Security for Ambient Assisted Living

Multi-factor Authentication in the Internet of Things[1]

Phillip H. Griffin
Griffin Information Security
Raleigh, North Carolina USA
phil@phillipgriffin.com

***Abstract*—This paper describes mechanisms for achieving strong, multi-factor authentication in Ambient Assisted Living environments. These mechanisms rely on biometric-based technologies to provide information security and privacy in the Internet of Things. The importance of user choice and ease of use of authentication methods in achieving universal access to services in assistive environments is described. Cryptographic algorithm and protocol solutions that depend on a Public Key Infrastructure for the protection of sensitive information are discussed. Lighter weight alternatives are then proposed that use authenticated key exchange to combat phishing and other attacks and provide mutual authentication and data confidentiality.**

Keywords—assistive environments; authentication; biometrics; key exchange; security

I. Introduction

Information and communications technologies (ICT) facilitate opportunities for interaction and information exchange between people, devices, and systems. ICT hold the promise of our delivering beneficial services to those living in assistive environments and connecting them to the world around them. A recent survey reports that ICT accessed internet services constitute the "technology with the greatest impact in promoting the inclusion of persons with disabilities" and the elderly [1]. With the proliferation of wireless computers and mobile phones, ICT have "heralded a new age not only of information sharing in general, but of the proliferation of web-based services that serve disabled and non-disabled communities alike" [1].

As “the number of elderly people and patients with reduced autonomy or with chronic diseases” continues to grow, the need to “keep these people at home while providing them” with “care and assistance” has become more acute [2]. The reliance of assisted living inhabitants on services provided through cloud and web-based systems over unsecured public networks exposes this vulnerable population to increased security risk. This risk is most evident in the field of telemedicine, which relies on the “use of telecommunications to, remotely, provide medical information and services” and to securely and reliably “transfer medical information and services from one place to another” [2].

While information security and privacy are critical to providing assurance that users of internet-based systems are protected, “few projects take into account this feature” [2]. Far too few researchers in fields related to Ambient Assisted Living (AAL) are teaming with information security and privacy experts to ensure that solutions are designed and implemented with these features in mind. In a recent study of European telemonitoring projects, Ermakova and Fabian searched the “EBSCOhost, IEEE Xplore, Emerald, ScienceDirect, AISeL, Springer, ACM Digital Library and Proquest” databases for papers dealing with the topics of both healthcare and cloud computing [3]. Of the “4222 publications” that matched their search criteria, they retrieved a “total of 11 dealing with security and privacy issues” [3].

As the availability and use of inexpensive mobile computing devices becomes more widespread, the wide varieties of biometric sensors they incorporate are becoming ubiquitous. Face, voice, gesture and touch biometric sensors are becoming commonplace and application providers no longer need to settle on just one biometric technology for authentication. Researchers and AAL providers are presented with new opportunities to exploit these sensors and to create designs that provide secure authentication and access to web-based services to a greater number of elderly and disabled users. In smart home and smart assisted living facilities, biometric sensors can also be used to enable secure biometric identification techniques that are easy to use by the elderly and disabled.

II. Secure Web Services for AAL

Providing biometric authentication options in AAL systems could make secure, universal access to services possible for millions of elderly, disabled, or impaired users. [4]. Universal Access (UA) is a design concept that seeks to provide "the utility of modern information technology to as broad a range of individuals as possible" [5]. Since the potential for integrating "security and usability effectively is greater with biometrics than with other authentication methods", biometric technologies are a "natural choice for implementing authentication in UA systems" [5].

Authentication systems based on UA concepts could provide access to greater number of users in assistive environments. Inclusive, flexible designs could help ensure that the elderly or impaired are not isolated AAL inhabitants excluded from the opportunity of securely "accessing,

[1] Accepted by IoT Ambient Assisted Living Workshop (IoTAAL) – IEEE Globecom 2015 Conference, San Diego, CA

participating and being fully included in social, economic and political activities" [1]. With over "one billion persons living with disabilities" in the world, many who are poor, it is critically import that AAL service providers offer solutions that help remove the "barriers to accessing Information and Communications Technologies (ICTs) by persons with disabilities" [1]. By creating products and services that improve accessibility for all users, they can help eliminate this "key driver of exclusion and poverty"[1].

People who suffer from a cognitive or physical disorder can have difficulty correctly entering a Personal Identification Number (PIN) on a keyboard or recalling the correct sequence of letters in a password. Biometric authentication using technologies such as fingerprints or speaker recognition integrated into AAL systems could provide "elderly and disabled users with effective alternatives to using passwords and PINs for secure access" to assistive services and information [4]. Even persons severely restricted to ICT device interactions using "nods of the head, eye movements, hand movements, or even by different thought patterns that are captured by a sensor" [6] could be empowered by AAL systems that provide access control using biometric technologies such as hand gestures or face recognition.

Biometric technologies can support both authentication and identification of individuals. For authentication, biometrics is used to match an individual to a claimed identity, a one-to-one match. For identification, biometrics is used to match an individual in a set of possible identities, a one-to-many match. In some assistive environments, such as within a care facility or within a user's home, the identity of the user may be well known or may have already been verified. In such contexts biometric identification may be appropriate for providing secure services that are convenient for users to access, perhaps based on biometrics that have relatively weak matching performance, such as a user's gait, facial expressions, or gestures [4]. Biometric technologies coupled with smart objects in AAL environments can enable secure, convenient access to communications, information, and services in smart homes and other assistive environments "that can be easy to use by elderly and disabled persons" [4].

III. Smart Object Authentication

A. People and possesions

Telebiometric systems connect biometric sensors to telecommunications networks. Telebiometric authentication objects (TAO) can associate monitoring, medical, and other equipment with individuals [7] and provide them with secure access to remote health care and assisted living services. TAO are smart objects that can be "uniquely identified using Radio Frequency Identification (RFID) tags" [8] and other types of identifiers. RFID-tagged objects transmit "a unique serial number via radio waves to an interrogator or reader" [9] that can be used by ICT systems to identify and interact with physical objects.

TAO allow "biometric sensors connected to a telecommunications network" to be incorporated into "multi-factor access control systems in the Internet of Things" [8]. A tagged physical object that has been registered with an access control system as being associated with an individual can be subsequently recognized as their possession. This possessed object can serve as "a low cost *something-you-have* authentication factor that eliminates the need for expensive individual tokens" [8] that a person must carry around with them. Instead, TAO can be familiar items in an AAL environment, such as doors, floors, and other telebiometric-enabled objects.

When an individual is enrolled in a biometric system a biometric reference template is created and stored for subsequent biometric matching of that individual. A template contains a person's biometric data "extracted from biometric samples provided by an individual during enrollment" [8]. A later biometric sample that can be matched to an individual's stored biometric reference template is "a *something-you-are* authentication factor that can uniquely identify an individual" [8].

The ISO/IEC 19785 biometric information exchange standard requires each biometric reference template in a biometric system to be assigned a unique template identifier. The value of a template identifier indirectly identifies "the person whose biometric sample matches the enrollment data in a given biometric reference template" [8]. When individuals in assistive environments are enrolled in a biometric system "they can be associated with a set of physical objects using their unique biometric reference template identifier and one or more unique RFID serial numbers" attached to or embedded within each object [8]. This person-object association is illustrated in Fig. 1.

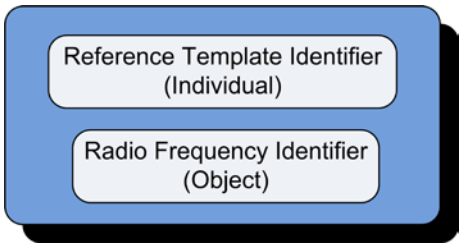

Fig. 1. Simple person-object association [8].

In an access control system, "registered person-object associations" can be used for multi-factor authentication [8]. To authenticate, a user would provide a biometric sample to a TAO-enabled application. The sample and one or more person-associated object identifiers would be transferred to an access control system where biometric and associated object matching would occur. If the user is matched to a biometric reference template that is associated with an identified object, access to some resource would be granted. If the user fails biometric matching, or if the user is matched but is not registered as being associated with an identified object, authentication fails for that object and resource access is denied.

The access control system can maintain lists of objects associated with an individual, and these lists can be "modified over time to adapt to changing user access permissions", changes to the set of person-associated objects in the user environment, and changes in the assistance needs of an

individual [8]. When a list of person-associated objects must be altered, modifications can be made without any action by or impact on assisted persons. They are not required to "reenroll in the biometric system" [8]. In group assisted settings, access to tagged smart objects can be shared, since each physical object can be associated with more than one uniquely identifiable individual.

B. *Protecting assisted persons*

RFID data associated with people and biometric data are personally identifiable information (PII) that should be protected during transfer and storage using efficient cryptographic techniques. Data protection can empower assisted living users to "manage their safety and security risk" and enable the reliable information management systems that "providers need to ensure high quality, safe, reliable service" [10]. Signcryption, a cryptographic primitive defined in the ISO/IEC 29150 standard, offers one alternative for providing these important data protection services.

The signcryption algorithm uses a hybrid cryptographic technique that "blends together signature and encryption schemes to perform digital signature and asymmetric encryption functions simultaneously" [10]. This technique can simplify key management and lower costs in AAL systems, reducing the number of keys and digital certificates vendors must provide for signing and encrypting data. Signcryption provides "confidentiality, data integrity, and origin authenticity in a single, efficient operation" [10]. Signcryption offers "secure data transfer and storage for biometric reference templates, person-object associations, and for the sensitive information in authentication request and response messages" [8]. A Transport Layer Security (TLS) *handshake* protocol can be coupled with signcryption to provide mutual authentication in assistive environments, and the TLS *record* protocol can ensure assisted persons have a secure channel for communications for access to services [11].

However, to achieve mutual authentication TLS requires the overhead of a Public Key Infrastructure (PKI) and for users to possess and maintain their own personal digital certificates. Though many secure websites "rely on TLS to authenticate the server to the client", mutual authentication using TLS is less common [11]. In the TLS protocol, "mutual authentication is an optional handshake feature less commonly used" since "not every client has a certified public key" certificate [11]. It is more likely for client authentication to rely on "sending a password to the server after the establishment of a TLS-protected channel" [12]. The increase in web spoofing attacks by imposter servers and the continued growth in phishing attacks rely on TLS client password authentication, failure of users to react defensively to alert and warning messages, and TLS flaws and implementation errors. These problems allow attackers to capture user credentials and other sensitive data.

Both signcryption and TLS are PKI-based and require assisted living users to understand "the complexities of certificate signature verification, trusted path validation", and "certificate validity periods and expiration dates" [11]. User carelessness and misunderstanding of these complexities can expose them to phishing and man-in-the-middle attacks. Authenticated Key Exchange (AKE) protocols can offer users less complex alternatives for authentication and secure access to services. Unlike TLS, several AKE protocols provide mutual authentication that does not "rely 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" [11].

IV. Authenticated Key Exchange

AKE protocols provide strong cryptographic protection based on user knowledge. Typically, user knowledge is in the form of a string of characters, such as a password, passphrase, or personal identification number (PIN). These authenticators are commonly input into a computing system by a user typing on a keyboard device. However, knowledge can be represented in other forms that can be input in other ways. Knowledge can be conveyed through password strings or through information extracted from biometric sensor data, such as collected speech or gestures. Both of these sources of knowledge, passwords and biometrics, can be used to operate an AKE protocol.

A. *Passwords*

Password-Authenticated Key Exchange (PAKE) is a "cryptographic protocol that allows two parties who share knowledge of a password to mutually authenticate each other and establish a shared key, without explicitly revealing the password in the process" [13]. PAKE operation does not require that users possess digital certificates or rely on the existence of a Public Key Infrastructure (PKI). PAKE protocols rely on a Diffie-Hellman key agreement scheme for key establishment.

Mechanisms for operating a PAKE protocol have been standardized internationally in the ISO/IEC 11770-4 Key management – Mechanisms based on weak secrets standard and in the ITU-T X.1035: Password-authenticated key exchange (PAK) recommendation. Passwords, passphrases, and PINs are considered "weak secrets" since a person can easily memorize them [11]. As illustrated in Fig. 2, a user enters their password into a browser-based application, which derives a cryptographic key based on the password.

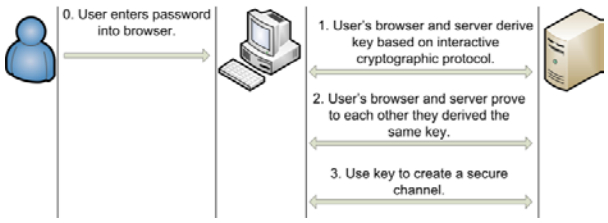

Fig. 2. PAKE-based web authentication (Source: Web 2.0 Security & Privacy (W2SP) 2009) [13].

The password credential is encrypted with this key before the encrypted password is sent to the server. If a man-in-the-middle attacker is eavesdropping on this communication they never see the actual password, since it is encrypted. If the server is an imposter that is "spoofing the user, it will not know the user password", step 2 in Fig. 2 will then fail, and "the

authentication session will end without revealing the user password" [11].

Otherwise, the server will use a preregistered copy of the user password to create the same key used to encrypt the password. Using this key, the server will decrypt the message and authenticate the user. When the user receives a response from the server encrypted under the shared symmetric key, mutual authentication will be achieved. The shared, established key is known only to the communicating parties, and a means to protect the confidentiality of messages sent between the user and the server is now established for subsequent communications.

By design, the PAKE protocol never exposes the user password to a server impersonation or eavesdropping attack during its operation. This feature of the PAKE protocol "prevents off-line dictionary attacks, a common password authentication problem." [11]. Mutual authentication relies on a previously shared "weak secret", an easy to memorize password. PAKE provides a strong key establishment mechanism, even when based on weak passwords, and the use of password authentication in PAKE protects users from man-in-the-middle attacks. Key establishment based on Diffie-Hellman key agreement ensures *perfect forward secrecy*, a protocol property that "guarantees that compromise of a session key or long-term private key after a given session does not cause the compromise of any earlier session" [14].

B. Biometrics

These important security features provided by PAKE are also provided in the Biometric-Authenticated Key Exchange (B-AKE) protocols recently defined in [15]. BAK-E extends PAKE knowledge representations "beyond the limitations of character string passwords to more general knowledge representations" [15]. Knowledge is extracted from biometric sensor data. With B-AKE, *something-you-know* authenticator values can be in the character string format expected by PAKE, or represented as binary values, or composed of "human-readable markup or other structured content" [15].

The schema for a B-AKE authenticator is a value of type **PW**, an ASN.1 'open type' [16]. The authenticator can be the value of any type in its encoded, string format, as illustrated in Fig. 3. An "encoded value of type **PW** is an opaque string, a series of octets that are independent of hardware, operating system, or programming language considerations" [15]. This format is ideal for unambiguous information exchange "between communicating parties that have different computing environments" [15], and **PW** can be treated the same as an ordinary password by key exchange processing tools.

```
PW ::= KNOWLEDGE.&Type  -- Implementation constrained

KNOWLEDGE ::= CLASS {
  &id    OBJECT IDENTIFIER  UNIQUE,
  &Type  OPTIONAL
}
 WITH SYNTAX { KNOWLEDGE &id [ DATA &Type ] }
```

Fig. 3. B-AKE biometric knowledge authentication string [15].

As in the PAKE protocol, B-AKE authenticators are treated as having no discernible format, structure or semantics for the purposes of Diffie-Hellman key exchange processing. For both protocols, authenticators "must be pre-established before protocol operation" [15]. Since the cryptographic processing in these protocols are identical, implementers can support knowledge-based authentication using both password strings and data extracted from biometric sensors. This common processing aspect allows implementers to offer users a choice of authentication methods that are more inclusive while still achieving mutual authentication.

A simple example of B-AKE authentication processing relies on speech recognition along with speaker recognition biometrics to provide two-factor authentication using data from a single biometric sensor. For this biometric technology type, a user voiceprint includes "a series of words or letters whose binary values can be extracted using speech recognition techniques, and then transformed into a character string" [15]. One authentication factor, *something-you-know*, comes from the words spoken by a user, which form the knowledge string used in B-AKE to create a symmetric encryption key.

The second authentication factor, *something-you-are*, contains biometric matching data. Both authenticator values can be protected during transfer using the B-AKE derived cryptographic key. B-AKE protocol processing is illustrated in Fig. 4.

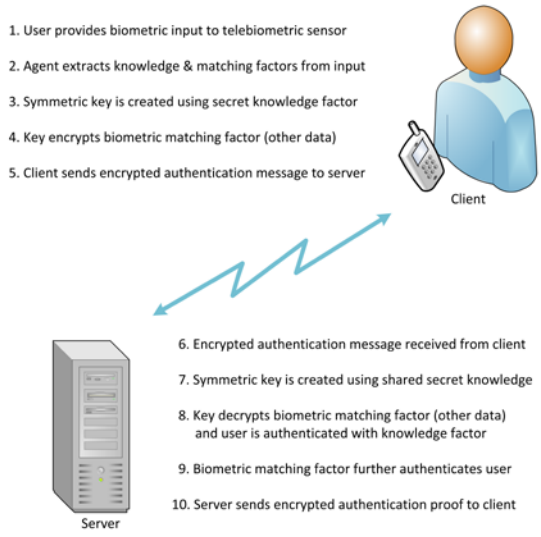

Fig. 4. B-AKE protocol operation [15].

When the client receives the confirmation message in step 10 of Fig. 4, mutual authentication is achieved and a shared key is established that is known only by the communicating parties. This shared secret key can be used to ensure the confidentiality of subsequent communications. As with PAKE, user credentials are protected "from the man-in-the-middle attack" and are never revealed "to an eavesdropper preventing an off-line dictionary attack" [14]. If the encrypted authentication message sent by the user is captured by an attacker, they will not know the **PW** value required to create the

key needed to decrypt the message, and the protocol will fail without revealing any private information.

The B-AKE protocol can be operated using any biometric technology type from which a knowledge value can be extracted from biometric sensor data and represented in an unambiguous format agreed to by the communicating parties. The use of speaker recognition, hand gesture, and gait biometrics are all described in [15]. In the case of gesture biometrics, extracted knowledge can be "in the form of a passphrase or password", complex hand signs "such as the clinched fist, the hand-over-heart salute, and the benediction gesture", or user knowledge represented as "movements completely unrelated to any language" [15].

Some types of biometric technologies may become suitable for use in AAL environments when "a contrived context for biometric matching" can be provided that helps to improve their matching performance [15]. The context itself as a tagged object registered to the user in the IoT might also serve as "an additional authentication factor" or "layer of defense" [15]. Yun leveraged a contrived context for biometric data collection with gait biometrics, a technology type identified with relatively weak matching performance. In a study of biometric identification that targeted a small number of users in a home environment, Yun collected biometric data using a "floor-based system, *UbiFloorII*, which consists of a large number of photo interrupter sensors in wooden tiles" and used the "walking and stepping patterns from the walking samples" collected from a two-dimensional biometric sensor grid for gait biometric matching [17].

A user's weak secret intended for use as knowledge in a B-AKE protocol, could be conveyed through a stepping pattern extracted from the "order and identities of tiles encountered as participants traverse the grid" [15]. Based on unique identifiers assigned to each floor tile, users could select a series of identifiers by performing a memorized stepping pattern over the tiles. This selected set of values could form the `PW` secret needed to operate a B-AKE protocol [15].

Using gait biometrics in AAL applications has several appealing aspects. The collection of biometric samples from assistive persons is "unobtrusive and typifies the motion characteristics specific to an individual" [17]. Gait can be measured without the cooperation of AAL inhabitants, and an individual's characteristics "can be detected and measured at both a low resolution and a long distance" [17]. When considered as a source of user knowledge, gait biometrics can also offer the opportunity of providing secure access and confidential communications.

Conclusions

Authenticated Key Exchange (AKE) protocols can provide persons living in assistive environments less complex alternatives for secure access to services and information. Both PAKE and B-AKE protocols ensure mutual authentication that helps protect AAL inhabitants from phishing and man-in-the-middle attacks without users needing to possess and manage digital certificates or understand the complexities of their proper use. Choice of authentication methods gained from coupling easy to remember passwords with multiple biometric technology offerings can help AAL providers eliminate the isolation of people confined to in-home and assistive care facilities. By providing users with greater flexibility in how they authenticate, a greater number of people will be able to connect to the secure services, information, and communities they need to thrive.

References

[1] ICT Consultation. (2013). The ICT opportunity for a disability-inclusive development framework. Retrieved July 1, 2015, from http://www.itu.int/en/action/accessibility/Pages/hlmdd2013.aspx

[2] Hamdi, O., Chalouf, M. A., Ouattara, D., & Krief, F. (2014). eHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues. *Journal of Network and Computer Applications*, *46*, 100-112. Retrieved July 1, 2015, from www.sciencedirect.com/science/article/pii/S1084804514001672

[3] Ermakova, T., & Fabian, B. (2013, July). Secret sharing for health data in multi-provider clouds. In *Business Informatics (CBI), 2013 IEEE 15th Conference on* (pp. 93-100). IEEE.

[4] Griffin, P. (2015). Web services security for all. *Information Systems Security Association Journal*, Vol. 12, No. 9, September 2014.

[5] Mayron, L. M., Hausawi, Y., Bahr, G. S. (2013). Secure, usable biometric authentication systems. In *Universal Access in Human-Computer Interaction., Design Methods, Tools, and Interaction Techniques for eInclusion*, Volume 8009, pp 195-204. Springer Berlin Heidelberg.

[6] Topkara, U., Topkara, M., Atallah, M. J. (2007, June). Passwords for everyone: Secure mnemonic-based accessible authentication. In *USENIX Annual Technical Conference* (pp. 369-374).

[7] Griffin, P. (2012). U.S. Patent Number 8,289,135. Washington, DC: United States

[8] Griffin, P. (2014). Telebiometric authentication objects. Complex Adaptive Systems 2014 Proceedings. *Procedia Computer Science*, *36*, 393-400.

[9] Banks J, Pachano M, Thompson L, and Hanny D. RFID Applied - 2007. Hoboken, New Jersey: John Wiley & Sons, Inc.

[10] Griffin, P. (2014). Telebiometric information security and safety management. *Communications Magazine, IEEE*, *52*(1), 186-192.

[11] Griffin, P. (2015). Transport layer secured password-authenticated key exchange. *Information Systems Security Association Journal*, Vol. 13, No. 6, June 2015.

[12] Alsaid, A., & Mitchell, C. J. (2006, July). Preventing phishing attacks using trusted computing technology. In *Proceedings of the 6th International Network Conference (INC'06) (pp. 221228).*

[13] Engler, J., Karlof, C., Shi, E., Song, D. (2009). Is it too late for PAKE? In Web 2.0 Security and Privacy (W2SP) 2009.

[14] ITU-T X.1035: Password-authenticated key exchange (PAK) protocol (2007). Retrieved July 1, 2015, from, http://www.itu.int/rec/T-REC-X.1035-200702-I/en

[15] Griffin, P. Biometric knowledge extraction for multi-factor authentication and key exchange. unpublished. Retrieved July 1, 2015, from http://phillipgriffin.com/whitepapers/CAS-2015.doc

[16] Larmouth, J. L. (2000). *ASN.1 Complete*. Morgan Kaufmann. Retrieved July 1, 2015, from http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf.

[17] Yun, J. (2011). User identification using gait patterns on UbiFloorII. *Sensors*, *11*(3), 2611-2639, doi:10.3390/s110302611. Retrieved July 1, 2015, from http://www.mdpi.com/1424-8220/11/3/2611/htm