The implementation and investigation of securing web applications upon multi-platform for a single sign-on functionality

Hsien-Yu Lee* and Nai-Jian Wang
Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

Received: 19-February-2016; Revised: 18-March-2016; Accepted: 20-March-2016
©2016 ACCENTS

Abstract
Nowadays, the world is moving toward mobilized communities as the development of internet and web applications. Almost all of the daily activities and transactions can be done through the internet. Web applications become trends as e-business and e-commerce systems continue to make our lives easier and better without our noticing. These web applications were developed from various frameworks, programming languages and platforms etc. over the internet. Computer technology is a time saving and quality improving revolution. When the enterprise will build up the vision of computer digitalization, i.e. hosting e-Enterprise engineering, cloud platform or information systems integration, etc. Under the web world, the single sign-on (SSO) concept was invented as problem-solving method about one login as you go authorized systems. In other words, web securities are confronting some challenges under the networked era of the emergency web. Therefore the SSO functionality based on multiple platforms and web enabling technologies is put forward and it also secures web applications developed from diverse programming. The proposed method of secure login utility is created as an obvious solution to the general functionality of SSO. Hereby, we also will reveal two application instances of the secure login utility to implement the idea of SSO realized in the enterprise systems.

Keywords
Security, Single sign-on, Web programming, MD5.

1. Introduction
Single sign-on (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. To verify that the users for all applications, they have been given the rights and eliminate further prompts when they are in a particular session during the process of switching applications [4]. Single sign-on (SSO) is a property of access control of multiple related sources, but independent software systems. Based on this property, a user logs in with a single ID and password to obtain access to a connected system or the other systems without having to use a different user name or password. In [5], what are the benefits of SSO? The benefits of SSO apply to many areas: 1) User experience: the most obvious benefit is that users can move between services securely and continuously without having to specify their credentials every time.

2) Security: provide the user credentials directly to the central SSO server, not the actual service that the user attempts to access and save, 3) Resource savings: IT administrators can save their time and resources with a central web access management services. To comprehend Enterprise Single Sign-On (SSO) [6], it is useful today to observe the three types of Single Sign-On services available: Windows integrated, extranet (web SSO), and an internal network (Server-based Intranet). Enterprise Single Sign-On provides services to store and transmit encrypted user credentials across the local and global internet. SSO always stores the credentials in the database. Because SSO provides a generic single sign-on solution, applications and adapters can use SSO to safely store and transmit user credentials across a variety of environments. Users do not always remember different credentials/passcodes for different applications/platforms. Therefore, we proposed the solution focused on web SSO applied upon a multi-platform method. In 1991, MD5 message-digest algorithm was designed by Ronald Rivest to replace an earlier hash function, MD4 in 1990 [1], [2]. The MD5 message-digest algorithm is widely used a cryptographic hash function producing
a 128-bit (16-byte) hash value, typically expressed as a 32-bit hexadecimal numbers in text format. MD5 has been used for a variety of cryptographic applications, and is also commonly used to verify data integrity [13]. In the following section, we are going to use this concept to propose the method of Secure Login Utility (SLU) <Universal Authenticated Key Generator, Captured User IP Address> and implement these applications/components in Java, .Net, PHP and BCD WebSmart ILE, about IBM As/400 Web System, and so on.

The key issue we are concerned (considered) is: Single Sign-On, it means that users can login only once and access to multiple functionality websites. Privacy, resources, integrity and segregation belonging to one user cannot be accessed by unauthorized users, cannot be tampered during transfer, and deeply considering about both global and local resource usage rules. Upon this key issue, we simply and easily adopt MD5 [2] message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number (stored in the field of AUTKEY(32)). We realized the Secure Login Utility – Universal Authenticated Key Generator by using Java and AS/400 CL/RPG. The utility will create a unique, authenticated key (stored in AUTKEY (32)) based on the MD5 algorithm in every real-time login action, and the server will also automatically capture this user’s unique IP address (i.e. 216.28.219.238).

2. Objectives – computer digitalization

During the past two decades, in virtue of the web has evolved into a global environment, addressing applications that range from simple, small-scale to complex large-scale enterprise applications distributed over the internet. Enterprises and companies are using the web to do business processes for their employees, to communicate with their partners and vendors, to integrate their back-end databases and information systems, and to perform all kinds of e-Commerce transactions. The most important one of the key benefits is that the programs, softwares, systems, and platforms will be well-maintained. The enterprise adopted computer technologies before the past three decades. Since then, the enterprise has gone step by step to apply Customer Relationship Management (CRM) and Supply Chain Management (SCM) systems, obtaining Electronic Data Interchange (EDI), Office Automation (OA), internet, Engineering and now Cloud Engineering, i.e. e-Commerce, e-Business, e-Marketplace, e-ERP and other information systems. And totally use computer to handle all purchasing and contracting business. The enterprise’s digitalization that connects administrative sections into the ERP system, e-Commerce systems and information systems and so on covers all kinds of use in a company. Therefore, there is an integration request between these enterprise information systems. In other words, these systems confront a challenge about a major authorization processing problem under the networked era of the emergency web. Hereby, we proposed the solution focused on web SSO applied upon a multi-platform method - Secure Login Utility.

3. Designs and implementations for a single sign-on functionality

3.1 The algorithm for secure login utility

In Figure 1, we illustrate the algorithm of the work and it for Secure Login Utility is depicted in order from top to bottom as below.

Figure 1 An illustration of the algorithm for secure login utility
3.2 The secure login utility-universal authenticated key generator
We realized the Secure Login Utility – Universal Authenticated Key Generator by using Java and AS/400 CL/RPG. The utility will create a unique, authenticated key (stored in AUTKEY (32)) based on the MD5 algorithm in every real-time login action, and in Appendix’s Figure 8 outlined the implementation sample codes for Secure Login Utility - Universal Authenticated Key Generator by using Java and AS/400 CL/RPG program.

3.3 Captured the user’s IP address automatically
The server will also automatically capture this user’s unique IP address (i.e. 65.216.158.152). According to the combined authorizing and auditing of both a unique, authenticated key and a unique IP address, we will secure all of login users until then logout systems. Although the IP address can be tampered by Hijacking during login, the generated authenticated key cannot be modified.

3.4 Designed table SQL layout
Hereby, we provide the designed table SQL layout, detailed in Figure 2.

3.5 Some results of creating token for authenticated key
a. Randomly create token stored in TOKEN(24) field.
b. Use MD5 Algorithm to generate authenticated key stored in AUTKEY (32) field.
c. Check for the login user’s authenticated key and IP address.
d. Finish verifying the login action and return the flag of true or false.

![Figure 3](image-url) Some results of creating token for authenticated key

-- Version: V7R1M0 100423 ------------------- AS/400 table SQL layout
-- Generated on: 02/07/16 20:36:55
-- Relational Database: FEDO10
-- Standard Option: DB2 for i
CREATE TABLE JLIB.JLOGININ ( LOGIND TEXT IS 'Login id code', KD TEXT IS 'Login id code', SYSID TEXT IS 'System id', AUTKEY TEXT IS 'MD5 Authenticated key', USERID TEXT IS 'User ID', TOKEN TEXT IS 'Input string for MD5 hashing', GENTMSTAMP TEXT IS 'Generate time stamp' );

Figure 2 The designed table SQL layout in IBM AS/400

Figure 3 shows the results of creating token for authenticated key.
3.6 Two application instances of the secure login utility

In order to verify the feasibility and practicality of the theory and method in this paper, the Secure Login Utility – Universal Authenticated Key Generator method which is developed by the author’s web group has been built and now is running in the enterprise. In the following Figure 4 and Figure 5, we are going to use this concept to implement and realize the proposed method applying on two applications developed in the Java Struts framework (https://www23.fpcusa.com/PsnWeb/logon.do) and WebSmart ILE (http://wd10.fpcusa.com:8010/pppubl ic/xlpp/VPPIRREL2.pgm?task=Open Enrollment Summary Reoprt2&TKN=xxxxxx) respectively. According to our realizations, the IP address can be tampered by Hijacking during login, the generated authenticated key cannot be modified. In 2013, there was an attack by Xie Tao [3] to break MD5 collision resistance in $2^{10}$ times. In virtue of the server’s techniques and programming skills, they could resist amount of trial by Hijacking in a second. Hence we have successfully secured the protection upon the Secure Login Utility. Currently, we can’t discover any methods or ideas to decipher this secure utility.

![Employee self service](https://www23.fpcusa.com/PsnWeb/logon.do)

**Figure 4** Employee self service–the look of output pages developed in Java

3.7 The design is beneficial to web information systems

Why the design is such beneficial [7-12], hereby, we justify it by illustrating two detailed figures which are representative many Sign-On in Figure 6 and Single Sign-On (SSO) in Figure 7 respectively. In Figure 6, we indicate the regular application of many login functionalities upon multi-platform from diverse web programming. Another Figure 7, it exhibits the beneficial application of a Single Sign-On functionality upon the same conditions. Obviously, there is only one difference whether the enterprise should adopt the SSO for their web systems and users or not.
Wellness Program Participation: Yes

Plan Type: FPCCUSA New Plan

**Figure 5** Employee healthcare enrollment—the look of output pages developed in websmart ILE

**Figure 6** Many login functionalities upon multi-platform from diverse web programming
Figure 7 Single login functionalities upon multi-platform from diverse web programming

4. Conclusions and recommendations

Internet and web applications, i.e. Cloud Computing, Semantic Web and e-Commerce have become several growing parts of our daily lives. No doubt, more opportunities are created to develop and deploy new web-based products and services. It is to say that it’s impossible without automated web-based help. Even project managers and IT engineers shouldn’t forget what have learned in their software engineering, programming and project management classes, they are expected to adopt new ideas and technologies as the evolving progress is getting mature. In this article, you will look at web security technologies over the internet that deeply affects to make up the enterprise business applications in a variety of different platforms and understood why companies/organizations such as ours might want to adopt and apply this method.

Web-based applications in the Cloud migrated from traditional ones benefit customers and the enterprise itself by providing application scalability and reducing hardware costs. Therefore web applications over the internet are involved within modern web topics and cloud computing to such an extent that the key issue of web security and Single Sign-On are considered. In other words, it’s always up to the user in readiness for such security applications in the coming era of the emergency web.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
Hsien-Yu Lee, his academic research interests include web technologies/evolution, intelligent computing, and evolutionary algorithm application. His industrial specialties include web technologies (Java, .Net, PHP) realization, database design and application, object-oriented programming (C++, Java), and server techniques. He has published several articles in reputed international journals.

In order to develop professional knowledge, enlarge diverse programming experience and increase project evaluation skills, Mr. Lee joins 10+ professional activities, these technical Journals certificated Reviewer/Editor listed several below - Studies in Engineering and Technology (SET), International Journal of Scientific Engineering and Technology (IJSET), International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), International Journal of Engineering Research & Technology (IJERT), ACCENTS Transactions on Information Security (TIS), International Journal of Advanced Computer Research (IJACR) and so on. Email: ebilllee@gmail.com

Nai-Jian Wang is an associate professor in the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan. He got his master and PhD degree from the Department of Electrical Engineering, University of California, Los Angeles (UCLA), USA. His research interests include multimedia signal processing, digital design on FPGA, embedded system, intelligent computing and optimization, and computer vision.
Appendix:

1. The implementation sample codes for Secure Login Utility - Universal Authenticated Key Generator by using Java and AS/400 CL/RPG program.
2. There is an authority on login action by using legal Auth. Key and automatically captured user’s IP address.

![Figure 8 Secure login utility–universal authenticated key generator by using Java and AS/400 CL/RPG](image)