Introduction to Computer Security
Term Paper Assignment
Winter 2007
January 7, 2007

For this course we expect every student to write a broad term paper on a topic area in computer security. We do not expect original research, but we do expect a student to gain in-depth knowledge in a specific area of interest. In other words, you should write a survey paper (or "white paper") that attempts to 1) explore the problem space and 2) explore the solution space for a particular area.

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

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

1. Title, author name (you), 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 in the case of buffer exploits, ironically many important papers are on-line as they have been written by the hacker community). The point of the source information is 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.

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.

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 or anomaly detection. A survey may broadly look at the conceptual space (including the differences between anomaly, misuse (or signature) modeling, and investigate various solution spaces including immunology, signature-based detection, data mining, etc. You also be more narrow; e.g., look at the subject of P2P protocol detection.
- 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.
- A compare and contrast paper on Acceptable Use Policies from three institutions (see attached page). SANS has sample policies at: `http://www.sans.org/resources/policies/`. One could also attempt a paper focusing on security policy considerations at institutions in terms of interaction with law enforcement. `http://www.sans.org/score/faq/law_enf_faq/`
- Some area of mutual interest to you and the instructor/s. Term papers in the past have been written on stegonagraphy. (see `http://www.jjtc.com/Steganography/` for a starter bibliography page). Tempest radiation is another possible topic (start with Ross Anderson).

Getting Started

Both texts 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 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/`