PROTECTION AGAINST MAN-IN-THE-MIDDLE ATTACK IN BANKING TRANSACTION USING STEGANOGRAPHY

Albina.N, U.J. Raju, K. G. Revathi, K. Raghava Rao

Abstract:

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. HTTP is not only used for communication purpose, it is also used for file/data transfer, chatting, etc. The HTTPS protocol to guarantee privacy and security in transactions ranging from home banking, e-commerce, and e-procurement to those that deal with sensitive data such as career and identity information. Users trust this protocol to prevent unauthorized viewing of their personal, financial, and confidential information over the Web. Even though the transfer of data can be attacked by the Man-in-the-Middle. This paper proposes a Steganography scheme that can be used to detect unauthorized modifications of HTTP communication. This allows detection of a possible attack on the communication. Unauthorized modification of the transmission is considered as the attacks in the banking transaction.

Index Terms: Hypertext Transfer Protocol (HTTP), Man-in-the-Middle attack, Steganography and Cued Click Points (CCP).

1. INTRODUCTION

The Hypertext Transfer Protocol (HTTP) is an application-level networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. HTTP is one of most important Internet protocols. It is used not only for data communication, it is also used to download files, access e-mails, calendars, instant messaging, maps and other services, which would require a usage of special programs. The HTTP must communicate large amount of personal information (e.g. the user's name, location, mail address, passwords, encryption keys, etc.), and should be very careful that no intruders hacks the personal information of the users. HTTP protocol must guarantee that the data is secured in home banking, e-commerce, and e-procurement [2]. Users trust this protocol to prevent unauthorized viewing of their personal, financial, and confidential information over the Web. In HTTP the hackers can attack the confidential information of a particular user. HTTPS is a secured HTTP request and responses using symmetric cryptography [1]. HTTPS is considering as a safe protocol. However, if the client gets all data by himself in the same network connection, there is a possibility to alter the communication using Man-in-the-Middle attack.

The Man-in-the-Middle attack [3] principle is to cut the connection between server and client and make the client to believe the attacker system as server and make the communication through the attacker system. This way, the attacker can modify victim's communication to a desired extent.

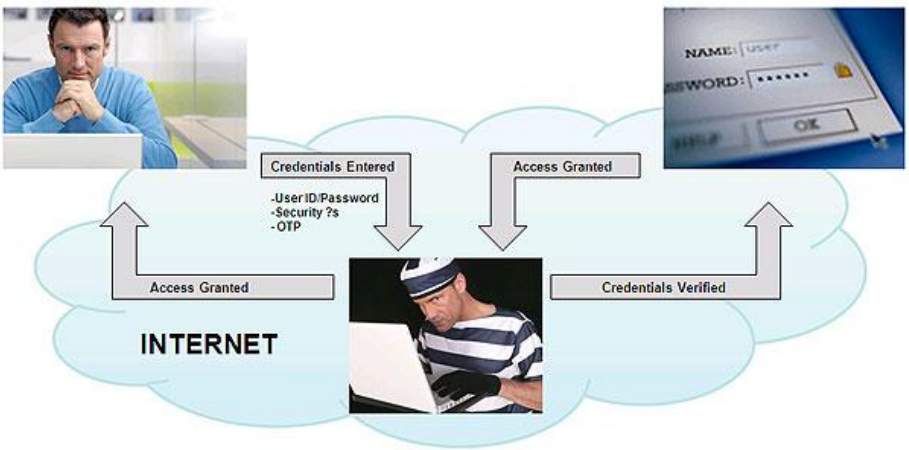

Fig 1 Man in the Middle Attack principle

This paper proposes a Steganography scheme that can be used to detect unauthorized modifications of HTTP communication. This allows detection of a possible attack on the communication. Unauthorized modification of the transmission is considered as the attacks in the banking transaction.

2. MATERIALS USED

2.1 Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, other than sender and receiver can read the information. Steganography is a form of security from the attacker's. The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties. Steganography includes the concealment of information within computer files. Steganography tries to hide the very fact that some added communication messages are being exchanged, while the cryptography serves as an additional protection layer [5]. Steganography send the confidential information in a document file, image file, program or protocol. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

2.2 Cued Click Point

Cued Click Points (CCP), a cued-recall graphical password technique [6]. Users click on one point per image for a sequence of images. In this securing of data is more efficient, speed, etc. The next image is based on the previous click-point. In this CCP technique we have to remember only one point in the image to secure our data so it is so easy for the user. In this each image we can memorize where the corresponding point was located. In this technique we can secure our data as the number of images increase the hackers find difficult in finding of the secret click-point so the attacker's work load increases. In the existing system, research and experience people have shown that text-based pass- words are fraught with both usability and security problems that make them less than desirable solutions. In the proposed system, users had high success rates, could quickly create and re-enter their passwords, and were very accurate when entering their click-points.

In this paper we use some module, In set authentication module, the user can set the password. In check authentication module, this represents not to collect, store, or transmit information beyond the computer that you use to access Password Checker. The security of the passwords entered into Password Checker is similar to the security of the password you enter when you log into Windows. The password is checked and validated on your computer, but is not sent over the Internet.

In update authentication module, the user can modify the previous authentication.

Login module provides security to the application. If you are already a member of this project, only you can access the application.

Customer information module intends to maintain the whole information about the customer name, addresses, Bank balance in bank industry. It also intends to maintain the personal information about the customer.

2.3 Advanced JAVA

J2EE to simplify application development in a thin client tiered environment [9]. J2EE simplifies application development and decreases the need for programming and programmer training by creating standardized, reusable modular components and by enabling the tier to handle many aspects of programming automatically.

These are some of the components and features provided by J2EE.

- The Java Development Kit (JDK) is included as the core language package.
- Write once and Run anywhere technology.
- Supports the intercommunication of java objects / other objects across the network.
- Java Database Connectivity 2.0 (JDBC).
- A security model is included to protect data both locally and in Web-based applications.

2.4 Eclipse Helios

Eclipse is an extensible, open source IDE (integrated development environment) [7]. The Eclipse platform, when combined with the JDT, offers many of the features you'd expect from a commercial-quality IDE: a syntax-highlighting editor, incremental code compilation, a thread-aware source-level debugger, a class navigator, a file/project manager, and interfaces to standard source control systems, such as CVS and Clear Case.

2.5 Apache Tomcat Server

Apache Tomcat (or Jakarta Tomcat or simply Tomcat) (Apache Tomcat 7.0 - Change log, 2011) is an open source servlet container developed by the Apache Software Foundation (ASF). The Java Servlet Pages (JSP) And Java Servlet is implemented by Tomcat, and provides a "pure Java" HTTP web server environment for Java code to run. Apache Tomcat includes tools for configuration and management, but can also be configured by editing XML configuration files.

2.6 Functional Requirements

2.6.1 Software Requirement Analysis

In this part of work, the development team visits the customer and studies their system. They investigate the need for possible software automation in the given system. By the end of the feasibility study, the team furnishes a document that holds the different specific recommendations for the candidate system. The requirement gathering process is intensified and focused specially on software. To understand the nature of the programs to be built, the system engineer or "Analyst" must understand the information domain for the software, as well as required function, behavior, performance and interfacing. The essential purpose of this phase is to find the need and to define the problem that needs to be solved.

2.6.2 System Analysis and Design

In this part of work, the software development process, the software's overall structure and its nuances are defined. In terms of the client/server technology, the number of tiers needed for the package architecture, the database design, the data structure design etc... Are all defined in this part. A software

development model is thus created. Analysis and Design are very crucial in the whole development cycle. Any glitch in the design phase could be very expensive to solve in the later stage of the software development. Much care is taken during this phase. The logical system of the product is developed in this phase.

2.6.3 Code Generation

The design must be translated into a machine-readable form. The code generation step performs this task. If the design is performed in a detailed manner, code generation can be accomplished without much complication. Programming tools like compilers, interpreters, debuggers etc... Are used to generate the code. Different high level programming languages like C, C++, Pascal, and Java are used for coding. With respect to the type of application, the right programming language is chosen.

2.6.4 Testing

Once the code is generated, the software program testing begins. Different testing methodologies are available to unravel the bugs that were committed during the previous phases. Different testing tools and methodologies are already available. Some companies build their own testing tools that are tailor made for their own development operations.

2.6.5 Maintenance

The software will definitely undergo change once it is delivered to the customer. There can be many reasons for this change to occur. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

3. RESULTS

Using of Steganography scheme we can secure our banking transaction in the network and this paper implements five different modules. In each module it performs various processes to secure of the confidential information of the clients.

3.1. Set Authentication

This module allows the user to set the password. After completing this process we have to check whether the password entered by the user is correct or not. After entering the password, user has to select different images. Then, the user clicks on one point per image for a sequence of images. These points will be stored and then checked for authentication.

Here we use a click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of Pass Points, Pass faces, and Story. A password consists of one click-point per image for a sequence of images. CCP offers both improved usability and security.

3.2. Check Authentication

This module is to check whether the given user name and the password is correct and it is valid one or not. In this the authentication the password is stored in the image using the Steganography scheme. This

authentication can be done by storing the form of tables in the SQL database & will be used to match the reference in future login.

3.3. Update Authentication

This module is used to modify the previous authentication. In this module the user can change the user name or password and can update some of his information and he can store his information confidentially. This kind of updating of information is done as to secure the banking information from the attackers is so important.

3.4. Login Details

In this module, user provides details and password through a user interface. The user can access this application only if he/she is already a member. In this module we use Data Encryption Standard (DES) algorithm is used to format the user name and password into the correct form and it is accessed by the interface. It checks for some condition and retrieve the user details. The DES has been extensively studied since its publication and is the most widely used symmetric algorithm in the world. When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message (http://www.vocal.com/cryptography/des.html).

3.4.1. Embed Encrypted String/File Watermark to Media File

Here ―Data Encryption Standard (DES) algorithm is used to encrypt the strings/files. The string/file can be of any length. But the password should be of 8 characters which is a limitation of DES algorithm. Once the string is encrypted, the encrypted string/file and the length of the string/file are embedded to the end of the media file.

3.4.2. Retrieve Watermark Message/File with Decrypt Password.

Here ―Data Encryption Standard (DES) decrypt algorithm is used to decrypt strings/files. Here the password is supplied to decrypt the string. The password should be of 8 characters which is a limitation of DES algorithm. Here the length of the watermark string/file and message is retrieved. The message is then decrypted with the supplied password. Finally the decrypted message is viewed and the media file is viewed.

3.5. Customer Information Management

This module represents to maintain the whole information about the customer name, addresses, Bank balance in banking database. This module intends to maintain the personal information about the customer. In this module the customer information's are stored in a secured manner using Steganography and Cued Click Points (CCP) technique from the attackers.

4. Discussion

In most of banking transaction the security is put in the hands of the user, the technical details might be perfect but if the user opens a hole in the security the attack will be possible. The security must be made reliable and easy to understand, the decision to override the security should be based on information that is clear to the user. The attacker in a man-in-the-middle scenario is not the ordinary "hacker". The attacker is a person with access to banking transaction in the Internet, so the attack might be considered to be some form

of an insider threat. It does not take a very skilled programmer to create a tool that can perform an attack. The tools and the programming libraries available today provide a good foundation for the creation of an attack tool. The skill required is to create a design capable of performing the desired task, and the complexity of this varies with the task. A plain sniffer-tool requires almost no design at all, while an active attack tool against a high security web service requires a more complex design.

The man-in-the-middle attacks are possible when a one-way trust relationship is used. The weak trust relation is then complemented by an authentication to establish the missing second trust relationship. Authentication in web services gives little protection against a man-in-the-middle attack. The only authentication that creates a problem for an attacker is when a hardware device is used to sign the user's intentions. All other authentication can just be forwarded between the user and the web service. The defense against man-in-the-middle attacks is to use a two-way trust relationship at the time when the connection is established, or to sign the user's intentions.

5. Conclusion

To reduce attacks, this paper has proposed a new scheme called Steganography which presents a way to blend additional information into an HTTP communication to provide an additional level of security. The proposed scheme uses two proxies, which checks authenticity of the HTTP communication. Also, successful human attack means to inspect all HTTP requests and responses personally. In this CCP gives more security. However the CCP is not user friendly. Even this technique is more protective, the attacker can learn the proposed system as the same key is used for more time. In future this system must be updated and it must overcome the disadvantages of the proposed system.

References

[1] E. Rescorla, "HTTP Over TLS‖ ," IETF RFC 2818, www.ietf.org/rfc/rfc2818.txt Last Accessed on February 3, 2010

[2] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol‖ ," IEEE Security and Privacy, vol.7, Jan-Feb. 2009, pp. 78-81, doi: 10.1109/MSP.2009.12

[3] D. Kristol and L. Montulli,"HTTP State Management Mechanism‖ ," IETF RFC 2965, www.ietf.org/rfc/rfc2965.txt Last Accessed on February 3, 2010

[4] J. Katz and Y. Lindell, "Introduction to Modern Cryptography: Principles and Protocols" Chapman & Hall/CRC Press, 2007, ISBN: 978-1584885511

[5] X. Liu, J. M. Kovacs, C.T. Huang, and M. G. Gouda, "A Secure Cookie Protocol‖ ," In Proceedings of 14th Computer Communications and Networks, San. Diego, California, USA, 2005

[6] Computer Security "ESORICS 2007 Lecture Notes in Computer Science," 2007, Volume 4734/2007, 359-374, DOI: 10.1007/978-3-540-74835-9_24

[7] "OSGI The footings of the foundation of the platform". The Eclipse Foundation. http://www.eclipse.org/osgi/. Retrieved 25 June 2008.

[8] "Apache Tomcat 7.0”Change log". http://tomcat.apache.org/tomcat-7.0- doc /changelog.html. Retrieved 2011-03-10.

[9] http://searchsoa.techtarget.com/definition/J2EE

[10] http://www.vocal.com/cryptography/des.html