Programmable SSL Interface and Its Application in Data Management with Multi-Layered Security Policy

Lin, H.; Yang, C.

National Research Council Canada
Institute for Information Technology

Conseil national de recherches Canada
Institut de technologie de l'information

NRC-CNRC

Programmable SSL Interface and Its Application in Data Management with Multi-Layered Security Policy

Hong Lin and Chunsheng Yang
May 2002

Programmable SSL Interface and Its Application in Data Management. Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002), Cancun, Mexico. May 20-22, 2002. pp. 497-500.
NRC 44917.

Programmable SSL Interface and Its Application in Data Management with Multi-Layered Security Policy

Hong Lin[1] and Chunsheng Yang[2]
[1]Department of Computer and Mathematical Sciences
University of Houston-Downtown
One Main Street, Houston, TX 77002, USA
Email: linh@uhd.edu[2] National Research Council of Canada
1500 Montreal Road, Ottawa, Ontario, Canada K1A 0R6
Email: Chunsheng.Yang@nrc.ca

Abstract

This paper presents an interface for secure data transfer between a web server and a client. It uses Secure Socket Layer (SSL) protocol to encrypt/decrypt the data that travel through the networks. The system administrators can select the cipher suites so that they can impose different security policy for different users. There is a cryptographic module in the web server of an application system. The web server maintains a database of users with users' passwords and security levels. The access control policies composite restrictions for users to access the database, and different users have different priority and expiration dates of its accessibility. The application of this programmable secure data transfer system in management of course records is also exploited in this paper. The management system allows students submit projects and view their records online on a timely base, and different policy will be used for different data, in accord with their security levels. The presented work is fundamental and can be extended to provide a framework for security and privacy control in e-Learning environments.

Key words: Security and Reliability, Internet based Educational and Training Systems, Secure Socket Layer, Web Server

1. Introduction

IP-based communications are now a reality due to advancements in communications infrastructure, processor technology, and data encoding techniques. Communications on IP networks facilitates access for participants beyond the boundaries of a private network, creating an open world for learning and communication.

However, enabling communication over open IP networks may create concern for privacy and security when sensitive information is transmitted. As the standard solution for applications where privacy is a prime concern, secure data transfer may be guaranteed using a combination of technologies such as secure sockets and secure encoding using secret shared states. Secure Socket Layer (SSL) [1] has become the standard for secure data transfer via internets and thus widely used in providing security and privacy services in e-Learning and e-Commerce sites. SSL is established upon TCP connection. A SSL handshake involves a phase for private key exchange using the server's public key. Then, the following data transfer will use symmetric encryption with the agreed private key.

Although its widespread use, the lack of understanding of the cipher suites causes the poor flexibility in deploying security policies in a multi-user environment. It depends on the power of existing tool, for example, Apache server with SSL module [2], to configure the security policy for all the clients. This restricts the availability of multi-layering security policies for different users in terms of cipher strength, access control and timing control.

During last years many e-Learning tools have been developed either in research or as industrial products. In the research area, a number of research groups worldwide are working now on Web-based education driven by the importance of integrating more flexibility and adaptability to e-Learning tools. We can reference in this context two popular projects: the Virtual

University Initiative from the United Nation University [3][4] (Ng S. T. Chong, UNU and Masao Sakaushi, University of Tokyo), and the InterBook and ELM-ART projects [5] [6] (P. Brusilovsky, Carnegie Mellon University, G. Weber, University of Trier Germany, and J. Eklund, Sydney University of Technology). In the industry area, many quite mature products are available in the market and used by many universities. Some of the well- known tools are LearningSpace (Lotus Development Corporation) [7], LearnLinc (LearnLinc Corporation) [8], Blackboard (Blackboard inc.) [9] and TopClass (WBT Systems.) [10].

However, an important element that is not discussed in existing solutions is the security and privacy (intellectual property control) aspect and the assessment of students. Therefore, the objective of this research is to provide a method for security policy control to the existing e-Learning environments. Specifically, we focus on a programmable interface that allows case wise policy control. Therefore, it implements a multi-layered policy control system. Also, because we handle the cipher suites and SSL connections directly, it allows further elaboration in every aspect.

2. The method

Currently privacy and security for e-Learning environments are provided only in an ad-hoc basis. The system presented here aims at providing an interface for programmable security control in a web server, and exploiting its application in a course record management system. With a rich set of cipher suites and SSL library, we implement an integration of policy based control for managing security, privacy and authentication. Privacy in addition involves the record keeping of privacy agreements. When a user connects to the server, a SSL session will be established for encrypted data transfer. After checking user's password, the server will access to the entry of the user in the database, load the predetermined cipher suite for that user, and use that cipher suite for the following data transfer. The server will also impose multi-layered access control on different users.

In this system, we use OpenSSL [11] library to program the interface. OpenSSL is a widely used open source for SSL protocol implementations. It provides a rich set of cipher suites and a rich set of functions for digital encryption/decryption. It also includes a public key interface (PKI) which can be used for private key generation and digital signatures.

The security and privacy module is applied to a course record management system in an e-Learning system, We use the security interface to provide encrypted data transfer, user authentication and access control. A privacy agreement will be kept for each user. Different user will have different security policy and valid period

We use a policy-based approach for specifying, negotiating, and managing privacy and security policies for students, teachers, and system administrators. The privacy policy describes how and what type of information may be shared with other users and the triggers and actions for privacy monitoring. Security policies specify the security details regarding the operation of the system. While the policies are developed and maintained in an internal table, the users develop and maintain the policies by using a Web-based interface.

3. Architecture

The system is composed of the following components:

HTTP server: HTTP server handles TCP connections and HTTP requests. HTTP server must be concurrent so that it can handles multiple connections simultaneously.

SSL module: the module which handles SSL connections. SSL module is built on top of the HTTP server. Whenever a security critical document is requested, it is invoked to handle data encryption and decryption.

Policy management system: the Policy Management System (PMS) works interchangeably with SSL module. It maintains a database of security policies established for each user. The database is dynamic: new users can add in, old users can be removed, and existing users can change their policy.

The above three modules: HTTP server, SSL module, and PMS form the architecture of the secure web access system. Applications to some specific areas can be built upon this base system by designing an interface of database management.

Student record access control interface (SRACI): Use the policy management system to provide the student record access control service. It maintains a table of security settings for data items which are deemed confidential, which can be modified by the user after password checking.

The architecture of the system is shown in Figure 1. Policy Database(PDB) maintains all secure access control parameters for all users. Policies are set item-wisely by PMS through the SSL interface provided by the SSL Module and HTTP server. Student Record Database (SRDB) contains all student records, including student names, ID numbers, grades, hand-ins, etc. Depending on students status (enrolled, non-enrolled, dropped, etc), student can select privacy policy for each piece of information stored in SRDB, which refers to PDB for detailed parameters of security settings. In Figure 1, solid lines are data flows, either in clear text or in cipher text, among modules; and dotted lines are control flows, which carry information about data encryption exchanged among modules.

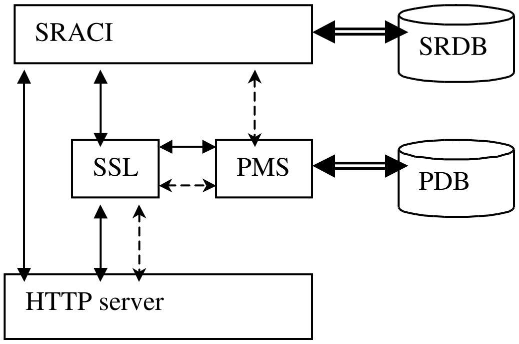

Figure 1. The architecture of the secure student record access system.

4. Implementation and Discussion

A typical scenario of a session of record enquiry is: A student connects to the web server and clicks on the button of record reviewer. A SSL session is started using a universal cipher suites for user ID and password checking. When the user select data items to view, SRACI forwards the request to PMS. PMS searches PDB for the cipher suites pre-set for corresponding data. Then a new SSL session is established for the specific data.

User privileges are set in accordance to status of the users in a hierarchical structure. Super user has the highest privilege which allows him to re-set all access parameters for every other user.

To provide a programmable interface, all the modules are designed from scratch. The following is the sketch of the main program segment of the SSL server, which is customized from Eric Rescorla’s code in his SSL book [13]:

```
  sock=tcp_listen();

  while(1){
    if((s=accept(sock,0,0))<0)
      err_exit("Problem accepting");

    if(pid=fork()){
      close(s);
    }
    else {

      // Read in user request

      // Contact PMS to load parameters for SSL
           connection

      // Initialize SSL session context according
           to pre-set parameters …
      ctx=initialize_ctx(KEYFILE,
                        PASSWORD);
      load_dh_params(ctx,DHFILE);
      generate_eph_rsa_key(ctx);
      sbio=BIO_new_socket(s,BIO_NOCLOSE);

      ssl=SSL_new(ctx);
      SSL_set_bio(ssl,sbio,sbio);

      if((r=SSL_accept(ssl)<=0))
        berr_exit("SSL accept error");

      // Data exchange goes here …

      destroy_ctx(ctx);
    }
  }
  exit(0);
}
```

We use the existing student records of the courses the present author taught as the experimental data. Experiments to test the stability of the server will be done via Internet using different web browser with different cipher strengths.

This SSL interface will provide a fundamental for a fully-fledged, portable, and multi-layered security policy management system for e-Learning. The proposed research is fundamental and initiative because we focus on direct handling of cipher suites and programming. The potential impact of this work is remarkable, e.g., providing students with a stricter course material submission and evaluation, supporting the entry of new learning paradigms into the education enterprise and addressing rising educational needs and cost.

A possible extension of this security policy management system is a secure mobile agent system. In the secure mobile agent system, instead of merely managing security policy control from the server side, i.e., maintaining a policy database, searching the policy for particular data items and establishing a SSL connection merely by the server, a mobile agent program migrates through the SSL channel to the client side with the policy data of the specific user. Thus, a portion of the policy control can be done by the client. This approach will not only improve the efficiency of the server because a part of the work load is transferred to clients, but also strengthen the integrity of the security management model because the behaviors of users are more predictable and more error-proofing.

5. Conclusion

We presented a fundamental framework of security policy management system used in database management. Instead of providing a uniform security policy for all clients, the proposed SSL interface program handles security policy based on user status and inputs, and establishes a hierarchy of privacy policies. Therefore, piece-wise security control is achieved. We use this model to design a student record management system, which allows web access to student records. This system can also be used in other applications. We found that a programmable SSL interface is useful in e-Learning because e-learning's heterogeneous nature of data management and transfer and its requirement for high performance in data transmission.

References

[1] SSL & TLS Essentials: Securing the Web, Stephen A. Thomas, John Wiley, 2000.

[2] Apache Server, available at http://www.apache.com/

[3] Virtual University Initiative Prospectus (September, 2000). Available at: http://www.ias.unu.edu/projects/download/prospectus.pdf

[4] N.S.T. Chong and M. Sakauchi. Classroom Anywhere: a new software foundation in distance learning. First international conference on distance education and open learning, september, 2000. Available at: http://www.con.unisa.edu.au/cccc/papers/refereed/paper9/paper9-1.htm

[5] G. Weber and M. Specht. User Modeling and Adaptive Navigation Support, in WWW-based Tutoring Systems. Proceedings of User Modeling '97, pp: 289-300. 1997. Available at: http://www.psychologie.uni-trier.de:8000/projects/ELM/Papers/UM97-WEBER.html.

[6] P.Brusilovsky, J. Eklund and E. Schwarz. Web-based education for all: a tool for development adaptive courseware, in the 7th International World Wide Web Conference, 1998. Available at: http://www7.scu.edu.au/programme/fullpapers/1893/com1893.htm

[7] LearningSpace 4.0 Whitepaper. Available at : http://www.lotus.com/home.nsf/welcome/learnspace

[8] LearnLinc 4.5 in Detail. Available at: http://www.ilinc.com/article.cfm?ArticleID=19&EID=0&PID=na

[9] Blackboard 5 features: available at : http://company.blackboard.com/products/infrastructure/index.cgi?SELECT=12

[10] TopClass Overview. Available at: http://www.wbtsystems.com/products/overview.html

[11] OpenSSL, available at: http://www.openssl.org/

[12] Redhat Linux, available at: http://www.redhat.com/

[13] Eric Rescorla, *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, 2001