Research Paper Computer Science

SBMOC - Secure Biometric Match-on-Card

* Jitendra P. Radadiya ** Dr. Dhaval Kathiriya

* Professor, Research Scholor of C.M.J. University shilong, Meghalaya

** Research Guide in computer science, C.M.J. University, Meghalaya

ABSTRACT

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity is needed to make sound access control decisions. A wide range of mechanisms are employed to authenticate identity, utilizing various classes of identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper or other non- automated, hand-carried credentials, such as driver's licenses and badges.

Keywords: cryptographic,authorization,fingerprint , mechanism,RSA,PIV, terminal, card

The PIV standard describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in NIST Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.

The PIV card as of today is a contact smart card with the following mandatory elements in the electronic chip:

- PIN code (the user always have to enter his PIN code to activate the card)
- Card Holder Unique ID (CHUID)
- Authentication data (one asymmetric key pair and corresponding certificate, using 1024- bit RSA and ECDSA)
- Two fingerprints

Depending on the sensitivity of the application, three security levels are defined:

- Some Confidence: only reads CHUID (what-you-have + what-you-know)
- High Confidence: fingerprint (one finger) authentication in unattended environment (what- you-have + what-you-know + what-you-are: three-factor)
- Very High Confidence: fingerprint (one finger) authentication in attended environment + PKI authentication (three-factor + cryptography)

Biometrics Implementation

Two fingerprint templates are stored on the PIV card. These templates must be compliant to ANSI INCITS 378 minutiae format (6 bytes per minutiae) and are readable upon authentication request to process the fingerprint comparison on the terminal side. The native scanning resolution of the device shall be 197 pixels per centimeter (classical 500 pixels per inch) in both the horizontal and vertical directions. The system will preferably use index fingers or thumbs and ANSI minutiae templates are prepared from images of the primary and secondary fingers. In order to improve the security level, the system may optionally request the authentication of both the primary and secondary fingers. A facial image (printed on the card body) is also digitally stored in the electronic chip for further reading and human-eye comparison between printed and stored images, no purpose of automated facial recognition here (for the moment).

Cryptography Implementation

PIV relies on US FIPS201 standards. FIPS201 employs cryptographic mechanisms to authenticate cardholders, secure information stored on the PIV Card, and secure the supporting infrastructure. FIPS201 and its supporting documents specify a suite of keys to be stored on the PIV Card for personal identity verification, digital signature generation, and key management. The PIV cryptographic keys specified in FIPS201 are:

- The asymmetric PIV authentication key, mandatory (RSA1024)
- A card authentication key for symmetric challenge-response, optional (2TDEA, CBC mode)
- An asymmetric digital signature key for signing documents and messages, optional (RSA1024)
- An asymmetric key management key, supporting key establishment or key transport, optional (RSA1024)
- A card management key to support card personalization and post-issuance updates, optional (2TDEA, CBC mode)

Cryptographically protected objects specified in FIPS201 include:

- The X.509 certificates for each asymmetric key on the PIV Card (RSA1024)
- A digitally signed Cardholder Unique Identifier (SHA1 + RSA1024)
- Digitally signed biometric data (SHA1 + RSA1024)
- The Security Object, which is a digitally signed (RSA1024) hash table (SHA1) of all stored data

Security Framework

Currently, FIPS 201 permits biometric data to be released only across the contact interface of a PIV Card, and only after activation of the PIV Card through presentation of the cardholder's PIN. These restrictions achieve two security objectives: communication of biometric data occurs only over a trusted communication channel that is not easily subject to eavesdropping attacks (namely, the wired contacts inside the smart card reader); and the PIV cardholder implicitly attests to the legitimacy of the smart card reader, as they indicate by entering the PIN on the smart card reader keypad. FIPS 201 enables biometric authentication to occur with- out im8posing a technical requirement for automatic authentication of smart card readers to PIV Cards. Such a requirement, it was believed, would add unacceptable key management costs (the PIV fingerprint object is digitally signed, and the signature can be used to verify authenticity and integrity of the data). This feasibility study evaluated the impact of contactless smart card, Match-on-Card and secure protocol on transaction performance, when the protocol meets these security objectives (SO):

- SO1: communication of biometric data shall occur only over a trusted channel that is not susceptible to eavesdropping attacks in the reader-to-card direction, nor spoofing or replay attacks in the card-to-reader direction
- SO2: communication of biometric data between the smart card and smart card reader shall occur only after the cardholder has indicated the reader is legitimate
- SO3: communication of biometric data from the smart card to the reader shall occur only after the cardholder has entered their PIN
- SO4: the approach should achieve the preceding security objectives without reader-to- smart-card authentication or associated key management infrastructure

These security objectives are aligned with the high-level security objectives of FIPS 201. They protect both the integrity of the biometric authentication transaction and the privacy of the cardholder's biometric data, whereas avoiding the potential cost of reader authentication key management.

Figure 1 depicts the basic principle of SBMOC: (1) establish a secure session, (2) smart card receives candidate template and process comparison and (3) smart card sends the signed OK/NOK decision.

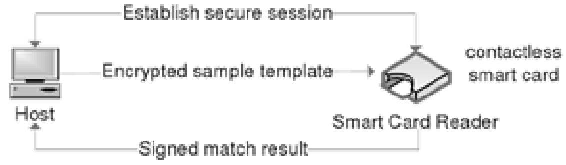

Figure 1: SBMOC principle

Our Protocol:

The main challenge here is to overcome the problem of potential, and easy, Man-in-the-middle attack or replay attack inherent to contactless communication, whereas the current generation of PIV Cards bases its security against these threats on the difficulty to discreetly probe the card's contacts. We proposed the use of a card's asymmetric key pair to process card authentication and to agree on two session symmetric keys for biometric data encryption and MACed decision. Figure 2 summarizes the exchange of commands between the user/reader and the card. It describes in sequence (from 1 to 10) the command exchanges (in/out) and the main security data associated. On the left part of the figure, are described the internal reader processes during the authentication protocol. The card internal processes are described on the right part of the figure:

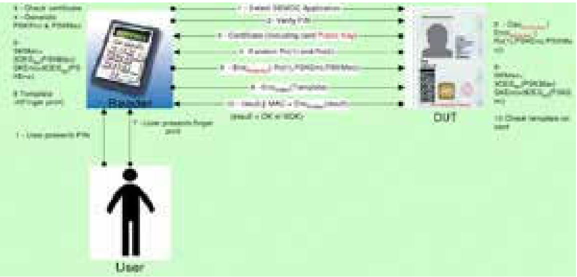

Figure 2: SBMOC framework

Table 1 summarizes the analysis of the authentication protocol against the NIST security objectives:

*visual authentication only, by the user accepting to enter the PIN code

Objective ID	Objective description	Sequence(s) that answer the objective
SO1	Eavesdropping attacks Eavesdropping attacks Replay attacks	Sequences 5, 9 Sequences 4 to 9 Sequences 3 to 10
SO2	Reader is legitimated before biometric data transmission	Sequence 2*
SO3	PIN is verified before biometric data transmission	Sequence 2
SO4	No reader authentication and key management	Full protocol

Table 1: Our protocol vs NIST Security Objectives

Our Implementation on Smart Card

For the smart card implementation of our protocol we used on-board key pair generation and the following APDU commands:

- Select SBMOC applet
- – This command is used to select the SBMOC application with a multi-application java card.
- Verify PIN
- – This command is used to verify the PIN code.
- Read RSA Public Key
- – This command is used to retrieve the RSA public key from the Smart Card.
- Write X509 Certificate
- – This command is used to write the X509 certificate in the Smart Card.
- Enroll Biometric Data
- – This command is used to enroll biometric data, i.e. the reference fingerprint template
- Read X509 Certificate.
- – This command is used to retrieve the X509 Certificate from the Smart Card
- Get Challenge.
- – This command is used to receive a 24-Byte random (8-Byte Rc1, 16-Byte Rc2) generated by the Smart Card.
- Send External Challenge
- – This command is used to send two 16-byte random PSKenc and PSKmac in the Smart Card to compute two 128-bit symmetric session keys for encryption and MAC.
- Verify Biometric Data
- – This command is used to verify biometric data, i.e. compare the reference fingerprint template VS the deciphered candidate fingerprint template and send MACed decision.

Once delivered to the NIST with previously seen commands, each smart card must be activated and personalized before the testing campaign. This splits on two phases: (1) initialization and (2) testing campaign.

Here is the card initialization process (done once at card delivery):

- Terminal: selects SBMOC applet
- Card: requests PIN verification
- Card: on-board RSA key pair generation
- Terminal: reads RSA public key and generate the X509 certificate
- Terminal: writes X509 certificate within the card
- Terminal: captures reference fingerprint and writes the reference template within the card

This process consumes about 20s to 30s because of the on-board key pair generation.

Here is a user authentication process (normal use during card lifecycle):

- Terminal: selects SBMOC applet
- Card: requests PIN verification
- Terminal: reads X509 certificate within the card
- Terminal: gets challenge from the card
- Terminal: sends challenge to the card
- Terminal & Card: compute session keys
- Terminal: captures candidate fingerprint, sends encrypted candidate template
- Card: decrypts candidate template, compares, sends decision
- Terminal: verifies decision and MAC

Conclusion : Our contribution was both the proposal of the SBMOC protocol and its implementation in a contactless smart card chip. For technical reasons we were obliged to use ANSI minutiae for- mat instead of ISO minutiae format in our available smart cards, this justifies our not so good timing results because of the in-card need to decipher double-sized data. This is particularly sensible with RSA1024 cards, however we fully enter in the timing specifications. As for our protocol, NIST didn't disclose other three competitors approaches of the secure protocol; a different protocol may also justify differences in timing results.

REFERENCES

[1] ANSI INCITS 378. Information technology - Finger Minutiae Format for Data Inter- change, 2004. | [2] A. Antonelli, Raffaele Cappelli, Dario Maio, and Davide Maltoni. A new approach to fake finger detection based on skin distortion. In Zhang and Jain [136], pages 221–228. | [3] Fingerprint Duplication Archive. How to duplicate your fingerprints. http://www.journalofaestheticsandprotest.org/4/fingerprint/fingerprint.pdf [last access on | 2008/06/15]. | [4] ASFIP. Attack standardization for fingerprint system certification. https://tokyo.emse.fr/trac/asfip/ [last access on 2009/09/10]. | [5] Julian Ashbourn. Practical Biometrics - From Aspiration to Implementation. Springer,2004. | [6] Multiples authors. Biometric evaluation methodology supplement. Technical report, Common Criteria, 2002. | [7] Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni. Fake fingerprint detection by odor analysis. In Zhang and Jain [136], pages 265–272. | [8] Claude Barral, Jean-Sébastien Coron, and David Naccache. Externalized fingerprint matching. In Zhang and Jain [135], pages 309–315. | [9] Claude Barral and Assia Tria. Fake fingers in fingerprint recognition: Glycerin super- sedes gelatin. In Cortier and et al. [28], pages 57–69. | [10] Claude Barral and Serge Vaudenay. A protection scheme for moc-enabled smart cards. | IEEE - Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the, 2006. | [11] G. Bebis, T. Deaconu, and M. Georgiopoulos. Fingerprint identification using delaunay triangulation. In Information Intelligence and Systems, 1999. Proceedings. 1999 Inter- national Conference on, pages 452–459, 1999. | [12] Bir Bhanu and Xuejun Tan. Fingerprint indexing based on novel features of minutiae triplets. IEEE Trans. Pattern Anal. Mach. Intell., 25(5):616–622, 2003.