Using ASP-Based Message Encryption Project To Teach Information Security Concepts

Qidong Cao
College of Business Administration, Winthrop University
Rock Hill, SC 29733, USA
caoq@winthrop.edu

John S. Davis
Department of Management, Clemson University
Clemson, SC 29634-1305, USA
davis@clemson.edu

Xue Bai
School of Business, Virginia State University
Petersburg, VA 23806, USA
xbai@vsu.edu

Orlando E. Katter
College of Business Administration, Winthrop University
Rock Hill, SC 29733, USA
Kattero@winthrop.edu

ABSTRACT

Information security has emerged as one of the most important subjects of information system (MIS) majors. This paper describes the use of a message encryption project based on Microsoft Active Pages (ASP) that encourages MIS students to explore some of the technical aspects of information security in some depth. This project served as a valuable pedagogical tool. Students having only limited programming and database experience benefited significantly from this course.

Keywords: Network security, client-side / server-side scripts, encryption, ASP.

1. INTRODUCTION

As computer network becomes an important part of the business world as well as our daily life, information security should be taught not only to the computer science students, but also to the business students. Hands-on projects, which are technical but simple to implement, can help motivate the MIS students explore the technical concepts in information security. On this basis, the authors assigned to MIS students a course project to develop a Web application providing message encryption. This project is simple enough for them to implement, as it requires elementary programming skills, which they already got from other courses. The project on the other hand lets the students explore, in some depth, some of the technical aspects of information security. The rest of this paper is organized as follows. Section 2 describes a doable project for business students. Section 3 provides an overview of message encryption. Section 4 presents an example of a student project. This is followed by discussion on pedagogical approach and a summary of student feedback in Section 5. Section 6 concludes by reviewing important aspects of the project.

2. A DOABLE INFORMATION SECURITY PROJECT

The choice of project was motivated by a desire to provide hands-on experience to students having limited technical backgrounds while requiring limited technical support. Because encryption plays such an important role in information security as discussed in the next section, the project provides students an opportunity to set up message encryption.

Choosing a web application reduces requirements for technical support. A typical message encryption project involves software running on client and server computers and requires substantial support of system administrators (because students and instructors lack necessary server and network permissions). However, the student project requires nothing more than maintaining student Web accounts that are already available.

This project is appropriate for the technical skills of most business students. Many business students know basic techniques for web site development. To prepare them for this project requires only introducing them to ASP, including methods for connecting Web pages to databases. Because the code for ASP applications is more readable than other programming languages, students have no serious problems becoming familiar with it. Also, as students present their projects, other students can easily learn the different techniques used by different students to implement information security.

3. AN OVERVIEW OF MESSAGE ENCRYPTION

An overview of message encryption may help explain the basis for the student project. There are two major classes of encryption algorithms (Stallings 2000): conventional encryption and public-key encryption. Conventional encryption uses one secret key for both encryption and decryption. This key is shared by message sender and recipient. Some popular conventional encryption algorithms are DES (FIPS PUB 1977), IDEA (Lai 1991), Blowfish (Schneier 1993), RC5 (Rivest 1994), CAST-128 (Adams 1997), RC2 (Rivest 1998) and TDEA (FIPS PUB 1999).

Public-key encryption generates keys in pairs. If one key is used to encrypt a message into a ciphertext, another key can decrypt the ciphertext into the original plaintext. Public-key encryption was first publicly proposed by Diffie and Hellman (1976). The most popularly adopted public-key encryption algorithm is the RSA encryption algorithm (Rivest 1978). The public-key encryption algorithms are largely used for digital signature and key distribution due to their heavy computational burden.

As a simplified system, the course project uses the conventional encryption algorithm without any requirements for key distribution. (Secret keys can be delivered in person within the class.) Students develop their own encryption algorithms that have to include all three basic operations: substitution, transposition, and exclusive or. Advanced students who are interested in more sophisticated encryption algorithms are referred to Web sites where free source code of some popular conventional encryption algorithms is available.

4. AN EXAMPLE OF STUDENT PROJECT

Students develop Web applications that can transmit encrypted messages back and forth between client and server computers. For example, one student developed a grade report system. It is based on a two-way Web site that allows a student to enter his/her unique user id and course ID (password) for retrieving his/her grade information from a database. The user IDs and grades have to be encrypted before transmission over the Internet. To complete this project the student creates his/her Web site that connects to a small database, and then adds encryption/decryption functions to the Web site. Interested readers may view or download this project (http://www.birdnest.org/caoq1/encryption/). In the home page of this Web site, a hyperlink (“Grades”) activates the grade report system. This system includes two ASP pages (index.asp and grades.asp) that connect to a Microsoft Access single-table database. This database stores for each student the user ID, the course ID, name and grades. The course IDs are encrypted before leaving the client computer. The grades from the database are encrypted before being sent from the Web server. Figure 1 shows cooperation between client and server computers.

When the hyperlink "Grades" is clicked, the client browser sends a request to the Web server for the ASP file "index.asp". The server processes the server-side script in this file and sends the resulting Web page to the client computer. The index.asp page has two forms. The first form has input boxes for user to enter his/her user ID and course ID, and two command buttons (Figure 2). (One may observe the functioning of this page by visiting the aforementioned Web site with a user ID “smiths1” and a course ID “abcde”). When the user clicks the command button ("Encrypt") the client-side script calls an encryption function that generates a secret key based upon the course ID, encrypts the course ID with this secret key, and then writes both user ID and the encrypted course ID into the text-input boxes of the second form (Figure 2). When the submit button ("Login") is clicked, the form takes action that again requests index.asp from the Web server as the client computer sends the user ID and the encrypted course ID along with the request. Again, the server processes the server-side scripts in index.asp, that reads the user ID and the encrypted course ID, and then searches database for a match of user ID. If there is no match, the resulting Web page is sent for the user to reenter a user ID. If a match is found, the server-side script retrieves the course

ID from the database and generates the secret key with the course ID. The secret key is used to decrypt the encrypted course ID from the client computer and then the decrypted course ID is compared with the course ID from the database. If there is no match, the resulting Web page is sent for the student to reenter a course ID. If two course IDs match perfectly, the user's browser is redirected to the second ASP file (grades.asp) that has access to the correct course ID that is stored in a server-side ASP object called a "session variable". This technique prevents users from directly accessing the grades.asp without a correct course ID. If a user tries to directly access the grades.asp with its URL, the session variable is null and the user's browser will be redirected to index.asp for the user to enter a course ID.

The second ASP file (grades.asp) retrieves and displays the student grades in the following way. The server processes the server-side script in the grades.asp that reads the course ID from the session variable and retrieves the corresponding record from the database. The second ASP file (grades.asp) retrieves and displays the student grades in the following way. The server processes the server-side script in the grades.asp that reads the course ID from the session variable and retrieves the corresponding record from the database. After retrieving a record, the server-side script uses a secret key generated with the course ID to encrypt student grades, writes encrypted grades into the first form of page and sends the resulting page to the client computer. If the user enters the correct course ID and clicks the command button ("Decrypt"), the client-side scripts in grades.asp will use a secret key based upon the course ID to decrypt grades and will display them in the second form of the page (Figure 3).

Figure 1. **An ASP-Based Message Encryption System**

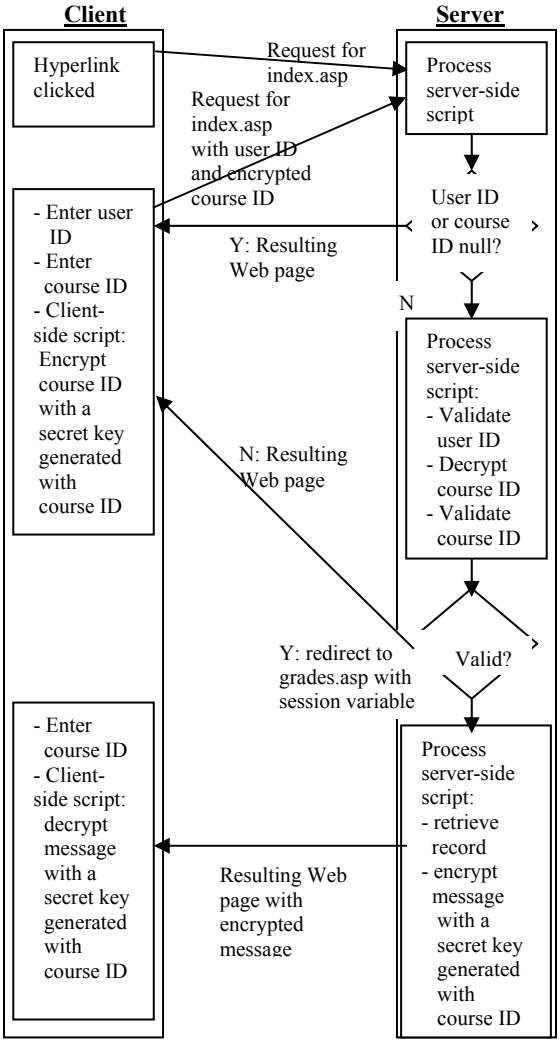


Figure 2. ASP Page: index.asp

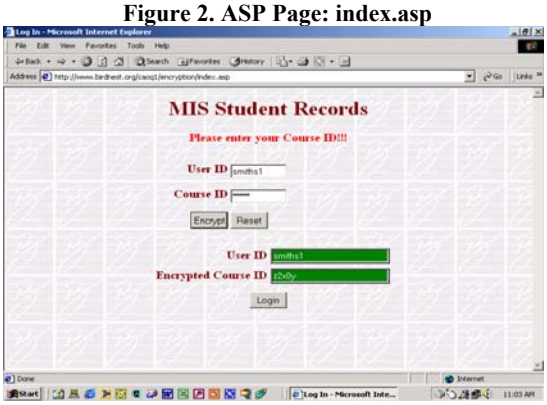
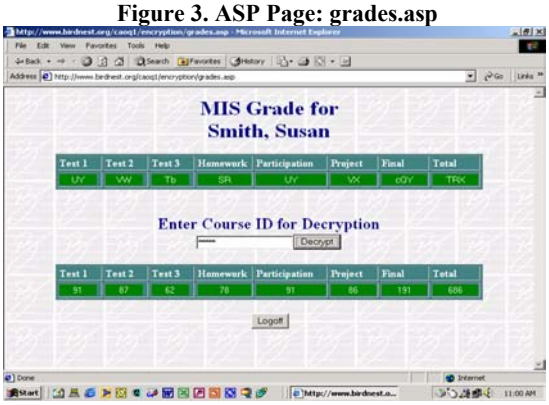


Figure 3. ASP Page: grades.asp



5. PEDAGOGY AND STUDENT FEEDBACK

This course project is a pedagogical tool that helps students understand the concepts of information security. The project moves those concepts beyond abstract concepts to a deeper understanding. In this section, Subsection 5.1 describes how the project is assigned to business students. Next, Subsection 5.2 presents the use of this project as a pedagogical tool for concepts of information security. This is followed by student feedback in Subsection 5.3.

5.1 Project Assignment

This assignment requires students to include the following basic components in their project:

(1) Create a personal Web site and upload it to the student Web account.
(2) Create a single table database and upload it to the student Web account.
(3) Connect the database to the Web site.
(4) Develop a query using a value of a primary key to retrieve and display a specific record.
(5) Develop and implement a simple symmetric key encryption algorithm that includes three basic operations: substitution, transposition, and exclusive or.
(6) Using the algorithm, encrypt the primary key and the database contents before they are transmitted over the Internet, and decrypt them after receipt from the Internet.
(7) For the purpose of project presentation and possible cryptanalysis, display ciphertext and its plaintext in the same page.

Key distribution is not a part of this project. Students are allowed to deliver the secret keys to users in person. Because some students are inexperienced in web applications, we give students a written tutorial covering the following:

(1) Basic HTML tags for creating a Web site.
(2) An example script for using ASP component to connect a database to a Web page. Students can connect their database to a Web page by simply filling in the absolute address of the database.
(3) An example script for declaring variables.
(4) An example script for retrieving a database record with a value of primary key. Students can use the example in their ASP pages by filling in a database table name and the field name of the primary key.
(5) An example script for writing form contents to variables or writing variable values into a form. Students can use these examples in their ASP pages by filling in variable names and form object names.
(6) Examples scripts for control structures of selection and repetition. Students learn these structures to code their simple encryption algorithms.

5.2 Project As Pedagogical Tool

To stimulate a deeper understanding, students should include in their project report a discussion on information security concepts they learned by analyzing their projects. Those concepts include the following:

(1) Discuss four general categories of attack (interruption, interception, modification and fabrication). Understand the danger of wiretapping and the importance of information security when messages are passed between client and server computers.
(2) Discuss differences between two major classes of encryption algorithms (the conventional encryption and the public-key encryption) and their applications (message encryption, key distribution, and digital signature). Explain three basic operations of conventional encryption/decryption (substitution, transposition, and exclusive or).
(3) Discuss cooperation between client and server computers for performing message encryption/decryption. (A message has to be encrypted and decrypted on the different sides.)
(4) Discuss differences between modern cryptography and restricted algorithms. Explain the security problems inherent in restricted algorithms.
(5) Discuss what issues influence selection of an encryption algorithm. Explain the dangers of cryptanalysis (ciphertext only, known plaintext, chosen plaintext and chosen ciphertext attacks, differential cryptanalysis, linear cryptanalysis) and brute-force attacks.
(6) Discuss threats to password.

5.3 Student Feedback

Students' work on this project and presentations of the projects stimulate discussions on information security concepts of which students may otherwise not have a clear understanding. The main points reported by students are listed below. They have said this project:

(1) Helped them see the cooperation between client and server computers when using the client-side and server-side scripts for encryption and decryption.
(2) Helped them understand the importance of protecting data to be transferred over the Internet,
(3) Clarified the basic mechanism for encrypting data.
(4) Encouraged in-depth discussion of information security.
(5) However, some of those students complained that they were asked to do something inappropriate for their background.

6. CONCLUSION

The pedagogical method of choice will usually be determined by such factors as educational background of students and objectives of their academic program. Many business students will be managers in the future. Development of a real information system is beyond the scope of a business curriculum and the level of their technical competency. However, developing a simplified system is within their capabilities and affords them a deeper understanding of concepts than they might otherwise achieve. In working on this project their effort was not limited to merely memorizing what their textbook says. Rather, students spent a good deal of time searching the Internet and library to get a clearer understanding of those concepts.

Through this hands-on project, students played dual roles during the course of their project. As "system developers", they learned the basic technical skills (Web site and database). As "managers", they used concepts that they learned in class to comment on their simple workable systems. The dual roles could help the future managers have better communications with technical personnel.

However, some may complain (as some of ours did) they are asked to do something inappropriate for their background. Therefore, for MIS courses without rigid prerequisites, this project might be assigned as just one of the options for a course project or might be assigned as a group project.

7. REFERENCES

Adams, M. Carlisle [1997], "Constructing Symmetric Ciphers Using the CAST Design." Designs, Codes, and Cryptography, 12(3), pp. 267-282.

Diffie, Whitfield and Martin Hellman [1976], New Directions in Cryptography, IEEE Transactions on Information Theory, 22(6), pp. 644-654.

Lai, Xuejia and James L. Massey [1991], "Markov Ciphers and Differential Cryptanalysis." Proceedings of EUROCRYPT, April 8-11, pp. 17-38.

National Bureau of Standards [1973], Federal Register, March 15.

National Bureau of Standards [1977], Federal Information Processing Standard 46.

National Institute of Standards and Technology [1999], Federal Information Processing Standard 46-3.

Rivest, Ronald, Adi Sharmir and Leonard M. Adleman [1978], "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." Communications of the ACM, 21(2), pp. 120-126.

Rivest, Ronald [1994], "The RC5 Encryption Algorithm." Proceedings of Second International Workshop on Fast Software Encryption, December 14-16, pp. 86-96.

Rivest, Ronald [1998], "A Description of the RC2(r) Encryption Algorithm." *RFC2268, http://rfc2268.x42.com*.

Schneier, Bruce [1993], Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Proceedings of Workshop on Fast Software Encryption, December 9-11, pp. 191-204.

Schneier, Bruce [1996], Applied Cryptography, John Wiley & Sons, Inc., New York.

Stallings, William [2000], Network Security Essentials, Prentice Hall, New Jersey.

AUTHOR BIOGRAPHIES

Qidong Cao is an Associate Professor at Winthrop University. His research interests include data mining, message encryption, production scheduling, and supply chain management. He has published in such journals as Computers & Operations Research, International Journal of Flexible Manufacturing Systems, International Journal of Production Research, and International Journal of Operations and Quantitative Management. He holds a Ph.D. in Industrial Management from Clemson University.

John S. Davis is a full professor at Clemson University. His research interests include decision support systems, human factors in computer systems, and design of information systems. He has completed research projects sponsored by the National Science Foundation and Department of Defense. He holds a Ph.D. in Information and Computer Science from Georgia Institute of Technology.

Xue Bai is an Assistant Professor at Virginia State University. His research interests include ERP, GIS, message encryption, speech recognition, and supply chain management. He has published in International Journal of Production Research. He is also the author of two MIS books. He holds a Ph.D. in Industrial Management from Clemson University.

Orlando E. Katter, Jr. is an Assistant Professor at Winthrop University. His research interests include computer architecture, information security, systems audit and control, and e-commerce systems assurance. He has presented at International Conferences in Shanghai and Brussels; he has been published in IEEE Southeastcon Conference and Carolinas Audit and Control Conference proceedings. He holds an M. S. in Computer Science from the University of North Carolina at Charlotte.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096