Biometric-Based Cybersecurity Techniques[1]

Phillip H. Griffin

Griffin Informtion Security,
1625 Glenwood Avenue,
Raleigh North Carolina, 27608 USA
phil@phillipgriffin.com

Abstract. This paper describes biometric-based methods for achieving strong, low cost mutual and multi-factor authentication on the Internet of Things (IoT). These methods can leverage telebiometric authentication objects (TAO), tagged physical objects functionally coupled with biometric sensors and connected to a telecommunications network. Methods presented are convenient for people to use, support Universal Access (UA) goals, and ensure the confidential exchange of information between communicating parties. The described one and two-factor authentication methods use cryptographic techniques to achieve mutual authentication and data confidentiality through password and biometric authenticated key exchange (AKE). These key establishment techniques rely on the use of a Diffie-Hellman key agreement scheme to create a strong symmetric key from a weak secret. AKE protocols can provide forward secrecy and prevent disclosure of user credentials during authentication attempts to thwart active phishing and man-in-the-middle attacks. TAO combined with AKE provides mutual authentication and strong, three-factor user authentication.

Keywords: Authentication · Key Exchange · Security · Telebiometrics · Universal Access

1 Introduction

Authentication of identity is a critical frontline control for managing risk of unauthorized access to information systems. To manage this risk, access control systems must balance ease of access by legitimate users against the need to defend the system from attack. Defending an information system includes ensuring availability while protecting the user, their credentials, and their sensitive data from exposure.

Access control systems achieve these goals through mutual authentication and strong multi-factor user authentication. This requires ensuring user credentials retain their integrity, and remain confidential throughout the entire authentication process, during transfer, processing and storage. The system must implement safeguards that thwart identity theft, phishing and man-in-the-middle attacks, yet still provide easy to use access. The role of human factors in successful attacks becomes a key consideration in the selection of these security safeguards.

[1] Final draft for review and publication submitted to AHFE 2016 Conference.

Biometrics-based access controls provide *something-you-are* authentication options that support ease of use and Universal Access (UA), an inclusive user-interface design concept. A primary goal of UA is to provide "the utility of modern information technology to as broad a range of individuals as possible" [1]. Biometric technologies are a "natural choice for implementing authentication" in systems that seek an inclusive design that strikes a balance between ease of use and security. The potential for integrating both "security and usability effectively is greater with biometrics than with other authentication methods" [1].

A biometric system creates a biometric reference template when an individual enrolls, and stores the template for later biometric matching. A biometric reference template can be associated with physical objects, each tagged with a unique Radio Frequency Identification (RFID) value. These tagged objects might be a secured door, a vehicle, a household appliance, a user workstation, or any other object that requires controlled access. Objects registered in the system and associated with an individual can serve as their *something-you-have* authentication factor.

Biometric sensor data is a rich source of information content "not limited to only the physiological and behavioral characteristics needed to support biometric matching" [2]. Both *something-you-know* and *something-you-are* information can be extracted from biometric sensor data to provide single factor and 2-factor authentication solutions. When coupled with tagged physical objects that serve as user possessions, biometric-based access control systems can provide strong, 3-factor user authentication that is convenient for people to use.

Knowledge extracted from a biometric sensor can be used to operate an Authenticated Key Exchange (AKE) protocol. AKE protocols can provide mutual authentication without reliance on Transport Layer Security (TLS), whose security depends "on trustworthy certificate authorities (CAs), a fully functional public key infrastructure (PKI), adequate browser certificate revocation checking, or changes to user behavior or in their understanding of certificate validation" [3]. AKE protocols thwart phishing, spoofing, and man-in-the-middle attacks to protect the user's access control credentials during the identity authentication process, and to ensure confidential communications following successful authentication.

Access control systems that combine TAO and AKE can provide strong, multi-factor authentication of identity without the cost and complexity of digital certificates or expensive, personally assigned user security tokens. Such systems need not rely on the existence of a ubiquitous, properly functioning PKI. By foregoing the use of PKI, users are freed from managing public key certificates, understanding the nuances of PKI trust anchors and hierarchies, interacting with and responding appropriately to system warnings and alerts, or constantly maintaining the secrecy of the private key components of their public-private key pairs [3].

2 Telebiometric Authentication Objects

Telebiometrics is the technology that merges biometric sensors with telecommunication networks. This connectivity enables local area and remote information exchange with biometric systems that provide user identification and authentication services. In order to use these recognition services, a "human being must come into physical con-

tact with telecommunications and biometric devices" [4], so both the safety of individuals and their security become concerns. Telebiometrics makes information security and safety management of distributed biometric devices possible, and enables their "real-time remote management and monitoring by system administrators" [4]. Telebiometric systems allow cybersecurity applications to support easy to use biometric techniques that provide secure access to authorized users of information technology and communications (ITC) systems and services.

A Telebiometric Authentication Object (TAO) associates an individual with one or more tagged physical objects [5] in a cyber-physical system. This association, when trusted by a relying party, allows an individual to use the tag identifier that is on or embedded in a physical object "to serve as a possession factor" [6], as a *something-you-have* authentication factor in an access control system. TAO are smart objects whose associations allow physical objects present in a user environment to serve as low cost authentication factors that are convenient for them to use. These objects can eliminate "the need for expensive individual tokens" [7]. Fig. 1 illustrates the structure and content of an information object representation of a person-object association.

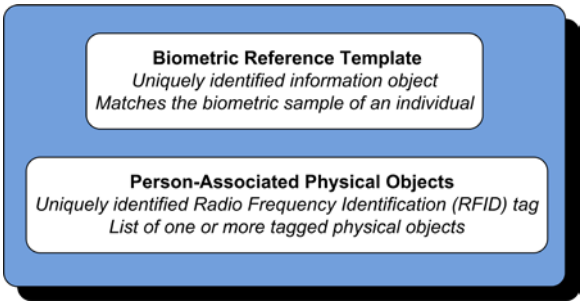

Fig. 1. A person-object association uniquely identifies an individual (*Biometric Reference Template*) that can be matched to their biometric sample, and a set of tagged physical objects (*Person-Associated Physical Objects*) that the matched individual is known to possess.

Physical objects in cyberspace may be "uniquely identified using Radio Frequency Identification (RFID) tags" [7] or other types of identifiers. RFIDs are wireless computing devices equipped with microprocessors and memory that beacon a unique identifier value using radio waves [7]. TAO can be any familiar object found in a user environment, "such as doors, floors, and other telebiometric-enabled objects" [8]. They may be public objects, and need not be a personal object "a person must carry around with them" [8].

A uniquely identified individual may be associated with more than one uniquely identified physical object, and a given physical object may be associated with more than one individual. Individuals authenticate by biometric matching a provided biometric sample against a biometric reference template value. This reference value is stored for subsequent biometric matching when the individual enrolls in a biometric system. During the enrollment process, a set of tagged physical objects assigned to the individual becomes their possession objects during subsequent identity authentication.

Reference Template Identification. Once a user is enrolled in a telebiometric access control system, their "biometric sample can serve as a *something-you-are* authentication factor." [7]. User identity is authenticated if a subsequent user sample can be matched against the biometric reference template created by the relying party when the user first enrolled. Each user and their template are uniquely identifiable in the access control system, and templates are typically stored in a database for easy search and retrieval during biometric matching and security assessment operations.

When the system creates a new template it is "assigned a unique identifier" and populated with operational and other information that may further identify the user [7]. The identifier of a biometric reference template serves as a proxy for the user identity and a database index for locating the user template. Since a template index value "indirectly identifies the person whose biometric sample matches the enrollment data in a given biometric reference template" [7], this value can serve as a constant used to monitor or track an enrolled individual over time. Access to all information in a biometric reference template, including its index value, should be restricted and its integrity and confidentiality protected from accidental or purposeful modification or exposure [9].

Person-Object Associations. The biometric reference template of a person enrolled in a biometric system can be associated with one or more physical objects, as illustrated in Fig. 1. This process establishes those objects to a relying party as known possessions of that individual. The personal "possession object" of an individual when presented during a subsequent authentication attempt can serve as their *something-you-have* authentication factor. A biometric match of an enrolled person is a *something-you-are* authentication factor. A biometric match coupled with a user possession can provide strong, two-factor authentication in an access control system.

A formal schema definition language such as Abstract Syntax Notation One (ASN.1) [10] can specify person-object associations. A formal schema can "support automated processing by syntax checking and programming language code generation tools" [7]. A series of international standards jointly maintained by ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), and ITU (International Telecommunications Union) define the ASN.1 language and its concrete information exchange formats, the ASN.1 encoding rules.

Every abstract value of every ASN.1 type has both compact binary formats and verbose, human-readable representations. Values in either format readily convert into the other based on standardized ASN.1 rules [10]. This capability allows an Application Programming Interface (API) to efficiently transfer and store compact binary information and leverage the benefits of text-based data representations when needed.

Binary formatted messages are beneficial "in environments constrained by mobility, limited battery life, or bandwidth (e.g., wireless communications using handheld and personal devices)" [4], conditions often encountered in distributed cyber-physical systems. Compact binary messages are also advantageous in systems that have "high volumes of transactions (e.g., mobile internet commerce) or limited storage capacity" [4]. Cyber system devices that "transfer data over radio waves or congested communications links", such as Telebiometric Authentication Objects (TAO) can also benefit "from using compact binary formats" [4].

The following example defines an ASN.1 schema for a person-object association. The association couples a biometric reference template identifier with a set of one or more physical object tags.

Example of a person-object association schema defined using ASN.1

```
Person-ObjectAssociation ::= SEQUENCE {
   person   BiometricReferenceIdentifier,
   objects  PhysicalObjectSet
}

BiometricReferenceIdentifier ::= OCTET STRING

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

RFID ::= OCTET STRING
```

A value of ASN.1 type `Person-ObjectAssociation` is a sequence of two values, a `person` and a set of one or more physical `objects`. The value of the `person` component indirectly identifies an individual. This component is an opaque string, a value of type `BiometricReferenceIdentifier`. The content of this string identifies or locates the biometric reference template that can match a biometric sample from the enrolled individual. This value may be a unique template identifier, a cryptographic hash of the template, a uniform resource locator (URL), or other type of identifier.

The value of the `objects` component contains a set of physical object identifiers associated with the individual indicated by the `person` component. This component is a value of type `PhysicalObjectSet`, a series of values of type `RFID`. These values are opaque strings containing the unique identifier of an RFID tag.

In an instance of communication, the abstract values of ASN.1 type `Person-ObjectAssociation` can be represented concretely in a compact binary format or in a verbose, human-readable format such as Extensible Markup Language (XML) markup or JavaScript Object Notation (JSON). Any value of any ASN.1 type converts readily from one format to the other [10]. This feature makes it possible for "information exchange applications to enjoy efficient binary transfer and compact storage of information" [7] in resource constrained environments without sacrificing the benefits of JSON or XML markup when needed.

Access control systems must protect the confidentiality, integrity and authenticity of credentials used for identity authentication during data transfer and while they are stored. Mutual and multi-factor authentication solutions are safeguards frequently used to achieve these security goals, but often these solutions come with high cost, increased complexity, and processing overhead ill suited for constrained environments. Biometric authentication combined with cryptographic techniques can meet these security goals while minimizing the problems found in the implementation of alternative safeguards.

3 Authenticated Key Exchange

Transport Layer Security (TLS) is a widely implemented security control for achieving mutual authentication and confidential information exchange between communicating servers that each possess digital certificates. In practice, while most secure web servers "rely on TLS to authenticate the server to the client, mutual authentication is an optional handshake feature less commonly used" [4]. Mutual authentication is often not possible using TLS "because not every client has a certified public key" certificate [12]. Instead of achieving strong mutual authentication, the typical TLS user authenticates to the server "by sending a password to the server after the establishment of a TLS-protected channel" [12]. Phishing, website spoofing, and man-the-middle (MITM) attackers exploit this deficiency "to capture user credentials and other sensitive information" [4]. Ironically, victims of such attacks send their credentials to their attackers across a secure channel.

Password Authenticated Key Exchange (PAKE)[2] and Biometric-Authenticated Key Exchange (B-AKE) provide alternatives for achieving mutual authentication confidential information exchange without users possessing public key certificates. Manulis, Stebila, and Denham [13] proposed augmenting the TLS protocol using PAKE to protect user credentials from spoofing, phishing and MITM attacks. However, PAKE and B-AKE protocols eliminate the need for relying on TLS or digital certificates at all. Both of these AKE solutions provide mutual authentication, defeat spoofing, phishing and MITM, and ensure confidential information exchange between communicating parties.

Access controls that rely on the "safe and secure operation of telebiometric systems" [4] must manage security risk that stem from "real-world factors such as 1) Human factors, 2) External environmental conditions, 3) System related issues" [11]. Using PAKE and B-AKE for mutual authentication helps reduce the risk of user credential capture by attackers during the identity authentication process. PAKE provides mutual authentication with single factor user authentication based on weak secrets. B-AKE builds upon the PAKE protocol, strengthening user authentication to two factors, *something-you-are* and *something-you-know*.

B-AKE leverages the rich information content collected by telebiometric sensors, by extracting user knowledge from biometric sensor data and using that knowledge as the weak secret needed to operate a PAKE protocol [2]. To perform biometric matching, B-AKE requires that the user first enroll in a biometric system. To operate the Diffie-Hellman key agreement scheme within PAKE for key establishment, the user must also have registered their personal identification number (PIN), password, or passphrase prior to attempting to authenticate [3].

A user and server must have previously shared secret knowledge prior to its use as an access control authenticator or for the operation of an AKE protocol. Typically, the shared knowledge is a password, a passphrase, or a PIN that the user enters through a keyboard device. When this knowledge is an identity authenticator, its value must

[2] Both ITU-T X.1035: Password-Authenticated Key Exchange (PAK) protocol (2007) and ISO/IEC 11770-4:2006 Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets standardize PAKE techniques.

precisely match the value expected by the relying party of the access control system. Otherwise, the Diffie-Hellman key agreement scheme will fail to produce the correct symmetric key needed to decrypt the user message. When used as the input to an AKE protocol, this knowledge value determines the symmetric encryption key used to ensure the confidentiality of information exchanged.

B-AKE operates using any biometric technology type from which extracted user knowledge is available, and extends traditional weak secrets to include a sequence of footsteps, a series of spoken word, or the “the finger positions and hand postures” used in a gesture or “during communication of hand sign languages” [14]. A B-AKE user "creates a symmetric encryption key using a weak secret", extracted *something-you-know* data, and uses this key to protect the "confidentiality of user credentials and other message data" transferred to a server during an identity authentication attempt [2].

If the server possesses the same *something-you-know* information as the user, "a key is created, the message decrypted, and mutual authentication achieved" [2]. User biometric data recovered from the encrypted message provides an additional biometric-matching authentication factor. B-AKE operation ensures that users "never reveal their knowledge or biometric credentials to imposter recipients or *man-in-the-middle* observers" [2]. The use of a Diffie-Hellman protocol for key establishment provides *forward secrecy*, when the user and server choose fresh random values each time they operate the B-AKE protocol. This capability provides additional protection in the event of a key compromise, by limiting the scope of information exposed to an attacker.

4 Telebiometric Authenticated Key Exchange Objects

Telebiometric technologies provide local and remote, single factor biometric authentication. When AKE protocols are coupled with Telebiometric Authentication Objects based on person-object associations, it is possible to create inexpensive mutual and multi-factor authentication solutions that provide secure access control and confidential communications to a broad community of users.

One variation of a Telebiometric Authenticated Key Exchange Object (TAKEO) protocol illustrated in Fig. 2 can achieve mutual authentication and multi-factor user authentication. When no tagged objects associated with the user are available, it is possible to perform a Biometric Authenticated Key Exchange (B-AKE) protocol [2] by omitting the possession factor from step 4 and eliminating step 10. B-AKE supports mutual authentication and 2-factor user authentication based on biometric matching and knowledge extracted from telebiometric sensor data.

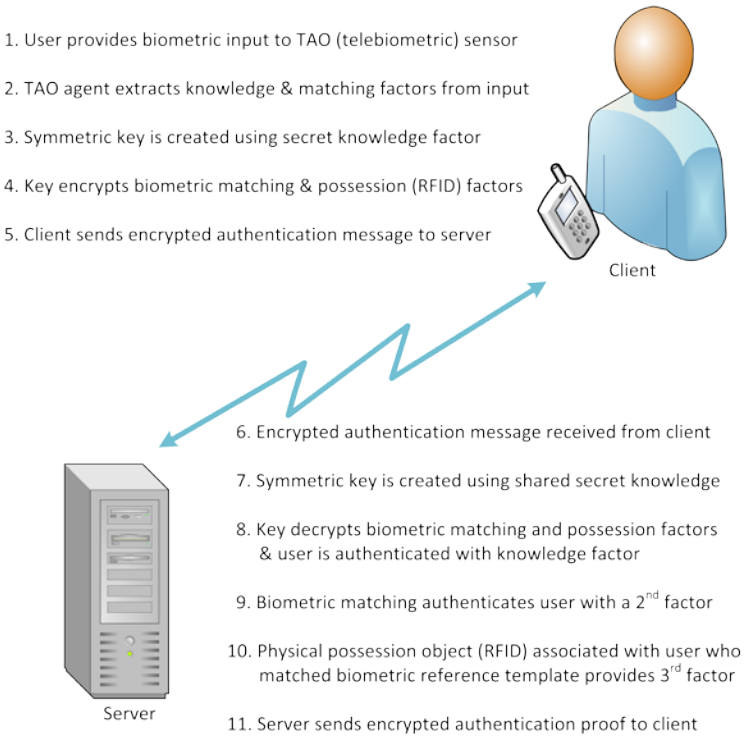

Fig. 2. The user (*client*) and relying party (*server*) perform a Telebiometric Authenticated Key Exchange Object (TAKEO) protocol to mutually authenticate their identities and establish a shared symmetric cryptographic key to ensure the confidentiality of subsequent information exchange. Strong three-factor authentication establishes the user identity to the relying party. Encryption protects user provided credentials under a cryptographic key based on a shared weak secret. The TAKEO protocol never exposes user credentials to a phishing or man-in-the-middle attacker.

Access control systems can use AKE to provide simple, single factor authentication solutions based on a user password credential protected during transfer by a PAKE protocol. This approach provides many of the benefits of TAKEO, but with less assurance of user identity, and may be beneficial in systems that must provide some level of availability to users, even when there are no telebiometric sensors or associated tagged objects available. Some implementations may also choose to manage risk by limiting access to high value assets when three-factor authentication is required and does not succeed, but users are able to authenticate successfully with one or two factors.

5 Conclusion

Access control systems that protect information assets using authenticated key exchange (AKE) protocols can help manage cybersecurity risk and provide easy to use, low cost alternatives for secure access to ITC network services and information. Password and biometric AKE protocols ensure mutual authentication to protect system users from active phishing, web site spoofing, and man-in-the-middle attacks, and provide forward secrecy, a desirable property in cryptographic protocol solutions that provide data confidentiality services. PAKE and B-AKE protocols do not require users to possess and properly manage digital certificates, or to understand the complexities of use when relying on a public key infrastructure to establish and maintain trust.

Biometric-based access controls allow security systems to provide mutual and multi-factor authentication solutions that give users a choice of authentication methods. Implementations can provide support for multiple types of biometric technologies, as well as user passwords, passphrases, and PINs. User choice supports the goals of universal access and can ensure elderly and physically or mentally disabled populations gain the ability to authenticate to ITC systems securely. Easily remembered passwords coupled with support for multiple biometric technology types can help internet service providers achieve universal secure access and serve a broad user base.

Telebiometric Authentication Objects coupled with PAKE and B-AKE protocols allow access control systems to provide low cost, mutual and multi-factor authentication solutions based on a Telebiometric Authenticated Key Exchange Object (TAKEO) protocol. TAKEO-based implementations can offer secure access control and confidential communications that can serve a broad community of users. By using a TAKEO approach, there is no need for users to possess personally assigned security tokens or digital certificates to authenticate their identities. Familiar tagged objects in their homes or workplace environments that have been associated with their biometric identifiers can serve as user possession objects that enable strong identity authentication.

References

1. Mayron, L. M., Hausawi, Y., Bahr, G. S.: Secure, Usable Biometric Authentication Systems. In *Universal Access in Human-Computer Interaction., Design Methods, Tools, and Interaction Techniques for eInclusion*, 8009 (2013), pp. 195--204. Springer Berlin Heidelberg
2. Griffin, P.H.: Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange. Complex Adaptive Systems Proceedings. Procedia Computer Science, 61 (2015), pp. 66--71. Elsevier B.V.
3. Griffin, P.H.: Transport Layer Secured Password-Authenticated Key Exchange. Information Systems Security Association Journal, vol. 13, no. 6, June, 2015
4. Griffin P.H. Telebiometric Security and Safety Management. Proceedings of ITU Kaleidoscope Conference – Building Sustainable Communities (2013)
5. Griffin, P.H.: U.S. Patent Number 8,289,135. Washington, DC: United States
6. X9 Financial Services. ANSI X9.117 Secure Remote Access - Mutual Authentication, 2012
7. Griffin, P.H.: Telebiometric Authentication Objects. Complex Adaptive Systems Proceedings. Procedia Computer Science, 36 (2014), pp. 393--400. Elsevier B.V.

8. Griffin, P.H.: Security for Ambient Assisted Living - Multi-Factor Authentication in the Internet of Things. In: IEEE Global Communications (GLOBECOM), IoT Ambient Assisted Living Workshop (IoTAAL), San Diego, California (2015)
9. International Organization for Standardization. ISO 19092 – Financial services – Biometrics – Security framework; 2008
10. Larmouth, J.: ASN.1 Complete. Morgan Kaufmann (2000)
11. Pour, B.: 'There's a Metric for That': How 'Big Data' Impacts Biometrics Market and Industry (2012)
12. Alsaid, A., Mitchell, C.: Preventing Phishing Attacks Using Trusted Computing Technology. Proceedings of the 6th International Network Conference (INC'06) (2006), pp. 221-228
13. Manulis, M., Stebila, D., Denham, N.: Secure Modular Password Authentication for the Web Using Channel Bindings. In *Security Standardisation Research: First International Conference, SSR 2014, London, UK, December 16-17, 2014. Proceedings (Vol. 8893, pp. 167-189)*. Chen, L., & Mitchell, C. (Eds.) Springer International Publishing (2014)
14. Fong, S., Zhuang, Y., Fister, I.: A biometric authentication model using hand gesture images. *Biomedical engineering online*, *12*(1), 111 (2013)