

Verification of Security Properties of a Biometric Authentication Protocol

Annie Salaiwarakul

Dr. Mark Ryan

Biometric Authentication

■ Advantages

- Uniqueness
- Non-transferable
- Authenticate the user
- Biometric objects cannot be stolen

■ Disadvantages

- Accuracy : False reject rate, False match rate and Fail to enrol rate
- Biometric features are unstable
- Violate user's privacy
- Loss of anonymity
- Biometric characteristic can be stolen

Biometric Authentication procedure

Enrollment:

Present Biometric



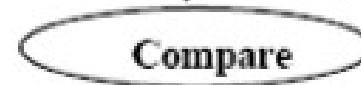
Process



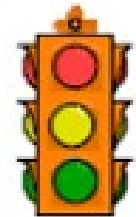
biometric code



Compare



No Match



Match

Verification:

Present Biometric



Process



biometric data



Biometric authentication Procedures

- Enrollment
 - The user's biometric code is stored
- Verification
 - The user's biometric data is read and compared with the stored data

Biometric Authentication Protocol

- Complement other methods of authentication e.g. password or smartcard.
- Guessable passwords / Transferable smartcards
- Biometric authentication promises a “non-transferability” property.

Range of Applications

- Logging into a local PC
- Passenger identification at a border control
- Authentication to a remote server in e-commerce transaction or on-line banking

Nature of Biometric data

- Biometric data is not secret, yet we should keep private as a matter of good practice.
- Biometric objects cannot be stolen, yet biometric data / characteristics can be.
- Biometric data could not be changed or replaced.

Review of [CPV02]

- Liqun Chen, Siani Pearson and Athnnsions Vamvakas, 2002
“A Trusted Biometric System”

Review of [CPV02]

- 3 components connected together
 - Smart Card (SC), Trusted Platform Module (TPM) and Trusted Biometric Reader (TBR)
 - SC is used for storing credential data such as biometric code or user's signature
 - TPM is inside TCP. It provides security functions e.g. platform integrity check and provide protected storage.
 - TCP (Trusted Computing Platform) – maintains privacy, provides protection against theft and misuse of secrets held on the platform.
 - TBR is a trusted biometric reader

Review of [CPV02]

- SC has to check the integrity metric of TPM and TBR
- The integrity metric – A challenger checks the appropriateness of the measurement processes and compares the supplied results of measurements (called integrity metrics) with the expected value.
- The SC is able to show a user the result of integrity checking e.g. by displaying a special image or value known only to the user.

[MSC]

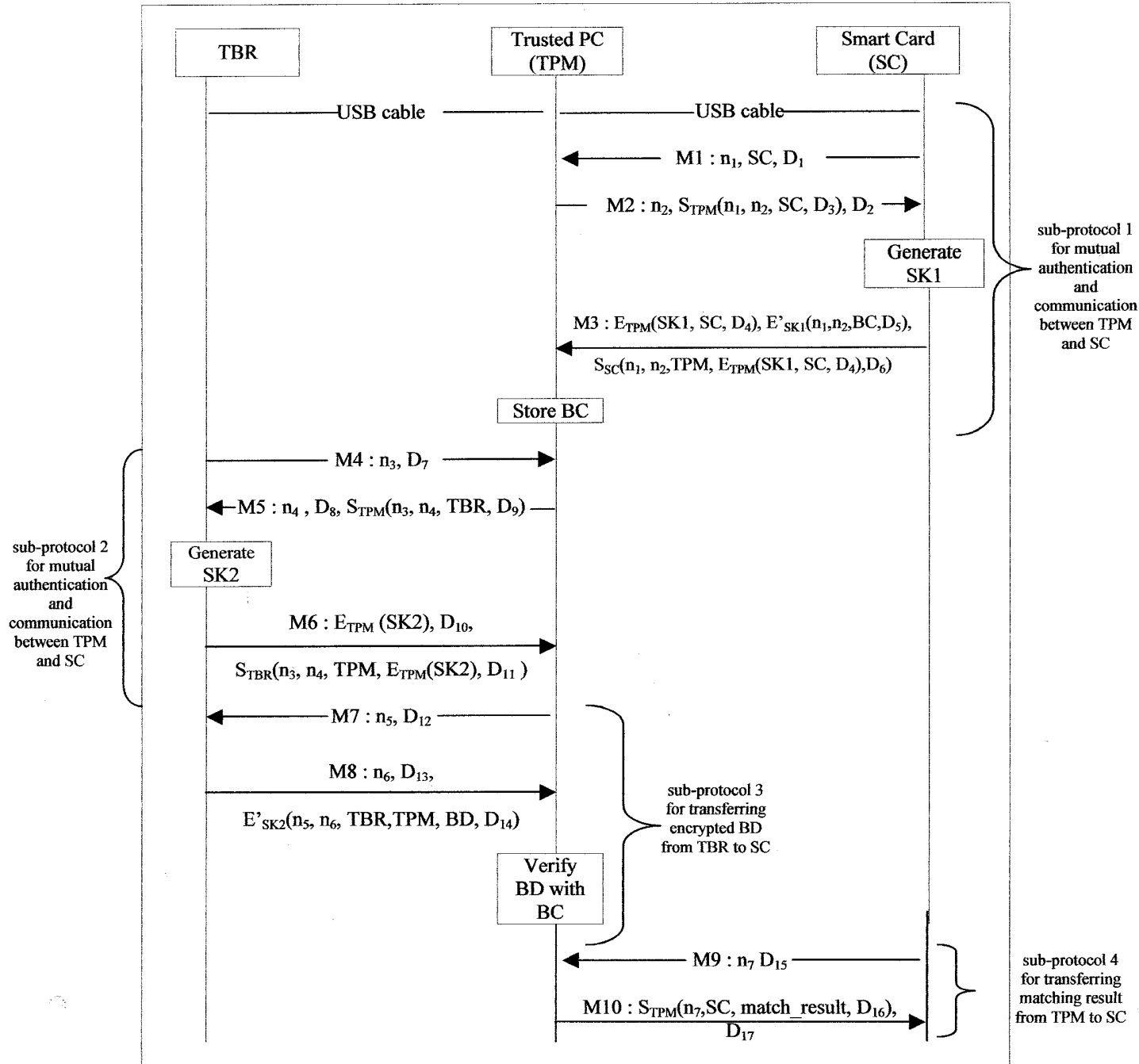


Figure 1 Message sequence chart of [CPV02]

Review of [CPV02]

- There are 4 sub-protocols run concurrently.
- Mutual authentication and communication between TPM and SC
- Mutual authentication and communication between TPM and TBR
- Sending biometric data from TBR to TPM
- Sending a matching result from TPM to SC

Properties

- Effectiveness
 - *The accessed TP is not given either the BC or BD until the integrity of both the TP and TBR is checked by the SC*
- Secrecy of BC and BD
 - *An attacker that listens to message on the SC/TP interface and the TBR/TP interface cannot obtain BD and BC*
- Correctness of BR
 - *The TBR is not given the BD until the user is convinced about the correctness of both TP and TBR integrity checking*

Checking “Effectiveness” property

```
(* M2 *)  
in(c,(nx2,m1,=certificateTPM));  
let(=n1,=nx2,=hostSC,imy)= checksign(m1,pkTPM) in  
if imy <> imtpm then 0  
else  
  event tpmChecked();
```

```
query ev: tpmgetBD() ==> ev: tpmChecked() && ev: tbrChecked().  
query ev: tpmgetBC() ==> ev: tpmChecked() && ev: tbrChecked().
```

```
(* M3 *)  
in(c,(m2,m3,m4));  
let (SK1,=hostSC,=empty) = dec(m2,skTPM) in  
let(=nx1,=n2,BC,=imsc) = sdec(m3,SK1) in  
let(=nx1,=n2,=hostTPM,m5,=scP1run) = checksign(m4,pkSC) in  
let(=SK1,=hostSC,=empty) = dec(m5,skTPM) in  
  
event tpmgetBC();
```

```
(* M4 *)  
in(c,(nx3,imx));  
if imx <> imtbr then 0  
else  
  event tbrChecked();
```

```
(* M8 *)  
in(c,(nx6,=certificateTBR,m10));  
let(=n5,=nx6,=hostTBR,=hostTPM,BD,=imtbr) = sdec(m10,SK2) in  
  
event tpmgetBD().
```

[MSC]

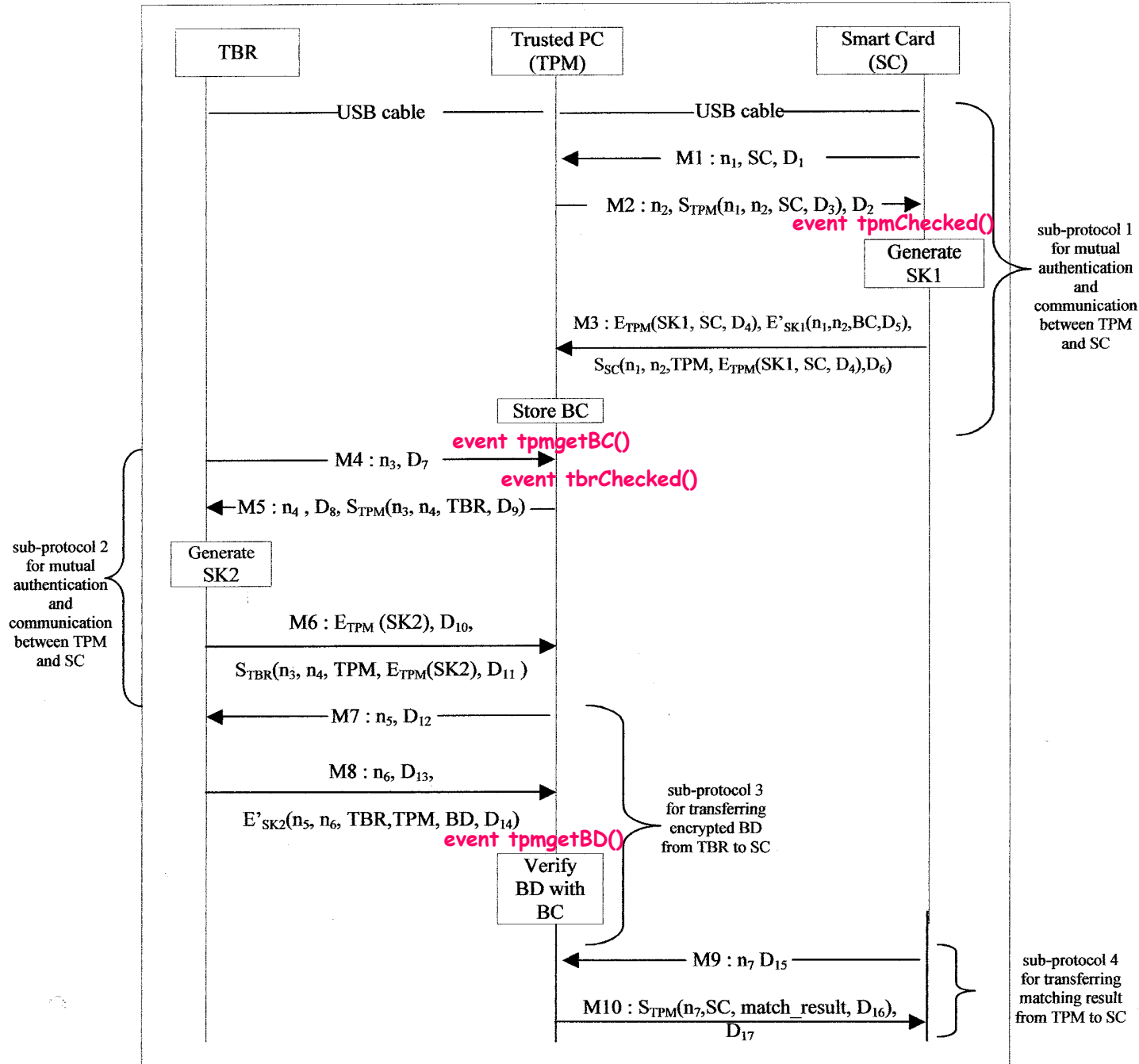


Figure 1 Message sequence chart of [CPV02]

Result

■ Effectiveness

RESULT ev:tpmgetBC() ==> (ev:tmpChekced() & ev:tbrChecked()) is true
RESULT ev:tpmgetBD() ==> (ev:tmpChekced() & ev:tbrChecked()) is true

Checking “Secrecy of BD and BC” property

query attacker : BC.
query attacker : BD.

■ Result

RESULT not attacker : BD[...,...] is true

RESULT not attacker : BC[] is true

Checking “Correctness of BR” property

- We cannot model the user in Proverif because we cannot predict the user’s behaviour, what she thinks and what she wants to do. Hence, we assume that if she gives her fingerprint, she is convinced that the CP and BR integrity is correct.

Future Work

- Formalize one more case study, [WSE04]
- Generic Platform for biometric authentication protocol
 - General & specific security properties
 - Requirements for biometric authentication protocol