan spent more than four billion yen (44 million dollars) to install the system, which reads the index fingerprints of visitors and instantly cross-checks them with a database of international fugitives and foreigners with deportation records, the Yomiuri Shimbun said.

Yahoo News of January 1st, 2009
The Finger Characteristic

Skin cross-section:

- epidermis: 0.03 – 0.15 mm
- dermis: 0.6 - 3 mm
- subcutaneous layer: 0.05 - 3 mm
Why Vein Recognition?

Expectations

- Good biometric performance
  - very few False-Rejects and False-Accept cases.

Vein recognition has reached product state

- Sony, Fujitsu, Hitachi, Techsphere, Morpho

Observed body parts

- Identifying the subcutaneous (beneath the skin) vein pattern
Fake Resistent Biometric Sensor

Capture devices for vein recognition

- Devices from Sony, Hitachi (finger) and Fujitsu, Techsphere (palm)
- Hybrid systems from Morpho (finger) and Fujitsu (hand)
Possible attacks on reference data

- **Cross-Comparison**: Identical template can establish unwanted links for one individual between several databases

- **Renewability**: The biometric characteristic can not be revised
  - Only 10 finger, 2 eyes, 1 face, ...
  - Once compromised, compromised for ever
  - For PW-based system you would expect renewal frequently (e.g. every 3 month)

- **Additional information**
  - almost for each biometric characteristic

**Is encryption of biometric references a sufficient level of protection?**
Hash Functions

Hashing the reference?

- Approach analog to UNIX Password authentication
- Public assessable file: /etc/passwd
  
  \[ \text{id:<login\_name>:hash(password)} \]

- Authentication:
  
  \[ \text{hash(input)} =?= \text{hash(password)} \]

\[\text{H(.)}\]

\[\text{H(x)}\]

simple

\[\text{close to impossible}\]
Challenges

Difference between passwords and biometric samples

\[ h(01000101) \text{ is not similar to } h(01010101) \]

- Biometric measurements are influenced by noise
- Cryptographic one way functions are (by purpose) extremely sensitive to smallest changes in the input data

Classical crypto hashing does not solve the problem either
Template Protection Scheme in ISO 24745
Template Protection Scheme in ISO 24745

Support for all biometric modalities

Feature extractor

Supplementary data

One-way function

Diversification

Bit extraction

Biometric sensor(s)

Shred

Pseudo Identifier

Auxiliary Data (Diversification Code)

ONE WAY

Support for all biometric modalities
Template Protection Scheme in ISO 24745

- Create features and discard biometric sample
- Supplementary data
  - Feature extractor
  - Biometric sensor(s)
  - Shred
  - One-way function
  - Diversification
  - Bit extraction
  - Pseudo Identifier
  - Auxiliary Data (Diversification Code)

ONE WAY

Create features and discard biometric sample
Template Protection Scheme in ISO 24745

Biometric sensor(s) → Feature extractor → Supplementary data → One-way function → Diversification → Bit extraction → Shred → Pseudo Identifier → Auxiliary Data (Diversification Code) → ONE WAY → Generate multiple binary derivatives
Template Protection Scheme in ISO 24745

Biometric sensor(s) → Feature extractor → Supplementary data

- One-way function
- Diversification
- Bit extraction

Shred

Pseudo Identifier

Auxiliary Data (Diversification Code)

Auxiliary data for generation of Pseudo Identifier
Template Protection Scheme in ISO 24745

Cryptographic one-way function with extra input

Pseudo Identifier

Supplementary data

Biometric sensor(s)

Feature extractor

One-way function

Diversification

Bit extraction

Auxiliary Data (Diversification Code)

Shred
Template Protection Scheme in ISO 24745

- Protected identifier verification string
- Pseudo Identifier
- Supplementary data
- One-way function
- Diversification
- Bit extraction
- Auxiliary Data (Diversification Code)
- Shred
Template Protection Scheme in ISO 24745
Biometric Transaction and Authentication Protocol (BTAP)
Financial Transactions

The relevant information in financial transactions:

• Which receiver account?
  - Receiver-Account-Number (RAN)

• What is the volume of the transaction?
  - Ordered Amount (ORA)

• From which sender account is the volume withdrawn?
  - Sender-Account-Number (SAN)

• Which natural person has initiated and confirmed the transaction data?
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:

- Client Computer
- Online Banking Server (OBS)
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

Client Computer

Banking Software (BSW)

Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

- Client Computer
- Banking Software (BSW)
- Biometric Transaction Device
- Online Banking Server (OBS)
Assumptions

For the Online-Banking-Scenario exists:
1.) A secure **Online-Banking-Server** (OBS)

- Communication with the Online-Banking-Software (BSW)
- Can recognize a Biometric Transaction Device (BTD) as reliable communication partner
- Implements the transactions
Assumptions (II)

For the Online-Banking-Scenario exists:

2.) An insecure customer PC hosting a standard unprotected **Online-Banking-Software** (BSW)

- The customer PC is exposed to trojanian horses, root-kits etc.
- The BSW communicates with the Online-Banking-Server (OBS) and transfers orders
  - Transaction-Order-Record (TOR) includes:
    - Transaction-Identifier (TID), Sender-Account-Number (SAN)
    - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Connected with the customer PC and the BSW is a trustworthy Biometric-Transaction-Device (BTD)
Assumptions (III)

For the Online-Banking-Scenario exists:
3.) A **secure** Biometric-Transaction-Device (BTD) which is quasi a **Biometric Secoder**

- Connected with the customer PC
- Trustworthy hardware, which has been evaluated according to Common Criteria
- Can not be manipulated by malware
- BTD can capture a biometric characteristic
- Can recognize a Online-Banking-Server (OBS) as reliable communication partner and can establish a communication with the OBS
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device** (BTD)

- Biometric samples of the customer are captured with BTD

Source: http://images.pennnet.com/articles/lfw/thm/th_121040.gif
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**
- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrollment

1.) Enrollment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**
- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions \((AD1)\) are stored
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**
   - Biometric samples are captured with BTD
   - Quantized binary vector generated from features
   - Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device** (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored

Recall Auxiliary Data (AD1): Bit-Indices = 0, 1, 2, 4, 5, 8, 11, 12
Transaction-Authentication-Protocol

BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored

Recall Auxiliary Data (AD1): Bit-Indices = 0,1,2,4,5,8,11,12
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and **relevant positions** (AD1) are stored

Recall Auxiliary Data (AD1): Bit-Indices = 0,1,2,4,5,8,11,12
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

- Biometrische samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
- Customer receives analog letter with PIN and enter these once

PIN-Letter
Deutsche Post
Lilli Muster
Online-Str. 5
99000 Bankfurt

Kartenummer: 123456
Karteninhaber: Lilli Muster

Online-Bank
Server-Allee-24
61004 Frankfurt
Mainin

Bankleitzahl: 500 703 40
Kontonummer: 4711

Transaction-Authentication-Protocol

{ 0,1,2,4,5,8,11,12 }
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**
- Biometrische samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions (AD1) are stored \(\{0,1,2,4,5,8,11,12\}\)
- Customer receives analog letter with PIN and enter these once

PIN = 4768 0569
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometrische samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions \((AD1)\) are stored\(\{0,1,2,4,5,8,11,12\}\)
- Customer receives analog letter with PIN and enter these once

**PIN-Letter**

Deutsche Post

Lilli Muster

Online-Str. 5

99000 Bankfurt

Online-Bank

Server-Alle-24

61004 Frankfurt Main

Bankleitzahl: 500 703 40

Kontonummer: 4711

Kartennummer: 123456

Karteninhaber: Lilli Muster

**PIN** = 4768 0569

**SBV** = 110101
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device** (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
- Postal PIN letter provides unique key
- Secret vector $CBV$ is generated from key with error correcting codec

\[ SBV = 110101 \]
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions \((AD1)\) are stored \(\{0, 1, 2, 4, 5, 8, 11, 12\}\)
- Postal PIN letter provides unique key
- Secret vector \(CBV\) is generated from key with error correcting codec

\[
SBV = 110101
\]

\[
110101 + 10
\]
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
- Postal PIN letter provides unique key
- Secret vector $CBV$ is generated from key with error correcting codec

$$SBV = 110101$$

$$110101 + 10$$
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
- Postal PIN letter provides unique key
- Secret vector $CBV$ is generated from key with error correcting codec

\[
SBV = 110101
\]

\[
110101 + 10 = CBV = 11010110
\]
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions (AD1) are stored \((0,1,2,4,5,8,11,12)\)
- Postal PIN letter provides unique key
- Secret vector \(CBV\) is generated
- Reduced binary vector \(RBV\) will be combined with the secret vector \(CBV\) with a XOR operation
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device** (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
- Postal PIN letter provides unique key
- Secret vector $CBV$ is generated
- Reduced binary vector $RBV$ will be combined with the secret vector $CBV$ with a XOR operation
BTAP - Enrolment

1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions (AD1) are stored \(\{0,1,2,4,5,8,11,12\}\)
- Postal PIN letter provides unique key
- Secret vectore \(CBV\) is generated
- Reduced binary vector \(RBV\) will be combined with the secret vector \(CBV\) with a \textbf{XOR} operation
**Transaction-Authentication-Protocol**

**BTAP - Enrolment**

1.) **Enrolment with Biometric Transaction Device (BTD)**
   - Biometric samples are captured with BTD
   - Quantized binary vector generated from features
   - Binary vector reduced down to reliable features ($RBV$) and relevant positions (AD1) are stored
   - Postal PIN letter provides unique key
   - Secret vector $CBV$ is generated
   - Reduced binary vector $RBV$ will be combined with the secret vector $CBV$ with a XOR operation

$RBV \quad 11001110$

$CBV \quad 11010110$

\[
\begin{array}{c}
11001110 \\
11010110
\end{array}
\]

\[
\begin{array}{c}
\text{XOR}
\end{array}
\]
BTAP - Enrolment
1.) Enrolment with **Biometric Transaction Device (BTD)**

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \((RBV)\) and relevant positions \((AD1)\) are stored
- Postal PIN letter provides unique key
- Secret vector \((CBV)\) is generated
- Reduced binary vector \((RBV)\) will be combined with the secret vector \((CBV)\) with a **XOR** operation

\[
\begin{align*}
\text{RBV} & \quad 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0 \\
\text{CBV} & \quad 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0 \\
\text{AD1} & \quad \{0,1,2,4,5,8,11,12\} \\
\end{align*}
\]

\[
\text{XOR} \quad 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\
\text{AD2} \quad 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0
\]
**Transaction-Authentication-Protocol**

**BTAP - Enrolment**

1.) Enrolment with **Biometric Transaction Device** (BTD)

- Biometric samples are captured with BTD
- Quantized binary vector generated from features
- Binary vector reduced down to reliable features \( (RBV) \) and relevant positions (AD1) are stored \( \{0,1,2,4,5,8,11,12\} \)
- Postal PIN letter provides unique key
- Secret vector \( CBV \) is generated
- Reduced binary vector \( RBV \) will be combined with the secret vector \( CBV \) with a XOR operation

\[
\begin{align*}
\text{RBV} & : 11001110 \\
\text{CBV} & : 11010110
\end{align*}
\]

\[
\begin{align*}
11001110 & \\
11010110 & \text{XOR} \\
00011000 & = AD2
\end{align*}
\]

- Auxilliary data \( AD1 \) and reference \( AD2 \) stored in BTD
BTAP - Enrolment

2.) Enrolment with **Online-Banking-Server (OBS)**

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$
  is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
BTAP - Enrolment

2.) Enrolment with **Online-Banking-Server** (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$
  is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
BTAP - Enrolment

2.) Enrolment with **Online-Banking-Server** (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$
  
  is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
BTAP - Enrolment

2.) Enrolment with Online-Banking-Server (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$
  is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
BTAP - Enrolment

2.) Enrolment with Online-Banking-Server (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$

  is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier
    according to ISO 24745
BTAP - Enrolment

2.) Enrolment with **Online-Banking-Server** (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$
  
  is stored with the customer record in the OBS-database

  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
BTAP - Enrolment

2.) Enrolment with Online-Banking-Server (OBS)

- Create a customer record with Account-Number (AN)
- Hash-value of secret key $SBV$ is stored with the customer record in the OBS-database
  - Hash-value corresponds to Pseudonymous-Identifier according to ISO 24745
Biometric Transaction and Verification
BTAP - Transaction

1. ) Operations of the Online-Banking-Software (BSW)

- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)

This TOR consist of:

- Transaction-Identifier (TID), Sender-Account-Number (SAN)
- Receiver-Account-Number (RAN), Ordered Amount (ORA)
Transaction-Verification

BTAP - Transaction

1. ) Operations of the Online-Banking-Software (BSW)

- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)

This TOR consist of:

- Transaction-Identifier (TID), Sender-Account-Number (SAN)
- Receiver-Account-Number (RAN), Ordered Amount (ORA)

- BSW transfers TOR to the Online-Banking-Server (OBS)
BTAP - Transaction

1. Operations of the Online-Banking-Software (BSW)
   - Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)

   This TOR consist of:
   - Transaction-Identifier (TID), Sender-Account-Number (SAN)
   - Receiver-Account-Number (RAN), Ordered Amount (ORA)

   ORA: 2.9 Mio EURO
   RAN:
   Bankleitzahl: 500 403 40
   Kontonummer: 4538

   BSW transfers TOR to the Online-Banking-Server (OBS)

   BSW transfers TOR to the Biometric-Transaction-Device (BTD) that is connected to the customer PC
BTAP - Transaction

2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)

- For approval of the intended transaction the customer
  - places his finger on the biometric sensor
  - and thus the BTD generates a probe sample
BTAP - Transaction

2. Operations of the Biometric-Transaction-Device (BTD)
   - The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
     - Receiver-Account-Number (RAN), Ordered Amount (ORA)
   - Approval of the intended transaction by probe sample
   - Auxiliary Data $AD1_{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
   - A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxiliary Data $AD1$
2. Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD_1 \{0,1,2,4,5,8,11,12\}$ is extracted from BTD-storage
- A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxilliary Data $AD_1$
BTAP - Transaction

2. Operations of the **Biometric-Transaction-Device (BTD)**
   - The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
     - Receiver-Account-Number (RAN), Ordered Amount (ORA)
   - Approval of the intended transaction by probe sample
   - Auxilliary Data \( AD_1 \{0,1,2,4,5,8,11,12\} \) is extracted from BTD-storage
   - A binarized fresh feature vector \( XBV \) is generated from probe \( XRV \) and the Auxilliary Data \( AD_1 \)
BTAP - Transaction

2. Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD1 \{0, 1, 2, 4, 5, 8, 11, 12\}$ is extracted from BTD-storage
- A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxilliary Data $AD1$
BTAP - Transaction

2. ) Operations of the **Biometric-Transaction-Device** (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD1\{0,1,2,4,5,8,11,12\}$ is extracted from BTD-storage
- A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxilliary Data $AD1$

Auxilliary Data ($AD1$): Bit-Indices = $0,1,2,4,5,8,11,12$
BTAP - Transaction

2. Operations of the Biometric-Transaction-Device (BTD)

- The relevant information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxiliary Data $AD1\{0,1,2,4,5,8,11,12\}$ is extracted from BTD-storage
- A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxiliary Data $AD1$

Auxiliary Data ($AD1$): Bit-Indices = 0,1,2,4,5,8,11,12
2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxiliary Data $AD1_{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
- A binarized fresh feature vector $XBV$ is generated from probe $XRV$ and the Auxiliary Data $AD1$

![Diagram showing the processing steps from probe to binarized feature vector]

Auxiliary Data ($AD1$): Bit-Indices = $0,1,2,4,5,8,11,12$
BTAP - Transaction

2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $A_{D1}^{(0,1,2,4,5,8,11,12)}$ is extracted from BTD-storage
- A binarized feature vector $XBV$ is reconstructed
- A secret vector $CBV'$ is reconstructed with XOR operation from the Auxilliary Data $A_{D2}$ that was stored in the BTD and from the binarized feature vector $XBV$
BTAP - Transaction

2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxiliary Data $AD\{0,1,2,4,5,8,11,12\}$ is extracted from BTD-storage
- A binarized feature vector $XBV$ is reconstructed
- A secret vector $CBV'$ is reconstructed
- The secret key $SBV'$ is freshly computed from $CBV'$

\[ SBV' = dec\ (CBV') \]
BTAP - Transaction

2. ) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD_{1}^{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
- A binarized feature vector $XBV$ is reconstructed
- A secret vector $CBV'$ is reconstructed
- The secret key $SBV'$ is freshly computed from $CBV'$
  \[ SBV' = \text{dec} (CBV') \]
BTAP - Transaction

2. Operations of the Biometric-Transaction-Device (BTD)

- The relevant information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)

- Approval of the intended transaction by probe sample

- Auxiliary Data $AD_1^{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage

- A binarized feature vector $XBV$ is reconstructed

- A secret vector $CBV'$ is reconstructed

- The secret key $SBV'$ is freshly computed from $CBV'$
  
  $SBV' = dec\ (CBV')$

\[\begin{array}{c}
\text{Transaction-Verification} \\
\text{BTAP - Transaction} \\
\text{2.) Operations of the Biometric-Transaction-Device (BTD)} \\
\bullet \text{The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:} \\
\hspace{1cm} - \text{Receiver-Account-Number (RAN), Ordered Amount (ORA)} \\
\bullet \text{Approval of the intended transaction by probe sample} \\
\bullet \text{Auxiliary Data } AD_1^{\{0,1,2,4,5,8,11,12\}} \text{ is extracted from BTD-storage} \\
\bullet \text{A binarized feature vector } XBV \hspace{1cm} 10001110 \text{ is reconstructed} \\
\bullet \text{A secret vector } CBV' \hspace{1cm} 10010110 \text{ is reconstructed} \\
\bullet \text{The secret key } SBV' \text{ is freshly computed from } CBV' \hspace{1cm} SBV' = dec\ (CBV') \\
\end{array}\]
BTAP - Transaction

2. Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxiliary Data $ADI_{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
- A binarized feature vector $XBV$ is reconstructed
- A secret vector $CBV'$ is reconstructed
- The secret key $SBV'$ is freshly computed from $CBV'$

$$SBV' = \text{dec}(CBV')$$
2.b) **Mirror-Operations of the BTD**

- A Transaction-Order-Seal (TOS') is computed
  - of the Transaction-Order-Record $TOR$
  - and the reconstructed secret key $SBV'$

\[
TOS' = MAC(h(TOR), PI') \\
PI' = h(SBV')
\]
2.b) **Mirror-Operations** of the BTD

- A Transaction-Order-Seal (TOS') is computed
  - of the Transaction-Order-Record \( \text{TOR} \)
  - and the reconstructed secret key \( \text{SBV'} \)

\[
\text{TOS'} = \text{MAC} (h(\text{TOR}), \text{PI'})
\]

\[
\text{PI'} = h(\text{SBV'})
\]
BTAP - Transaction

2.b) Mirror-Operations of the BTD

- A Transaction-Order-Seal (TOS') is computed
  - of the Transaction-Order-Record TOR
  - and the reconstructed secret key SBV'

\[ TOS' = MAC(h(TOR), PI') \]
\[ PI' = h(SBV') \]

- Implementation option with HMAC:
  \[ TOS' = h(PI' XOR OPAD, h(PI' XOR IPAD, TOR)) \]
2.b) **Mirror-Operations of the BTD**

- A Transaction-Order-Seal (TOS') is computed
  - of the Transaction-Order-Record \( TOR \)
  - and the reconstructed secret key \( SBV' \)

\[
TOS' = MAC(h(TOR), PI')
\]

\[
PI' = h(SBV')
\]

- Implementation option with HMAC:

\[
TOS' = h(PI' \ XOR \ OPAD, h(PI' \ XOR \ IPAD, TOR))
\]

- The seal (TOS') is transferred to the Online-Banking-Server
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

Client Computer

Banking Software (BSW)

Biometric Transaction Device

Online Banking Server (OBS)
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

- Client Computer
- Biometric Transaction Device
- Banking Software (BSW)
- Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:

- Client Computer
- Biometric Transaction Device
- Online Banking Server (OBS)
- Banking Software (BSW)
Elements in the Online-Banking-Scenario:

Client Computer

Banking Software (BSW)

Biometric Transaction Device

Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:

- Client Computer
- Biometric Transaction Device
- Banking Software (BSW)
- Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

Client Computer

Banking Software (BSW)

Biometric Transaction Device

Online Banking Server (OBS)
Elements in the Online-Banking-Scenario:

- Client Computer
- Banking Software (BSW)
- Online Banking Server (OBS)
- Biometric Transaction Device
Elements in the Online-Banking-Scenario:

- **Client Computer**
- **Banking Software (BSW)**
- **Online Banking Server (OBS)**
- **Biometric Transaction Device**
Elements in the Online-Banking-Scenario:

Client Computer

Banking Software (BSW)

Online Banking Server (OBS)

Transaction Device
Elements in the Online-Banking-Scenario:
Online-Banking-Scenario

Elements in the Online-Banking-Scenario:

- Client Computer
- Banking Software (BSW)
- Biometric Transaction Device
- Online Banking Server (OBS)
BTAP - Transaction

3. ) Operations of the Online-Banking-Server (OBS)

- Compares his own reconstruction of TOS with the delivered TOS ' from the BTD: 
  \[ TOS == TOS' \]

- The transaction is person- and data-authentic, if TOS and TOS' are identical.
Summary

The proposed data privacy friendly Biometric-Transaction-Authentication-Protocol provides

• a data-authentication and at the same time
  a person-authentication.

- Thus a strong link between the customer and the relevant information is established
- The bank can verify that a (authorized) natural person (individual) i approved the transaction.
Why use Biometrics for Online-Banking?
Why use Biometrics for Online-Banking?

The main threat is the automatisation of attacks
Why use Biometrics for Online-Banking?

The main threat is the automatisation of attacks

- A biometric authentication factor can prevent automated attacks.
Why use Biometrics for Online-Banking?

The main threat is the automatisation of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?
Why use Biometrics for Online-Banking?

The main threat is the *automatisation* of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!
Why use Biometrics for Online-Banking?

The main threat is the **automatisation** of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!
- The TAN-generator is currently the most secure protocol....
Why use Biometrics for Online-Banking?

The main threat is the *automatisation* of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!

- The TAN-generator is currently the most secure protocol....
Why use Biometrics for Online-Banking?

The main threat is the *automatisation* of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!
- The TAN-generator is currently the most secure protocol....
Why use Biometrics for Online-Banking?

The main threat is the automatisation of attacks

• A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

• TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!

• The TAN-generator is currently the most secure protocol....
Why use Biometrics for Online-Banking?

The main threat is the automatisation of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!
- The TAN-generator is currently the most secure protocol....
Why use Biometrics for Online-Banking?

The main threat is the *automatisation* of attacks

- A biometric authentication factor can prevent automated attacks..

But thats provided already with TAN-generators?

- TAN-generators / Chip-cards are lost frequently as it happens with other PDAs (mobile phones)!
- The TAN-generator is currently the most secure protocol....

... but one should always have an additional arrow in the quiver.
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