

Homework 3

Due: March 12, 2008, 10:00 PM EST

-
- Please submit your solutions on MyCourses as a PDF file. We believe it should be fairly trivial for you to generate a PDF file, especially with all the stuff available at software.brown.edu and in the CS department. We will not accept other formats.
 - Keep your answers short, and to the point. Be brief and concise, and draw pictures where appropriate.
-

Problem 1 Kerberos is an authentication platform we learned about in class. Let's talk about some of the properties of Kerberos version 5 ¹:

1. How does this system help us assure the authenticity of the authentication server?
2. How do we know that the ticket granting server is not compromised?
3. Why do we need a ticket-granting server and an authentication server? Can they be combined? Why or why not? If so, how could this change the message exchanges?
4. You may have noticed that the user's password is very well protected. What are the two precautions this system uses to defend it?
5. This system relies on pre-existing shared secrets. Sometimes that is inconvenient, especially considering to make this system work you need to highly guard your shared secrets. What is a way we could safely extend this to add a user to the system without requiring physical access to the system?

Problem 2 Let's analyze an alternate Diffie-Hellman key exchange.

1. Do a step-by-step Diffie-Hellman key exchange with a finite additive cyclic group for G , a generator $g = 2$ and $a = 7, b = 5, p = 11$.
2. What is their final shared secret?
3. Why is this weaker than multiplicative cyclic groups?
4. How could Eve (the malicious party intercepting the communications) solve for a and b ?

Problem 3 MD5 cryptographic hashes are a common tool in computer security. Tell us about the following properties of MD5:

1. How can you safely convey it to your target audience?
2. Create a MD5 hash for the following phrases using the md5sum command-line tool found in Windows and Linux
 - (a) The class was late in the day.
 - (b) The class was late in the may.

¹<http://tools.ietf.org/html/rfc4120>

3. Why are these hashes so different? Specifically what steps in the process cause this great variation and how?

Problem 4 BitLocker allows users several authentication options. Discuss the pros and cons (at least 3 pros and 3 cons) of each of the following:

1. Trusted Platform Module (TPM)
2. TPM + PIN
3. TPM + PIN + USB Key
4. TPM + USB Key
5. USB Key

Problem 5 A useful tool for making sure a filesystem has not been tampered with could be creating a hash tree for the volume over sectors. If a malicious user boots it and modifies anything on the filesystem with external tools the hash will fail and the user will be alerted next time they boot up. The hash tree needs to be calculated every time the system is shut down. This needs to be efficient without tons of recursion, so we will implement it as a n -ary tree, where $n = 5$.

1. Write pseudocode for how this would be done for a drive of size x sectors..
2. How would you incrementally update the hash? For example, if you only wrote to one block on the drive.
3. What is the running time generating the top-tier hash if we have x sectors. Presume the time it takes to call the hash function is always equal to one.
4. Where should you store the root hash?