Biometric Electronic Signatures

By Phillip Griffin – ISSA Fellow, Raleigh Chapter

This article discusses mutual and multi-factor authentication based on passwords combined with biometrics.

Abstract

Biometric sensor data is rich in information content. A microphone, camera, or touch-screen device can collect sensor data for matching a user's biometric sample against a previously enrolled biometric reference template. This user sample can serve as a *something-you-are* authentication factor.

That same sensor data can also contain something a user knows, user knowledge, a *something-you-know* authentication factor. Both biometric matching data and user knowledge can be extracted from the same sensor data to enable strong, two-factor identity authentication. When user knowledge is a shared "weak secret" known only to communicating parties, it can be input into an authenticated key exchange (AKE) protocol, such as the password AKE (PAKE).

By operating an AKE protocol, communicating parties can achieve mutual authentication and establish a secure communications channel. A PAKE protocol can be coupled with biometrics to form a biometric AKE (BAKE) protocol. BAKE can enable two-factor user authentication and mutual authentication. However, BAKE is not only useful for authentication of a user identity. BAKE can be extended to create a biometric electronic signature that is convenient for use in electronic commerce, government signing, and automated smart contract applications.

Introduction

The *ISSA Journal* article, "Transport Layer Secured Password-Authenticated Key Exchange," describes using a password-authenticated key exchange (PAKE) protocol[1] "to achieve mutual authentication" [1]. PAKE has been proposed as a means of preventing phishing and man-in-the-middle attacks when embedded in the transport layer security (TLS),[2] and without "major changes to the TLS protocol" [1]. In their "Security Standardization Research" (SSR 2014)[3] conference paper [2] described in the *ISSA Journal* article, Manulis, Stebila, and Denham propose to augment the TLS protocol following a successful TLS handshake.

The addition of PAKE to TLS enables secure client-side authentication for the many users who lack digital certificates and who must rely instead on passwords to authenticate their identities. By inserting PAKE within the TLS protocol, client-side passwords are protected from exposure to attackers lurking on the line or impersonating the target server. The PAKE protocol provides mutual authentication so that password users can gain assurance they have connected to the intended server without exposing their credentials in the clear.

However, the use of PAKE for authentication and secure communications does not depend on the TLS protocol. PAKE can be used without TLS and to some advantage. PAKE "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" [1]. When combined with biometrics, PAKE offers a strong two-factor authentication alternative to TLS, one "well suited for implementation in resource-constrained environments, those limited by processing speed, limited memory, and power availability" [3], such as the Internet of Things (IoT).

1 Wikipedia, "Password-Authenticated Key Agreement," https://en.wikipedia.org/wiki/Password-authenticated_key_agreement.

2 Douglas Stebila, "Secure Modular Password Authentication for the Web Using Channel Bindings," https://www.douglas.stebila.ca/research/papers/SSR-ManSteDen14/.

3 SSR 2014, "Security Standardisation Research," http://ssr2014.com/.

These systems can provide convenient, easy-to-use, cost-efficient authentication and secure communications solutions in constrained environments, those not able to support the overhead of a PKI. Figure 1 provides a high-level depiction of the steps in a BAKE protocol.

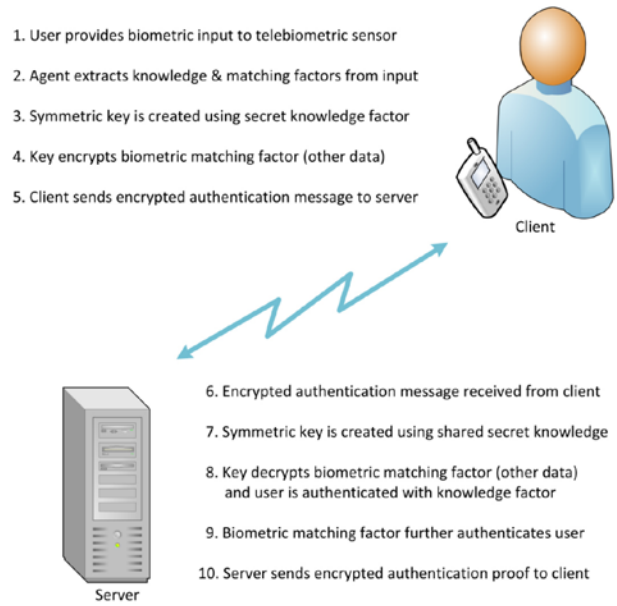

Figure 1 – Biometric authenticated key exchange (BAKE)

The PAKE protocol, and by extension BAKE, are based on a Diffie-Hellman key agreement scheme for key establishment. Instead of relying on public-private key pairs, PAKE relies on a weak secret shared by communicating parties. A weak secret is something a user can easily recall. Several PAKE mechanisms have been standardized internationally in the ITU-T X.1035: "Password-Authenticated Key Exchange" (PAK) recommendation[4] and in the ISO/IEC 11770-4 Key management – mechanisms based on weak secrets standard.[5]

Knowledge extraction

Secret knowledge shared between a user and server can be collected from a user and "presented to the system in many ways and formats" [4]. These range from "a simple password entered through a keyboard device, to a PIN entered using a smartphone touch screen, to human speech recorded by a microphone" [4]. Once data that contains user knowledge is collected, it must be converted or mapped into a suitable string format before it can be input into a PAKE protocol.

User knowledge can be extracted from biometric sensor data,[6] the same data source that collects user biometric matching samples. Many biometric types contain user knowledge, but an easily understood example is the case of voice biometrics. Consider a user with an established server account associat-

4 ITU, "X.1035 : Password-Authenticated Key Exchange (PAK) Protocol," http://www.itu.int/rec/T-REC-X.1035-200702-I/en - Freely available.

5 ISO, "ISO/IEC 11770-4:2006," https://www.iso.org/standard/39723.html.

6 Phillip H.Griffin, "Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange," *Procedia Computer Science*, Volume 61, 2015, Elsevier, freely available at http://www.sciencedirect.com/science/article/pii/S1877050915029804.

ed with a passphrase that is registered in some format of the words "how now brown cow." By speaking this phrase into a microphone sensor, both biometric matching data and user knowledge can be presented by the user to an identity-authentication system.

The collected raw sensor data can be passed along to a biometric verification system for user matching. The same sensor data can also be processed using a speech recognition tool such as the Google Cloud Speech API[7] to convert the user's speech into text. These converted words can be processed to map them into the exact format expected by the server, perhaps a set of words concatenated to form the string "hownowbrowncow."

This string format is suitable for input into a PAKE protocol. When this secret is associated with a server account, the user can be authenticated by simply speaking this phrase. The speakers words are "extracted from a voice biometric sensor using speech recognition techniques and formed into a password string" [4]. This input string returns a key from the Diffie-Hellman process and that key can be established on the server based on the password associated with the user account. The user credentials are never transferred in the clear.

Other biometric technology types can also be used with BAKE. Besides voice, sensors that can collect fingerprints and hand and facial gestures are now widely available on many mobile devices. They are also making their way into assisted living and healthcare environments where observations of user gestures can be collected by "image-based biometric authentication system" [3] sensors.

Gesture biometrics

In 2013, Fong, Zhuang, and Fister [5] described using captured video images of the hand gestures of an individual as input to an image-based, biometric authentication system. The authors referred to the data in these gestures, a "sequence of hand signs," as a "biometric password" [5]. The collected hand sign images, which represented letters of the alphabet, provided a context from which biometric feature extraction could be performed on the "hand shape and the postures in doing those signs" [5].

When the gestures provided by an individual represent characters or character strings in a user password, the sensor data collected can provide two distinct authentication factors, *something-you-are* biometric matching data and *something-you-know* user knowledge data. This capability is illustrated in the American Sign Language (ASL) symbols shown in figure 2. The results of their research implementation demonstrated that it is possible to collect two authenticator factors from a single user authentication attempt. The results also demonstrated that two authentication factor types could be collected using a single sensor input.

Other more traditional biometric technology types could also be used with hand gestures instead of relying hand shapes and

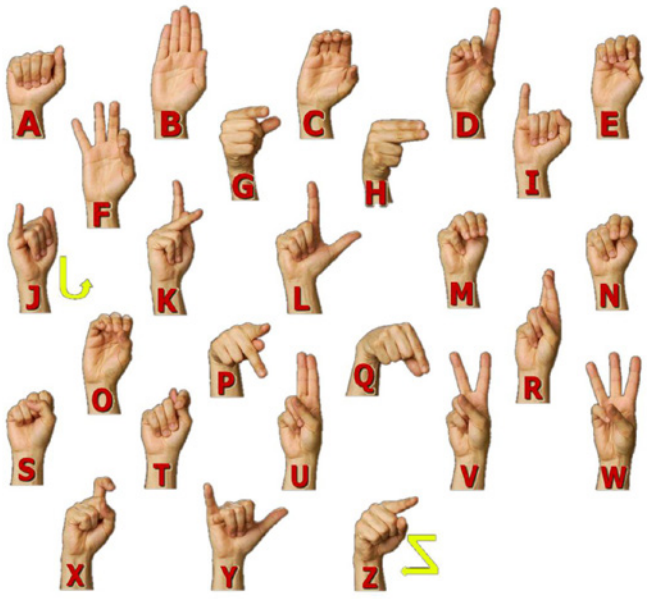

Figure 2 – American sign language (ASL) [7]

postures. User fingerprint matching data can be collected at distance from an individual's hand signs and extracted from captured images. If more than one sensor is used, a voice or face biometric can be collected and coupled with gestures collected by a different sensor. The gestures could provide a password value and the voice or face a biometric. Biometric authentication coupled with strong confidentiality protection during data transfer by using PAKE makes it possible to provide services to users with diverse abilities, such as greater access to information , and opens the possibility of providing new services, such as trusted remote-document signing.

Biometric electronic signature

The definition of an electronic signature (e-signature) can vary by legal jurisdiction. In the United States, an e-signature is specified under the Uniform Electronic Transaction Act (UETA)[8] and the Electronic Signatures in Global and National Commerce (ESIGN) Act.[9] These acts define an electronic signature as any process, symbol, or electronic sound performed by an individual and associated with information that the individual agrees to accept and sign, and an indication of intention to conduct an electronic transaction.

The 2017 version of the X9.84 Biometric Information Management and Security standard[10] specifies three new biometric-based e-signature techniques. These techniques are the biometric electronic signature token (BEST), signcrypted BEST (SBEST), and biometric electronic-signature authenticated-key exchange (BESAKE). Two of these techniques,

7 Google, "Cloud Speech API," https://cloud.google.com/speech/.

8 "Electronic Transactions Act Summary," Uniform Law Commission, http://www.uniformlaws.org/ActSummary.aspx?title=Electronic Transactions Act.

9 GPO, "Public Law 106 - 229 - Electronic Signatures in Global and National Commerce Act," US Government Publishing Office , https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html.

10 ANSI, "ANSI X9.84-2010 (R2017): Biometric Information Management and Security for the Financial Services Industry," ANSI, https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.84-2010+(R2017).

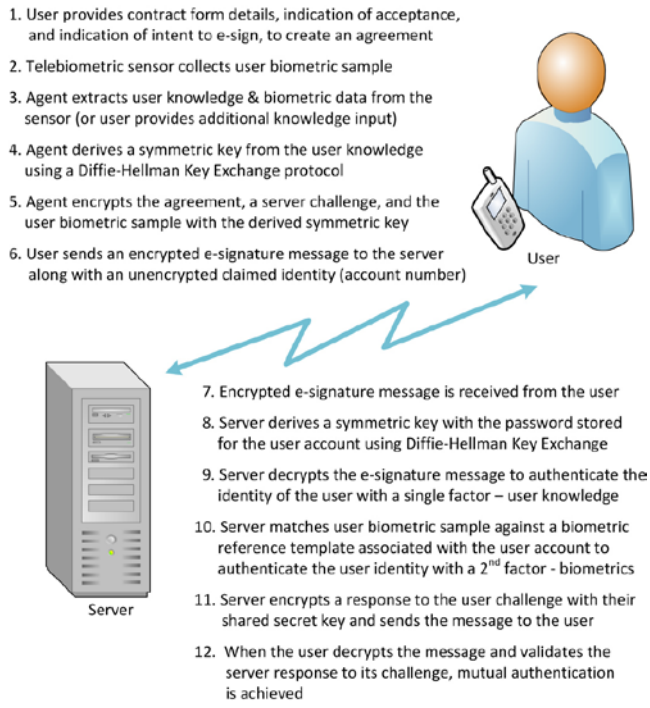

Figure 3 – Biometric electronic signature authenticated key exchange (BESAKE)

BEST and SBEST, rely on a functioning public key infrastructure (PKI). The BESAKE technique extends BAKE to create an e-signature protocol without the need for digital certificates.

These three techniques can be used to electronically sign agreements of any type or format. All three are intended for use in electronic commerce and other commercial or governmental signing events. These techniques provide multi-factor user authentication and mutual authentication, and protect the confidentiality of e-signer biometric data and other information. The X9.84 biometric e-signature techniques combine biometric authentication with cryptography and are suitable for use in cloud and distributed-ledger environments, including smart contract applications.

Figure 3 describes the BESAKE processing steps and illustrates how the BAKE protocol can be used for purposes other than user authentication, extending TLS, and establishing a secure communications channel.

Steps 1-6 in figure 3 describe how an encrypted BESAKE e-signature token is created. The token contains a proper e-signature agreement, including indications of acceptance of terms and intention to e-sign. The token also contains user biometric information, a server challenge, and any other data needed by a contract application. Steps 7-12 describe the processing required when validating the claimed identity of the e-signer. Processing of the actual agreement is left to the application.

BESAKE can be used to authorize a transfer of value in a smart contract. The encrypted results of steps 1-6 in figure 3 can be placed safely in a cloud, distributed ledger, or smart contract

```
BiometricData ::= SEQUENCE {
   version     Version,
   templateID  BiometricReferenceTemplateID  OPTIONAL,
   bsp         BiometricServiceProvider  OPTIONAL,
   type        BiometricType  OPTIONAL,
   biometric   BiometricData
}

Version ::= INTEGER { v1(1) } ( v1, ... )

BiometricReferenceTemplateID ::= OCTET STRING

BiometricServiceProvider ::= URI

URI ::= VisibleString (SIZE(1..MAX))

BiometricType ::= OBJECT IDENTIFIER -- Any identified type

BiometricData ::= OCTET STRING (SIZE(1..MAX)
```

Figure 4 – BESAKE biometric data schema

environment. In a smart contract context, chain code will cause steps 7-12 in figure 3 to be processed when a smart contract event signals that the contract has been performed. Step one of the BESAKE process can contain any type value object (i.e., a deed of trust) or transfer instrument permitted by an application. This might be in the form of digital currency, fiat currencies issued by governments, or commercial products such as zCash[11] or Bitcoin. Digital documents, including electronic checks and payment card authorizations and other promises to pay or transfer value may also be used.

Step 10 in figure 3 describes the second phase in multi-factor authentication of the user identity. The user may be enrolled in a biometric system local to the relying party server or enrolled with a third-party biometric service provider (BSP). Third-party enrollment and verification would require that the relying party server trust the BSP. One possible abstract syntax notation one (ASN.1) schema [6] to support user biometric matching portability is described in figure 4.

Here, an optional biometric reference template identifier can be provided to speed up locating the template of the claimed identity during the biometric matching process. When necessary, an optional URI can be included that locates the BSP needed to perform the matching using a specific template. Finally, an optional biometric technology type identifier can be included to identify the type of biometric sample data in the message.

Conclusion

Authenticated key-exchange protocols such as PAKE-based BAKE can be used to achieve strong, two-factor user authentication. BAKE can be implemented by pairing biometric matching data and user knowledge extracted from a single biometric sensor. Many different biometric technology types can provide two authentication factors, all without the overhead of TLS, digital certificates, and a properly functioning PKI.

The BAKE protocol can be used to create low cost, convenient-to-use, access control systems that can "help manage

11 zCash, "Internet Money," zCash, https://z.cash/.

the security risk of unauthorized access" [3] to information resources and to provide secure communications in resource-constrained environments unable to support certificate-based solutions. BAKE can also help to improve the user authentication experience, building user trust through mutual authentication, assurance that users are "actually connected to the systems they intended to connect to—systems that they can trust" [3].

BAKE ensures that user authentication credentials and other sensitive data are protected from man-in-the-middle and phishing attacks during the transfer of user authentication credentials, and during subsequent communications. BAKE can be extended into a protocol for e-signatures, BESAKE, to support e-signing documents in any format and type. Encrypted BESAKE message tokens are suitable for use in electronic commerce transactions and to authorize the transfer of value in smart contracts and other distributed-ledger technologies.

References

1. Griffin, P.H. (2015). "Transport Layer Secured Password-Authenticated Key Exchange," Information Systems Security Association Journal, Vol. 13, No. 6 (ISSA), The ISSA Journal, June, 2015. Retrieved September 12, 2017, from http://www.issa.org/?x9.
2. Manulis, M., Stebila, D., & Denham, N. (2014). "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. Retrieved September 13, 2017, from http://www.springer.com/us/book/9783319140537.
3. Griffin, P.H. (2017). "Secure Authentication on the Internet of Things," IEEE SoutheastCon 2017. Retrieved October 2, 2017, from http://ieeexplore.ieee.org/abstract/document/7925274/.
4. Griffin P.H. (2018) "Adaptive Weak Secrets for Authenticated Key Exchange," in Nicholson D. (eds) *Advances in Human Factors in Cybersecurity.* AHFE 2017. Advances in Intelligent Systems and Computing, vol 593. Springer, Cham. Retrieved October 4, 2017, from https://link.springer.com/chapter/10.1007/978-3-319-60585-2_2.
5. Fong, S., Zhuang, Y., & Fister, I. (2013). "A Biometric Authentication Model Using Hand Gesture Images," Biomedical engineering online, 12(1), 111. Retrieved October 1, 2017, from http://www.biomedical-engineering-online.com/content/12/1/111/.
6. Larmouth, J.L. (2000). "ASN.1 Complete," Morgan Kaufmann. Retrieved October 3, 2017, from http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf.
7. Vicars, W. (2011). Fingerspelling & Numbers: Introduction, American Sign Language University (ASL). Retrieved October 4, 2017, from http://www.lifeprint.com/.

About the Author

Phillip H. Griffin, CISM, has over 20 years experience in the development of commercial, national, and international security standards and cryptographic messaging protocols. Phil has a Master's of Information Technology, Information Assurance and Security degree and has been awarded 10 US patents at the intersection of biometrics, radio frequency identification (RFID), and information security management. He may be reached at phil@phillipgriffin.com.