Oct 20th, 11:30 AM - 11:55 AM

Teaching Cybersecurity in an Undergraduate Engineering Course

Xiuli Qu
North Carolina A&T State University, xqu@ncat.edu

Xiaohong Yuan
North Carolina A&T State University, xhyuan@ncat.edu

Abstract
Organizations create a huge amount of sensitive and confidential data, which must be protected from unauthorized access or disclosure. Nowadays, most organizations store their business data in digital formats. With the increasing use of digital data, data breaches are more often and serious in recent years. Therefore, it is very important for next-generation engineers to be aware of the importance of information security, and be able to recognize vulnerabilities and threats to an information system and design user-friendly and effective security measures. To achieve it, two modules of information systems security, including lectures and in-class labs, were developed and taught in an undergraduate engineering course at North Carolina A&T State University. The learning objectives, teaching materials, and assessment outcomes of the two course modules are presented in this paper. Our survey results show that the course modules achieve the learning objectives and improve students' interest in pursuing cybersecurity-related careers.

Keywords: Engineering Education, Database Security, Usable and Effective Security

Location
KC 400

Disciplines
Engineering Education | Information Security

Comments
This work is supported by the National Security Agency (NSA) under the award H98230-17-1-0332. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSA. This research is conducted under a North Carolina A&T State University IRB approval.

1. INTRODUCTION

Organizations create a huge amount of data, including customer and personnel information, operations data, business transactions, financial data, and so on. These data are critical and valuable assets. Most of these data are very sensitive and confidential, and must be protected from unauthorized access or disclosure (CyberEdge Group, 2016; Vonnegut, 2016). Over the past 10 years, most organizations transformed their business data into digital formats, and store their data on servers, desktops, laptops or somewhere on the Internet. With the increasing use of digital data, data breaches occur more often and seriously. For example, the number of reported data breaches in the U.S. has increased by about 45%, from 1093 in 2016 to 1579 in 2017 (Statista, 2018). According to the Identity Theft Resource Center (2018), more than half of the data breaches in 2017 occurred in the business sector, and about 60% of the data breaches in 2017 were caused by hacking (including phishing, ransomware/malware and skimming attacks). Based on the numbers of accounts affected, the worst data breach in history is the disclosure of Yahoo's user information occurred in 2013 and 2014 and uncovered in 2016. It is estimated that all 3 billion Yahoo user accounts have been compromised in the data breaches, which resulted in a loss of about $350 million in Yahoo's sale price (Armerding, 2018). Therefore, it is very important for companies of all sizes to actively protect their data and information systems through sufficient cybersecurity measures and user compliance with the security measures.

The protection of information systems is a Systems Engineering process, which must start from the development of an information system. Potential threats to the system must be identified in the analysis phase of information system development. Countermeasures to the threats must be designed in the design phase and implemented and tested in the implementation phase. Since users are often the weakest point in the security of an information system, usable security design is critical in information system development. As one of the careers for Industrial and Systems Engineering (ISE) graduates, systems analysts and project managers must understand the importance and goals of information security, and be able to recognize vulnerabilities and threats to an information system and design user-friendly security measures to handle them. Therefore, two modules of information systems security, including lectures and in-class labs, were developed and taught in a required course of the undergraduate ISE curriculum at North Carolina A&T State University (NC A&T).

In this paper, we present the topics and materials of information systems security in the two course modules, and the assessment and outcomes. The

remainder of this paper is organized as follows. The course in which to teach the two modules is introduced and related courses are reviewed in Section 2. In Section 3, we present the learning objectives, teaching materials and assessment instruments of the two modules. After that, our survey results and learning outcomes are provided in Section 4. Finally, the conclusions and limitations are discussed in Section 5.

2. BACKGROUND AND RELATED WORKS

2.1 Background

ISEN380-Information Technology for Industrial and Systems Engineers is a 3-credit required course of the undergraduate ISE curriculum at NC A&T. It focuses on the concept of systems development life cycle (SDLC) and the planning, analysis and design techniques used in the SDLC of enterprise information systems (Valacich, George, & Hoffer, 2015). The techniques taught in this course include data-flow diagramming, entity-relationship (E-R) diagramming and relational database modeling. This course also introduces system requirements determination, prototyping, human interface design principles, information systems testing, user training methods, and the concept of object orientation programming. In this course, in-class labs and a lab project provide students with hands-on experience in designing and implementing databases and human interfaces using Microsoft Access.

A common SDLC model of an information system consists of the Planning, Analysis, Design, Implementation and Operation phases. During the SDLC of an information system, potential threats to the system should be identified in the Analysis phase. Countermeasures to the threats and user-friendly secure interface must be designed in the Design phase and implemented and tested in the Implementation phase. In the Operation phase, user compliance with security measures and policies is crucial for protecting sensitive data from unauthorized access and exposure. Therefore, the security modules developed for ISEN380 introduce the security topics related to the SDLC of an information system, such as common threats to databases, countermeasures to the threats, usable security design principles, and so on.

2.2 Related Courses

Most undergraduate Computer Science (CS) curriculums include elective courses covering cybersecurity topics. For example, the CS Department at North Carolina State University (NC State) offers two undergraduate cybersecurity courses, Computer Security and Network Security, which both introduce basic concepts

and techniques in information security and management (NC State Department of Registration & Records, 2018). The CS Department at NC A&T offers four undergraduate cybersecurity courses, Fundamentals of Information Assurance, Computer Systems Security, Applied Network Security and Security Management for Information Assurance (NC A&T CS Department, 2018). These courses also cover the topics of information systems security. Such cybersecurity courses are commonly offered at undergraduate and graduate levels in CS departments.

Although it is very important for next-generation systems engineers to be aware of the importance of information security, cybersecurity threats and user-friendly security design, few ISE or ISE-relevant programs offer undergraduate courses covering cybersecurity topics. To our best knowledge, the Department of Industrial, Manufacturing and Systems Engineering at Texas Tech University is the only undergraduate Industrial Engineering (IE) program that offers elective cybersecurity courses (Texas Tech University Academic Catalog, 2016). These courses introduce the topics of information systems security and cybersecurity issues of software development and infrastructure. Unfortunately, such cybersecurity courses are rarely included in undergraduate IE or ISE curriculums. In addition, although user-centered interface design principles are usually introduced in at least one required course of an undergraduate ISE curriculum, user-friendly security design is not covered in any regular ISE courses.

3. LEARNING OBJECTIVES, MATERIALS AND ASSESSMENT

Since a database is the backbone of an information system and database security plays an important role in information systems security, one security module introduces common threats to database security and countermeasures to be considered in database design. The other module covers usable security issues in human interface design. Meanwhile, two in-class labs were designed for students to learn how to implement security measures in a database. The two security modules, including lectures and labs, were developed for ISEN380 and offered in the spring 2018 semester. On completion of these security course modules, students should be able to:

- explain the importance of information systems security,
- explain the importance of database security and threats to databases,
- describe commonly-used database security measures,
- describe the meaning and measures of user authentication,
- implement a user-friendly Login form for a Microsoft Access database, including password encryption, and

- implement access control and data encryption in a Microsoft Access database.

3.1 Database Security

The database security lecture introduces database security topics for an introductory course (Murray, 2010). Database security refers to the collective measures used to preserve the confidentiality, integrity, and availability (CIA) of databases. The main database security measures are access control, inference control, flow control and data encryption (Bourgeois & Bourgeois, 2014). As such, the lecture introduces the concepts of the four main database security measures and focuses on the two types of database access control mechanisms (discretionary access control and mandatory access control). The lecture also introduces the importance of database security, threats to databases, role-based access control, and database auditing and backup. The expected learning outcomes of this lecture are that students should understand the importance of database security and threats to databases, and be able to describe common database security measures.

Sample Assessment Questions

Which of the following is a threat to databases?

(a) Authorized disclosure of information to authorized users
(b) Authorized modification of information by authorized users
(c) Granting all privileges to all authorized users
(d) Granting privileges only to authorized users who need them to perform their tasks

Which of the following does Access Control refer to?

(a) Preventing authorized users of a statistical database from accessing information about individuals.
(b) Providing additional protection for sensitive data that is transmitted through the communication networks such as the Internet.
(c) Regulating the flow of information among accessible objects.
(d) Restricting access to a database system by assigning rights and privileges to users and database objects.

Which of the following is a privilege that can be granted at the account level of discretionary access control?

(a) MODIFY
(b) READ
(c) UPDATE
(d) WRITE

3.2 Usable Security in Human Interface Design

Usually, security is viewed as a burden by information system users because it causes inconvenience and reduces their productivity (Lampson, 2009). Consequently, users ignore or bypass security controls if possible, and hence become the weakest point in information system protection. Therefore, designing usable security functions is important in the SDLC of secure information systems. As such, the usable security lecture first introduces the three approaches to usable security: (1) making security invisible, (2) making security understandable, and (3) educating users. The lecture focuses on how to educate users to understand security policies and how to make users aware of their behavior's contributions to security. The lecture also introduces the importance of information systems security, conflicts between security and usability, the meaning and measures of user authentication, general rules of creating strong passwords, and the principles for usable security design (Lampson, 2009; Payne & Edwards, 2008). The expected learning outcomes of this lecture are that students should understand the importance of information systems security and the principles for usable security design, and be able to describe the meaning of user authentication, and the approaches to usable security.

Sample Assessment Questions

Why are most security messages and reminders ignored by users?

(a) Users do not believe that they are at risk.
(b) Users thought that other users will ignore such messages and reminders.
(c) Users want to share the access with other persons who can not access the information system.
(d) Users want to share the information with the public.

Which of the following is a rule for creating strong passwords?

(a) Do not use special characters in your password.
(b) Do not use words that can be found in a dictionary.
(c) Set a password with less than 8 characters.
(d) Use only uppercase characters in your password.

Which of the following is an approach to usable security? (Please check all correct answers.)

(a) Do not involve users in the design of security
(b) Educating users about security
(c) Keeping security issues from users
(d) Making security functions and algorithms to work better and invisible
(e) Making security understandable

3.3 Database Security Labs Using Microsoft Access

In order for students to gain a better understanding of database security measures, two in-class labs were designed for ISEN380 students to learn how to implement security measures in a Microsoft Access database. The two labs were developed to implement database access control and data encryption using the security functions available in Microsoft Access 2016 (Harkins, 2009). The two labs provide students hands-on experience of implementing user access control in an Access database, and hashing passwords and encrypting an Access database. In addition, students can also gain experience in user authentication and user-centered security design.

In the first lab (Lab 1), students are required to create a Login form to control the access to a database, and to hash passwords stored in a database table. In the lab, a simplified Access database is provided to students. This database is used to collect and manage the information of prospective students of the ISE Department. The simplified Access database consists of three tables and four forms. Figure 1 shows the three tables and their relationships, and figure 2 shows the four forms in the database provided for the lab. In the lab, first, students need to create a table named "User" which stores usernames, passwords and access levels, and then insert two records in the User table. Table 1 shows the two records to be inserted into the User table. Next, students are required to create a Login form to control the access to the database. The Login form (see figure 3) should consist of two text boxes for users to type in their username and password, respectively, and a button for user authentication. When the Login button is clicked, the username and password typed in are compared to the pairs of usernames and passwords stored in the User table. If matched, the user can open the database; otherwise, the access is denied. The last task of Lab 1 is to create a simple encryption function and use it to hash passwords in the User table. To help students better understand Lab 1 tasks, a few YouTube videos are provided to students before the lab.

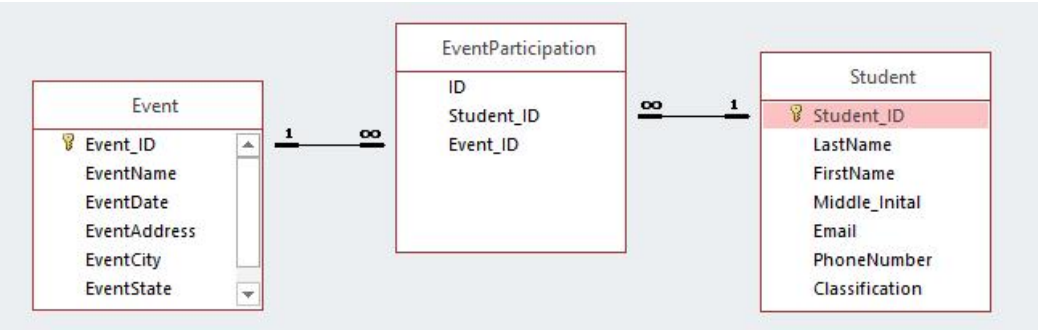
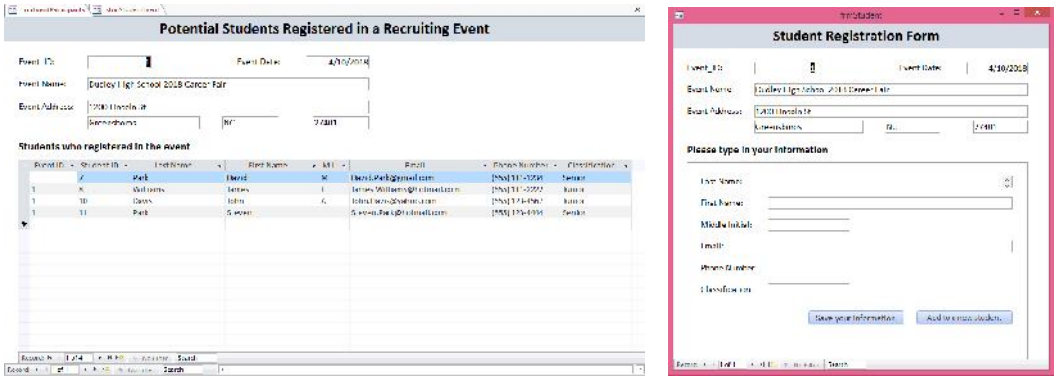


Figure 1: Relationships of the three tables in the database provided for Lab 1



(a) *(b)*

Figure 2: Two forms with subforms in the database provided for Lab 1

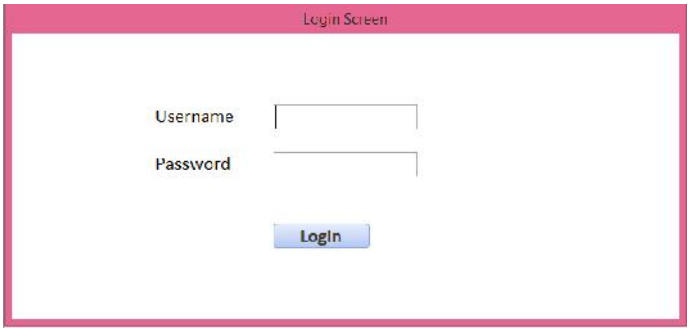


Figure 3: Login form to be created in Lab 1

Username	**Password**	**AccessLevel**
Recruiter	Password	ADMIN
Student	Everyone	GUEST

Table 1: Two records in the User table

In the second lab (Lab 2), students can learn how to control user access to data, and how to split and encrypt an Access 2016 database. In the lab, students start from the Access database they created in Lab 1. First, students are required to revise the Login form to control user access to data. If an administrator logs in, the form in figure 2(a) will open for the user to manage the information of prospective students. If a user logs in as a guest, the form in figure 2(b) will open to allow the user to type in and save his information, but block the user from accessing the information of other students. After that, students practice (1) splitting the Access database into two databases (a backend database storing data

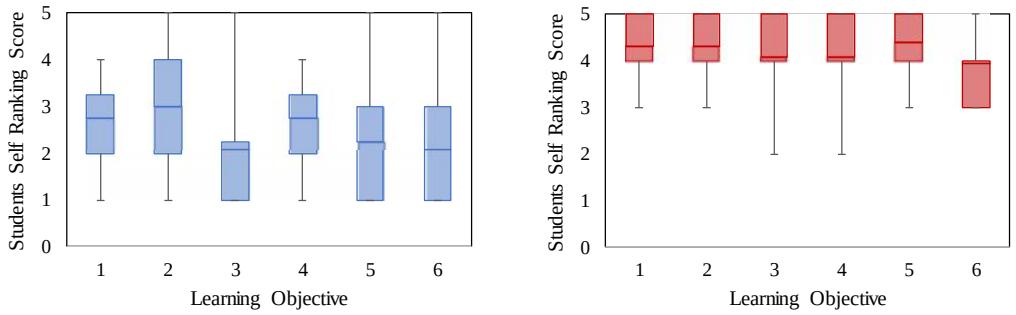
in tables, and a frontend database containing the forms); (2) encrypting the backend database by setting a password; (3) securing the frontend database by changing the database startup options.

4. RESULTS

The two security course modules, including the lectures and labs, were taught in the spring 2018 semester at NC A&T. The two modules were taught in two consecutive weeks in late April after completing the lectures and labs of database design and human interface design. Twenty-eight (28) ISE undergraduate students were enrolled in ISEN380 in the semester.

Voluntary and anonymous surveys were conducted before and after the two modules. Thirteen (13) students in the class participated in both the pre-survey and post-survey. Before taking the two security course modules, none of them had taken any cybersecurity course or training or had other experience with cybersecurity. Most of them (10 out of 13) are interested in learning cybersecurity topics. However, only one participant was interested in pursuing a career in cybersecurity before taking the course modules. In the post-survey, 5 of the 13 participants are interested in pursuing a career in cybersecurity. All participants agreed that the course modules helped them understand cybersecurity.

The majority of participants (12 out of 13) agreed that they met the learning objectives of the course modules. Figure 4 shows the survey results of students' self-rankings for the six learning objectives pre and post the two course modules. In the figure, the middle lines within boxes indicate the averages, and the boxes show the range of the middle half (from the first quartile to the third quartile). The results in figure 4 show the improvement of the participants in all six learning objectives after taking the course modules.



(a) Pre-survey results *(b) Post-survey results*

Figure 4: Self ranking scores on the learning objectives pre and post the course modules

5. CONCLUSION AND LIMITATIONS

This paper presents two course modules designed to prepare future systems analysts or engineers with the security concepts and basic skills needed in information systems analysis and design. The lectures of the course modules introduce the importance of information systems security and database security, thrusts to database security, common database security measures, and the approaches and principles for usable security design. The two in-class labs provide students hands-on experience of implementing access control and data encryption in a Microsoft Access database. The two course modules were taught in an undergraduate engineering course in spring 2018. Our survey results show that the course modules achieve the learning objectives and improve students' interest in pursuing cybersecurity-related careers.

One limitation of this study is that only 13 students participated in both the pre-survey and post-survey because the surveys were not mandatory. Thus, no statistically significant results were concluded from the survey data. The course modules will be taught at NC A&T once per academic year in the future. We will collect more data by conducting the same surveys when the course modules will be taught in the future. In class and labs, we also observed that several students struggled with quiz questions and lab requirements. In the future, we will add a few examples or real-world stories in the lectures to demonstrate database security measures and conflicts between security and usability. We will also revise the lab instruction to eliminate students' misunderstanding of lab requirements. The materials in the lectures and labs will be continuously improved based on students' feedback to attract more students' interest in cybersecurity.

ACKNOWLEDGEMENTS

Steven Mason helped in developing the two in-class labs presented in this paper. Theanna Drennon and Teddy Parker provided the feedback to the lab instruction after testing the labs. The authors thank their help in the development of the course modules.

This work is supported by the National Security Agency (NSA) under the award H98230-17-1-0332. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSA. This research is conducted under a North Carolina A&T State University IRB approval.

REFERENCES

Armerding, T. (2018). The 17 biggest data breaches of the 21st century. Available at https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Bourgeois, D. & Bourgeois, D. T. (2014). Information systems security. In D. T. Bourgeois (Ed.), *Information Systems for Business and Beyond*. Online Publisher: Pressbooks. Available at https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/

CyberEdge Group (2016). 2016 cyberthreat defense report. Available at https://webroot-cms-cdn.s3.amazonaws.com/4814/5954/2435/2016_cyberedge_group_cyberthreat_defense_report.pdf

Harkins, S. (2009). 10 tips for securing a Microsoft Access database. Available at http://www.techrepublic.com/blog/10-things/10-tips-for-securing-a-microsoft-access-database/

Identity Theft Resource Center (2018). ITRC data breach overview 2005 to 2017. Available at https://www.idtheftcenter.org/images/breach/Overview20052017.pdf

Lampson, B. (2009). Usable security: How to get it. *Communications of the ACM*, 52(11), pp.25-27.

Murray, M. C. (2010). Database security: What students need to know. *Journal of Information Technology Education*, 9. Available at http://www.jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf

NC State Department of Registration & Records (2018). Undergraduate and graduate CSC course catalog. Available at https://www.acs.ncsu.edu/php/coursecat/directory.php?subject=CSC

NC A&T Computer Science Department (2018). Undergraduate student handbook. Available at https://www.ncat.edu/coe/departments/comp/pdfs/UG%20Handbook2018.pdf

Payne, B. D. & Edwards, W. K. (2008). A brief introduction to usable security. *IEEE Internet Computing*, *12*(3), 13-21.

Statista (2018). Annual number of data breaches and exposed records in the United States from 2005 to 2018. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Texas Tech University Academic Catalog (2016). 2016-2017 BSIE recommended curriculum. Available at https://catalog.ttu.edu/preview_program.php?catoid=2&poid=949&returnto=160

Valacich, J. S., George, J. F., Hoffer, J. A. (2015). *Essentials of Systems Analysis and Design*. 6th Edition. Pearson Prentice-Hall.

Vonnegut, S. (2016). The importance of database security and integrity. Available at https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity/