CS 4235: Introduction to Information Security August 23, 2011

Problem Set 1: Case Study Research

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

You should complete this problem set in a group of no more than five students. Please sign up on the wiki under a topic that interests you; list your name as well as your email address so that your other group members can contact you.

Turn in your writeup and talk on **September 20, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

Information Security Case Study. Information security protection and failure has widely affected todays technology. This case-study research gives you a chance to investigate one particular area of current relevance and impact and to hear about other areas from your classmates. With your group, research the topic of your case study. Good starting points are Google and Wikipedia; you will probably discover that the initial sources that you discover will point you in some further directions.

Let me know if you have trouble finding information, and I can help you find some initial sources. In many cases, the opposite problem is likely: you will probably find much more information than you can reasonably cover in a class presentation. Your group should decide how to handle large quantities of information. You could try to give an overview of the entire area, or you could instead choose something specific within the area and focus your research on the specific sub- topic or incident.

Your group should prepare:

- a 15-minute presentation that you will give to the rest of the class, and
- a two-page writeup summarizing your findings.

Your goal should be to inform your classmates about the particular case study that your group researched. There are a number of good presentation programs available: Microsoft Powerpoint, OpenOffice Presenter, Apple Keynote, Slidetex, and others. Fifteen minutes is not long, so I would expect your group to base your talk on about three to five sources. Additional sources can help you understand the area, but you may not be able to fit them into your talk.

I have provided initial topic assignments for on the wiki. Please sign up for a group by the end of this week, or I will place you in a group. If a group of you wants to present on a different topic than one of those listed on the wiki, you are welcome to do so, if you consult me first.

Although you are expected to use outside sources for information, you:

- must not copy-and-paste text or figures from those sources, and
- must cite the sources. A citation should provide sufficient information for myself or anyone else to find the source that you used.

If you are unsure whether or not you are using outside material appropriately, please ask me rather than guessing.

CS 4235: Introduction to Information Security September 1, 2011

Problem Set 2: Software Vulnerabilities

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three questions, each with several parts. Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup and talk on **September 15, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **15 points** Pfleger and Pfleeger, Section 1.11, Exercise 14.
2. **15 points** Pfleeger and Pfleeger, Section 1.11, Exercise 20.
3. **20 points** The Ware report from 1970 emphasizes defenses for physical attacks and leakage points. In many of todays computing systems, however, physical attacks are relatively uncommon compared with other kinds of attacks.
    - Give three distinct reasons, with appropriate justications, why this is so.
    - In the Checkoway *et al.* paper on automotive security, the authors point out that it is possible to compromise the automotive system even without physical access to the car itself. From the paper identify at least one flaw of each type that creates a vulnerability: (1) design; (2) implementation; (3) process
4. **20 points** Discuss Ken Thompson's *Reflections on Trusting Trust* article in the context of Java applets. What, if anything, would need to be changed? What about byte-code verifiers, interpreted languages, disassemblers, etc. might you have to consider?
5. **30 points**

    print_display.c:

    ```
    #include <stdlib.h>
    #include <stdio.h>

    int main(){
      char display[512];

      strcpy(display, getenv("DISPLAY"));
      printf("Your display environment variable is %s\n", display);

      return(0);

    }
    ```

The system administrator accidentally set the suid (set user id) bit on this program, which is owned by root and lives in /usr/bin.

- Describe the vulnerability present in this program.
- Write a program to exploit this vulnerability and obtain the root shell. Be clear and concise. If you use a language other than C or Perl, please be extra clear.
- Argue/demonstrate that your exploit works.
- Rewrite print_display.c to be safe.

CS 4235: Introduction to Information Security September 15, 2011

Problem Set 3: Vulnerabilities

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three questions, each with several parts. Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup **September 29, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **15 points** Pfleeger and Pfleeger, Section 3.10, Exercise 15. For the "design requirements", concentrate on specifying a security policy for the processor, in terms of both its abstract functionality and physical properties.

2. **15 points** Consider Automated Teller Machines (ATMs), which use a customers bank card and secret Personal Identification Number (PIN) for common banking tasks like withdrawals, checking account balances, etc.

   Identify at least three distinct input/output paths on an ATM, and name the endpoints of each.

   For each of the above paths, describe the extent to which it qualifies (or doesn't) as a "trusted I/O path". Focus on confidentiality and integrity of data as it travels between the two endpoints. For this analysis, you may want to research some of the relevant known attacks on ATMs.

3. **20 points** Find an example of a specific security flaw in a commonly used commercial operating system (e.g., Windows, Linux, Mac OS X) in the past year. Good sources include CERT, the Microsoft Security TechCenter, or `securityfocus.com`.

   Choose a flaw that has very significant security implications (e.g., favor arbitrary remote code execution over local denial of service). Give a high-level summary of the flaw and its implications, in your own words. Classify the nature and cause of the vulnerability: for example, is it the result of flawed code in an unsafe language? an incomplete or inconsistent specification? a flawed design in terms of modularity and/or encapsulation? Justify your answer.

4. **20 points** In UNIX, the Internet Daemon (now called xinetd on some versions of UNIX) provides the handshaking that occurs when a TCP/IP connection. Xinetd is susceptible to a Denial of Serice attack, where many connections are made to the same service. When too many connections are made within a specified short period of time, xinetd will terminate that service for a short period of time and print error messages of the form:

```
inetd[354]: telnet/fcp server failing (looping), service terminated
```

Various attack programs exist to launch thousands of connections on a specific port, overloading the machine. See `http://www.cotse.com/dos.htm` for some examples of source code designed to mount denial of service attacks.

Explain the design alternatives that the designers of an Internet service like xinetd considered when they decided to implement inetd. What are some alternative designs that solve this vulnerability? Do they introduce new vulnerabilities?

5. **30 points** In this problem, you will try to understand how UNIX generates password files, and then try to crack some passwords!

   - Examine the source code or man page for crypt. How does this program take a plaintext password and generate the ciphertext that we see in /etc/password, or /etc/shadow? What cipher is used to generate the cipher from the plaintext?
   - Using crypt(3) on a UNIX machine, generate the ciphertext for security and netsecurity. What do you observe? Why?
   - `passwd` typically uses something called a salt to generate the password for each user. Why?
   - Consider the following password file generated with crypt(3):

     ```
     root:IWpIzqD0jR1.c:100:100:Charlie Root:/home/root:/bin/sh
     cs4251:UNzrFi5aYL9DU:101:101:CS4251:/home/cs4251:/bin/sh
     mysql:WqCBVG36lcuAc:102:102:MySQL:/home/mysql:/bin/sh
     guest:FTQinpjr.VRM.:103:103:Guest:/home/guest:/bin/sh
     test:LF2c9qM5l6X7Q:104:104:Testing:/home/test:/bin/sh
     ```

     Run the default mode of John the Ripper (`http:www.openwall.com/john/`) on the password file. One of the passwords will be cracked. Which one? Why (which rule of John was applied)? One of these passwords will be cracked. Which one? Why (which rule of John was applied)?
   - Try the "wordlist" mode of John. Which password is cracked now? Which rule of John was applied? (*Hint:* John's default wordlist is very small by default. You may have to augment this wordlist with one of your own.)
   - One of the users has a password that is a rotated version of a dictionary word. Modify Johns rule list to incorporate this feature. Which password does this now reveal? Please include the source for your modifications to the rule list.
   - One user is predisposed to using leetspeak (4 for a/A, 1 for i/I and l, 3 for e/E). His password is also a dictionary word. Modify john.conf to incorporate this feature. Which password is revealed?
   - One user likes to swap two adjacent characters of a dictionary word. Can you modify john.conf to do this using existing syntax? If not, how can you incorporate this feature? What is the password that is revealed?

CS 4235: Introduction to Information Security November 8, 2011

Problem Set 4: Attacks

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three questions, each with several parts (plus a fourth fun activity). Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup **November 22, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **One-Time Pads (30 points).** Eve has been eavesdropping on Alice and Bob's communications with each other for some time. They appear to be using a one-time pad to keep their messages secret. Eve suspects that the plaintexts are just English sentences encoded in the standard ASCII character set, and the ciphertexts are generated using bitwise exclusive-or (XOR) with the pad. For example, in ASCII the character 'a' has hexadecimal value 61 (or 01100001 in binary), which when bitwise-XORed with the hexadecimal pad value 83 (10000011 in binary) yields the hexadecimal ciphertext e2 (11100010 in binary).

   Knowing that the one-time pad is hard to use properly, Eve has been storing every ciphertext sent between Alice and Bob, and XORing pairs of them to look for any anomalies. One day she notices that a pair of ciphertexts XOR to a value (shown below in hexademical) that appears "strange". She suspects that Alice and Bob may have reused part of their pad, and asks you to recover the plaintexts.

   - (10 points.) Why has Eve been XORing pairs of ciphertexts? What is "strange" about the XOR value below that she found?
   - (10 points.) Formulate and describe your approach for helping Eve. The messages may be time-sensitive, so your attack should work as quickly as possible.
   - (10 points.) Give as much of the plaintexts as you can find.

   ```
   03 03 0b 4f 45 5b 48 09 0b 54 54 1b 4f 1d 0d 12 45 57 0c 54 48 00
   02 45 4e 2a 19 0b 09 53 00 3a 55 1f 19 15 01 07 45 48 11 17 17 54
   0b 5a 55 53 28 05 4b 0a 55 01 55 02 04 44 58 4f 42 00 07 45 49 1b
   52 01 00 1f 1c 0a 4f 15 0b 01 1c 00 1e 0e 44 42 1a 08 00 17 0d 04
   4c 44 42 48 53 2b 51 11 00 11 06 00 43 54 4f 10 02 45 13 42 01 1a
   00 49 0a 11 00
   ```

2. **Port Scanning (40 points).** In this hands-on problem, you will re-create some of the results that we performed in lecture, using the `nmap`.
   - (10 points) Explain how port scanning works, and why an attacker might run a port scanning tool.
   - Download the nmap tool and install it somewhere where you can run it. (`http://nmap.org/download.html`).
   - (5 points) Run `nmap` against `porter-square.cc.gt.atl.ga.us`. What ports do you see open on the machine? How did `nmap` discover this? Copy the output of running the tool into your writeup. Based on the list of open ports, make your best guess at the services running on this machine. *Extra credit:* Extra credit if you can figure out the versions of services running on the machine! (This will require tools other than `nmap`.)
   - (5 points) Use `nmap` to determine the version of the operating system that `porter-square` is running. What operating system is running? How does `nmap` determine the operating system?
   - (10 points) Use `nmap` (or, if you prefer, a script) to determine all hosts on `130.207.0.0/16` that are running a Web server. *Hint:* You can use some options in `nmap` to scan an entire network subnet, and to restrict the scanning to a particular port. This will go much, much faster if you ise the "-p" option in `nmap`.
   - (10 points) Find a machine on the wide-area Internet that has the Simple Mail Transport Protocol (SMTP, port 25) open. List the IP address of the machine that you found and show the output from your `nmap` tool. This is called an "open mail relay". How might an attacker be able to use an open mail relay?

3. **Search Engine Optimization Competition (30 points + quiz bonus points).** *Complete in your project groups!* Construct a Web page that comes up #1 (or as high as you can manage) in Google's search engine when a user searches "radiator palace summit seaweed". The winner of the competition will be judged *in class* on November 22. All members of the group will receive 5 quiz bonus points!

4. **For fun: Tor.** Run and install Tor (`http://torproject.org/`, if you haven't done so before. More to come on anonymity and privacy on the next (and last!) problem set!

CS 4235: Introduction to Information Security December 6, 2011

Problem Set 5: Cryptography and Anonymity

Instructor: Prof. Nick Feamster *College of Computing, Georgia Tech*

This problem set has three **optional** questions, each with several parts (plus a fourth fun activity). Answer them as clearly and concisely as possible. You may discuss ideas with others in the class, but your solutions and presentation must be your own. Do not look at anyone else's solutions or copy them from anywhere. (Please refer to the Georgia Tech honor code, posted on the course Web site).

Turn in your writeup **December 14, 2011** by 11:59pm. *Please upload your solutions to T-Square. Other forms of submission will not be accepted!* We will be providing more information about how to turn in your assignment as the due date approaches.

1. **Crypto Hacks (25 Points).** Alice and Bob are good friends. To save time, they agree to simply find one good pair of primes, p and q and therefore use the same public modulus, $n = pq$. To save confusion over who signed which message, they select different exponents e_a and e_b. Show that, in this system, it's possible to decrypt a message M sent to both of them if $\gcd(e_a, e_b) = 1$. That is, given,

$$\begin{aligned} C_a &= M^{e_a} (mod n) \\ C_b &= M^{e_b} (mod n) \end{aligned}$$

an adversary can compute M.

2. **Internet Transparency (40 Points).** Various projects are now trying to monitor the availability of various Web sites, informations and services. Two such systems are Herdict (`http://herdict.org/`), and Google's Transparency Report (`http://google.com/transparencyreport/traffic/`. Herdict relies on manual reports of downtime and unavailability, whereas Google's transparency report uses anomalies in traffic volumes to discover reachability problems from various regions for a particular service.
   - **10 points.** What are the possible sources of inaccuracy of each approach? How would you verify the accuracy of information reported from each of these systems?
   - **30 points.** Design and build a simple system that takes reports from the Herdict Web site and automatically measures their reachability properties from a variety of different locations. For this purpose, you may need access to a set of distributed servers. The PlanetLab testbed (`http://planet-lab.org/`) is a good resource for this. I can provide you an account if you need one.

3. **Anonymity (35 Points).** Download and install Tor.
   - **(15 Points).** Identify the locations of the various entry and exit nodes that you can use in Tor. What is the distribution of entry and exit nodes across Internet service providers and countries? Provide a table of the top 10 countries and ISPs (autonomous systems) that host Tor entry and exit nodes.

- **(20 Points).** The Tor Metrics page has some interesting examples of statistics of Tor usage in different countries during times when countries attempted to block Tor. For example, see `http://goo.gl/6Pcfn` for an example of when Iran blocked Tor. Find at least two other examples of cases where Tor appears to have been blocked in a country. *Include a graph from the Tor metrics page and a description of what you think is going on.* How would you have stopped these events?