CSCI 667 - Homework 2*

Assigned September 19th, 2024; Due 11:59pm on October 3rd, 2024

Prof. Adwait Nadkarni

Note: This homework assignment is worth 55 points.

1 Symmetric Crypto {45 points}

1 {10 points} A cryptosystem that offers *perfect secrecy* prevents an eavesdropper who observes an encrypted transmission from learning anything about the plaintext, other than its size.

Show with a counterexample that the Substitution Cipher doesn't provide perfect secrecy.

2 {15 points} You have a filesystem utility `fsec` that encrypts your files. Assume that the system is perfectly implemented and designed. To secure your file, you can choose either **a**) an 8 byte alphanumeric password selected by you, or **b**) an 8 byte random key selected by the system (used as a key). Which is more secure against brute force attacks and why?

3 {20 points} You are designing a wireless electric meter reader system. The meter receives requests for read-outs from a reader truck as it drives down the street (past the meter, once a week, i.e., there is one legitimate exchange per week). The request must be authentic for the meter to respond. If the request is deemed authentic, the meter will transmit the current reading (**no security is required for the response**). Assume that packets are never dropped and the truck comes every week without fail. The adversary should never be able to *replay* a request and get a response at any time. The following are constraints on the problem:

- No encryption or HMACing is allowed.
- The meter can only hold 32 bytes of memory in non-volatile storage.
- Assume you get to fill the meter with some information before deploying it. The information placed in the meter should allow it to authenticate requests for a full year.

Hint: the SHA2 output size is 256 bits (also 212, and other larger sizes, but considering 256 bits here).

(a) {5 points} What information do you put in the device initially?

(b) {10 points} Describe the request and response format (using the cryptographic notation we have used), and give one or two sentences how it achieves authenticity.

(c) {5 points} How does the meter detect replayed or forged requests?

*Last revised on September 24, 2024.

2 Key Sharing, The Pedantic Way {10 points}

At a recent conference, Prof. Pedantic met a potential collaborator, Prof. Feckless. Over drinks, Prof. Pedantic and Feckless outlined a new super-secret research project that they would collaborate on throughout the year. Due to the nature of the work, both professors agreed that any future email between the two parties should be encrypted.

1 {3 points} Suppose that during their encounter, Prof. Pedantic and Feckless securely exchanged a random, 16 bit key, k_{16}. Later, back at their respective institutions, they realize that 16 bits is too small. They decide to use the short key to communicate a longer secret, chosen by Prof. Pedantic, as follows:

$$\text{Prof. Pedantic} \rightarrow \text{Feckless} : E_{k_{16}}(k_{256}, \text{MAC}_{k_{16}}(k_{256}))$$

They then communicate using the 256 bit key k_{256} as follows:

$$\text{Prof. Pedantic} \leftrightarrow \text{Feckless} : E_{k_{256}}(M, \text{MAC}_{k_{256}}(M))$$

What is the flaw in the two professors' logic?

2 {7 points} Suppose that the two professors each share a (separate) key with a trusted mutual friend, Dean Bureaucracy. With Dean B's help, can they now securely exchange a key such that an external eavesdropper (i.e., anyone who is not the professors or the Dean) cannot learn it? If so, how? If not, why not? You can assume that Dean B is honest.

Submission Instructions

Submit your solution as a single PDF using Blackboard. To upload your assignment, navigate to the "Concepts of Computer Security (Spring 2024) course. Use the "Homework 2" assignment.

Writeups submitted in Word, ASCII, PowerPoint, Corel, RTF, Pages, and other non-PDF formats will not be accepted. Consider using LaTeX to format your homework solutions. (For a good primer on LaTeX, see the Not So Short Introduction to LATEX.)

Note that you may submit a PDF scan of hand a hand written solution; however, you will receive **0 points** if the instructor cannot read your hand writing. If the instructor has any difficulty reading your hand writing, you may not submit hand written solutions for future assignments.

Please post questions (especially requests for clarification) about this homework to Piazza.