A Trusted Biometric System

**L. Chen, S. Pearson, A. Vamvakas,
'A Trusted Biometric System',
Technical Report HPL-2002-185, HP Laboratories Bristol,
12 pp., 2002**

Paul Schmieder

University of Auckland

21. September 2007

Outline

Functioning

how does it work?

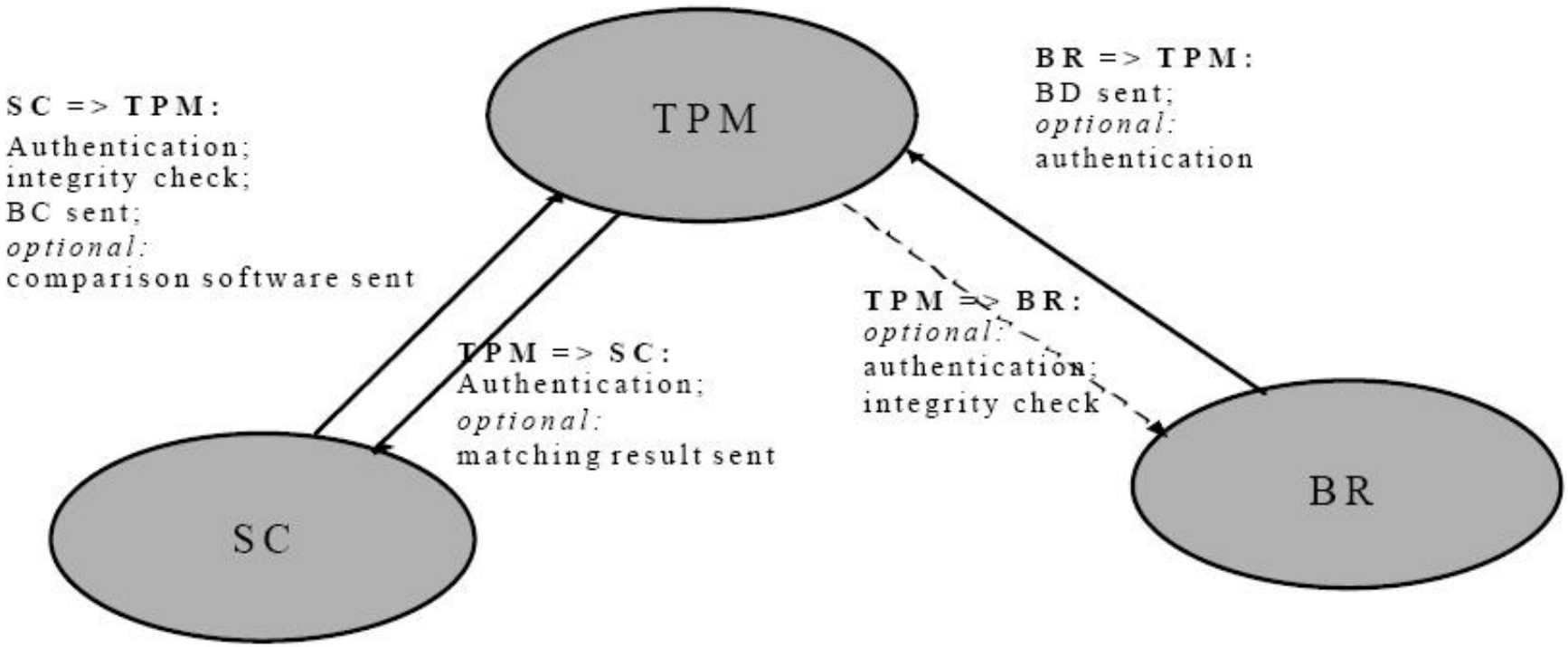
- usage of a hardware-based tamper-resistant trusted chain
- consists of Trusted Platforms, Trusted Biometric Readers and Smart Cards
- different from other systems because of combination of user authentication with entity integrity checking

Threads

Threads

- malicious platform
- malicious biometric reader
- interception of communication between platform and biometric reader
- interception of communication between smart card and platform

Overview


TPM
SC
BR
SC => TPM:
Authentication;
integrity check;
BC sent;
optional:
comparison software sent
TPM => SC:
Authentication;
optional:
matching result sent
BR => TPM:
BD sent;
optional:
authentication
TPM => BR:
optional:
authentication;
integrity check

Appreciative comments

advantage of integrity check

- secure feature to check the status of devices
- fairly simple to implement

introduced mechanismn

- provide possible implementation

Appreciative comments

advantage of integrity check

- secure feature to check the status of devices
- fairly simple to implement

introduced mechanismn

- provide possible implementation

Appreciative comments

advantage of integrity check

- secure feature to check the status of devices
- fairly simple to implement

introduced mechanismn

- provide possible implementation

Critical comments I

authentication process

- attempt to verify the digital identity of the sender (wikipedia)
- authentification between every entity
- not explained how

opens new security vulnerability

- different PCs + TPRs = different checksums
- bunch of checksums hold by Smart Card
- increased possibility of "false positive match"

Critical comments I

authentication process

- attempt to verify the digital identity of the sender (wikipedia)
- authentification between every entity
- not explained how

opens new security vulnerability

- different PCs + TPRs = different checksums
- bunch of checksums hold by Smart Card
- increased possibility of "false positive match"

Critical comments I

authentication process

- attempt to verify the digital identity of the sender (wikipedia)
- authentification between every entity
- not explained how

opens new security vulnerability

- different PCs + TPRs = different checksums
- bunch of checksums hold by Smart Card
- increased possibility of "false positive match"

Critical comments I

authentication process

- attempt to verify the digital identity of the sender (wikipedia)
- authentification between every entity
- not explained how

opens new security vulnerability

- different PCs + TPRs = different checksums
- bunch of checksums hold by Smart Card
- increased possibility of "false positive match"

Critical comments II

feasibility with Smart Card

- holds information; e.g. biometric code, keys
- how inform user about 'failure'
- special value only know by the user

Do you think displaying a special value or picture is a good method to indicate whether the system is trusted?

Or do you maybe have an even better idea?

State of art of biometric recognition systems

Measurements of biometric recognition systems

- false accept rate (FAR) - probability of positive match between not identical datasets
- false reject rate (FRR) - probability of negative match between identical dataset

Biometrics	FAR	FRR	Subjects	Comment
Face	1 %	10 %	37437	Varied lighting, indoor/outdoor
Fingerprint	1 %	0.1 %	25000	US Government operational data
Hand geometry	2 %	0.1 %	129	With rings and improper placement
Iris	0.94 %	0.99 %	1224	Indoor environment
Iris	0.0001 %	0.2 %	132	Best conditions
Keystrokes	7 %	0.1 %	15	During 6 months period
Voice	2 %	10 %	310	Text independent, multilingual

tamper-resistant

tamper-resistant

- being protected against deliberate application altering

smart card checks integrity

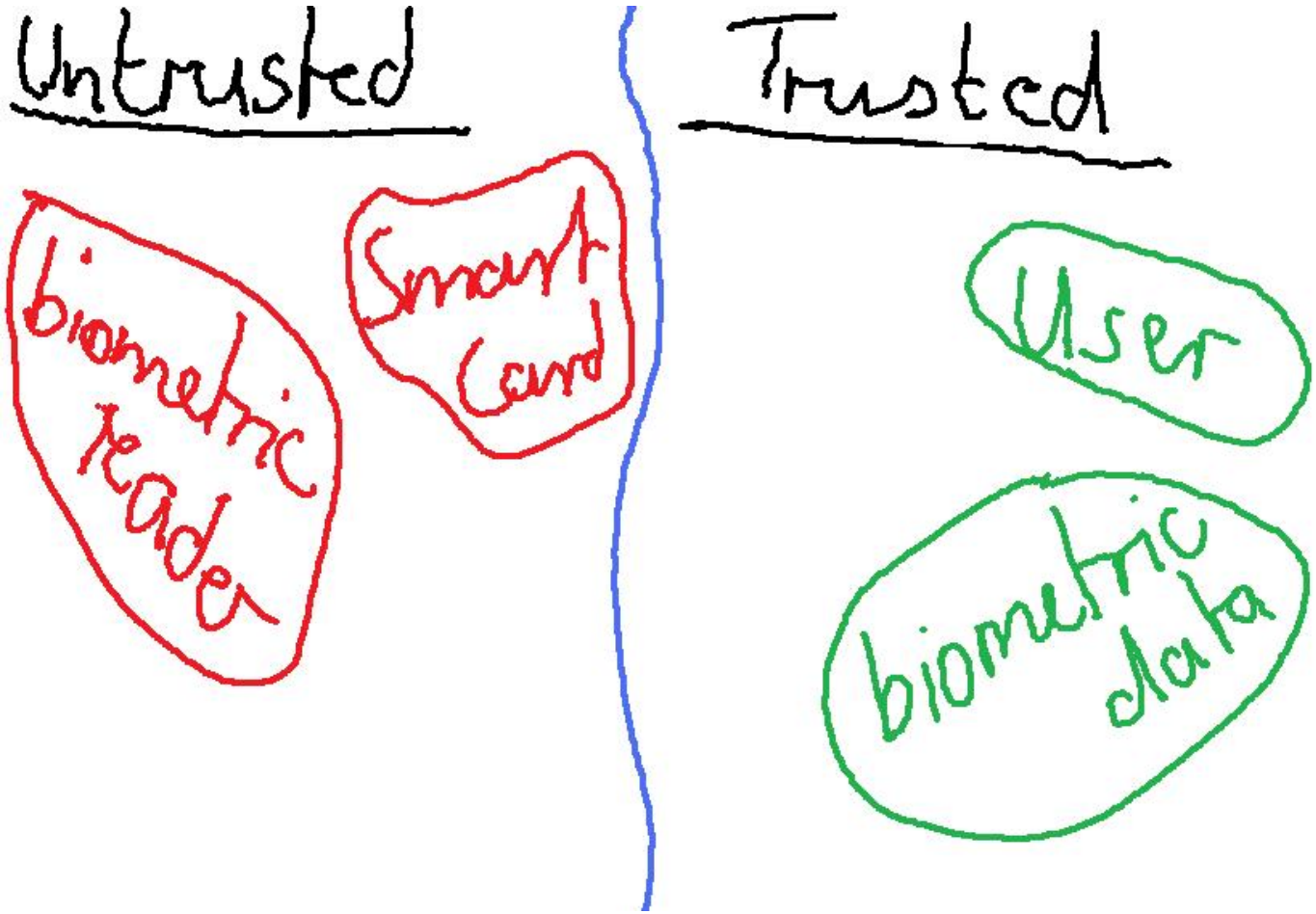
integrity check

- integrity value of software is generated (checksum or message footprint)
- generated integrity value is compared with the stored integrity value

way of checking

- communication protocol includes interrogation of BR and TPM integrity status
- based on public key infrastructure and symmetric cryptographic

Trustness


Untrusted
Trusted
biometric reader
Smart card
User
biometric data

plastic cards

my necessary card collection

- University of Auckland
- UoA Access Card third floor
- UoA Access Card fourth floor
- flat access
- bus
- driver license
- VISA
- Eftpos

plastic cards

my useful card collection

- SubCard (Subways)
- one Card (Foodtown)
- GoCall Telephone
- AA member
- German EC
- BBH