MEDINFO 2013
C.U. Lehmann et al. (Eds.)
© 2013 IMIA and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-289-9-930

Securing SSL-VPN with LR-AKE to Access Personal Health Record

Kimura Eizen[a], Saito Masato[b], Kobara Kazukuni[c], Nakato Yoshihito[b], Kuroda Takuji[d], Ishihara Ken[a]

[a] *Dept.Medical Informatics of Medical School of Ehime Univ.,* [b] *BURSEC Inc,*
[c] *Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology (AIST),*
[d] *SHIKOKU MEDICOM Inc.*

Abstract

Using SSL-VPN requires special considerations for well-known issues such as attackers exploiting web browser vulnerabilities and phishing sites using man-in-the-middle attacks. We used leakage-resilient authenticated key exchange (LR-AKE) to develop a comprehensive solution to SSL-VPN issues. Our results show that the LR-AKE should contribute to building a robust infrastructure for personal health records.

Keywords:

SSL-VPN, LR-AKE, PHR, EHR, security, Phishing attack.

Introduction

Even though SSL-VPN is widely used for securing regional health networks because of their ease of client setup, it still has some issues. We must consider the potential risk that an authentication server may be attacked and that authentication information may be revealed. In the event of such an attack, we must restore authentication capability by reissuing authentication information to the compromised users quickly and safely for sustainable healthcare. We should develop and evaluate more secure and robust authentication protocol to resolve these issues to make healthcare professionals and patients to use SSL-VPN for accessing PHR easily and safely.

Methods

Leakage-resilient authenticated key exchange (LR-AKE (1)) is an authentication protocol in which a user and a server authenticate each other. LR-AKE is based on public key cryptography theory and has strong inherent forward security. LR-AKE divides the shared secret key into two keys: the client secret (CS) and the server secret (SS). LR-AKE authenticates by comparing the SS with the information calculated from CS and the password entered by the user. After successful authentication, the client and the server simultaneously update the CS and SS, respectively, to new versions. Even if an attacker tries to log in using a stolen key, the client and the server have already renewed the CS and SS during the previous authentication process so that an attacker cannot login.We developed the LR-AKE One Time Password (OTP) client application for iPhone. A user first launches the LR-AKE OTP client and enters the master password. The client makes a calculation with this password and the CS, and communicates the result to the LR-AKE authentication server. If the authentication succeeds, the LR-AKE client copies an OTP onto the clipboard. The user then launches a web browser and accesses the SSL-VPN router. The user enters his ID on the login screen and pastes the OTP password from the clipboard. The VPN router confirms the password to the LR-AKE authentication server using the RADIUS protocol. After successfully establishing a VPN, the user sees the portal site. When the user requests a remote desktop service (RDS), the web browser starts a RDS session using ThinRDP in the same window. ThinRDP is the remote desktop client software that tunnels RDS protocol over HTTPS to display the screen of the remote desktop server on the web browser using only the native functions of HTML5. The user can then finally seamlessly log into the remote server.

Results and Discussion

Our approach only requires a user to install the LR-AKE OTP client application and load the initial CS data file on the user's mobile device. There is no need to configure additional devices or certificates. An HTML5-ready web browser can process VPN and remote desktop communications seamlessly.

In this study, we stored the CS data in the LR-AKE OTP client application's data area. We issued multiple CSs to every mobile device and confirmed that we could match every CS to the correct user. If one of the user's devices becomes inoperable, we have only to revoke the SS corresponding to the CS of the inoperable device. The user is still able to access the SSL-VPN router from other devices without changing the master password or suspending the account.

We can detect the fraudulent attempt promptly by noticing when a deprecated CS is used in a new authentication session. When an attacker successfully authenticates before the authorized user attempts to authenticate, the user notices that a fraudulent action has taken place because CS/SS synchronization was broken and the user can no longer authenticate successfully. LR-AKE has a advantage over other authentication protocols because of its early detection of fraudulent access.

We currently do not have a standard authentication process between LR-AKE servers and websites. Before deploying the scheme for protecting PHR, we must investigate additional use cases to clarify the inter-server protocols. We developed the LR-AKE OTP client as a native application. To improve its user-friendliness, we may implement LR-AKE OTP with JavaScript so that the user does not have to install it.

References

[1] SeongHan S, Kazukuni K, Hideki I, editors. Secure PAKE/LR-AKE Protocols against Key-Compromise Impersonation Attacks. The 31st Symposium on Information Theory and its Applications (SITA2008); 2008