CS426: Computer Security **Fall 2010**

Homework #1

Due date & time: 1:30pm on September 10, 2010. Hand in at the beginning of class (preferred), or email to the TA (twykoff@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 1:30pm the day after it is due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required. (2) Problem 1 requires you to start at least one week before it is due.

Problem 1 (15 pts) Go to security focus mailing list website (*http://www.securityfocus.com/archive*), and subscribe to the bugtraq mailing list and at least one other mailing list there. Subscribe for at least one week, read the messages, and write down what you have learn from this experience. You could write a detailed description of one vulnerability reported in the mailing list, your sense of what are the common vulnerabilities, or any other thing.

Problem 2 (6 pts) Identify two computer security control measures on your computer(s). Which of the three properties Confidentiality, Integrity, and Availability do they aim at providing? What kinds of adversaries they **cannot** defend against?

Problem 3 (8 pts) Find a recent (2009 or 2010) computer security incidence that has been reported in the media, and analyze the incidence. For example, what was the main vulnerability that was exploited, what security principles were violated, what could have done to prevent the incidence, etc.

Problem 4 (5 pts) Use a few sentences to prove that for any cipher that offers perfect secrecy, the number of the possible keys must be at least as large as the number of plaintexts.

Problem 5 (17 pts) Cryptanalysis

- (3 pts) Explain what do ciphertext-only attacks, known-plaintext attack, and chosen plaintext attack mean?
- (2 pts) What attack can be used to break the substitution cipher under a ciphertext-only attack? Explain the simplest way to break it under a known-plaintext attack?
- (8pts) Suppose that everyone in the world is using the DES algorithm in the ECB encryption mode, and you can use a chosen plaintext attack against everyone. Show how to perform a dictionary attack such that, after an expensive but doable initialization step, everyone's key can be recovered in very little time. Write pseudo code both for the initialization step and for the function to recover everyones key.

- (4pts) How effective would the above attack be under known-plaintext (instead of chosen plaintext) attacks? What if everyone uses the CBC encryption mode with the IV randomly chosen?

Problem 6 (6 pts) Block cipher security Assume that you are doing an exhaustive key search attack and can check 2^{32} (or about 4G) keys per second, how long would it take to for you to search through all keys while attacking ciphers of the following key lengths: 56, 80, 112, 128? You must use year, month, day, and hour for time units.

Problem 7 (6 pts) Block cipher key size

- In the ideal block cipher with 64-bit blocks, there are $2^{64}!$ possible keys. How many bits one needs in order to represent the keys in binary? Show your calculation steps.
- Repeat the above question for the ideal block cipher with 32-bit blocks.

Problem 8 (12 pts) There are three desirable properties for cryptographic hash functions: Preimage resistant, Second preimage resistant, and Collision-resistant. For each of the following applications of hash functions, explain which of these three properties are needed and which are not.

- Alice poses to Bob a tough math problem and claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not bluffing. Therefore, Alice writes down her solution, appends some random bits, computes its hash and tells Bob the hash value (keeping the solution secret). This way, when Bob comes up with the solution himself a few days later, Alice can verify his solution but still be able to prove that she had a solution earlier.
- Passwords are stored in a password file, in hashed form. To authenticate a user, the password presented by the user is hashed and compared with the stored hash. A user who gains read access to the password file should not be able to log in by this method. (Assume that the mischievous user does not modify the system in any way before trying to log in.)
- A system administrator, concerned about possible breakins, computes the hash of important system binaries and stores the hash values in a read-only file. A program periodically recomputes the hash values of the files containing the system binaries, and compares them to the stored values. A malicious user who is able to overwrite one of the "protected" files should not be able to change the file without detection.

Problem 9 (25 pts) Read the following paper and write a summary of what you have learned from it.

- Nikita Borisov, Ian Goldberg, David Wagner: Intercepting Mobile Communications: The Insecurity of 802.11. (Available from the handout page.)