Encouraging Active Learning through Multimedia & Interactive Courseware

Andy Ju An Wang, Ken Yetsko, Jamie Licitra, and Tony Armstrong
School of Computing and Software Engineering
Southern Polytechnic State University
1100 South Marietta Parkway, Marietta, GA 30060
jwang@spsu.edu

Abstract - The paper presents the architecture and preliminary design of MICS (Multimedia and Interactive Courseware for Information Security), which consists of a collection of interactive multimedia animations to enhance our curriculum in trustworthy computing. Each animation illustrates some important concepts and encourages the user to examine these concepts in depth. These animations require active participation and reasoning to improve the student's understanding and to make learning enjoyable and challenging. MICS covers the standard topics of security, privacy, reliability, and business integrity, but for each topic there is one or more projects implemented with interactive animations for the student to participate in. For each animation project, there are continuing questions requiring students to seek and record information about their sessions, and answer sheets students can use to submit their findings for a grade. These interactive animations will challenge students to examine the topics in a substantial way. Since the projects will have a detailed guide in audio or text format, they can be used as supplementary exercises for on-site programs as well as distance learning programs.

Index Terms – Active learning, Multimedia, Interactivity, Information security.

1. INTRODUCTION

Active learning is more than just the student being involved in what they are learning. Active learning must be interactive. It must engage students within the learning process in such higher-order thinking tasks as analysis, synthesis, reasoning, and evaluation [21]. Many learn more by doing than just sitting in a classroom listening to lectures. Studies have shown that not only do students prefer interactive learning strategies, but that these interactive strategies also do a better job of promoting the development of students’ skills [21]. Since many students respond to different teaching styles, interactive learning also provides a diverse way to teach the lesson, in hope of reaching the students that are more visual or hands-on.

There are three different models for interactive learning, with different engaging levels. The first is the TV model, where the student is passively watching and receiving predetermined information at a predetermined pace. The second model is the newspaper model. This model allows the student to select which page to read and can do that at their own pace. The third model is the game model where the player interacts with the game content, providing immediate feedback and making decisions on the fly. Interactive learning requires interactive courseware. It would be helpful to look into the evolution of interactive courseware and describe what interactive courseware is.

Interactive courseware is computer software and associated materials designed for educational or training purposes, usually multimedia in nature that teaches a lesson which is many times accompanied by a test or a quiz. Interactive courseware can contain one or more of many components including video, audio, games, simulations, a pre-test to determine a student’s level of understanding going into the lesson, a post-test to determine how much the student learned after the lesson, and interaction so the student can choose the path that most interests them. Ideally, the courseware would contain a mix of these components to maximize the effect. Too much video or animation is less interactive and engaging. To quote a Chinese proverb, “I see, and I forget. I hear, and I remember. I do, and I understand.”

In the 1960’s, interactive courseware, or computer-based training (CBT), was first used for U.S. military training and was implemented on large mainframe computers. The military was really the only one who had enough money to develop and use CBT. It was evident early on that this type of training was more effective than standard in-class lectures [22]. With the popularity of personal computers with Internet connection, web-based training allows anyone in the world to take a course with a nominal cost. The web and networks changed the distribution of interactive courseware from disks to servers. This has a number of advantages in that the material is easier and quicker to update, it is also less expensive to produce and update in both cost and time to market, anytime, anywhere learning as long as you have an Internet connection, and interaction with other online learners. Another advantage is that it allows for backend databases to monitor the progress of students and it reduced the operating system specific requirements for the interactive courseware.

There are many components to creating effective interactive courseware. According to [1], “Effective e-learning environments should include instructional integrity; learner focus; tracking, management, and reporting options; live interaction and collaboration; and integrated content.” With these goals in mind, there must first be an idea on the scope of the topic to be covered. An outline or flowchart would aid in
this task. Next, a list of system requirements must be made. That way, decisions on software and file formats can be made. Now the content must be developed and integrated into the lesson. Next, all the components of the courseware, such as the lesson, animations, video, audio, quizzes, games, etc. must be integrated into a package. Finally, the courseware must be made available to test for bugs and effectiveness [6]. The lesson should have a text component. This can be enhanced with audio such as text to speech or other sound effects to stress important or key points in the lesson. There should be elements to maintain learner focus such as video and or animations. There also should be a quiz and reporting system to report the results for tracking and management. A game integrating the courseware would enhance the learning experience and help maintain learner focus. Games can be one of the most powerful learning tools as they can be engaging and fun. Since games usually require quick reactions and feedback, the lesson material must not only be read but learned. The material learned and reinforced by playing a game increases student recollection.

This paper reports our experience in developing multimedia, interactive courseware for an information security course. The rest of the paper is organized as the following: Section 2 provides some background on MICS (Multimedia and Interactive Courseware for information Security). Section 3 describes the overall structure of MICS. Section 4 gives more details about the architecture of MICS. Section 5 proposes a concrete example called “Cyber War” for a typical animated exercise to practice network security. Section 6 presents another game-like exercise for Web security: “Cyber Protect”. Section 7 summarizes MICS development and discusses further research activities.

2. THE MICS PROJECT

Prior research [1, 4, 5, 6, 17, 21, 22] has shown that interactive courseware arouses interests and generates motivation providing a more engaging experience for the learner. In interactive learning, students are not passive recipients of information, but are engaged with the lesson’s material and it is responsive to their actions. On-line learning that merely allows the learner to navigate content or take an online test is sometime mislabeled as interactive. Merely being able to access the lesson through a web browser does not meet the criteria for meaningful interactivity outlined above, unlike, for example, that provided by an interactive simulation where a learner can actively explore a simulated system or process.

Many students find the material in a traditional information security course (e.g. applied cryptography, networking security, building secure software, etc.) abstract and dry. Indeed, a computer science curriculum based on old teaching techniques may seem dull and irrelevant to the modern student. A multimedia presentation during a lecture by an instructor is just a passive use of technology. In contrast, a student who can control a multimedia visualization is making active use of such technology. The difference between passive and active use of technology is similar to the difference between watching a laboratory demonstration and performing an experiment. When interactive simulations are added to an online course, such as we tried to incorporate in the MICS project, learners and course material developers communicate with more than words and images. The students and the course material developers must share the in the simulation if they are to communicate effectively about it. By “share” we mean that the developers must understand the subject matter and how best to get across the important points and the student must have a general idea what is required of them in the simulation experience. Sharing simulations and interactive lesson materials can take on-line learning far beyond the on-campus experience as it provides opportunities for group learning, exploring multiple perspectives, and using collaborative learning to develop and share alternative views.

While some topics addressed in program security (e.g., [2]) are best learned by writing programs, many topics in trustworthy computing are better illustrated and learned in other ways. These topics include buffer-overflow attacks and prevention, privacy issues and their consequences, system reliability, business integrity, risk analysis and auditing, etc., which are best taught through a series of live exercises or lab practice. However, teaching practical information security is difficult. First of all, information security covers a wide range of technologies including program security, operating security, database security, network security, administering security, etc. Addressing a comprehensive set of practical security techniques requires careful selection of the topics and particular attention to the way the topics are presented to the students. Second, the instructor is faced with the difficult decision of choosing the right balance between a theoretical discovery (the hands-off part) and a practical component (hands-on part). Such a difficulty is more evidently manifested when the information security course is taught in the situation where no existing course as a prerequisite course that covers the foundational principles of information security such as the Bell-LaPadula model and PKI (public key infrastructure). Third, teaching hands-on practice in information security requires substantial effort on the part of the instructor. This is especially the case when the university has limited computing resources and limited supporting technical staff. Furthermore, if the information security course covers too much technical details on password cracking or network attacks, there is a concern that the class may get out-of-hand or that the class may be flagged as a “hacking course”. From the perspective of students, learning through doing or hands-on practice is always time-consuming without appropriate tool support. This is extremely an issue for distance education.

In this paper, we present MICS, a multimedia and interactive courseware for information security, which represents a valuable tool to teach the practical aspects of information security and the dynamics of computer attack and defense techniques. MICS intends to complete the trustworthy computing course transformation to an active-learning curriculum. It gives more freedom for both the instructor and students to teach/learn security concepts, principles, protocols, design, and implementation in a more hands-on approach. MICS has significance not only for its innovative content, but
also for its use of visual technology and network-based learning. The trustworthy computing class is ideal to begin the infusion of such technology because the students are relatively sophisticated by this point in their studies, and the mechanics of getting things to work can be incorporated naturally into the curriculum.

The use of interactive animation is expected to stimulate the creativity of the students while enhancing their learning. Since the programs run over the network with a standard web browser, MICS will have a positive impact on nontraditional students, many of whom are single parents, particularly women trying to raise children and balance work commitments while attending college. As a byproduct, the interactive animation framework used to produce the animations will be made available and will allow educators to extend this work to other areas.

This MICS project is partially supported by Microsoft Corporation and it was started at the beginning of 2005. By the end of this year, MICS will have two direct impacts on our curricula: First, it will create new supplementary material of “Introduction to Trustworthy Computing” for our existing WBIT 4520 Information Security in our WebBSIT program. Second, it will update our existing courses related to trustworthy computing, which include CS 6293 Information Security, IT 4363 Information Security Concepts and Administration, and IT 6823 Information Security Administration. The research and development result of this project will transform the trustworthy computing curriculum at SPSU into one that is both challenging and exciting. The WebBSIT program reflects the academic standards of the on-site IT departments, while providing the convenience and flexibility for busy people to learn without traveling to a campus. The program of study provides a solid background in the technical, user-centric and managerial skills required by today's information technology managers. Graduates will pursue careers in programming, systems design, information security, network administration, database design and e-commerce, among others.

MICS has been inspired by a number of related research and development work including the research from the areas of program and algorithm animation, visualization for program monitoring and debugging, integrated multimedia systems, as well as an exploding literature on the use of the World Wide Web for teaching.

3. THE ARCHITECTURE OF MICS

The goal of MICS is to produce a national model for an undergraduate/graduate curriculum in trustworthy computing that uses interactive technology. MICS implements a hands-on approach to teaching and learning trustworthy computing. Complemented with a carefully designed curriculum, MICS is developed to enhance student learning through active use of interactive animations.

The focus of MICS is on developing a collection of hands-on lab materials based on the four pillars of trustworthy computing proposed by Microsoft: Security, Privacy, Reliability, and Business Integrity.

(1) Security

- Program Security: The animation demonstrates the common scenarios of programs infected by malicious code. The animation shows how viruses attach to programs, how viruses gain control, virus signatures, and virus prevention. Students will experiment with the common practice of securing a computer so that an intruder cannot crash her/his computer or make unauthorized alterations to her/his data. Tools and techniques for analyzing malicious software such as viruses, worms, and “Trojan Horses” will be illustrated. Students will be able to practice via the animation with their hands at studying malware using system monitoring tools, disassemblers and debuggers in a simulated environment.

- Network Security: The animation will help students to become familiar with networking protocols, TCP/IP/UDP header inspection, firewall and IDS (intrusion detection system) concepts. It illustrates the secure by design principle in a networking environment. It offers the student opportunities to work with intrusion detection and intrusion prevention technologies, as well as pitfalls of using active response techniques and how to mitigate them. This animation will also provide students with up-to-date knowledge on the latest hacks and how to defend against these attacks.

- Wireless Security: This animation will help students in assessing wireless security through network sniffing, examining indoor and outdoor wireless network implementations, identifying potential weaknesses in wireless networks, and learning wireless LAN intrusion detection techniques. Using the animation, students will gain hands-on experience examining wireless networks from the perspective of an attacker, learning the techniques used to exploit wireless weaknesses, and how to protect an organization with wireless networks from attack.

(2) Privacy

- “Gold Standard”: This animation demonstrates the “Gold Standard” for privacy: Authentication, Authorization, and Auditing. The differences among these keywords will be illustrated through interactive animations.

- Protecting Identity: This animation will illustrate how identity theft can happen. A number of identity theft scenarios will be demonstrated: (a) Pretexting, the illegal practice of obtaining such information under false pretenses, for example, someone calls your financial institution and pretends to be you. (b) Phishing, sending messages via the Internet purporting to be from financial and other service providers. Recipients are typically asked to update information or to verify passwords. (c) Shoulder surfing, which can be done either by watching as you type in your password or by a malicious program collecting your key strokes. (d) Dumpster diving, which is retrieving discarded data from normal trash.
(3) **Reliability**
- DDOS: This animation helps students to understand the importance of reliability and availability. It first shows how DOS (Denial of Services) and DDOS (Distributed Denial of Services) attacks could be launched by attackers, and then it teaches students how to protect their system against DOS or DDOS.
- **Data Integrity**: This animation shows how to protect data consistency, accuracy, or correctness for a database. Some threats to data integrity will be demonstrated, including script injection, cascading deletes, and inserting a threat to referential integrity.

(4) **Business Integrity**
- **Policy and Procedure**: This animation illustrates the goals and means of implementing business integrity in trustworthy computing. Students will have a series of wizard-guided sessions to create a security policy or regulation for a mock organization. In addition, this animation will provide an online quiz on enforcing trustworthy computing in business practice. Students will test their knowledge about fundamental concepts in business integrity: Responsiveness, Fair Information Principles, Usability, and Transparency in a multimedia animated environment.

There are eight subsystem in MICS: (1) Cryptosystems, (2) Program Security, (3) Operating System Security, (4) Database Security, (5) Network Security, (6) Intrusion Detection and Prevention, (7) Web Security, and (8) Administering Security. Each of them includes business integrity as well as privacy and reliability. As a basis of these eight components, there is a framework for interactive animation, which is critical to productivity on the rest parts of MICS. The high-level architecture of MICS is illustrated in Figure 2 below.

The Framework of MICS defines that how each component is organized and presented. Each topic will have one or more assignments working with one or more interactive animations specified by URLs. A guide for instructors will show how to incorporate these animations into a standard trustworthy computing curriculum even if the complete syllabus is not used. Each animation project contains five major sections. First is an overview of the activity including some information on its definition and historical development. Second is the usage of the activity, explaining how it should be employed including specific syntax or operating requirements. Third is a discussion of the activity’s use in trustworthy computing practice. The fourth section is a detailed, guided, set of exercises. The last section is a discussion of further research topics related to the activity in this exercise. For each animation project, there will be continuing questions requiring students to seek and record information about their sessions, and answer sheets students can use to submit their findings for a grade.

4. **THE DETAIL DESIGN OF MICS**

As we discussed in Section 2, the standard information security course suffers from the same problems as any "hands-off" course offered in computing curricula. There are tremendous opportunities for developing projects with a strong visual and audio component. MICS concentrates on developing a significant number of interactive animations suitable for undergraduate/graduate trustworthy computing courses. Below is a list of animation projects that would fit off course offered in computing curricula. There are tremendous opportunities for developing projects with a strong visual and audio component. MICS concentrates on developing a significant number of interactive animations suitable for undergraduate/graduate trustworthy computing courses. Below is a list of animation projects that would fit with the plan presented here. The list is far from complete and is only a representative sample. Each animation includes an interactive component described below along with the concepts to be illustrated.

4.1 **Cryptosystems**
- **Animation 1**: Basic Cryptography - classical cryptosystems: transition ciphers, substitution ciphers, Vigenere cipher, one-time pad, Enigma machine.
- **Animation 2**: Data Encryption Standard (DES).
- **Animation 3**: Public Key Cryptography: Diffie-Hellman, and RSA.
- **Animation 4**: Key Management: key exchange, key generation, storing and revoking keys, digital signature.

4.2 **Program Security**
- **Animation 1**: Trojan Horses and Computer Worms
- **Animation 2**: Computer Viruses: boot sector infectors, executable infectors, multipartite viruses, TSR viruses, polymorphic viruses, macro viruses, other forms of malicious logic
- **Animation 3**: Common Security-Related Programming Problems: improper choice of initial protection domain, improper isolation of implementation detail, improper change, improper naming, improper de-
5. CYBER WAR: LEARNING THROUGH PLAYING

This section discusses a concrete example in MICS, a game called “Cyber War”, which is adapted from [5]. The ultimate goal of the game is to perform a multi-step cyber attack or cyber defense that is as realistic as possible. There are two armies, called Red Army and Blue Army, fight with each other in the cyber space. There are three levels in this game discussed briefly below.

5.1 Level 1: Find the Secrete

The user chooses to be the Red Army or the Blue Army at the beginning. The Red Army plays the attacking role, i.e., trying to attack and compromise a set of computers, while the Blue Army plays the defense side, trying to detect the attacks and protect the computers. The final goal of the Red Army is to obtain a file named secret.txt stored on each of the computers for the Blue Army. There could be multiple copies of the file and decoy copies could be present too. The only files that had to be retrieved are those whose contents start with the keyword SECRET. The goal of the Blue Army is to detect the attacks coming from the Red Army. In addition, the Blue Army could execute some counter-measures to slow down or confuse the attackers. In particular, the Blue Army could freely decide where to store the secret file. The only requirement is that the file be on a mounted file system.

5.2 Level 2: Catch the Flag

In this level, each army tries to break into the opponent’s headquarters computer system and perform a “modification or alteration” attack. For instance, the Blue Army may redirect the Red Army’s missiles to a different target, or the Red Army may insert a piece of false intelligence information into Blue Army’s command database. Each army has to perform a number of tasks, for example, scan a network or break into a host. Each task has to be completed in a limited amount of time, for instance, 30 minutes. The first army that achieves the task will get 50 points. If the other army completes the task within the specified time, it receives 30 points. In this level, the armies have to concentrate on attack techniques. The goal is to be prepared for the unknown and to be able to deal with unforeseen problems.

5.3 Level 3: Redirect the Missiles

In this level, each army tries to break into the opponent’s headquarter computer system and perform a “modification or alteration” attack. For instance, the Blue Army may redirect the Red Army’s missiles to a different target, or the Red Army may insert a piece of false intelligence information into Blue Army’s command database. Each army has to perform a number of tasks, for example, scan a network or break into a host. Each task has to be completed in a limited amount of time, for instance, 30 minutes. The first army that achieves the task will get 50 points. If the other army completes the task within the specified time, it receives 30 points. In this level, the armies have to concentrate on attack techniques. The goal is to be prepared for the unknown and to be able to deal with unforeseen problems.
6. CYBER PROTECT: A MULTIMEDIA TRAINING TOOL

This is a simulation game based on the cyber security training software developed by the Defense Information System Agency (DISA) in 1999 [4]. The design for the simulation will have a similar framework as in [4], including servers, routers, terminals, hubs, LANs, among others. The game focuses on teaching the students the basics in information security, especially network security. In doing so, the game provides the players with some ability to engage in the network construction, selecting and deploying new network components. The players can construct the virtual network from wires, routers, servers, etc. Security practice is not just installation of hardware and software but the configurations as well. These configurations such as TCP/IP, ports, service packs, critical updates, and disabling certain accounts like “Guest” are extremely important to security today. This also includes account settings and password enhancement.

The participant is exposed to a wide spectrum of security threats and must make practical decisions for allocating resources using elements of risk management. A user will log in and decide if he/she would like to join an existing game where he/she can act as a hacker, as an internal user or start a new game as an ISO (information security officer). If he/she joins a game as a hacker, he will be asked if he/she would like to know the outer shell of the network only or the entire network. Once he/she sees the information requested, he/she will be able to select from a series of attack types. After running an attack, a message informing the user why the attack was not successful or successful should appear. Points will be deducted from the ISO and given to the hacker for every successful attack.

If the user selects to be an ISO, the game will include the most functionality as [4] but with more detail description of the devices being added. It allows the database to decide based on vendor/model what its capabilities are. The quarter system is kept to make the gameplay more realistic. At the end of the game, an ideal cyber protection network diagram will be displayed so that the user can better learn and understand the concepts of cyber security. As part of the report, recommendations for the best hardware and software for cyber security will be included. There will be several ways to print and report the information about the attack or security defenses.

7. CONCLUSION AND DISCUSSION

The MICS project will produce a collection of animations and interactive courseware for "Introduction to Trustworthy Computing". The courseware will cover the standard topics normally found in these courses, but for each topic there will be one or more projects for the student to participate in. The new projects will use interactive animation that will challenge the students to examine the topics in a substantial way. Each new project will be specified by a URL which can be accessed by any standard Web browser. An instructor could use the syllabus as is or just incorporate selected projects into an existing course. Since the projects will have a detailed guide in audio or text format, they can be used as supplementary exercises for students who are having trouble or wish to gain more insight into a particular topic.

The MICS uses Macromedia Flash and ActionScript 2.0 as the major technique for implementation. Flash represents a professional standard for high-impact Web experiences using graphics, animation, sound and video. ActionScript allows more interactivity. We are investigating other software tools for their suitability in further development in MICS.

ACKNOWLEDGMENT

This project is partially supported by Microsoft Research Initiative: Trustworthy Computing Curriculum.

REFERENCES

