International Journal of Engineering & Technology, 7 (3.24) (2018) 646-650

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Implementation of System Environment for Smart Authentication Service

[1]Young-Gee Min, [2]Bong-Hyun Kim, [*3]Eon-Gon Kim

[1,3]Department of Information & Communication Engineering, Hanbat National University, 125 Dongseodaero, Yuseong-Gu, Daejeon, 34158, Republic of Korea

[2]Department of IT Convergence, 310 Daehakro, Yeongdong-Eup, Yeongdong-Gun, Chungcheongbuk-Do, 29131, Republic of Korea

**Corresponding author Email:* [1]minyounggee@gmail.com, [2]bhkim@u1.ac.kr, [*3]egk8996@hanbat.ac.kr

Abstract

Background/Objectives: As the various security threats increase, security accidents are frequent due to leakage of ID and password and illegal stealing. As a result, various cyber crimes and property damages are occurring due to the leakage of personal information online.
Methods/Statistical analysis: Security technologies are continuously being developed to protect information by blocking illegal activities such as accessing, browsing, copying, stealing or destruction of certain information by unauthorized persons. The use of existing web services is usually a method of using the ID / password method or the mobile phone authentication number by using a mobile phone or the like. These existing methods are limited in terms of operation, time, inconvenience in use, and functional limitations.
Findings: Therefore, in this paper, we set the access control time and restrict the re-login of the web server with the same ID and password for the access control time, so that after a third party who illegally logs in to the web server is forcibly logged out from the web server, Prevents re-login with username and password, re-login to the web server, arbitrarily changing the user ID and password to prevent the user from legitimately logging in to the web server. Also, through the setting control time, the user can re-issue the password to the web server operator by requesting the web server to secure time for logging in to the web server.
Improvements/Applications: In this paper, we have implemented a system environment to provide smart authentication service. Through this, we developed an Android-based smartphone app client that can be installed on the smartphone and perform subscription, configuration, and various functions, and implemented a smart certification service environment that performs various information and statistics management.

Keywords: *Smart Authentication, Authentication Management Server, Push Server, Web Access Notification, PC Client.*

1. Introduction

Recently, due to the development of the internet environment, various services are available on the web, so user authentication for the use of the web service is often required. In the case of the current system environment, an ID and a password are determined in order to access the Internet, a service of a web site to be used by the user, and various personal information are input to proceed with member registration. After that, it uses the method of using the site after logging in using the registered ID and password[1,2].

However, as various security threats increase, security accidents are frequent due to leakage of ID and password and illegal stealing. As a result, various cyber crimes and property damages are occurring due to the leakage of personal information online. Security technologies are continuously being developed to protect information by blocking illegal activities such as accessing, browsing, copying, stealing or destruction of certain information by unauthorized persons.

There are conventional techniques for preventing a third party from illegally accessing a web service with a user's ID or password if the user's ID or password for the web service is illegally leaked[3,4].However, there are disadvantages that it is inconvenient to use or it is difficult to take a permanent access restriction measure of a third party[5].

Therefore, in this paper, we have implemented a system environment to provide smart authentication service.

In the proposed service system, (1) a user transmits a push message to a specified user terminal when logging in with a user ID and a user ID, thereby confirming the login of the web service, If you confirm the approval button, you do not need to send additional authentication number separately.(2) In case of unauthorized login of a third party, the use of the denial button is forcibly logged out and the use time limit setting of the corresponding web site service is also enabled.(3) Providing login information for a plurality of web services to be transmitted to a user terminal, providing connection status monitoring for a plurality of web service servers in real time, and blocking a third party's unauthorized access by providing access control methods for services, illegal authentication can be comprehensively blocked.

2. Related Review

As the number of various security threats increases, security accidents due to the leakage of IDs and passwords and illegal stealing are frequently occurring. As a result, various cyber crimes and property damages are occurring due to leakage of personal information on the internet[6].Security technology for protecting information by blocking illegal activities such as accessing,

browsing, copying, stealing or destruction of specific information by unauthorized persons is continuously being developed in Korea. Domestic technologies to prevent a third party from unauthorized access to a web service with a user's ID or password if the user's ID or password is illegally leaked to the web service are as follows.

(1) How to prevent the third party from accessing the web service by registering the lock on the registered web service

(2) The registered web service is locked, and the user installs a dedicated app on his / her smartphone so that the lock status is automatically released when the web service is accessed, and the user is locked again after use

(3) When the web service is logged in, an authentication message including an authentication number is transmitted to a designated user terminal in addition to the user's ID and password, and the received authentication number is additionally input to the web service, thereby preventing unauthorized access of the third user

(4) A method to prevent a third party other than the user from illegally logging into the Web service with a user ID and password by sending a short message to the specified user terminal when logging in with the user ID and password to the Web service

However, the technique of (1) originally blocks the connection of the third party, but it is inconvenient to register the blocking status in every web service every time, and the disconnection must be canceled again when the user uses the blocking registration. (2) does not provide a fundamental solution if a user unlocking method is hacked, even if a third party steals his or her web service.(3) can prevent illegal access by a third party due to illegal leakage of the user ID and password, but it is difficult to know which web service the user has registered. Further, when the user is using the terminal, there is an inconvenience that the user terminal information (telephone number) is input every time to access a specific web service, and the authentication number received by the user terminal is input again to the web service server.(4) in the case of confirming the short message of the login through the user terminal, the user logs on to the specific web service server through the user mobile phone or the personal computer capable of accessing the internet to forcibly log out the illegal login of the third party, And furthermore, only forcibly logging out a third party illegitimate login is temporarily blocked from accessing a specific web server[7-9].Accordingly, when the user forcibly logs out illegal log-in of a third party, the third party usually re-logs in to the web server and arbitrarily changes the password or the ID so that the user can log in to the web server and disable control of the user information a problem arises.

Currently, the following security technologies are continuously being developed in the United States, Europe, and Japan to protect information by blocking illegal activities such as accessing, browsing, browsing, copying, and destruction of certain information by unauthorized persons.

(1) A technology to prevent a third party other than the user from illegally logging in to the web service with a user ID and password by sending a short message to the specified user terminal at the login of the web service with the user ID and password

(2) A technique for transmitting an authentication message including an authentication number to a specified user terminal in addition to the user's ID and password when logging in to the web service and for preventing the illegal connection of the third user by additionally inputting the received authentication number into the web service and logging in

(3) A technology that identifies the login from a region other than the specified region when logging in to the web service and restricts the login if the region is not the specified region or requires additional specified destination authentication[10][11].

3. Service Module

In this paper, we have implemented a system environment to provide smart authentication service.

When a user logs in to a web server with a user ID and a password, the web server determines whether the user ID is an application for the login notification service. If it is determined that the login notification service is a registered user ID, a login information message is generated and transmitted to the smart authentication management server. The login information message includes the user ID and login time information logged in to the web server. Upon receipt of the login information message, the smart authentication management server generates a login notification message to inform the user of the login information in the form of a push message, and transmits the generated login notification message to the user terminal. The smart authentication management server extracts the user ID from the login information message and searches whether the same user ID as the extracted user ID exists in the management member information of the smart authentication management server. If the same user ID as the user ID extracted for the web server exists in the management member information of the smart authentication management server as a result of the search, the management server transmits the management information to the user terminal based on the contact information of the user terminal mapped to the user ID Send a login notification message[12,13].Figure 1 shows the smart authentication service operating environment and system configuration.

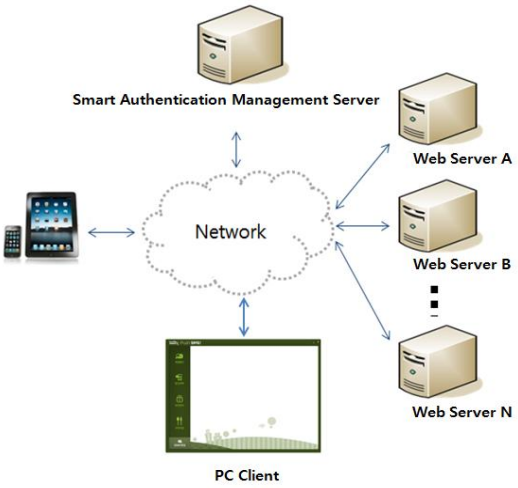

Figure 1: System configuration and operating environment

Figure 2 is a diagram showing the service operation flow in the smart authentication service. In order to use the login notification service, the user terminal first transmits a login notification service application message to the web server for using the login notification service. Application of the login notification service can be performed using a user terminal or a personal computer capable of connecting to a web server through a network and transmitting and receiving data. The application of the login notification service is to send the login information to the smart authentication management server when logging into the web server with the user ID and password. In the Web server, the user ID that requested the login notification service is registered and stored. When logging in to the Web server with the user ID and password, the Web server determines whether the user ID is the login notification service. As a result of the determination, if the log-in notification service is the applied user ID, a login information message is generated and transmitted to the smart-

authentication management server.

The login information message stores the user ID and log-in time information logged in to the web server. Upon receipt of the login information message, the smart authentication management server generates a login notification message to inform the user of the login information in the form of a push message, and transmits the generated login notification message to the user terminal.

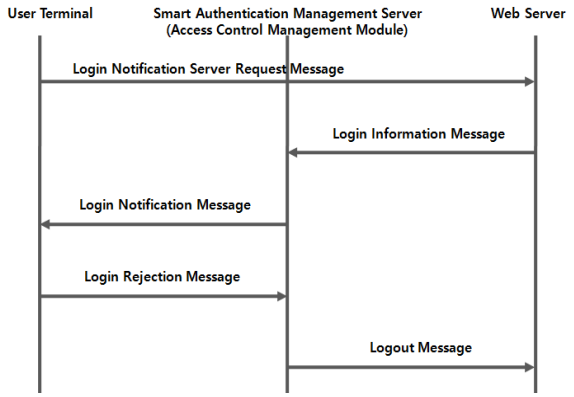

Figure 2:. Service operating flow

The user himself or herself logs in to the web server or a third party that the user allows to log in to the web server and receive the login notification message. Press the OK button or ignore the login notification message and continue to connect to the web server and use the web service provided by the web server. However, if the third party illegally logs in to the web server by inputting the user's ID and password, the user enters a user command for forcibly logging out the web server by pressing the reject login button. The user terminal generates a login rejection message in response to the input user command, and transmits the generated login rejection message to the smart authentication management server.

In order to generate a login rejection message for forcibly logging out the Web server, set the access control time to restrict the re-login for a certain time with the same user name and password for the Web server, the control time can be included in the login refusal message and generated. A user interface for setting a connection control time is activated through a connection management application executed in a user terminal, and a user sets a connection control time for blocking the re-login of the web server when creating a login reject message. In addition, connection control time can be set differently for each Web server[14].

Upon receiving the login rejection message, the smart authentication management server generates a logout message for forcibly logging out the login of the web server, and transmits the generated logout message to the web server. In the logout message, information on the user ID and the access control time is stored. The Web server extracts the user ID of the logout message, forcibly logs out the login of the web server of the extracted user ID, and blocks restart login of the connection control time[15].

In this paper, we overcome the disadvantage that the login notification message is transmitted in the form of a push message in order to relieve the management burden of the user's web server login, the user can manage login of the web server by requesting login information of the registered web server at any time through the connection management application executed in the user terminal

4. System Implementation

In this paper, we set the access control time and restrict the re-login of the web server with the same ID and password for the access control time, so that after a third party who illegally logs in to the web server is forcibly logged out from the web server, Prevents re-login with username and password, re-login to the web server, arbitrarily changing the user ID and password to prevent the user from legitimately logging in to the web server. Also, through the setting control time, the user can re-issue the password to the web server operator by requesting the web server to secure time for logging in to the web server. Figure 3 shows the security authentication software configuration.

The Smart Authentication Management Server is implemented to support the following functions.

(1) Receive and process access control time setting information from a user terminal to a valid Web server.

(2) Smart authentication When receiving a login information message of a user from a web server registered in the management server, classify it by web server, store and manage the login information of the web server, register from the user terminal to the smart authentication management server When receiving the login information request message of the Web server selected among the Web servers being done, the login notification message including the unit time login information to the selected Web server is pushed by the user (push) message method To the terminal.

(3) Furthermore, in response to the login information response message, the smart authentication management server, when receiving a login rejection message to the Web server selected from the user terminal, causes the user ID to block the login of the selected Web server as the user ID to the Web server. The logout message includes time information of the setting connection control.

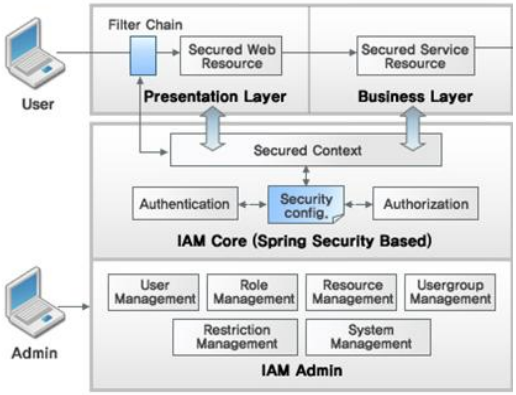

Figure 3:. Security authentication S/W configuration

In addition, we implemented our own Push Center based on IOCP without using Push Service provided by existing OS in figure 4.

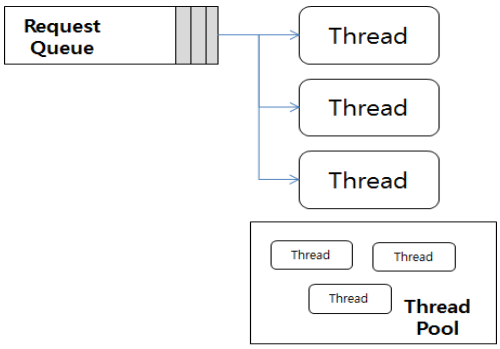

Figure 4:.I/O completion port and multithread

IOCP (Input/Output Completion Port) is an API that supports simultaneous asynchronous I/O operations in a Windows

operating system environment. An IOCP object is created and associated with a number of sockets, or file handles. When I/O service is requested to the object, completion of I/O service is announced by a message queued to the I/O completion port. It is not necessary for a process requesting an I/O operation to be notified of completion of an I/O service, but instead the process only checks the message queue of the I/O completion port to see the progress of the I/O request. IOCP manages and supports multiple threads and concurrent operations in figure 5.

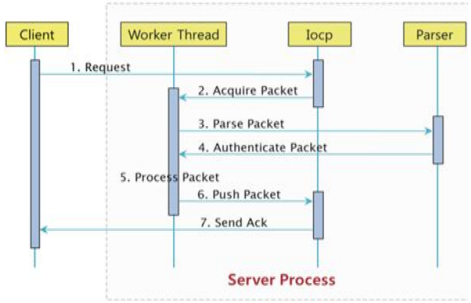

Figure5:.IOCP push solution structure

Push server is implemented as Logic which takes advantages and compensates for shortcomings and optimizes push message transmission.

A push sender that requests and receives a push message from the CP and sends it to the device, a push receiver that is installed in the device and manages the connection with the push sender, a push receiver that receives the message, and a dispatch module that is required to accommodate various CPs. Based on the XMPP protocol, it is composed of a flexible architecture applicable to various DB systems such as Mysql, Mssql, and Oracle. It is a flexible system configuration that can be interlocked regardless of the existing legacy system structure, and it is developed with a structure that can easily interoperate with various middleware.

We have developed a function that can control the setting information from the server by keeping the connection (Keep Alive) and the number of connection attempts to reduce the load on the phone. It is designed to maintain the minimum number of servers and hardware on the assumption that sufficient service is performed through reduction of server load. Figure 6 shows the push server process architecture.

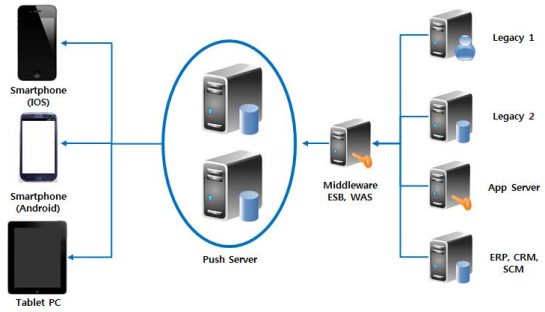

Figure 6:. Push server process architecture

Finally, we have developed an Android app that allows you to register to a web service server, process login / logout messages, process statistical information.

The process procedure is as follows. Enter the ID of each web server and the identifier of the web server to control access through the access management app. The login notification message includes the name of the web server, the login confirmation button of the web server, and the login reject button of the web server. A user interface for setting a connection control time is activated through a connection management application executed in a user terminal, and a user sets a connection control time for blocking the re-login of the web server when creating a login reject message.

5. Conclusion

Web services security damage is continuing due to diverse camouflage techniques such as phishing, pharming, and other new financial frauds, which are used to steal information from a fake site on a customer's PC as a hacking threat. Also, due to increased bandwidth and increased inflow of unhealthy traffic (worm etc.), the possibility of leakage of large amount of confidential information is increasing, and it is gradually becoming difficult to respond to various security threats. Various security issues arise from various types of terminals and applications, and establishment and implementation of security policies for individual terminals and services is becoming more and more difficult. The damage caused by Internet infringement and hacking is not limited to personal user damage, but it causes harm to organization and society in general through connected networks.

Mobile-based web service applications are increasing day by day due to the high penetration rate of Android-based operating system and the increase of mobile applications. However, there are not many developed and popular web service authentication security service products that are convenient and effective.

Therefore, in this paper, we have implemented a system environment to provide smart authentication service. Finally, when the user logs in on the web, he / she can notify the user of the login using the app push to the registered smartphone, and if the person to be logged in is not his / her, the user can immediately logout from the program. In addition, we developed web service authentication security technology that disables login for a set time, and implemented a system environment that enables web access notification and control authentication service using smart device.

References

[1] Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil Pairing. Asiacrypt 2001. LNCS, 2248, 514–532.
[2] Fujioka, A., Saito, T., & Xagawa, K. (2012). Applicability of OR-proof techniques to hierarchical identity-based identification. CANS 2012, LNCS, 7712, 169–184.
[3] Wen-Bin Hsieh, Jenq-Shiou Leu. (2017). An Improved Mutual Authentication Mechanism for Securing Smart Phones. Wireless Personal Communications, 97(2), 2911–2924.
[4] Xue, K., Ma, C., Hong, P., & Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications, 36(1), 316–323.
[5] Anderson, K., Jimmy, D., Narayan, A., &El Gamal, A. (2014). Grid-spice: a distributed simulation platform for the smart grid. IEEE transfer Industrial Informatics, 10(4), 2354–2363.
[6] Fan Wu, Lili Xu,Saru Kumari & Xiong Li (2018). An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Networking and Applications, 11(1), 1–20.
[7] Burnett, A., Byrne, F., Dowling, T., &Duffy, A. (2007). A Biometric Identity Based Signature Scheme. International Journal Information Security, 5(3), 317–326.
[8] Mets, K., Ojea, JA. & Develder, C. (2014). Combining power and communication network simulation for cost effective smart grid analysis. IEEE Communication Survey Tutorials, 16(3), 1771–1796.
[9] Jiang, Y., Lin, C., Shen, X., & Shi, M. (2006). Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. IEEE Transactions on Wireless Communications, 5(9), 2569–2577.
[10] Bresson, E., Chevassut, O., & Pointcheval, D. (2003). Security proofs for an efficient password-based key exchange. In: Proceedings of the 10th ACM conference on computer and communications security, 241–250.

[11] Chen TH, & Shih WK (2010). A robust mutual authentication protocol for wireless sensor networks. ETRI Journal, 32(5), 704–712.
[12] Anderson, D., Zhao, C., Hauser, C., Venkatasubramanian, V., Bakken, D., &Bose, A. (2012). A virtual smart grid—real-time simulation for smart grid control and communications design. IEEE Power &Energy Magazine, 10(1), 49–57.
[13] Fazeli, M., Asher, G., Klumpner, C., Yao, L., & Bazargan, M. (2012). Novel in-tegration of wind generator-energy storage systems within microgrids. IEEE Trans Smart Grid, 3(2), 728–737.
[14] Sung, A., Zu, J., Chavez, P., & Mukkamala, S. (2004). Static Analyzer for Vicious Executavles (SAVE). In: 20th Annual Computer Security Applications Conference, 326–334.
[15] Das, AK., Chatterjee, S., &Sing, JK. (2014). Formal security analysis and verification of a password-based user authentication scheme for hierarchical wireless sensor networks. International Journal of Trust Management in Computing and Communications, 2(1), 78–102.