CS-301 Fall 2020 Mini-Exam 4

September 15, 2021

1 ChoiceAgain

You think about buying new Customer Relationships Manager (CRM) software for your company from a new startup in Lausanne. You know that your company's relationship with your customers is the most important thing for the business. Thus, you want to make sure that the CRM software does not have any security vulnerabilities. Once bought, this software will be running on your own servers. Which of the following practices does the startup need to follow to convince you that their software is sufficiently safe for your company? For each practice, say Yes or No and justify your answer.

1. Fuzzing their code
2. Have an Intrusion Detection System to protect their network
3. Run symbolic analysis
4. Have the most up to date antivirus on their employers machines

Remember that you should not ask for impossible protections, as that will prevent you from buying any software.

2 TAChat

Alice has heard a rumor that the COM-301 TAs have built a chat application that they use for preparing and discussing mini-exam questions. Alice is very intrigued by this process and decides to study the application. Just out of curiosity! Alice would never cheat... Through her analysis, Alice discovers some details about how the TA's chat application works. She asks you to extract TAs chat history from the server and let her know what they talk about.
The TAs have deployed the chat as an internal service in EPFL and it is not accessible over the internet from outside campus. The server has an asymmetric key *(pks,sks)* and the public part is known to all TAs and Alice. To restrict the chat service to TAs, the server has a whitelist of the TA devices' MAC addresses, and it only accepts connections from those MACs. When someone

wants to access the server, they perform the following protocol:

1. Client: Create a new Diffie-Hellman key (pkc, skc) and send pkc with the new message m to the server.
2. Server: Check that the client's MAC is in the whitelist. Otherwise disconnect.
3. Server: Add m to the list of all messages $msgs$.
4. Server: Derive the shared key $k = \textit{Diffie-Hellman}(pkc, sks)$, then encrypt and send the chat history $history = Enc(k, msgs)$ to the client.

Consider two scenarios:

1. Alice has given you access to her office and WiFi password in EPFL. Can you get access to the chat history? What capabilities do you need?
2. Due to the Corona outbreak, EPFL has closed the campus to students. Alice shares her credential for EPFL's VPN with you, so you can connect to the service. Will you be able to use the same eavesdropping attack as in the previous part?

For both scenarios describe clearly how you would carry out the attack and what capabilities you need to carry it out. Justify why you have those capabilities in the given scenario.

3 WeaselNews

WeaselNews is spreading lies about the Coronavirus and the Swiss government has asked you to prevent Swiss citizens from accessing their website. Because WeaselNews is worried about its freedom of speech, the company hosts all their servers on the north pole. Devise a censorship approach to block access to WeaselNews and assess your suggested approach based on its effectiveness in Switzerland and its impact on the rest of the world (will this create a problem for people living in other countries?). Can users bypass this censorship? If yes, how?
Note: You do not need to come up with a perfect censorship which is uncircumventable. We will grade how well you understand the degree of protection that your proposed censorship approach provides.

4 Flipagram

Flipagram is a website that allows clients to share photos with friends. Flipagram requires clients to login before using the system. To reduce the number of fake users on the platform, Flipagram restricts the number of users registered

per IP to a maximum of 5. When a client logs onto Flipagram, the server sends to the client all new pictures recently posted by this client's friends. The photos are then displayed by the client's browser. Every time a client posts a photo on Flipagram, a TCP connection is created from the client's device to Flipagram's server. This connection is used to send the photo to the server who will store it. To increase the number of visits, clients can only upload one photo per hour.
Give two examples of Denial of Service attacks on Flipagram's server: one that would exhaust the server's bandwidth, and one that would exhaust the server's kernel and CPU resources. For each attack, state clearly (in one or two sentences) how the adversary performs the attack and what capabilities they need to have to perform the attack.

5 Sawit

Bobby works at AcmeCorp, an organization that expects its employees to only work and not waste time on other activities. Bobby feels that he needs a break from time to time. He enjoys visiting Sawit, a site that allows users to post their favorite memes. Bobby does not want AcmeCorp's IT team to learn about his meme-related activities. He decides to use DNSSEC to resolve Sawit's IP address, and then HTTPS to connect to Sawit. Evaluate whether Bobby's setup will ensure that the following scenarios do not happen:

1. The IT team finds out that Bobby has been posting memes making fun of AcmeCorp. They inform his boss, who fires him. Assume that the IT team only has access to Bobby's network traffic and not, for example, to the content that Bobby has posted on Sawit.

2. The IT team hears from Bobby's colleague that he is visiting Sawit during his work time. They catch him in the act of posting memes about AcmeCorp by replacing Sawit's DNS record returned by the DNS resolver with an IP address of AcmeCorp's fake Sawit site. When he visits the fake site and posts memes about AcmeCorp, they inform his boss who fires him. Assume that the IT team only has access to Bobby's network traffic, and their fake server.

Justify your answer. If your answer is no in any of the scenarios, explain what Bobby could do to be protected.

6 Cafe

Part I. Rita has heard the best coffee in town is served at Ricco's Cafe. She gets there and while she waits for her coffee she wants to watch the new TikTok hits. It turns out that the WiFi network at Ricco's Caffe has no encryption. Ricco warns Rita that it is not safe to use this connection, but Rita disagrees. Rita connects to the WiFi, and tests that she has Internet connectivity by visiting https://cutestkittens.com. It loads without issues. Rita says to Ricco: "See, no

problem! That access was totally safe!"
If Rita is correct and the access to cutestkittens.com was safe, explain why she is correct. If she is not correct, provide a network attack against Rita.
Part II. Now that she has tested her WiFi access, Rita decides to have the only muffin sold in the cafe. She does not remember whether she has enough money so she tells Ricco: "Let me check if I have enough money in my bank account." and starts typing https://QuiteSecBan... on her phone's browser. The next client in line, Randy, also wants the muffin, so he decides to stop Rita from buying it and wants to prevent her from checking her bank account.
Describe a network attack that Randy can do to prevent Rita from checking whether she has enough money in her account. For each attack, describe clearly (in one or two sentences) how Randy performs this attack and what capabilities he needs to have to perform the attack.

7 getPassword

Consider the following C function for getting a password from the standard input and checking it (strcmp compares two strings, and returns 0 if strings are equal, or a number that is not equal to zero if they are not):

```
int getPassword() {
1:    int isCorrect = 0;
2:    char password[12];
3:    printf("Enter your password > "); gets(password);
4:    if(strcmp(password, "C0m301-Adm1N") == 0) isCorrect = 1;
5:    return isCorrect;
}
```

Consider the following fuzzing strategy: a fuzzer generates and feeds strings composed of multiple " characters (null string terminators), of length up to 15. Is this strategy able to uncover a vulnerability? If yes, identify which vulnerability and explain why the fuzzer finds it. If not, propose an alternative approach to test (may or may not be fuzzing) that uncovers a vulnerability. Explain why your approach would find that vulnerability.

8 PDFuzz

Alice has developed a PDF viewer. She has decided to test this software to find security issues and decided to use fuzzing to automate it. 1) Does Alice need to use a generation-based fuzzer or a dumb fuzzer can cover the program? Justify your answer. 2) How about black-box fuzzing vs white-box fuzzing? Is it necessary to give the fuzzing team access to the code? Justify. Note: The pdf file format is public and anyone can read and use it.

9 Choice

Alice has created a start-up that provides e-voting over a central server. Alice is worried about security vulnerabilities in the e-voting server. She has only heard about address sanitizer and semantic analysis. Alice wants to use these as protections when deploying her e-voting server to handle an important election and process votes in real time. She asks you for advice on whether these measures are useful in her scenario. Do you think she should use any of these measures? Justify.

Some bugs can only be detected by either an address sanitizer or by semantic analysis. Give one example for each direction (only detectable by an address sanitizer, and only detectable by semantic analysis) and justify.