CS3235 Group Assignment 1 - Survey

September 6, 2004

Due by 5pm on Friday, October 8, 2004

This course only briefly outlines a wide range of computer security topics. The group assignments allow you to explore a topic, or some other area of computer security that interests you, in some depth.

First, you must either

- select a project from the list below, or
- think of a project on your own.

Assignment 1 will be a survey of the selected project area. Assignment 2 will be further work on the same topic, perhaps involving an implementation, so make sure you are interested in the project.

Secondly, reserve the project by emailing me the title, a brief outline of what you intend to do with the second part of the project (2-3 paragraphs), and your group members. You should do this as soon as possible, to ensure that you can get the topic you want. Make sure that you select something that interests you! You may work in groups of (upto) four students. Do not bother asking for a group of five.

1 Possible assignment list

This list is an amalgamation of various lists, but feel free to suggest your own topic:

1. Malicious programs and biology: how computer worms, viruses, etc. compare to their biological counterparts
2. Comparison of security requirements in different environments (academic, medical, military...)
3. Differential timing analysis
4. Electronic voting protocols
5. Security techniques for digital video/multimedia
6. Data security for E-transactions
7. Smart card security
8. Denial of service attacks
9. Electronic currency
10. Elliptic curve cryptography
11. Intrusion detection and prevention software
12. Automating policy checking to ensure your computer/site meets a given policy
13. Authenticating users and systems
14. Security for IEEE 802.11

15. Password authentication for web applications
16. Single Sign-On (SSO)
17. Classical cryptography
18. Image authentication techniques for copyright protection
19. Intrusion detection and response
20. Public key infrastructure (PKI)
21. Securing data on laptops
22. Digital Video Watermarking
23. Audio Security
24. Factoring a number
25. Checking for primes
26. Electronic voting machines and computer security
27. New access control mechanisms for the UNIX system
28. Rights and amplification of rights in a capability-based system
29. Secure electronic mail: proposed standards
30. Analyzing and/or testing programs for vulnerabilities
31. Intrusion detection and incident response
32. Analyzing a system's or site's security.
33. Comparing Windows NT security tools and UNIX security tools
34. Attacking systems; how, who, why, and so forth

Assignment 1

Assignment 1 is to write a survey of the selected project area. Your survey should be in the form of a formal paper, with a title, abstract, appendicies and so on. The survey should include an overview of the project area, with specific details on any technical points that interest you, with references to the important works/papers/research/products that have contributed to the development of the subject area. You can ask your Tutor or Lecturer for advice on your selected topic...

Your completed assignment should be submitted in **hardcopy** to your tutor by the deadline. You should also submit an electronic version to Hugh in PDF format. Your assignment should contain:

1. A cover page with your name(s), matric number(s) and SOC Unix user id(s).
2. Your survey paper, with abstract and appendicies

COOPERATING VERSUS CHEATING

You are allowed to discuss the problems with your friends, and to study any background material with them, but the assignment *should be your own group's work*. **Copying** and **cheating** will be grounds for failing the assignment.

I will be specifically looking for your own interpretation of what you discover, and will be harsh in my marking if I suspect that you have "cut-and-pasted" large chunks of good-sounding stuff from the Internet. I would much prefer having a shorter paper that covers the topic area, and then reflects your interests and interpretations, than a longer paper that has a lot of obviously copied material.