Adaptive Weak Secrets for Authenticated Key Exchange*

Phillip H. Griffin

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

Abstract. This paper describes biometric-based cryptographic techniques that use weak secrets to provide strong, multi-factor and mutual authentication, and establish secure channels for subsequent communications. These techniques rely on lightweight cryptographic algorithms for confidential information exchange. Lightweight algorithms are suitable for use in resource constrained environments such as the Internet of Things where implementations require efficient execution, limited access to memory and small code size. Password Authenticated Key Exchange, and Biometric Authenticated Key Exchange protocols based on user knowledge extracted from biometric sensor data, both rely on weak secrets. These secrets are shared between a client and an access controlled server, and used as inputs to Diffie-Hellman key establishment schemes. Diffie-Hellman provides forward secrecy, prevents user credentials from being exposed during identity authentication attempts, and thwarts man-in-the-middle and phishing attacks. This paper describes the operation of these protocols using an adaptive knowledge substitution process that frequently modifies the weak secrets used for protocol operation without requiring disruptive user password changes. The password substitution strings used to implement this process can be far longer and more complex than the weak secrets people can easily memorize. The process described in this paper allows people with diverse abilities to use simple, easily recalled, quickly entered passwords and still benefit from the strength of long, complex strings when operating cryptographic protocols.

Keywords: Authentication · Biometrics · Key Exchange · Password · Security

1 Introduction

Information and Communications Technologies (ICT) provide a variety of services and make available opportunities that can enrich peoples lives and benefit our society as a whole. Recent research reveals that ICT-connected devices constitute the "technology with the greatest impact in promoting the inclusion of persons with disabilities" [1]. The growing ubiquity of smart phones and networked devices in the Internet of Things (IOT) heralds "a new age not only of information sharing in general", but an era of new opportunities to provide services to "disabled and non-disabled communities alike" [1].

In a world of over a "billion persons living with disabilities" [1], it is import that ICT applications and services are universally accessible. Access control systems that follow Universal Access (UA) design guidance can help remove barriers to ICT ac-

**Submitted to 8th International Conference on Applied Human Factors and Ergonomics (AHFE 2017) - Human Factors in Cybersecurity - Personal Copy* cess and reduce the exclusion of the elderly and infirm [1]. Following UA principles can help all people enjoy the benefits of securely "accessing, participating and being fully-included in social, economic and political activities" [1].

Universal access is a methodology that incorporates human factors into user interface design in an effort to provide "the utility of modern information technology to as broad a range of individuals as possible" [2]. Considering the vast differences between individuals, who may be young, elderly, healthy, infirm, disabled or not disabled, provision of a single, monolithic access control interface is not likely to achieve the goals of UA. Serving the needs of a diverse population requires offering people choices in the ways they gain access to information and communications systems. There is greater potential for integrating "security and usability effectively" in access control systems based on "biometrics than with other authentication methods" [2]. This makes biometric technologies a "natural choice for implementing authentication in UA systems" [2].

People have diverse abilities that may impede or prohibit their use of a particular access control method or interface. Individuals afflicted with "dyslexia can have problems in remembering the digits in the correct order", or have trouble spelling or reading [3]. This can make password-based access control using a keyboard device difficult. Users with degenerative arthritis, "limited use of arms or hands", and those with a "cognitive impairment will find most biometric systems much easier to use and provide them a greater level of security" [3]. Since every individual is not capable of using every type of computer input device or every biometric technology type, authentication systems with user interface designs that offer users a variety of choice alternatives will be capable of offering access to greater numbers of users.

Identity authentication is a critical security control for managing the risk of unauthorized access to information and communications technology (ICT) systems. The cost of deploying credentials that enable strong user authentication can be prohibitive. User convenience can also be an issue and creating effective, inclusive design can be a challenge. Offering authentication methods that include passwords and biometrics or that combine the two can lead to low-cost, secure solutions that are convenient and easy to use by persons with diverse abilities.

2 Biometric-Based Cryptographic Techniques

Weak secrets are those "that can be easily memorized" by a user and that are often "chosen from a relatively small set of possibilities" [4]. Passwords, passphrases and Personal Identification Numbers (PIN) are examples of weak secrets. They are easily recalled by users, typically short in length, and are composed from a limited set of characters. Weak secrets are commonly used in access control systems today, and serve as a *something-you-know* identity authentication factor.

Weak secrets also play a role in authenticated key exchange (AKE) protocols, where they function as shared secret inputs to a Diffie-Hellman key exchange process. Password Authenticated Key Exchange (PAKE) is a protocol that allows two remote parties "to establish a secure communication channel" between them "without relying on any external trusted parties" [5]. Establishment of the secure channel is based "on a shared low-entropy password", a weak secret known to both parties. This shared secret is used in the PAKE protocol to provide implicit identity authentication [5].

In a Password Authenticated Key Exchange (PAKE) protocol the confidentiality of user authentication credentials is protected by encryption from identity theft, man-in-the-middle (MITM), and phishing attacks during transfer [6]. PAKE has been suggested as a way to remediate these attacks in the Transport Layer Security (TLS) protocol by inserting PAKE following the TLS handshake [7]. This approach still relies on digital certificates, which can be cost prohibitive in some applications. In practice, neither digital certificates nor TLS are needed by PAKE for access control systems to achieve mutual and multifactor authentication.

Biometric Authenticated Key Exchange (BAKE) is a "biometrics-based protocol for authenticated key exchange" [8] that relies on PAKE. The BAKE protocol extracts "knowledge shared by communicating parties" needed to operate a PAKE protocol "from data collected by biometric sensors" [8]. Once extracted, this user knowledge is input to a PAKE protocol to derive an encryption key. This key is used to protect a user biometric sample, a *something-you-are* identity authentication factor, during a user authentication attempt. By including a biometric sample in the user credentials protected during transfer by PAKE and BAKE, both protocols can achieve 2-factor user authentication.

Telebiometric Aauthentication Objects (TAO) are “tagged physical objects" that have been associated with a user by a relying party. This association allows TAO to be used as a *something-you-have* identity authentication factor. These objects are "functionally coupled with biometric sensors and connected to a telecommunications network” [9]. TAO combine telecommunications networks with biometric sensors to enable identity authentication and user identification services. These 'smart objects' enable IoT access controls that offer “strong, low cost mutual and multi-factor authentication” that are frequently readily available (i.e., smart phones) and can be easy for many people to use [6].

During the user authentication phase of a PAKE or BAKE protocol, TAO can be included in the user credentials to provide an additional identity authentication factor. By combining biometric authentication with registered TAO during operation of an AKE protocol, 2- and 3-factor user authentication can be achieved. User credential transfer and subsequent information exchange needed to achieve mutual authentication require that all data transfers be protected by strong encryption.

3 Internet of Things Security Limitations

Building a world of universal healthcare, ambient assisted living, and IoT-based services for reliable delivery to remote environments requires secure, universal access to ITC resources. As the 5th generation (5G) of mobile and wireless networks replace existing infrastructure, "future networks are likely to benefit from high reliability and security, very high speeds and increased reach and mobility" [10]. Though coming improvements in network security are helpful, implementers still need to ensure "data protection and privacy" of stored user data [10]. They must also protect the authenticity and confidentiality of sensitive user authentication credentials and the end-to-end "secure, reliable and consistent exchange of data between devices, applications and platforms" [10].

As the expanding IoT ages, it will contain ever growing numbers and types of devices, "information technology systems and software applications" that once deployed, must maintain their ability to continue "to communicate, exchange data, and use the information that has been exchanged" [11]. Effective encryption solutions are needed that can perform well on both small IoT devices, and on larger platforms in the data centers they access. These solutions must be capable of being implemented, not only on high speed networks and resource rich servers, but on the small computing devices that will still be common on the IoT for many years to come.

The need to secure devices in the IoT has fueled research and development of a family of lightweight cryptography solutions, "cryptographic primitives, schemes and protocols tailored to extremely constrained environments" [12]. The term 'lightweight' should not be viewed negatively. The term does not imply that lightweight cryptography is 'weak', but that it offers efficiencies in its "execution time, runtime memory (i.e. RAM) requirements, and binary code size" [12]. Lightweight algorithms can provide "the cryptographic strength needed to protect sensitive user credentials during identity authentication, and during subsequent communications" [13].

Both PAKE and BAKE rely on Diffie-Hellman key exchange for cryptographic key establishment. The user establishes a key to protect their credentials when attempting access, and the accessed server establishes the same key to perform mutual authentication and protect client-server information exchange during transfer. Once a key is available, a symmetric key algorithm is used to protect the confidentiality of user credentials during an authentication attempt and subsequent communications.

User credentials may include a biometric sample collected from the user to provide a *something-you-are* identity authentication factor. Credentials may also include one or more physical objects associated with the user biometric reference template and known to the server [9]. These authentication objects may be tagged objects that have been preregistered with the server for use as *something-you-have* authentication factors [9]. When these objects are coupled with telecommunications-enabled biometric sensors, they can be "used for mutual and multifactor authentication in access control systems" [13].

4 Lightweight Cryptographic Algorithms

The Advanced Encryption System (AES) algorithm is considered "an excellent and preferred choice" for "almost all block cipher applications" [14]. However, the AES algorithm is "not suitable for extremely constrained environments such as RFID tags and sensor networks" [14]. These environments are common in the IoT, where applications may require "security and hardware efficiency" [14], but are constrained by limited power, communications bandwidth, or processing capabilities.

The ISO/IEC 29192 lightweight cryptography standard specifies symmetric key-based cryptographic primitives for block cipher, stream cipher, hash function, and Message Authentication Code (MAC) algorithms. Part 2 of the series will soon define four symmetric block ciphers, the PRESENT, CLEFIA, SIMON, and SPECK algorithms described in the following tables. The PRESENT and CLEFIA lightweight algorithms first appeared in the current version of the standard, the 2012 edition. Both algorithms had been introduced some five years earlier, PRESENT at the CHES 2007 Workshop on Cryptographic Hardware and Embedded Systems [14] and CLEFIA at FSE 2007, the Fast Software Encryption Workshop [15].

As shown in Table 1., the PRESENT cipher has "a block size of 64 bits and a key size of 80 or 128 bits"[16]. PRESENT requires 32 processing rounds, with each of the rounds consisting of a "sequence of simple transformations" [16]. Each processing round introduces a new round key, with the last round key used for final processing. The creators of PRESENT considered hardware efficiency in their design resulting in an implementation that required only 1580 GE to encrypt a 64-bit block using an 80 bit key [14].

Table 1. PRESENT algorithm characteristics

PRESENT-128 and PRESENT-80			
Block Size (bits)	**Key Length (bits)**	**Number of Rounds**	**Round Keys**
64	128	31	32
64	80	31	32

As shown in Table 2., the CLEFIA cipher has "a block size of 128 bits and a key size of 128, 192 or 256 bits" [16]. The number of processing rounds and the number of round keys needed varies by key length. Longer keys have greater processing requirements. CLEFIA has a structure "based on a generalized Feistel network" [13] and that is used "data processing part and the key schedule" [16].

Table 2. CLEFIA algorithm characteristics

CLEFIA			
Block Size (bits)	**Key Length (bits)**	**Number of Rounds**	**Round Keys**
128	256	26	52
128	192	22	44
128	128	18	36

Work began in 2015 to add SIMON and SPECK block cipher families to a revision of the ISO/IEC 29192-2 standard. Approval of this revision is expected in 2017, but the revised standard has yet to be published. SIMON and SPECK are relatively recent block cipher proposals created by "researchers from the National Security Agency (NSA)" of the United States [17].

Both algorithms offer "efficient and secure" encryption that provide a means of achieving solutions that are "low-cost and easy to implement and deploy on multiple platforms" [17]. These algorithms target a range of platforms and applications, from "mobile devices, through RFID tags to electronic locks" [17]. Their cryptographic strength and efficiency makes them "appealing for use in IoT applications" [13].

SIMON and SPECK both offer "very competitive performance, small memory footprint" that beats "most existing lightweight ciphers in terms of efficiency and compactness" [17]. Both block cipher algorithms are based on "very simple and elegant" designs built on the Addition/Rotation/XOR (ARX) philosophy [17]. The class of ARX algorithms rely on a set of "simple arithmetic operations: modular addition, bitwise rotation (and bitwise shift) and exclusive-OR" [18].

Table 3. SIMON, and SPECK algorithm characteristics

SIMON and SPECK	
Block Size (bits)	**Key Length (bits)**
128	256
128	192
128	128
96	144
96	96
64	128
64	96
48	96

As shown above in Table 3., the range of key sizes to be standardized for SIMON and SPECK span those supported by both their PRESENT and CLEFIA predecessors. Both algorithms offer cryptographic strength sufficient to protect user credentials and subsequent information exchange in the operation of the BAKE and PAKE protocols. They make flexible IoT implementation designs to manage security risks possible, offering "great performance on hardware and software platforms" [19] The SIMON block cipher is "designed towards hardware applications and SPECK for software applications" [19].

5 Adaptive Password Substitution Strings

When a user first establishes an account on a multi-user computer system, they are assigned a system-unique identifier. This account name or user identifier (user ID) is presented by the user along with identity authentication credentials during subsequent login events. Information management and security information used to control user access may be associated with a user account name and stored by the system.

One or more user identity authenticators, such as a password or biometric reference value will also be stored and associated with the user ID. To establish a biometric authenticator, then user must enroll in a biometric system to create a biometric reference template for each biometric type being enrolled. Biometric reference templates are used by the access control system to match user biometric samples during authentication attempts subsequent to enrollment.

When Telebiometric Authentication Objects (TAO) are used to authenticate a user in an access control system, an identifier of each user possession must be associated with the user ID or biometric reference template of the user. When a BAKE or PAKE protocol is used for multifactor user authentication, user selected knowledge information must also be bound to the user ID and known to the server before being used for identity authentication and to operate a BAKE or PAKE protocol.

User knowledge information known to a server and associated with a user account can be used as a *something-you-know* authentication factor. This knowledge can be presented to the system in many ways and formats, ranging from a simple password entered through a keyboard device, to a PIN entered using a smart phone touch screen, to human speech recorded by a microphone, to "observations of a sequence of gestures collected by an image-based biometric authentication system" [13]. For use as an input to an AKE protocol, each type of knowledge presentation must be presented to the protocol in a character string format. For example, the words of a human speaker can be extracted from a voice biometric sensor using speech recognition techniques and formed into a password string.

It is usual to consider "gestures based on American Sign Language (ASL) hand signs" [13] as single character values that collected together may be short, and easy for the user to recall and present. This can lead to AKE inputs that may be easily guessed by an attacker, or to system-forced frequent changes to user passwords. Such changes may be disruptive to users and lead to behaviors that thwart security goals.

User-memorized passwords can be associated with complex password 'substitution strings' selected by a server. The password and substitution strings can be securely stored on the server and preloaded on a user controlled device at the time a password is selected by the user and registered to the system. This password to substitution string mapping is illustrated in the first two columns of Table 4.

Table 4. Password substitution strings before and after mutual authentication acknowlegement

User-Memorized Password		**1st Substitution String Value**	**2nd Substitution String Value**
	A	`N|f4&64ejotU$5$E`	`PoQd,8H'*6Z0v|oH`
	H	`7#ktM0tzcbvz/+uN`	`+Qm\2XE&nw]vgGy|`
	F	`B[p8Gu56Wg54TjQj`	`F_lH.(uU67Jgq2~O`
	E	`/7|-:?%Xc|X$Tsv/`	`;}-c%y.,rS[Pm:h:`

In Table 4., the user presents the password 'AHFE' to the access control system using ASL hand signs [20]. Prior to operation of a PAKE protocol, each letter is mapped to its associated substitution value to become the effective password string, "N|f4&64ejotU$5$E7#ktM0tzcbvz/+uNB[p8Gu56Wg54TjQj/7|-:?%Xc|X$Tsv/". This derived value is used as the password input to the PAKE protocol, which uses the

Diffie-Hellman protocol to create an encryption key. This key is used with a cipher to protect user credentials sent to the server, along with an unprotected user ID, during the authentication process.

On receipt of the encrypted user message, the server uses the plaintext user ID to located the password substitution strings of the user. The server uses these string to form the effective password needed to derive the same symmetric encryption key used to encrypt the message, then decrypts the ciphertext. Once the user has been authenticated, the server responds to assure the user of its identity.

During this final mutual authentication step of the PAKE protocol, all information exchange are encrypted using the shared secret key. During this protected communication, the server can create and load a new set of password substitution strings on the user device and on the server. On both devices, the current password substitution strings and the new strings are maintained until the user responds to the server, indicating the new strings have been received.

The server may then update their copy of the password substitution strings to a new set of values to be used during the next user authentication attempt, as shown in the third column of Table 4. The user can also update their local copy of the new strings without any changes to their actual password value, 'AHFE'. Both user and server may maintain the replaced strings to mitigate the risk of substitution string update errors. In this way the user and the server can dynamically adapt to new effective password values without disruptive changes to the familiar password memorized by the user. This adaptive processes can be performed as frequently as each user access, and effectively provides the user with an automated, one-time-password capability. This reduces the likelihood from forced user password changes of "access to an account by an attacker who has captured the account's password" and who can guess the new password chosen by the user as a replacement based on their prior selections [21].

6 Conclusion

Biometric Authenticated Key Exchange (BAKE) and its underlying Password AKE protocol rely on weak secrets that can be used to provide strong, affordable mutual and multifactor authentication. Both protocols protect user credentials during identity authentication, enable forward secrecy, and are resistant to man-in-the-middle and spoofing attacks. They can leverage lightweight block ciphers to secure communications when using AES is not practical. BAKE and PAKE do not require users to manage digital certificates or to rely on the existence of a functioning public key infrastructure. When offered as choice alternatives, these security techniques provide support for universal user access.

The lightweight block ciphers defined in ISO/IEC 29192-2 are designed for use in resource constrained environments, such as those found in the IoT. Lightweight cryptography is not weak, but uses fewer resources than algorithms commonly found in desktop and data center environments. The algorithms can protect user credentials during identity authentication attempts, and they can provide confidentiality services during subsequent communications.

Once BAKE and PAKE have established a secure channel for communications, user password substitution strings can be securely refreshed. These user password proxies can be changed as frequently as needed without changing the underlying user password. This process ensures that complex, frequently changing secrets that are far too difficult for a user to memorize are used as inputs to BAKE and PAKE, while ensuring user convenience is maintained. User can avoid frequent password changes, choose easily recalled and easily entered passwords, and still enjoy the security benefits of password complexity and frequent password changes.

References

1. ICT Consultation. (2013). The ICT Opportunity for a Disability-Inclusive Development Framework. Retrieved February 25, 2017, from http://www.itu.int/accessibility
2. Mayron, L. M., Hausawi, Y., & Bahr, G. S. (2013, July). Secure, usable biometric authentication systems. In *International Conference on Universal Access in Human-Computer Interaction* (pp. 195-204). Springer Berlin Heidelberg. Retrieved February 22, 2017, from https://www.researchgate.net/profile/Gisela_Bahr/publication/
3. Center for Excellence in Universal Design. (2013). Cardholder Authentication. Retrieved February 25, 2017, from http://universaldesign.ie/Technology-ICT/Irish-National-IT-Accessibility-Guidelines/Smart-Cards/Making-Smart-Card-Services-Accessible/Cardholder-Authentication/
4. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 11770-4
5. Hao, F., & Shahandashti, S. F. (2014). The SPEKE Protocol Revisited. *SSR*, *14*, 26-38. In: Chen, L., Mitchell, C. (eds.) Security Standardisation Research: First International Conference, SSR 2014, London, UK, December 16–17, 2014. Retrieved February 23, 2017, from https://eprint.iacr.org/2014/585.pdf
6. Griffin, P.H.: Biometric-based cybersecurity techniques. In *Advances in Human Factors in Cybersecurity*, (2016), pp. 43-53. Springer International Publishing
7. Griffin, P.H.: Transport Layer Secured Password-Authenticated Key Exchange. Information Systems Security Association (ISSA) Journal, vol. 13, no. 6, June, 2015
8. 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.
9. Griffin, P.H.: Telebiometric Authentication Objects. Complex Adaptive Systems Proceedings. Procedia Computer Science, 36 (2014), pp. 393--400. Elsevier B.V.
10. International Telecommunications Union (ITU) Broadband Commission for Sustainable Development. (2017). Digital Health: A Call for Government Leadership and Cooperation between ICT and Health. Retrieved February 28, 2017, from http://www.broadbandcommission.org/Documents/publications/WorkingGroupHealthReport-2017.pdf
11. World Health Organization, Atlas of eHealth Country Profiles 2015: The use of eHealth in support of universal health coverage. Retrieved February 28, 2017, from http://www.who.int/goe/publications/atlas_2015/en/
12. D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov. (205). Triathlon of Lightweight Block Ciphers for the Internet of Things. *IACR Cryptology ePrint Archive* 2015: 209.
13. P. Griffin. (2017, April). Secure Authentication on the Internet of Things. IEEE SoutheastCon 2017.

14. Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. Retrieved January 22, 2017, from https://link.springer.com/chapter/10.1007/978-3-540-74735-2_31
15. Shirai T., Shibutani K., Akishita T., Moriai S., Iwata T. (2007) The 128-Bit Blockcipher CLEFIA. In: Biryukov A. (eds) Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, vol 4593. Springer, Berlin, Heidelberg. Retrieved January 18, 2017, from https://link.springer.com/chapter/10.1007/978-3-540-74619-5_12
16. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2012). ISO/IEC 29192-2 Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers
17. A. Biryukov, A. Roy, and V. Velichkov. (2014). Differential analysis of block ciphers SIMON and SPECK. In *Fast Software Encryption* (pp. 546-570). Springer Berlin Heidelberg.
18. A. Biryukov, V. Velichkov, and Y. Le Corre. (2016). Automatic search for the best trails in arx: Application to block cipher speck. In *Fast Software Encryption–FSE.*
19. S. Bhasin, T. Graba, J. Danger, and Z. Najm. (2014). A look into SIMON from a side-channel perspective. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on* (pp. 56-59). IEEE.
20. W. Vicars, *American Sign Language (ASL)*. (2011). Retrieved January 14, 2017, from http://www.lifeprint.com
21. Y. Zhang, F . Monrose, and M . K. Reiter. "The security of modern password expiration: An algorithmic framework and empirical analysis." In Proceedings of the 17th ACM conference on Computer and communications security , pp. 176- 186. ACM, 2010.