Signcryption for Biometric Security

By Phillip H. Griffin, CISM

Biometrics is the "something you are" identity factor used in authentication and identification systems. Organizations that rely on biometric technology should ensure the confidentiality, integrity and authenticity of their biometric assets. To manage security risk, biometric information should be protected from unauthorized access and modification.

Biometric assets should be protected while at rest and during transfer, both within the firewall perimeter and across public networks such as the internet. A signcryption cryptographic operation protects information with a digital signature and encryption. Signcryption can be used to manage security risk and to provide assurance of the confidentiality, integrity and authenticity of biometric information.

Signcryption is a relatively new cryptographic primitive, standardized last year as ISO/IEC 29150 [1]. Signcryption uses "an asymmetric encryption scheme and a digital signature scheme combined in a specific way", along with "a specially developed algorithm" [1] to perform both encryption and digital signature functions simultaneously. This efficient cryptographic technique provides data integrity, origin authentication, and data confidentiality in a single operation.

Hybrid Cryptographic Primitives

The signcryption primitive is a hybrid cryptographic primitive. Hybrid cryptography is that "branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystems". These problems include those encountered securing large iris scan, DNA, or fingerprint sets that require systems "to process long messages quickly" [2].

Though signcryption was only approved recently as an international security standard, hybrid cryptography is not a new technology. Authenticated encryption is a family of familiar hybrid cryptographic techniques commonly used to secure network communications. These techniques use "a shared-key based transform" that relies on a symmetric encryption scheme "to provide both privacy and integrity" [3]. Signcryption can be considered the asymmetric analog of authenticated encryption.

The Transport Layer of the Secure Shell protocol (SSH), some versions of the Secure Sockets Layer (SSL) protocol, and the Encapsulating Security Payload (ESP) protocol are all based on authenticated encryption methods. These protocols use the "Encrypt-and-MAC (E&M)", "MAC-then-encrypt (MtE)", and "Encrypt-then-MAC (EtM)" [3] authenticated encryption methods to "provide privacy and reliability" [4] services or "confidentiality, data origin authentication", and connectionless integrity [5].

These hybrid cryptographic methods are based on symmetric key encryption. Since "symmetric encryption schemes and MAC algorithms" rely on shared key, symmetric approaches to provide their security services, non-repudiation is not possible [2]. Since signcryption uses an asymmetric approach, several signcryption schemes can provide non-repudiation. However, until recently no standardized signcryption message schema could be used to manage biometric information security and protect biometric data.

Protecting Biometrics

This past April, a new signcryption message schema and processing protocol was presented to the ID360 Global Forum on Identity at the Center for Identity at the University of Texas, Austin. In a poster session, Protecting Biometrics Using Signcryption [6], a signcryption cryptographic message schema was defined. Three modes of processing were described, including one to support signcryption of selected components of a biometric transaction or reference template. The paper proposed standardization of a new cryptographic message type, named SigncryptedData, to be included as a part of the X9.73 Cryptographic Message Syntax (CMS) [7] standard.

Type `SigncryptedData` is derived from the `SignedData` type currently used to secure electronic mail, and biometric reference templates, Type-98 records in ANSI/NIST ITL [9] and DoD EBTS biometric transactions. The `SignedData` type is also used to manage biometric

information and security in the X9.84 and ISO 19092[1] biometric security standards.

The X9.84 biometric information management and security standard describes how messages containing biometric information can be bound cryptographically to a set of security and other metadata attributes [10].

This binding under a digital signature in a `SignedData` message wrapper provides origin authenticity and data integrity, and binds biometric data to security management information, such as Need-To-Know (NTK), Information Security Marking (ISM), and Geospatial Intelligence (GEOINT) information. Without the protection of a digital signature, accidental and malicious changes to data can go undetected, and data integrity cannot be assured.

The increased need for sharing biometric information among law enforcement, defense, and intelligence agencies has made origin authenticity of biometric information crucial for organizations that share biometrics. Decisions based on the accuracy and reliability of biometric information can affect National Security. It is crucial that decision makers receive biometric information that is free from tampering and that has originated from a trusted source. Biometric data and associated security metadata must be protected from removal and malicious or accidental modification.

Digital signatures alone do not provide biometric data confidentiality. X9.84 requires that the biometric data elements in an information object, such as a biometric reference template or a DoD EBTS transaction, be kept confidential to prevent unauthorized access and to ensure the privacy of individuals. The proposed `SigncryptedData` type extends the security protection of the SignedData message type to provide assurance of the confidentiality, data integrity, and origin authenticity of biometric information.

Implementation

A secure signcryption message can be implemented in both XML markup and a compact binary format using a single schema defined in the U.S. national standard, X9.73, and the recently proposed `SigncryptedData` type. Any type of biometric information in any format can be protected by a signature and encryption using the `SigncryptedData` cryptographic type. The protected content could be objects

1 The ISO 19092:2008 Biometrics Security Framework was derived from the ANSI X9.84 standard.

WHAT IS DOD EBTS?

The Department of Defense (DoD) Electronic Biometric Transmission Specification (EBTS) [8] was developed by the Biometrics Identity Management Agency (BIMA) to transport and store biometric data and associated DoD-relevant information. This information is transferred from biometric collection devices to a BIMA storage, matching, and distribution point. Biometric matching services are provided by BIMA to the DoD and its information-sharing partners using ABIS, the Automated Biometric Identification System.

ABIS is a central biometric storage and matching engine that responds to DoD EBTS match request transactions. ABIS sends biometric matching results and distributes biometric and associated information. ABIS transactions can be used to exchange information in one of several traditional formats, or in an Extensible Markup Language (XML) format. The DoD EBTS XML schema can support fast, efficient transactions using an analogous Abstract Syntax Notation One (ASN.1) schema that can transfer and exchange information in both compact binary and XML markup formats.

The latest version, DoD EBTS 3.0, was published as an emerging standard in 2011. It is based on the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Information Technology Lab (ITL) standard [9]. ITL and DoD EBTS transactions are not signed objects. These standards rely on an optional ITL Type-98 Information Assurance record to protect selected content in environments where use of the record is mandated. Best ITL guidance calls for the Type-98 record to contain a SignedData message, such as the version defined in the X9.73 CMS standard [7].

currently protected using the `SignedData` type, such as a DoD EBTS transaction, a biometric reference template, a Biometric Enabled Watch List (BEWL), or an X9.84 biometric system event journal.

The `SigncryptedData` type can be used to sign and encrypt an entire biometric object, or only specific components of the object, such as those components that should be kept confidential. Three processing modes for the `SigncryptedData` type have been proposed. These modes are identified as *signcrypted-content, signcrypted-attributes,* and *signcrypted-components*. In the s*igncrypted-content* mode, biometric data of any type is signcrypted. In the *signcrypted-attributes* mode, biometric data and associated attributes of any type are signcrypted. In the *signcrypted-components* mode, one or more components of the biometric data is signcrypted, then the resulting object is bound to one or more attributes under a digital signature.

Of these three modes, the *signcrypted-components* mode holds the most promise for protecting biometric information and associated security metadata attributes. This mode allows a biometric object containing signcrypted components to be cryptographically bound together with a set of security attributes using a digital signature. Signature processing follows the processing requirements for the X9.73 `SignedData`[2] type.

One attribute must contain a manifest, a list of the signcrypted components in the initial biometric object. This manifest must be included in the signed attributes, to ensure they are bound to the biometric object under a digital signature and available to the intended message recipient. The format and information contained in the manifest varies with the type of biometric object. For XML instance documents, such as BEWL or DoD EBTS transactions, XML Path (XPath) expressions can be used to locate the signcrypted elements. A list of XPath expressions forms a manifest that identifies the location of each signcrypted element in the biometric object.

A recipient of a `SigncryptedData` message uses the manifest to locate the elements in the XML instance document that contain signcrypted data. The signature on each signcrypted element in the list can then be verified and its plaintext content can be decrypted and recovered. Recovered plaintext can then be used to reconstruct the original XML document prior to XML schema validation.

Conclusion

Biometric information objects may carry personally identifiable information (PII). Some objects, such as DoD EBTS transactions, may be used to identify suspected terrorists or criminals; individuals that may be anonymous or whose identities are known. In some jurisdictions where information must be shared, biometric data and other PII data may be subject to laws that require privacy protection when this information can identify an individual.

In law enforcement, defense and intelligence environments, other information, such as the geolocation of an event or encounter, may be classified. Access to this information may be restricted based on a security classification level or need-to-know basis. Selected components in a message can be protected using signcryption to ensure that any sensitive information remains confidential. The biometric information object as a whole can be cryptographically bound together, perhaps with a set of security metadata, under a digital signature to give the object integrity and origin authenticity.

Signcryption cryptographic safeguards can protect the confidentiality, integrity, and authenticity of biometric information at rest, and as it travels across unprotected networks, such as the Internet. Other hybrid cryptographic techniques, such as authenticated encryption, have proven themselves as reliable cryptographic safeguards in network security protocols such as IPSec, SSH, and SSL. Signcryption is the asymmetric key analog of authenticated encryption that provides a way to integrate digital signatures with encryption schemes into a single, efficient cryptographic function. A recently proposed `SigncryptedData` cryptographic message type can be used to protect biometric information assets, such as DoD EBTS transactions, biometric watch lists, biometric reference templates, and biometric system event journals.

2 When there are attributes in type `SignedData`, the`messageDigest` and `contentType` attributes are required.

This article presents some research and study results and the author's description of them. The opinions expressed here do not necessarily represent the opinions of the DoD, BIMA, or Booz | Allen | Hamilton.

About the Author

Phillip H. Griffin, CISM | is an Associate at Booz | Allen | Hamilton serving as a subject matter expert for the Biometrics Identity Management Agency (BIMA). At BIMA, he is responsible for National Information Exchange Model (NIEM) packaging of their DoD Electronic Biometric Transmission Specification (EBTS). He has served as editor of the X9.84 and ISO 19092 biometric information management and security standards, cofounded and chaired the OASIS XML Common Biometric Format (XCBF) and OASIS Security Standards Joint Committees, and currently represents BIMA on the OASIS Biometric Identity Assurance Specification (BIAS) committee. Mr. Griffin has over 15 years experience in the development of information assurance and security standards and secure message protocols. He can be contacted at ***phil@phillipgriffin.com.***

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 July 21, 2012, from http://www.signcryption.org/publications/pdffiles/Dent-survey-eprint-04-210.pdf

3. Bellare, M., & Namprempre, C. (2008). Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Journal of Cryptology*, *21*(4), 469-491. doi:10.1007/s00145-008-9026-x. Retrieved July 21, 2012, from International Security & Counter Terrorism Reference Center database.

4. Freier, A., Karlton, P., & Kocher, P. (1996). *The SSL protocol version 3.0*. Retrieved July 21, 2012, from http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt

5. Kent, S. (2005). *IP encapsulating security payload (ESP)*. Retrieved July 21, 2012, from http://ietfreport.isoc.org/rfc/rfc4303.txt

6. Griffin, Phillip H. (2012). *Using Signcryption To Protect Biometric Information*. ID360: The Global Forum on Identity, The Center for Identity, University of Texas at Austin. Retrieved July 21, 2012, from http://phillipgriffin.com/innovation.htm#ID360

7. X9 Financial Services. (2010). *ANSI X9.73:2010 Cryptographic Message Syntax - ASN.1 and XML*. U.S.A.: American National Standards Institute (ANSI).

8. BIMA. (2011). Electronic Biometric Transmission Specification (EBTS). Retrieved June 21, 2012, from http://www.biometrics.dod.mil/Files/Documents/Standards/DoD_EBTS_v3_0.pdf

9. ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. [IEPD]. Retrieved June 12, 2012, from http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

10. X9 Financial Services. (2010). *ANSI X9.84:2010 Biometric Information Management and Security*. U.S.A.: American National Standards Institute (ANSI).