Introduction to Computer Security
Term Paper Assignment
Spring 2009
March 25, 2009

Each student is expected to write a term paper on a topic area in computer security. The paper should be based on "library research"— information that the student assembles primarily from published sources. The student is not expected to obtain novel research results. All writing in the paper, however, should be original.

Survey papers are recommended. A survey paper should motivate and define a problem area and then develop and evaluate one or more potential solutions to that problem.

The paper should meet the standards of scholarship of a paper to be submitted for publication. The paper should be written in your own words. All sources consulted should be explicitly cited. Bibliographic entries should be complete. Direct quotation should only be used when appropriate. All direct quotations should be clearly identified in the text. Plagiarism is a violation of academic integrity. When such violations are discovered a grade of 0 will be given on the assignment and the infraction will be documented and reported according to university policy.

Deliverables

Paper Proposal: Due at Midterm exam

By the midterm, each student should have a topic in hand, and should turn in the following for criticism:

1. Title, authors name, abstract, and outline for your paper. The more detailed the outline, the better.

2. An annotated bibliography for your paper that includes between 5-10 seminal papers for the topic in question. Each paper should have a 1-2 paragraph abstract written for it by you that summarizes the important parts of the paper.

   In general, the source is ideally a book, journal article, or conference article. A bibliography with all web URLs will not be looked upon favorably. However, for some topics in computer security it may be necessary to use web sources. For example, in the case of buffer exploits, many important papers are on-line as they have been written by the hacker community. In such cases please give a justification for using a significant number of self published sources. The bibliographic citation serves at least two purposes. It helps the reader determine the authority of the source by indicating where it has been published, and implicitly how carefully it has been reviewed. It also should be sufficient to help the reader find the

original paper. Thus it is acceptable here to list both an original source, and a web URL if available.

Professors Hook and Binkley will divide the proposals and papers based on title and abstract. Each proposal and paper will be reviewed by one faculty member. For the proposal we will give you feedback on:

1. Appropriateness of topic
2. Scope of the proposal
3. Quality and appropriateness of the sources
4. Detailed review of the individual elements (title, abstract, outline, annotated bibliography)

It is the intent of the proposal assignment to set you up for success on the final paper. The proposal and final paper are reviewed independently. You are not constrained to follow the outline in the proposal in the final paper.

Final Paper: Due last lecture

The final paper should ideally be 10-15 pages long and should not be longer than 20 pages. **It is due at the beginning of the last lecture.**

You do not need to hand in an outline with the final paper. The final paper should contain a bibliography, but the bibliography should not include annotations. The contributions of the sources should be clear from the text of the paper.

The paper is graded on:

1. Appropriateness of topic
2. Organization of paper
3. Quality of exposition
4. Technical understanding of the problem
5. Appropriate awareness and selection of prior work as expressed in the narative body of the paper (source selection goes beyond suggested starting points in assignment or texts, student made serious attempt to identify seminal sources in an area by chasing down influencial sources)
6. Appropriate selection and documentation of sources in the bibliography (strength of sources, completeness of citation)
7. Compliance with assignment parameters (e.g. length of paper)

Students enrolled in 591 will be held to a higher standard than those enrolled in 491. In particular, graduate students are expected to show a greater command of the literature.

Suggested Topics

- The use of computers in elections. A survey paper might review the different kinds of voting machines, discuss their level of automation, discuss vulnerabilities inherent in their design, and summarize vulnerabilities found with specific implementations. Note: this issue is not limited to the United States.
- Intrusion Detection. Write a survey paper on one aspect of intrusion detection including any of the following as the general topic area:
  - algorithms used in machine intelligence approaches including Bayesian MI (algorithms in question may be used in spam detection as an example)
  - honeypots, honeynets, and darknets
  - botnets
  - evolution and detection of p2p-based network protocols
- Exploit writing by hackers, in particular a history and analysis of buffer overflow exploits including solutions for this problem is one possibility. A recent book on rootkits on windows systems might also be another avenue for exploration.
- Some area of mutual interest to you and the instructor/s. Term papers in the past have been written on steganography. (see `http://www.jjtc.com/Steganography/` for a starter bibliography page). Tempest radiation is another possible topic (start with Ross Anderson).

Getting Started

The Anderson text has an excellent bibliography. Other texts, particularly the two by Matt Bishop, also have excellent bibliographies. At the end of every chapter Bishop gives an excellent road-map to the original sources for every topic he covers. The library is another excellent starting place for research papers. In addition, two particularly useful web resources are citeseer `http://citeseer.ist.psu.edu/` and google scholar pages `http://scholar.google.com`.

The Scholarship Skills class web page lists several useful resources, including writing guides and handbooks `http://web.cecs.pdx.edu/~sheard/course/SkolSkillsW06/index.hmtl`.

PSU has a writing center `http://www.writingcenter.pdx.edu/`. Students with limited writing experience have found this resource particularly helpful.

Here are starting points for two of the suggested topics. If you select one of these topics please find additional sources as well. If you use only these sources your grade will be no higher than a B.

- Intrusion detection:

1. D. Denning. An Intrusion Detection Model. IEEE Transactions on Software Engineering. 1987.
2. W. Lee and S. Solfo. Data mining approaches for intrusion detection. In proceedings of the 7th USENIX Security Symposium, San Antonio, TX, Jan. 1998.
3. S. Robertson, E. Siegel, M. Miller, and S. Stolfo. Surveillance detection in high bandwidth environments. In Proceedings of the 2003 DARPA DISCEX III Conference. IEEE Press, April 2003.
4. S. Forrest, S. Hofmaeyr, and A. Somayaji. Computer Immunology. "Communications of the ACM, 1996.
5. J. Jung, V. Paxson, A. Berger, and H. Balakrishnan. Fast Portscan Detection Using Sequential Hypothesis Testing. In Proceedings of the IEEE Security and Privacy Conference, Oakland, CA. May 2004.

- Buffer overflow exploits:

1. Crispin Cowan, et al. "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade," `http://www.immunix.org/StackGuard/discex00.pdf`
2. Mudge, "How to write Buffer Overflows," (October 1995). `http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html`
3. Aleph One, "Smashing The Stack For Fun And Profit," Phrack Magazine 49 (November 1996). `http://www.phrack.org/phrack/49/P49-14`
4. `http://www.phrack.org/phrack/62/p62-0x07_Advances_in_Windows_Shellcode.txt`

- Denial of Service

  The following is a rather interesting paper (on the subject of exploits) that could possibly be worked into a more general discussion of network-based exploits or denial of service attacks:

1. Staniford, Paxson, Weaver: How to 0wn the Internet in Your Spare Time Proceedings of the 11th USENIX Security Symposium (Security '02) `http://unix.za.net/docs/computers/hacking/owning/`