BIOMETRIC AUTHENTICATION OBJECTS FOR ACCESS CONTROL[1]

Phillip H. Griffin

phil@phillipgriffin.com
Griffin Information Security Consulting, Raleigh, North Carolina (United States)

Abstract

An individual can be identified using a *something-you-are* authentication factor by matching their biometric sample to a previously stored biometric reference template. The value of a unique index field in a matched template indirectly identifies that individual. A physical object tagged with a radio frequency identifier can be uniquely identified. When a tagged physical object is associated with the biometric reference template of an individual, the individual can use that object as a *something-you-have* authentication factor. Trusted person-object associations establish biometric authentication objects. These biometric-enabled tagged objects can be used by relying parties to inform authentication decisions in access control and privilege management systems. Biometric authentication objects allow the creation of low cost, multi-factor authentication systems that are convenient for people to use. Systems based on biometric authentication objects do not require the use of individual security tokens and digital certificates.

Keywords: access control, ASN.1, authentication, biometrics, RFID, signcryption.

ASSOCIATIONS

Person-object identifiers can be associated by simply placing them together in a file or in a database row. To form a trusted person-object association, the value of a radio frequency identification (RFID) tag can be cryptographically bound to a biometric reference template identifier using digital signature or signcryption techniques based on a public key infrastructure [1]. Signcryption is a hybrid cryptographic primitive that both signs and encrypts information efficiently in a single operation to provide confidentiality, data integrity, and origin authenticity [2]. The cryptographic binding that associates a person with an object under a digital signature can include roles and other attributes that confer rights and privileges (e.g., object owner, lessee, privacy policy, etc.). Information security management attributes may also be included, such as the number of authentication factors required for access, the number of biometric match attempts allowed, or time of day usage restrictions.

Biometric authentication objects have the potential for use in access control solutions that are less expensive to implement than solutions that rely on the use of digital certificates and hardware security tokens issued to each user. Current research seeks to define data and security architectures for a convenient, inexpensive multi-factor authentication system for access control based on the recent U.S. patent 8,289,135 *Associating a Biometric Reference Template with a Radio Frequency Identification Tag* [3].

SCHEMA

International standardization of a cryptographic message syntax (CMS) schema for digital signatures and encryption has been proposed recently for the protection of biometric and other sensitive information when in transit and at rest [4]. This schema can protect and bind person-object associations and attributes. The proposal includes definition of a new *SigncryptedData* cryptographic message type to support signcryption key management techniques [5].

[1] Accepted by Future Security 2013, 8th Security Research Conference, Berlin, September 17th-19th, 2013

A schema for the association of a biometric reference template to a list of one or more RFIDs can be defined using Abstract Syntax Notation One (ASN.1) [6] as follows:

```
SimpleAssociation ::= SEQUENCE {
   individual       BiometricTemplateID,
   physicalObjects  RFIDs
}

BiometricTemplateID ::= OCTET STRING

RFIDs ::= SEQUENCE (1..MAX) OF RFID

RFID ::= OCTET STRING
```

To create a trusted biometric authentication object, a value of type *SimpleAssociation*, along with any attributes, would be signed in a value of ASN.1 type *SignedData* or both signed and encrypted in a value of type *SigncryptedData*.

IMPLEMENTATION

The goal of current research is to create a security context that provides the benefits of multi-factor authentication while eliminating the need for an individual to possess, transport, or interact with an assigned security token or digital certificate. To implement such a system, when a user enrols in a biometric system, a uniquely identifiable biometric reference template is created from their biometric samples and stored in a template database for subsequent matching. The user's template identifier is then associated with one or more RFID tag values of physical objects that the user is authorized to access, such as a device, the doors of a building, or a vehicle.

In order to access a biometric authentication object, a user provides a biometric sample. The sample is used to create biometric match data. This match data, along with the RFID tag value of an object are presented to a decision engine that determines whether access should be granted. If the user can be matched to a stored biometric reference template, and the matched template identifier is found to be associated with the provided RFID value, then user access may be granted. Otherwise, access is denied, perhaps even following a successful biometric match. Attributes that are bound to a person-object association may also influence the outcome of an access control decision.

REFERENCES

[1] International Organization for Standardization / International Electrotechnical Commission. (2011). ISO/IEC 29150 Information technology – Security techniques – Signcryption.

[2] Dent, Alexander W. (2004). Hybrid Cryptography, Cryptology ePrint Archive Report 2004/210. Retrieved May 29, 2013, from http://www.signcryption.org/ publications/pdffiles/Dent-survey-eprint-04-210.pdf.

[3] Griffin, P. (2012). U.S. Patent No. 8,289,135. Washington, DC: U.S. Retrieved May 29, 2013, from http://www.google.com/patents/US8289135

[4] Griffin, P. (2013). Telebiometric Security and Safety Management. Proceedings of ITU Kaleidoscope 2013 Conference – Building Sustainable Communities. Retrieved May 29, 2013, from http://www.itu.int/en/ITU-T/academia/kaleidoscope/2013/.

[5] Griffin, Phillip H., Protecting Biometrics Using Signcryption. Proceedings of ID360: The Global Forum on Identity, the Center for Identity, University of Texas at Austin, 2012. Retrieved May 29, 2013, from http://phillipgriffin.com/innovation.htm#ID3602.

[6] Larmouth, John, *ASN.1 complete*. San Francisco: Morgan Kaufmann Publishers, 2000. Retrieved May 29, 2013, from http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf