Featured Articles

PKI Platform for Campus Information Systems Using Cloud-based Finger Vein Authentication and PBI

Tsutomu Imai
Kenta Takahashi, Ph.D.
Takeshi Kikuchi
Satoshi Saito
Masaki Konno

OVERVIEW: Incidents involving leaks of personal information from universities, companies, and other organizations resulting from such attacks as unauthorized login are on the rise, creating a major problem for society. Unfortunately, the on-premises adoption of biometric authentication is made difficult by high costs, including the installation and operation of dedicated servers and modification of existing systems. Hitachi teamed up with Kyoto Sangyo University to run a demonstration project that combined cloud-based finger vein authentication with existing campus information systems on site in order to identify the problems associated with installation and operation and to prepare for wider deployment. The results will enable the implementation of safe, secure, and convenient academic systems and social infrastructure.

INTRODUCTION

THERE is an active program of collaborations and partnerships between industry and academia in Japan, including Hitachi, Ltd. Recently, there has been a call for initiatives aimed at commercialization that will enable the generation of sustainable innovation by combining the work of universities and other research institutions with the needs of corporations.

To energetically promote collaboration between industry and academia, the Japan Science and Technology Agency and the New Energy and Industrial Technology Development Organization have hosted Innovation Japan, the country's largest forum for matching up industry and academia. Hitachi has offered cloud-based finger vein authentication for safe, secure, and convenient personal identification to Associate Professor Toyokazu Akiyama of Kyoto Sangyo University, which exhibited at Innovation Japan 2013. The spread of Internet services has led to a rapid increase in the threat of unauthorized logins using techniques such as password list attacks. The recognition by Associate Professor Akiyama of the need to ensure stronger user authentication in the future in university information systems as well as elsewhere led to his agreeing to joint research aimed at overcoming the problem with the intention of using the work to create a business.

This article describes the joint demonstration project for incorporating public key infrastructure (PKI) into campus information systems using cloud-based finger vein authentication and a new technology for template-based public biometric infrastructure (PBI).

INTEGRATION OF CAMPUS INFORMATION SYSTEMS

Background and Objectives

The spread of Internet services has been accompanied by a rapid increase in the use of password list and other techniques for attacks on user authentication data, such that protecting this data is one of the major challenges facing providers of Internet services.

For university information systems, the challenges include providing stronger user authentication to support the handling of personal information. However, the adoption of more secure techniques such as biometric authentication is associated with high costs, including the installation and operation of dedicated servers and modification of existing systems.

In response, Kyoto Sangyo University and Hitachi undertook a joint demonstration project to identify the challenges associated with the installation and operation of cloud-based finger vein authentication. The joint research used a prototype cloud-based finger vein authentication system and a prototype system developed by Kyoto Sangyo University that provides a way to simplify use of PKI to study the potential for using a new biometric technique to provide more secure authentication at universities.

Research Objectives

The research involves assessing the efficiency, convenience, and issues associated with integrating Hitachi's cloud-based finger vein authentication into campus information systems at Kyoto Sangyo University.

In practice, this consisted of integrating the prototype cloud-based finger vein authentication system made up of a single sign-on (SSO) cloud-type authentication management service and a finger vein authentication product into an authentication server developed by Kyoto Sangyo University using the Shibboleth[*1] middleware, which has been adopted as a standard by the Academic Access Management Federation in Japan (GakuNin[*2]), thereby establishing an upward migration path for authentication from a GakuNin Shibboleth environment to Hitachi's cloud-based finger vein authentication.

The project also sought to reduce the amount of work required for installation at the university by identifying the changes that need to be made to GakuNin Shibboleth and setting it up as a model. The user experience was also surveyed with the aim of highlighting issues of concern or needing investigation in relation to installation and user operation.

Research Results

The research produced the following three conclusions:
(1) Cloud-type authentication management service and Shibboleth were successfully integrated using Security Assertion Markup Language (SAML) 2.0, and the settings required to achieve this were identified.
(2) It was confirmed that the identity provider (IdP) authentication server can be configured by adding additional settings to the defaults provided by Shibboleth.
(3) Integration of the Shibboleth and cloud-type authentication management service IdPs can be achieved by storing the uniform resource locator (URL) for Shibboleth IdP remote user authentication in the Shibboleth service provider (SP) module, and integrating the Shibboleth SP module and cloud-type authentication management service IdP.

From these conclusions, the changes that need to be made to GakuNin Shibboleth were identified and set up as a model. It was further concluded that this research can be utilized when universities that belong to GakuNin adopt Hitachi's cloud-based finger vein authentication to reduce the amount of work associated with making changes to their server settings.

The research also found that the authentication system was suitable for practical use, being just as good as the identification (ID) and password authentication in current use with respect to perceived speed, usability, and accuracy of identification. This implies that it is worthwhile to adopt the system as a way of reducing the security risks (including interception and spoofing) associated with the keyboard entry of an ID and password.

On the other hand, it was anticipated that eliminating all user resistance to the introduction of the new system would prove difficult. Instead, rather than adopting cloud-based finger vein authentication for all users at once, including students, it was deemed desirable to foster an environment in which the use of biometric authentication would gradually spread through the university by introducing it progressively, starting with a limited user base, such as academic staff engaged in specific work.

PKI PLATFORM INCORPORATING PBI

Background and Objectives

With web browsers having become widely used as an interface for Internet access, along with strengthening interoperation with local devices as in Web Real-Time Communications (WebRTC), there is a growing need for new forms of communication such as peer to peer (P2P) that are unlike those of the past.

With the spread of WebSSO technology, meanwhile, the environment is being put in place to allow end users to demonstrate their authenticity via SSO servers. Unfortunately, SSO only provides a way for end users to verify with applications that they are who they claim to be. It offers no direct mechanism for end users to verify the identity of other users.

Research Objectives

The research was intended to make GakuNin more useful by extending the scope of SSO to encompass those areas required for P2P communications and content signatures.

Kyoto Sangyo University studied how to combine WebSSO and PKI to provide a way for end users to verify each other directly from a web browser, and conducted research and development to identify the associated security issues.

The joint research project has the potential to make it possible to implement more secure simple

[*1] Shibboleth is a registered trademark of Internet2.
[*2] "GakuNin" is a registered trademark of the National Institute of Informatics, Research Organization of Information and Systems.

PKI authentication for web applications by combining cloud-based finger vein authentication with research and development by Kyoto Sangyo University.

Research Overview

On the assumption that end users can be authenticated using WebSSO, Kyoto Sangyo University set out to create a simple PKI environment that allows the request, issue, and use of certificates online from a web browser. In doing so, it took note of the following considerations.

(1) Achieving security with respect to malicious websites
(2) Avoiding any need for complex key management by users
(3) Using it with WebRTC and other new applications

Progress is being made on standardizing the Web Cryptography Application Programming Interface (API) and implementing it in different browsers to provide a JavaScript[*3] API for encryption processing in a browser. While the standardization documentation makes reference to key management being separate to JavaScript, at the time the study was being conducted no such functions were available in browsers. While providing encryption functions in all web browsers is impractical, a test environment was needed to allow the above work to proceed without waiting for the Web Cryptography API to be ready.

Accordingly, an encryption function was implemented externally to the browser and a framework established for function testing (see Fig. 1).

A key management server coded as Node.js[*4] was installed on the local personal computer (PC) and Socket.IO was used to issue operation requests from JavaScript running in the web browser. These operations included the generation of key pairs, transmission and reception of certificate signing requests (CSRs), and Public Key Cryptography Standard #12 (PKCS#12) storage. Unauthorized manipulation of keys from JavaScript can be prevented by having the key management server API not allow access to keys.

A prototype mechanism for simplifying key management through automatic mapping of web applications and keys had already been implemented using the above framework.

The research project included an investigation into extending the existing functions of the key management service and using them for PBI. PBI includes encryption and decryption using biometric information as the private key and an electronic signature function. As the key management server used in the research stores keys in encrypted form (PKCS#12 format) using a pass phrase, the pass phrase must be entered when the key is used.

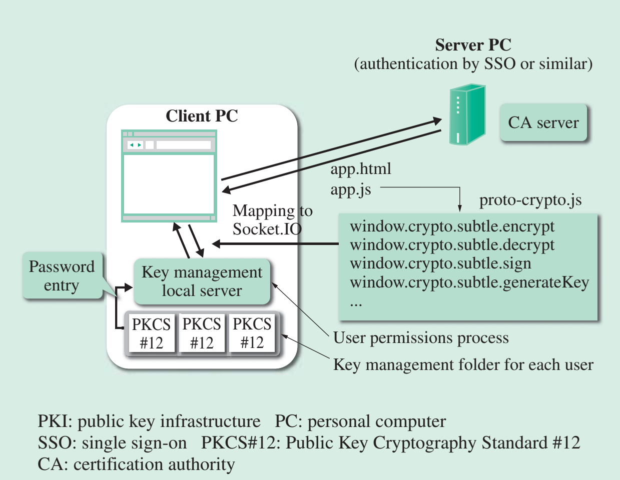

Server PC
(authentication by SSO or similar)
CA server
Client PC
app.html
app.js
proto-crypto.js
Mapping to Socket.IO
window.crypto.subtle.encrypt
window.crypto.subtle.decrypt
window.crypto.subtle.sign
window.crypto.subtle.generateKey
...
Password entry
Key management local server
PKCS #12
PKCS #12
PKCS #12
User permissions process
Key management folder for each user
PKI: public key infrastructure PC: personal computer
SSO: single sign-on PKCS#12: Public Key Cryptography Standard #12
CA: certification authority

Fig. 1—Framework for Simple PKI Function Verification.
Hitachi has developed a prototype for Kyoto Sangyo University that simplifies PKI key management by implementing encryption externally to the browser on a client PC.

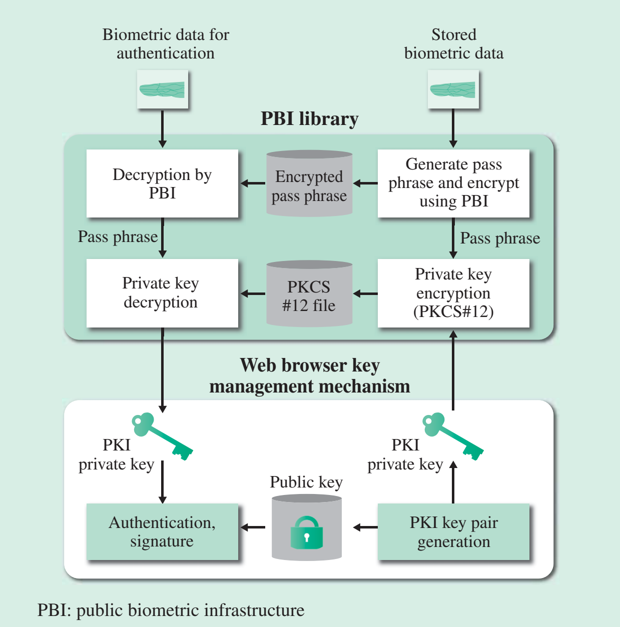
This provides PKI-based user (client) authentication that is both “empty-handed” (does not require a card or similar) and does not use a password by storing the pass phrase encrypted by PKCS#12 encryption using the PBI function for encryption and decryption with biometric information as the private key, and by using the biometric information again to decrypt it when needed for authentication. Fig. 2 shows a model of interaction between the PBI library and the web browser key management mechanism.

Fig. 3 shows the testing framework for PBI that extends the key management server based on the interaction model in Fig. 2.

As the keys encrypted using PKCS#12 in the test environment are software tokens, they can be used for functional testing of finger vein authentication even though it does not affect the ease of falsification in practice. However, during system development it became apparent that the use of tokens was outside the scope of the Web Cryptography API specification and that use of tokens in the API was explicitly prohibited.

In practice, when using tokens that are difficult to falsify, as is the case with PBI, a higher level of assurance (LoA) is assumed, and it is likely there will be cases where it will be desirable to enforce applications having an explicit requirement for the use of tokens with a difficulty of falsification above

[*3] JavaScript is a registered trademark of Oracle and/or its affiliates.
[*4] Node.js is a trademark of Joyent, Inc.



PBI: public biometric infrastructure

Fig. 2—PBI Interaction Model and Web Browser Key Management Mechanism.
By using PBI encryption and decryption functions, client authentication can be achieved without needing to enter a pass phrase.

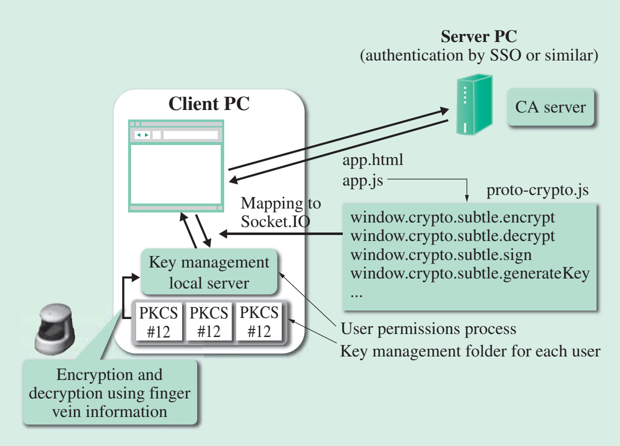

Server PC
(authentication by SSO or similar)
Client PC
CA server
app.html
app.js
proto-crypto.js
Mapping to Socket.IO
window.crypto.subtle.encrypt
window.crypto.subtle.decrypt
window.crypto.subtle.sign
window.crypto.subtle.generateKey
...
Key management local server
PKCS #12
PKCS #12
PKCS #12
User permissions process
Key management folder for each user
Encryption and decryption using finger vein information

Fig. 3—Testing of PBI Interaction Model on Framework for Testing Simple PKI.
The need to enter a pass phrase is eliminated by extending the key management server and using the finger vein authentication scanner.

a certain level. For example, it is believed that the ability to specify such tokens will be desirable in situations such as when specifying a guarantee level with software like Shibboleth 3 and Authentication Engine developed by Kanazawa University. Further investigation is needed with a view to extending the Web Cryptography API.

Research Results

The research produced the following three conclusions.
(1) While implementation of the encryption processing provider is outside the Web Cryptography API specification (is left up to the vendor), with regard to selecting an authentication method with security in accordance with the guarantee level, a mechanism is needed to pass web application requests to the browser to select an appropriate provider.
(2) The framework used for this research was implemented on the basis of using software tokens, with an option to use either a password or finger veins for authentication when using the tokens, and it is anticipated that the addition of an API for specifying the authentication method on the provider will be needed.
(3) The research and development work included investigation of a model for interaction between the PBI library and the web browser key management mechanism, with application on a simple PKI testing framework. Specifically, the work demonstrated that it is possible to provide PKI-based user (client) authentication that is both “empty-handed” and does not use a password by storing a pass phrase encrypted by PKCS#12 encryption, and using the biometric data again to perform decryption during authentication.

Based on the above, as actual web application development using the PKI testing framework is currently incomplete, there is a need to develop applications and conduct operational testing to determine the issues once progress has been made on Web Cryptography API standardization and the specifications have been clarified. In the case of the hardware tokens used by the Web Cryptography API, while this has been discussed at the World Wide Web Consortium (W3C) Workshop on Authentication, Hardware Tokens and Beyond, it is anticipated that it will still take some time, including for things like coordination between hardware vendors. Until then, the intention is to continue with pre-emptive testing using the framework that has been developed.

CONCLUSIONS

This article has described research and development at Kyoto Sangyo University, Hitachi’s cloud-based finger vein authentication, and work on establishing an authentication platform that incorporates PBI technology.

It was found that practical and innovative solutions can be built by sharing information with the customer in the workplace and combining research by both parties.

In the future, Hitachi intends to continue working with Kyoto Sangyo University to implement applications in GakuNin and supply social infrastructure services that can be used in such fields as electronic payments, courier delivery, government agencies, and leisure industries.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to everyone involved at Kyoto Sangyo University for their extensive assistance with the joint demonstration project and the trial results described in this article.

REFERENCES

(1) T. Akiyama et al., “Survey of Installation of PKI Platform Using Cancellable Biometric Authentication and PBI for Campus Information Systems, and its Operational Issues,” Kyoto Sangyo University Researcher Database System (2014) in Japanese.

(2) T. Akiyama, “Potential of New Safer and More Reliable Biometric Authentication,” The Japan Agency for Local Authority Information Systems (J-LIS) (Mar. 2015) in Japanese.

(3) Y. Kaga et al., “Biometric Authentication Platform for a Safe, Secure, and Convenient Society—Public Biometrics Infrastructure—,” Hitachi Review **64**, pp. 472–479 (Nov. 2015).

(4) Kyoto Sangyo University News Release, “Implementation of Authentication Technique for Secure Use by Universities Utilizing Template-based Public Biometric Authentication Infrastructure,” http://www.kyoto-su.ac.jp/more/2014/305/20141022_cloud.html in Japanese.

(5) Hitachi Systems, Ltd. News Release, “Implementation of Authentication Technique for Secure Use by Universities Utilizing Template-based Public Biometric Authentication Infrastructure” (Oct. 2014), http://www.hitachi-systems.com/news/2014/20141022.html in Japanese.

(6) Hitachi News Release, “Successful Prototype of Biometric Identification System for Electronic Payments Using Finger Vein Information” (Jun. 2014), http://www.hitachi.co.jp/New/cnews/month/2014/06/0609.html in Japanese.

(7) Innovation Japan—University Trade Fair, http://www.jst.go.jp/tt/fair/ in Japanese.

(8) Academic Access Management Federation in Japan (GakuNin), https://www.gakunin.jp/En-fed/.

(9) Hitachi Systems, Ltd., “Cloud-type Authentication Management Service Security Solution,” http://www.hitachi-systems.com/solution/t01/shield/ in Japanese.

(10) Hitachi Solutions, Ltd., “AUthentiGate Authentication Management System,” http://www.hitachi-solutions.co.jp/AUthentiGate/sp/product/feature.html in Japanese.

ABOUT THE AUTHORS

Tsutomu Imai

Smart ID Solutions Department, Engineering Service, Cloud Services Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the design of finger vein authentication systems.

Kenta Takahashi, Ph.D.

Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in research & development of information security, biometrics and cryptographic systems. Dr. Takahashi is a member of the Information Processing Society of Japan (IPSJ), and The Institute of Electronics, Information and Communication Engineers (IEICE).

Takeshi Kikuchi

Security Product Department 1, Security Solution Division, Hitachi Solutions, Ltd. He is currently engaged in the development of finger vein authentication software.

Satoshi Saito

Business Service Department, Solution Business Administration Group, Hitachi Systems, Ltd. He is currently engaged in the business promotion of the PBI cloud-type finger vein certification service.

Masaki Konno

New Business Development Center, Research & Development Division, Hitachi Systems, Ltd. He is currently engaged in new business development for biometric authentication services.