Web Services Security for All

By Phillip H. Griffin – ISSA Fellow, Raleigh Chapter

Secure web services currently play an important role in information sharing and in smart meter and smart home systems integration. This article proposes standardization of existing web-services security tokens to enhance their performance and suitability for use in resource-constrained environments. Creation of a new security token to support both biometric authentication and biometric identification is also proposed.

Abstract

Secure web services currently play an important role in information sharing, and in smart meter and smart home systems integration. They can also help to strengthen our communities, promoting the inclusion of disabled and non-disabled persons, if more authenticated access methods can be offered. Greater availability can be provided for all users by standardizing alternative authentication methods for secure access to web services. More alternatives, such as biometric authentication, will enable better support for the accessibility needs of impaired and elderly users. Greater web service availability can give more users access to the information and services they need from the always-on Internet. Standards for web services are key requirements for providing greater access to the Web for all users and for enabling the development of new technologies.

Service-oriented architecture (SOA) and software design have made it possible for information and communication technology (ICT) applications to cooperate across the worldwide Web. Loosely coupled applications can be constructed from discrete, reusable service components that communicate asynchronously through web-service messages. These messages may be based on a variety of proprietary or standardized formats, but it is common for web-service messages to be specified using the Simple Object Access Protocol (SOAP) defined by the World Wide Web Consortium (W3C).

Web services have become increasingly important to both individuals and business organizations. They can facilitate information exchange between people and ICT systems and between distributed applications. Today, web services help make the integration of new functionality into existing systems, such as smart metering and smart home networks, less complex. Solutions built using service-oriented software can often be integrated into existing systems without the need for extensive system modifications. The benefits of web services can be extended to greater numbers of people if additional authentication methods that reduce barriers to access can be provided.

The information, services, and increased opportunities that web services make available help to enrich the lives of individuals and our society as a whole. Web access allows people to obtain government services, read books, view films, attend school, and more. According to a recent survey, web services and the ICT devices used to access them constitute the "technology with the greatest impact in promoting the inclusion of persons with disabilities" [1]. Along with mobile phones, they 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].

People of all ages who suffer from physical or cognitive disorders can have difficulty typing in a PIN or remembering the correct order of characters in a password. Biometric technologies, such as face and voice recognition, can provide elderly and disabled users with effective alternatives to using passwords and PINs for secure access to web services and information. Standardized secure biometric identification can enable convenient access to services in smart homes and other environments that can be easy to use by elderly and disabled persons.

This paper proposes International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) standardization of existing web-services security tokens to enhance their performance and suitability for use in resource-constrained environments. Creation of a new security token

to support both biometric authentication and biometric identification is also proposed. This new standardization work should build on existing web services and SOAP recommendations. A new biometric security token should leverage the recent efforts in ITU-T to create a new cryptographic message syntax (CMS) standard. This work includes support for the signcryption cryptographic primitive defined in the ISO/IEC 29150 standard, a new CMS type recommended in "Telebiometric Security and Safety Management" [2].

Integration

Smart grid messaging

Smart meters connected to smart homes are a cornerstone of a global vision for achieving the benefits of a smart grid. Smart metering systems result from the convergence of information and communications technologies (ICTs) with existing electricity and gas distribution systems. Smart homes result from the convergence of ICTs with home appliances and devices. For the smart grid vision to be realized, implementations must be efficient, reliable, and secure.

Web-service messages are used to integrate smart meter and smart home systems into existing energy provider systems. The security of these messages as they travel across unprotected networks is critical for safe and reliable smart grid operation. Secure web services provide authentication between communicating applications and help to ensure data integrity, origin authenticity, and the confidentiality of personally identifiable information and sensitive business data. Secure messaging provides a safeguard for both energy providers and their customers.

Smart meter and other smart grid implementations can benefit from a compact data representation that can be stored, processed, and transferred efficiently. These implementations need to be based on widely accepted standards for information exchange to increase the chances of interoperability. Current ITU-T web-service recommendations based on the Abstract Syntax Notation One (ASN.1) standards can address these needs.

The processing and transfer efficiency and data compression requirements of smart grid messaging can be met by ITU-T recommendation X.892 Fast Web Services. X.892 is a generic application of ASN.1 and specifies an extension of the W3C SOAP standard that provides "compact and easily-processed binary encodings of XML data" [3].

The X.892 recommendation makes possible SOAP messages "that require less network bandwidth and less processing power" and provide a "higher transaction processing rate" than messages that use the XML character encoding specified in the W3C SOAP standard [3].

As with W3C SOAP messages, X.892 messages can be extended to provide necessary security services. These characteristics make X.892 messages ideal for use in smart grid and other resource-constrained environments, such as the mobile telecommunications environment increasingly favored by individuals for ICT access.

Zone-based security

Secure web-service messages enable the implementation of SOA security zones. Security zones are a design concept used to separate parts of an integrated computer solution into areas that have common security requirements. When integrating new smart grid technology into existing utility systems, a SOA security zone can be placed between a utility's business operational networks and advanced metering infrastructure (AMI) networks [4]. This serves to insulate the business systems from the AMI by allowing them only to communicate and exchange information indirectly with each other using authenticated SOAP messages processed in the SOA security zone.

Smart home networks can also benefit from this design. A SOA security zone might be used to isolate the home network from the AMI backhaul network of meters, collectors, repeaters, and field area network (FAN) routers. The SOA security zone concept can also be used to insulate mobile device users from servers on the Internet, restricting information exchange to only secure messages.

Typically, a SOA security zone will be protected by network firewalls, intrusion detection systems, security event monitoring, and audit logging [4]. This allows the SOA security zone to function as a demilitarized zone (DMZ) between the AMI and utility business networks, facilitates cyber security management, and informs security incident response and disaster recovery processes.

Secure web-service messages are a critical component of SOA security zone integrations. Organizations that integrate smart grid solutions will benefit greatly from standardized web-services security messages. Standard security messages promote vendor interoperability and can reduce the time and effort needed for systems integration. Greater options for vendor selection are created when secure messaging solutions are based on vendor-neutral standards rather than on proprietary and ad hoc formats.

Authentication

Enabling technologies

Access to information and web services is spreading rapidly due to the explosive increase in the use of mobile phones. Mobile phone usage has seen increases in both developed and developing nations, but the changes have been most dramatic in the latter. For example, there are currently some 700 million mobile phone users in Africa, far more than the number of users in North America. As mobile phones continue to evolve into ever more sophisticated platforms for Internet access, there are increased opportunities for providing a greater variety of standardized authentication methods for user access.

Mobile devices, such as smartphones and tablet computers, contain a "rich array of sensors" that can support "many authentication methods beyond passwords and PIN codes, including biometrics" [5]. When mobile device users are presented with multifactor authentication solutions that offer "multiple ways to authenticate," these users have the potential to choose access methods that are best suited to their own unique abilities and needs [5]. Multiple alternatives for multifactor authentication have the potential "to improve usability by offering multiple ways to authenticate and to improve security by providing several proofs of identity" [5].

When offered choice alternatives, users can avoid choosing authentication methods they are unable to use due to a disability or their environment. Alternative authentication methods that enable access to secure web services should be standardized. A new web-services security token that supports biometric technologies could be used to construct access control solutions for users who are unable to access the Web using password authentication, or unable to use keyboard devices.

Biometric authentication

Current web-service security standards rely on conventional methods of access control that better meet the needs of computer applications than human beings. Users are commonly required to enter a user name and password or secret number through a keyboard to gain access. When keyboard use is required for authentication, disabled and elderly users may not be capable of gaining access to information and services.

People who suffer from learning disorders, such as dyslexia or developmental arithmetic disorder, can have problems processing symbols in a passphrase or in remembering the correct order of digits in a PIN. Their use of voice or fingerprint biometrics for authentication can be much easier. People without hands or arms may be unable to use a keyboard device. These users and those of all ages who suffer from cognitive impairments may find it easier to gain secure access to the web using biometric systems that offer a variety of authentication choices. Not every person can use every biometric technology type.

When an authentication system can offer a variety of alternative biometric technologies for access, a greater number of users will be able to succeed in gaining access. A SOAP extension to support biometrics could be defined as a secure message using the SigncryptedData type recently proposed and approved for ITU-T standardization in a new work item assigned to SG17 [2]. Using a cryptographic message syntax (CMS) SigncryptedData type, a biometric security token could be defined as follows:

```
<S:Envelope xmlns:S="...">
 <S:Header>
  <wsse:Security xmlns:wsse="...">
   <wsse:SigncryptedData
     xmlns:wsse=
      "http://schemas.xmlsoap.org/"
     Id="biometric-security-token"
     ValueType="wsse:SG17v1"
     EncodingType="wsse:PER">
       MIIEZzMJMzCCA9CzPHGzAwIBA ...
   </wsse:SigncryptedData>
  </wsse:Security>
 </S:Header>
<S:Body>
    ...
</S:Body>
```

The new SigncryptedData type has three processing modes: signcrypted-content mode, signcrypted-attributes mode, and signcrypted-components mode:

1. In the signcrypted-content mode data content of any type can be signcrypted.
2. In the signcrypted-attributes mode, data content of any type along with attributes of any type can be signcrypted.
3. In the signcrypted-components mode, elements of the data content are signcrypted, and then the resulting content is digitally signed along with a set of associated attributes. This process cryptographically binds the attributes to the data content [6].

A SigncryptedData message contains a set of per-message-recipient information to support multiple message recipients. Each element in the set provides a cryptogram and information for the entity whose public key is used by the message sender to perform signcryption operations. The same recipient public key is used to signcrypt message components and to sign the overall message [6]. The message contains a cryptogram that is smaller and more efficiently processed than the results of a sign-then-encrypt or encrypt-then-sign process. SigncryptedData and its processing are described in great de-

tail in "Signcryption Information Assets," *The ISSA Journal*, June 2012.[1]

Future standardization

Smart web services

Standards such as X.892 that enable fast, efficient, and secure web services can help turn the vision of a smart grid into reality. Increased processing rates and reduced power requirements made possible by X.892 messaging are characteristics that make it ideal for use in smart metering applications, in home network systems, and in other resource-constrained environments. Implementations of X.892 could gain the benefits of compact, efficient, binary processing for data transfer and storage, and still leverage XML markup when needed.

X.892 Fast Web Services can meet these requirements if the recommendation remains aligned to the SOAP standard, and if X.892 messages promote secure web service access. Currently, X.892 is based on an old edition of SOAP. The SOAP standard has seen two new editions since publication of X.892 in 2005. These changes to SOAP present risk to X.892 adopters of not complying fully with current SOAP requirements. A revision to update and align X.892 could mitigate this risk and provide users assurance of alignment with the current edition of W3C SOAP.

X.892 does not support SOAP messages represented in ASN.1 Basic Encoding Rules (BER) format. BER is commonly used in cryptographic messaging [2] and other information security standards to define the schema for signed email, X.509 digital certificates, and the X.500-series Directory. X.892 requires that the ASN.1 Packed Encoding Rules (PER) be used and does not support BER.

While X.892 does not prohibit the use of web services security (WSS) security token profiles in its SOAP messages, the standard does not support the BER encoding of the PKCS7 token. X.509 digital certificates are distributed using the PKCS7 token during secure information exchange. The content of PKCS7 tokens is the BER encoded SignedData type specified in the cryptographic message syntax (CMS) protocol [2] used to support signed and encrypted email and other secure messaging applications.

X.892 was developed in tandem with the X.891 Fast infoset standard. The PER restriction ensured that X.892 provided the most compact SOAP messages possible when used with the X.891 standard. However, if BER encodings were permitted, X.892 could support widely deployed security standards such as CMS, and benefit SOAP implementations that include WSS PKCS7 security token elements. Permitting the use of BER would require revising X.892.

While not as compact or efficient to process as PER, SOAP messages containing WSS content would be less complex if represented in only one set of encoding rules. BER SOAP messages would still be much smaller and more efficient to process than W3C SOAP messages represented in XML markup. Permitting BER in X.892 would simplify the use of WSS security tokens in fast web services, and could broaden adoption of X.892 in applications that use SOA and SOAP messaging for integration.

Web services security

The OASIS Web Services Security (WSS) standard specifies a set of security tokens that facilitate authentication of computer systems and human users that rely on SOAP messages to access web services. WSS includes tokens to support the use of X.509 digital certificates, certificate revocation lists (CRLs), signed security assertion markup language (SAML) assertions, and user name/password-based authentication.

The format and type of WSS security tokes are unrestricted. The W3C SOAP standard allows security tokens in any format to be mixed freely within SOAP messages. This allows a binary format such as BER encoded X.509 based signatures to be associated with one SOAP element and an XML format such as a SAML assertion to be associated with another element in the same SOAP message. SAML and X.509 objects are both signed, but not using the same signature protocols.

WSS specifies a security token that supports user name and password authentication. Though this type of something-you-know authentication is widely used to provide single-factor authentication, it is no longer considered strong authentication when used without other authentication factors. The WSS standard does not provide security tokens that support something-you-are biometric authentication (e.g., voice recognition, fingerprints, etc.), or something-you-have registered objects (e.g., smart meters, mobile phones, or objects containing embedded radio frequency identifiers). Strong authentication requires the use of at least two authentication factors.

A new international WSS recommendation should be created jointly by ITU-T and ISO/IEC to support a wider variety of user and system authentication methods. Impaired users would benefit from the improved accessibility provided through a choice of authentication methods. All web-services users would benefit from the provision of strong, multi-factor authentication. Users of smart home solutions could benefit from access to web services based on biometric identification.

Biometric token

Impaired persons and the elderly should not be excluded from securely "accessing, participating and being fully-included in social, economic, and political activities" [1]. With some "one billion persons living with disabilities" in the world, it is critically important that international standards development organizations (SDOs) take action to remove the "barriers to accessing information and communications technologies (ICTs) by persons with disabilities" [1]. SDOs should create standards that improve accessibility and help to eliminate this "key driver of exclusion and poverty"[1].

1 P. Griffin, "Signcryption Information Assets," *The ISSA Journal*, June 2012, volume 10, issue 6 – http://c.ymcdn.com/sites/www.issa.org/resource/collection/03B356A7-5235-40A9-A8FD-57261DFD6A4F/ISSA_Journal_June_2012.pdf.

The few authentication alternatives provided in the OASIS Web Services Security standards severely limit the ability of disabled and elderly users to access web services securely. These limitations restrict users with disabilities, making it difficult to enhance "their educational and entrepreneurial opportunities," "to stay in touch with friends and family, to manage their finances, or shop online" [7]. They may have "difficulties which make inputting data difficult in the prescribed time period," or they may be "physically able to use the authentication technology" but encounter "confusion or difficulties understanding how to use the authentication due to an information or intellectual disability or age-related cognitive impairment" [8]. Unimpaired users are also restricted from web-services access in environments that prohibit "the use of a keyboard or keypad, as happens with tiny portable devices" or while they are in "hands-free situations" such as "construction work sites" or during the "operation of a motor vehicle" [7].

The goal of universal access (UA) is to provide "the utility of modern information technology to as broad a range of individuals as possible" [9]. With the potential of integrating "security and usability effectively [being] greater with biometrics than with other authentication methods," biometric technologies are a "natural choice for implementing authentication in UA systems" [9] that can serve the needs of impaired users. A new standardized method of biometric authentication to web services could make access for millions of elderly and disabled users possible.

Users restricted to interaction with a computing device using "nods of the head, eye movements, hand movements, or even by different thought patterns that are captured by a sensor"[7] might easily gain secure access to web services using biometric technologies available on mobile devices such as face recognition or fingerprints. Both authentication and identification are possible with biometrics. In some environments, such as within a user's smart home where identity had already been verified, a standardized method for biometric identification would allow vendors to provide secure web services that were convenient and easy for users to access, perhaps based only on a user's gait, facial expressions, or gestures.

Recommendations

ITU-T should revise X.892 to align with the latest edition of the SOAP standard approved by the W3C. This revised version of X.892 should be extended to improve support for SOAP messages that contain widely deployed security token formats, such as the binary X.509 digital certificates used for web-services security. A revised X.892 should support SOAP messages represented in the ASN.1 Distinguished Encoding Rules (DER) and the Basic Encoding Rules (BER) required by CMS, X.509, and other commonly used information security standards.

A new international Web Services Security (WSS) recommendation should be created to standardize security enhancements to X.892 SOAP messages. WSS messages should be defined using an ASN.1 schema that supports multiple binary encoding rules and XML data representations. This new generic application of ASN.1 should be developed with the security experts in ISO/IEC SC27 and ITU-T Study Group 17 (SG17). The WSS recommendation should support cryptographic algorithms and mechanisms appropriate for use in resource-constrained smart meter, smart home, and other wireless telecommunications environments.

A wide variety of WSS authentication mechanisms should be defined to provide alternatives for secure access web services by disabled and elderly users. A new WSS standard should specify the schema and processing of SOAP message security tokens for digital certificates, security assertions, user names and passwords, and biometrics. The digital certificate token should be based on the current ITU-T X.509 recommendation. The security assertions token should be based on ITU-T X.1141 Security Assertion Markup Language (SAML 2.0), as updated to support the latest version of SAML. A user name and password token should be based on the UserName token specified in the OASIS WSS standard.

A new web-services security token should be created to enable both multimodal telebiometric authentication and identification. The design of this new token should take into consideration the authentication needs of disabled and elderly web services users who benefit from having many standardized alternative means of authentication available. The token

design should also seek to maximize the benefits of standardized biometric identification tokens in the home network and other smart grid applications.

The format and security requirements for this new token should be based on those specified in the draft OASIS WSS XCBF Token Profile. Message security should rely on the new 'x.CMS' standard currently being progressed in SG17. Tokens should be signed and their biometric data and other sensitive information should be encrypted using the ASN.1 SigncryptedData type being defined in the new CMS draft standard [2]. A new schema designed by SG17 biometric, security, and ASN.1 experts should replace the current XCBF schema.

References

[1] ICT Consultation. (2013). The ICT Opportunity for a Disability-Inclusive Development Framework. Retrieved March 26, 2014, from http://www.itu.int/accessibility.

[2] Griffin, P. (2013). Telebiometric Security and Safety Management. Proceedings of ITU Kaleidoscope 2013 Conference – Building Sustainable Communities (K-2013). Retrieved March 26, 2014, from http://www.itu.int/en/ITU-T/academia/kaleidoscope/2013/.

[3] Recommendation ITU-T X.892 (2005). Information Technology – Generic Applications of ASN.1: Fast Web Services.

[4] The Smart Grid Interoperability Panel – Cyber Security Working Group. (2010). NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Security Architecture and Security Requirements.

[5] IBM Research. (2013). Usable Mobile Multi-Factor Authentication. Retrieved March 26, 2014, from http://researcher.ibm.com/researcher/view_project.php?id=2718.

[6] Griffin, Phillip H. (2012). Using Signcryption to Protect Biometric Information. Retrieved May 28, 2012, from http://phillipgriffin.com/innovation.htm.

[7] Topkara, U., Topkara, M., Atallah, M. (2007). Passwords for Everyone: Secure Mnemonic-based Accessible Authentication. Retrieved March 26, 2014, from http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2671&context=cstech.

[8] Australian Banker's Association. (2007). Guiding Principles for Accessible Authentication.

[9] Mayron, L. M., Hausawi, Y., Bahr, G. S. (2013). Secure, Usable Biometric Authentication Systems. Universal Access in Human-Computer Interaction, Design Methods, Tools, and Interaction Techniques for Inclusion, Volume 8009, pp 195-204.

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 of Information Technology, Information Assurance and Security degree, and he has been awarded nine US patents at the intersection of biometrics, radio frequency identification (RFID), and information security management. He may be reached at phil@phillipgriffin.com.