

Towards the Development of Laboratory Exercises for Computer Security Awareness

Sponsoring faculty: Dr Rose Shumba

Students: Alicia Coon, Sara Raffensperger, and Louisa Ehinlaiye Ometere
Computer Science Department
Indiana University of Pennsylvania

General Project Description

The general public is often isolated from awareness and training opportunities in information security, yet the security of the cyberspace rests on the security of all its components. Although there is a reasonable number of websites with tips on protecting home computers [16, 17, 21], these often have some technical vocabulary or are not known by the public, hence are seldom referred to. The goal of this project is to enhance the public's understanding and acceptance of information security issues through awareness and education. Investigators will investigate, develop and pilot test hands-on exercises, which are based on the "best-of-breed" security tools¹ and techniques for home computer protection². The output from this project will be a set of Windows-based hands on exercises that can be used in securing a home computer. The exercises will be pilot tested with the IUP community³ through a series of one hour weekly workshops aimed at enhancing IUP community's understanding and acceptance of security issues. Feedback from the pilot test will be used to improve the exercises. Each participant will receive a CD with the materials covered in the workshop. After attending the workshop, participants will be given a month in which to implement the learnt techniques, after which a post workshop questionnaire survey will be administered. The aim of the survey is to assess impact of the hands-on exercises on the IUP community's understanding of information security issues.

Such a project, if successful, will: 1) enhance investigators' knowledge and understanding of information security issues through an evaluation of available security tools and techniques, 2) enhance IUP community's understanding of the Internet and the associated risks and vulnerabilities; this will help address issues of online safety, critical literacy, and transfer of ethical behavior to the online environment, 3) spawn research projects into better tools and techniques for protecting home computers, 4) enhance the public's confidence in the use of computer based systems to perform critical functions and to process, store, and communicate sensitive information securely, and 5) create a baseline of materials for our planned public awareness and education project; an information assurance outreach program aimed at raising parent, general community, and junior and senior girl's awareness of security issues. Funding for this later project will be sought from organizations like Cisco, NSA and NSF..

¹ Only home grown and publicly available security tools will be considered

² Wherever we refer to home protection, we implicitly include cases where wireless technology is used.

³ The IUP community refers to the students and faculty mainly from non-computer science and related disciplines.

Specific questions/Hypothesis

1. What techniques and security tools are currently used by the public for home computer protection?
2. How effective are the available techniques and security tools in the protection of home computers?
3. What techniques and security tools can we identify and recommend as the “best of breed” for home computer protection?
4. Can we integrate the identified “best of breed” security tools, techniques and the host security theories and concepts into hands on exercises for home computer securing?
5. Will the developed exercises be effective in enhancing understanding and acceptance of security issues by the public?

Methods

Investigators will investigate, develop and pilot-test hands-on exercises, which are based on the “best-of-breed” security tools and techniques for home computer protection.

1. The investigation will involve an effective evaluation of available security tools and techniques, including those currently used in home computer protection. To effectively do the evaluation, the investigators will:
 - a. Carry out some background research work on: 1) Security risks and countermeasures associated with Internet connectivity, especially in the context of "always-on" or broadband access services, such as cable modems and DSL. CERT gives an overview of risks and countermeasures associated with the Internet [3]. [4, 5, 6, 7, 8, 17] are also good sources for Internet risks and vulnerabilities. 2) Host security. The investigators will have to understand host hardening techniques and related tools. [11, 12, 13, 14, 15] are good references for host security. The Cybersecurity course (COSC316) is a requirement for the successful completion of this project. One investigator has successfully completed the COSC316 course. The other two investigators will be registering for the course in the spring of 2005. In addition to the stated references, the investigators will study and understand some much related research work by the sponsoring faculty. During the summer of 2003, the faculty worked on approaches to improve and augment the teaching of the Cybersecurity course at IUP [18]. Host security tools were evaluated. The evaluated tools were then integrated into the Cybersecurity Basics course theories and concepts. Study of such work will help investigators identify the host hardening techniques, possible security tools, and the different tool categories for home computer protection. 3) Tips for home computer protection. Investigators will study some literature available for home computer protection [16, 17]. 4) Wireless security. Investigators will also study some work on the wireless security. There is quite an extensive collection of materials on wireless security, ranging from recommendations for wireless security to

tools for protecting wireless networks. [22, 23, 24, 25, 26] are just a few examples of such work that will be studied.

b. Identify tools and techniques currently used by IUP community in securing home computers. A questionnaire survey will be administered. The aim of the questionnaire survey is to gather data on security tools and techniques currently used to protect home computers. 550 and 30 multi-disciplinary students and faculty respectively will participate in the survey. The sample size, calculated using the sample size calculator given in [2], is based on the IUP student and faculty population of 12000 and 600 respectively. Results from the survey will be analyzed to give the list of commonly used tools and techniques, if any, for home computer protection.

c. Evaluate the identified tools
Investigators will evaluate commonly used tools and techniques and other host hardening tools and techniques identified through survey and background research respectively. The investigators will be expected to download and install the tools. For each identified tool or technique, investigators will figure out the purpose, available support materials, effectiveness in securing a home system, host hardening category for the tool, and evaluate its usability: easy of installation and the understandability of the produced output. An evaluation report for each tool or technique will be produced. From the collection of evaluation reports, the “best of breed” tools and techniques that can effectively be used in home computer protection will be identified.

2. Development of the hands on exercises

Using the set of evaluation reports, the security tools and techniques will be integrated with the host security theories and concepts into the hands-on exercises.

3. Pilot testing the developed exercises

Three, one hour, weekly workshops on securing home computers will be hosted by the investigators for the IUP community. A maximum of 20 participants per workshop are expected. Announcements for the workshop will be posted on the IUP home page, computer science department website and flyers will be distributed all over campus. The announcements will clearly encourage girls and women to participate. At the end of each workshop, the participants will evaluate the workshop. Each participant will be given a CD with a collection of all materials covered in the workshop. Feedback will be used to improve the hands-on exercise.

4. Evaluate the impact of the hands-on exercises on understanding of security issues

A month after the workshop, a post workshop questionnaire survey will be administered. The aim of the post workshop survey is to assess the impact of the hands on exercises on the understanding of security issues by the IUP community. Survey questionnaires will be mailed to all participants. Participants will be given two weeks, in which to return the completed questionnaires. The results will then be analyzed.

References

1. <http://www.chartwellsystems.com/sscalc.htm#ssneeded>.
2. http://www.cc.gatech.edu/classes/cs6751_97_winter/Topics/quest-design/.
3. www.cert.org/tech_tips/home_networks.html
4. www.tuketu.com/dsl/information-security/Securing%20DSL.htm
5. members.aol.com/gaf5200/myhomepage.
6. seattlepi.nwsourc.com/business/hack221.shtml
7. www.tech-forums.net/computer/topic/701.html
8. www.3com.com/corpinfo/en_US/technology/tech_paper
9. www.sarc.com
10. www.agnitum.com
11. www.linuxsecurity.com/resources/host_security-1.html
12. www.nic.com/~dave/SecurityAdminGuide/SecurityAdminGuide-4.html
13. www.digitalsecurityconcepts.com/host_security.htm
14. www.bb-zone.com/SLGFG/chapter24.html
15. Garfinkel, S. Spafford, G, Schwartz,A; Practical Unix and Internet Security; O'Reilly; Third edition; 2003.
16. <http://www.cert.org/homeusers/HomeComputerSecurity/>
17. <http://www.staysafeonline.info/enroll.adp>
18. Harding, J. Gender and design and technology education. The Journal of Design and Technology Education, 2, (1), 1997.
19. Clarke, V., Teague, G. (1994). Encouraging girls to study computer science - Should we even try? Australian Educational Computing. www.schools.ash.org.au/litweb/gender.html
20. Durndell,A. Glissov, P.,Siann, G. Gender and computing: Persisting differences. Educational Research, 37, (21).
21. www.cerias.purdue.edu
22. <http://www.computerworld.com/mobiletopics/mobile/technology/story/0%2C10801%2C72164%2C00.html>
23. csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
24. www.palowireless.com/wireless/security
25. www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-1.html
26. <http://techdir.rutgers.edu/wireless.html>

Impact on the goal of CREU

The successful completion of this project will:

1. Provide a positive research experience for a team of undergraduate female students majoring in computer science.
2. Advance the knowledge and understanding of information security issues by investigators through the stated background research and evaluation of security tools.
3. Provide an environment for exchange and dialog among the participating female investigators and the faculty. This will give value to girls' learning styles, skills and strengths. Many research studies report that boys often prefer to work alone on a computer problem, whereas girls prefer to work collaboratively in groups where they can explore the problem verbally [19].

4. Encourage participation by female students in a very unique computer application area, information assurance. It is believed that an exposure to a wide range of computer applications can help develop an appreciation of the uses of computers by female students.
5. Present information assurance in a context that emphasizes its social relevance. Research shows that girls are more likely to choose and enjoy information technology subjects if they are presented in such a context [19].
6. Increase level of confidence by the workshop participants through hands-on exercises.

7. Enhance communication skills for the investigators through workshop hosting. All the above will contribute towards the generation of interest and enthusiasm among the investigators and workshop participants hence motivate them into considering further studies in computer science. This is in line with the goal of CREU, to increase the number of women who continue on to graduate school in computer science.

Finally, the sponsoring faculty is a female whose research interests are in information assurance and gender and computer science. The faculty acting as a mentor will encourage the investigators to seriously consider pursuing graduate studies in computer science.

Student Activity and Responsibility

All the students will be involved with all the activities, however one student will be responsible for the successful completion of the activity.

Time	Student Activity	Student responsible
Fall 2004 (September 2004)	Background research report	Alicia Coon
	Design of questionnaire	Louisa Ometere
	Questionnaire administration	Sarah Raffensperger
	Evaluation of techniques and tools	Alicia Coon
	Production of evaluations reports	Sarah Raffensperger
Spring 2005	Developing the exercises	Alicia Coon
	Workshop preparation	Louisa Ometere
	Running of the workshops	ALL
Summer 2005 (May)	Administering the post workshop questionnaire	Lousia Ometere and Sara Raffensperger

Faculty Activity and Responsibility

1. Read and comment on the background research paper
2. Help with the design and administration of the questionnaire
3. Works closely with the students during the evaluation of the security tools and techniques to identify the “best of breed” tools and techniques.
4. Work closely with the students during the integration of the host security tools, techniques and the host security theories and concepts.

5. Help with the production of the workshop announcement and its distribution.
6. Help with the analysis of the results from the post workshop questionnaire.