214573 Midterm Exam Solutions
2nd semester 2005

1. Describe the seven critical characteristics of information. How are they used in the study of computer security?

   Solution: The critical characteristics of information define the value of information. Changing any one of its characteristics changes the value of the information itself. There are seven characteristics of information:
   1. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication.
   2. Confidentiality is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
   3. Integrity is the quality or state of being whole, complete, and uncorrupted.
   4. Utility is the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. Possession is the quality or state of having ownership or control of some object or item.
   5. Confidentiality is ensuring that only those with rights and privileges to access a particular set of information are able to do so, and those who are not are prevented from doing so.
   6. Accuracy is the quality or state of information being free from mistakes or errors.
   7. Possession is the quality or state of having ownership or control of some object or item.

2. How does a threat to information security differ from an attack? How can the two overlap?
   Solution: A threat to information security differs from an attack in that a threat is the potential to use or exploit vulnerability within the information system. The threat is the weakness in the system that is used for the attack. An attack is the realization of the threat that causes damage to the information system. The two overlap in that the threat agent actually causes the attack on the system.

3. How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? What other controls can reduce this threat?

   Solution: Employees constitute one of the greatest threats to information security. To prevent such acts of human error or failure, dual controls are effective in a way that a second party can verify commands that they wish to execute. Requiring the user to type a critical command twice is another example of dual control.

   Dual controls reduce the threats from human error because the additional people required confirming the task would check for any errors, which will prevent mistakes, and in the event of malfeasance, would require collaboration by two individuals.
   In addition to dual controls, other methods that can be used to reduce human error are to automatically save all data on back up drives, require approval before deleting any information, have the system confirm all decisions with user prior to execution, and limit access of certain drives and applications to certain employees with clearance.

214573 Midterm Exam Solutions
2nd semester 2005

4. (8 points) How can you or an organization protect yourself or itself from a Man-in-the-Middle attack?
   Solution: Various defenses against MITM attacks use authentication techniques that are based on:

   - Public keys
   - Stronger mutual authentication
   - Secret keys (high information entropy secrets)
   - Passwords (low information entropy secrets)
   - Other criteria, such as voice recognition or other biometrics

5. What are the three types of password attacks? What can a systems administrator do to protect against them?

   Solution: The three types of password attacks are: Password Crack, Brute Force, and Dictionary:

   Password crack: Attempting to reverse calculate the password is called "cracking." Cracking is used when a copy of the Security Account Manager data file can be obtained. A possible password is taken from the SAM file and run through the hashing algorithm in an attempt to guess the password.

   Brute Force: The application if computing and network resources to try every possible combination of options of a password.

   Dictionary: A form of brute force for guessing passwords. The dictionary attack selects specific accounts and uses a list of commonly used passwords with which to guess.

   To protect against password attacks, security administrators can:
   a) Implement controls that limit the number of attempts allowed.
   b) Use of a "disallow" list of passwords from a similar dictionary.
   c) Require use of additional numbers and special characters.

6. Tripwire is a program that is used to assure the integrity of the files on a Windows or Unix workstation. In one incarnation, the Tripwire executable uses the computer's cryptographic library to compute the MD5 hash code for every file in directories that are specified by the Tripwire configuration file. Tripwire then creates a database that consists of each file's name and MD5 code. This database is stored on the computer's hard disk.
   Mr. Thaksin configures Tripwire to compute the MD5 values of all the programs in his /bin and /usr/bin directories. A month later, he runs the Tripwire program again to see if any of the MD5 codes have changed. The database that is generated perfectly matches the database of MD5 values generated when Ben first ran Tripwire. But unbeknownst to Ben, his files have been compromised by an attacker.
   Describe three attacks that are consistent with this scenario, and how you would defend against them.
   Solution: Many correct answers are possible, including:
   Change the database, so that it contains the MD5 values of the modified files, rather than the original files.

Change the function that calculates MD5, so that it returns the old values, rather than the new ones.
Hack the kernel so that the Tripwire program thinks it is reading the files in the /bin and /usr/bin directories, when it is in fact reading other files (presumably the original copies).
Hack the Tripwire program, so that it says that nothing is wrong, when in fact something is.
Hack Mr. Thaksin's operating system, so that he sees the Tripwire program report that everything is okay, when in fact it is reporting something else.
One answer will not be accepted. Students will not receive credit for arguing that MD5 is weak and that the attacker could simply modify the new files so that they have the same MD5 as the original files. Any student who loses credit for this answer is invited to produce two different files that have the same MD5 hash code.

7. The year is 2050 and Moore's law has continued to hold, doubling computer performance every 18 months. Is it time to retire AES-128? How about AES-192 or AES-256? Explain your reasoning.
Solution: Today, 80 bit symmetric keys offer only decent security. In our scenario of the future, computers will be about 2^{31} times faster, implying that 111 bit keys are questionable. At this point, the security of AES-128 is in question (only one student thought about the lifetime of the data being protected; it may be time to retire the cipher if the data needs to stay secure long after 2050, which is often the case). AES-192 and AES-256 are still fine. Of course, Moore's Law is not believed to hold for so long ...

8. Mr. Thaksin is setting up branch offices all over the country to assist other TRT candidates in becoming governors. This is a very delicate operation, and Mr. Suriya, his head of communications security, has decided to use a one-time pad to encrypt all communications from the branch offices back to central office. Because one-time pads are expensive to distribute by courier, Mr. Suriya plans to distribute to each office j a unique 56-bit key k_j . This key will be used with DES to encrypt a separate one-time pad that will be sent over the Internet to each office. The offices will then use the one-time pad to encrypt the messages that they send back.
Mr. Sonthi is an unbounded adversary. Describe how he could decrypt messages sent with this scheme from the branch offices to headquarters, and what additional information (if any) he would need to do so. The less extra information he needs, the more points you will receive.
Solution: First solution: Mr. Sonthi can try all possible DES keys, produce all 2^{56} possible pads, and then see which of these pads produces reasonable messages when it is XORed with the bit stream sent from the branch office to HQ. Second harder solution: if Mr. Sonthi can obtain a matched cipher text and plaintext pair (under the one-time pad), he can learn part of the pad. He can then decrypt the encrypted pad under all DES keys, and learn the actual pad (it is the one that matches the partial pad). At this point, he can read all the messages. No credit will be given to students who said that the one-time pad would probably be used twice. The problem said that the pads were only used once.

214573 Midterm Exam Solutions
2nd semester 2005

9. You are watching an encrypted conversation between Alice and Bob. You notice that the prefixes of many of the cipher texts agree for several hundred bytes. In addition, these identical prefixes are always a multiple of 16 bytes long. However, you never observe two identical chunks of cipher text of any significant length following the identical prefixes. Conjecture what cipher is being used, what mode of operation is being used, and what Alice and Bob are doing wrong.

   Solution: The answer we had in mind was AES (or DES) under CBC mode, (incorrectly) using the same IV for every message. Full credit will be given for an answer such as AES or DES in ECB mode, with some explanation (e.g., all messages have long, common headers.)

10. In its next chip, Intel finds a way to make the stack non-executable. Does this solve the problem of buffer-overflow attacks? Explain briefly.
    Solution: No. It's still possible to maliciously modify the return address and parameters on the stack, which could cause undesired behavior.

11. List three techniques that virus writers use to make their viruses harder to detect:
    Solution:
    - Putting the virus somewhere other than the head or tail of the executable.
    - Polymorphism (changing the code of the payload with each infection).
    - Detecting whether the virus is being run in emulation.

12. Give one reason why "simplicity" an important criterion in the design of secure systems.
    Solution: There are many: the system will be easier to analyze; implementations will be less likely to have bugs.

13. In the RSA scheme, the modulus $n = pq$ is chosen as a product of two large primes $p < q$. To make factoring n as hard as possible, Mr. Thaksin decides to make the smaller prime p as large as possible, and thus chooses p and q as consecutive primes.
    Explain briefly why Mr. Thaksin's approach is flawed. You can assume that p and q are reasonably close to each other.
    Solution: p and q being consecutive primes, and reasonably close, they are $\approx \sqrt{n}$. more precisely, p is the largest prime $< \sqrt{n}$ and q is the smallest prime $> \sqrt{n}$. So, an adversary just needs, for instance, to try all odd integers from $\sqrt{n}$ down, and test whether $n \bmod t = 0$. He will stop at the first prime he hits and get p.

14. List three controls that could be applied to detect or prevent salami attacks.

    Solution:
    1. Analyze the source code (extremely difficult)
    2. Find indications of an attack (ex. an account that grows without deposit transactions)
    3. Random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery.
    4. Don't ignore what appear to be errors in computer-based financial or other accounting systems.

214573 Midterm Exam Solutions
2nd semester 2005

15. What is the fundamental difference between symmetric and asymmetric encryption?

Solution: Asymmetric encryption is also known as public key encryption. It uses two different keys to encrypt messages, the public key and the private key. Symmetric is different because it uses only one key to encrypt and decrypt messages. Symmetric encryption is much faster for the computer to process, however it raises the costs of key management.

Symmetric encryption, also called private key encryption, is where the same key is used to conduct both the encryption and decryption of the message. Both the sender and receiver must own encryption of the key. The problem with symmetric encryption is getting a copy of the key to the sender.

Asymmetric encryption, also called public key encryption, uses two different keys. Either key may encrypt or decrypt the message, but one key must be used for encryption only and the other must be used for decryption only. The technique has the highest value when one key is used as a private key and the other is used as a public key. The public key is stored in a public location where anyone can use it. The problem with asymmetric encryption is that it requires four keys to hold a single conversation between two parties.

Due to the number of keys involved in asymmetric encryption, it is not as efficient to use as symmetric encryptions in terms of CPU computations and key management.