7.1.2019

IoT Security Final Exam Questions

Due Date is 8.1.2019 at 18.30

1. When shopping at Costco, after you've selected your purchases you take your cart full of goods to one of the registers. The check-out clerk scans your goods, totals what you owe, and upon receiving payment from you gives you an itemized receipt. However, you can't then simply exit the building with your goods. At the exit you're required to go by a staffmember who inspects your receipt. If the receipt looks okay (appears to match the number and types of items in your cart), the staffmember draws a line with a permanent marker down the receipt and hands it back to you. At this point, you can exit the building and take the goods to your car.
   (a) (15 points) Identify two security principles illustrated by Costco's approach. For each, describe in a single sentence what aspect of Costco's approach reflects the principle.
   (b) (5 points) Identify an attack that Costco seeks to prevent by having the staffmember draw the line down your receipt. Briefly describe how the attack works.
2. Consider the following encryption mode for applying AES-128 with a key K to a message M that consists of l 128-bit blocks, M1, . . . , Ml . The sender first picks a random 128-bit string, C0, which is the first block of ciphertext. Then for i > 0, the i th ciphertext block is given by Ci = Ci−1 ⊕ AES-128K(Mi). The ciphertext is the concatenation of these individual blocks: C = C0 || C1 || C2 || · · · || Cl .
   (a) (5 points) What is the intent behind the random value C0? (I.e., what is it meant to achieve.)
   (b) (10 points) Is this mode of encryption secure? If so, state what desirable properties it has that make it secure. If not, sketch a weakness.
   (c) (5 points) Suppose we replace the computation of Ci with Ci = AES-128K(Ci−1 ⊕ Mi). Does this make the mode of encryption more secure, less secure, or unchanged? Briefly explain your answer.
3. Consider the use of Twitter for botnet command-and-control. Assume a simplified version of Twitter that works as follows: (1) users register accounts, which requires solving a CAPTCHA; (2) once registered, users can post (many) short messages, termed tweets; (3) user A can follow user B so that A receives copies of B's tweets; (4) user B can tell when user A has decided to follow user B; (5) from the Twitter home page, anyone can view a small random sample (0.1%) of recent tweets.
   (a) (8 points) Sketch how a botmaster could structure a botnet to make use of Twitter for C&C. Be clear in what actions the different parties (individual bots, botmaster) take. Assume that there is no worry of defensive countermeasures.
   (b) (8 points) Briefly describe a method that Twitter could use to detect botnets using this C&C scheme.
   (c) (2 points) How well will this detection method for Twitter method work?

(d) (2 points) Briefly discuss a revised design that the botmaster could employ to resist this detection by Twitter

4. You return to Javalicious, the handy coffee shop nearby with free WiFi. You again settle in for an afternoon of web-surfing and tweeting. You know that the network sends all packets unencrypted, and you are not surprised to again see Prof. Evil seated at the table next to yours, using a laptop connected to the same WiFi network. For your web connections, consider the basic security properties of confidentiality, integrity, and availability. For each of these, analyze three scenarios: • DNSSEC-only means that for a given web site, your laptop looks up all of the domain names for your web session using DNSSEC (including NSEC3); your actual web traffic, however, uses HTTP. • HTTPS-only means that for a given web site, your laptop looks up all of the domain names for your web session using ordinary DNS; your actual web traffic, however, uses HTTPS. • DNSSEC+HTTPS means that both your domain name lookups use DNSSEC and your actual web traffic uses HTTPS. At the end of each section, supply a brief explanation for your answers whether this is applicable or not.
   (a) (5 points) Confidentiality of your web connection content:
   (b) (5 points) Confidentiality of keeping private what sites you communicate with:
   (c) (5 points) Integrity of your web connections:
   (d) (5 points) Availability of your web connections:
5. PlopIt! is a popular service that allows users to store files "in the cloud". For any file that a user wishes to make accessible to different Internet systems, the user uploads the file (via their browser) to PlopIt! and receives back a URL that provides direct access to the file. Each URL has the form https://plopit.com/storage/user/hash, where user is the name of the user who uploaded the file, and hash is the SHA-256 hash (64 hexadecimal digits) of the contents of the file. For example, such a URL might look like https://plopit.com/storage/Alice/9b65...e7e6 . Users can then share these URLs with their friends or whomever they wish to allow to access the uploaded file. Users can also mark their uploads as "public," enabling anyone to view them via a browsing and search facility provided by PlopIt!.
   (a) (5 points) Describe an attack on user security or privacy that this design enables. In your description, include mention of who might seek to launch the attack. Make as few assumptions about the attacker's capabilities as possible.
   (b) (3 points) Describe a way that PlopIt! can defend against this attack. Your defense should require minimal changes on their part, and not disrupt their service model of enabling users to share files with friends.
   (c) (5 points) PlopIt! has become successful enough that they incur significant expenses for disk storage and network capacity. To reduce the volume of data they deal with, PlopIt! changes its upload mechanism to use compression, as follows. When a user wishes to upload a file, the uploader breaks the file into blocks. Before uploading a given block, the uploader sends a SHA-256 hash of the block's contents to see whether the server already has that block. If so, the browser avoids sending the block. Given this compression (and assuming that PlopIt! uses the defense you developed Final Exam Page 13 of 18 CS 161 – SP 11 in the previous question), describe how two parties, Alice and Bob, can use PlopIt! to secretly communicate even though they have no means of directly sending information to one another. Assume that Alice and Bob had an opportunity in the past to agree on how their scheme will work—but they were not able to agree upon any specific

PlopIt! URLs to use for communication. For full credit, your scheme should enable Alice to transmit modest-sized messages (dozens to hundreds of bytes of data) to Bob without requiring a great deal of effort.

(d) (3 points)Describe how you can use your scheme to transmit GBs of data to Bob in a feasible amount of time.

(e) (4 points) Suppose that a warden monitors Bob and prevents Bob from engaging in any use of the PlopIt! site. The warden allows Alice to send PlopIt! URLs to Bob, however, because the warden likes to taunt Bob with the warden's censorship of the site. The warden does not allow Alice to send anything else to Bob. Describe how Alice and Bob can have agreed upon a scheme in advance that allows Alice to send an n-byte message to Bob by sending Bob a total of n PlopIt! URLs. Assume that the warden validates each URL to make sure that it does indeed point to a file stored in PlopIt!.