Contents

EXERCISE 1

Security of Technical Systems in Organizations

This chapter includes hands-on exercises with accompanying solutions. The purpose is for students to try the exercises on their own or in a lab setting. These exercises help clarify many concepts related to the topic area. They can be used in conjunction with Chapters 1 and 2 of the accompanying book.

Exercise: File Protection Using Encryption

Fileverifier++ is an encryption-based file protecting utility. It can help detect unauthorized edits on your files via widely used encryption algorithms, such as the SHA family. It can be downloaded for free from https://sourceforge.net/projects/fileverifier/. Answer Questions 1 to 3 using Fileverifier++.

Question 1

Warm-up—Routine verification of file content

1. Create a folder named "testfolder" on your desktop.
2. Create five TXT files in "testfolder" and name them file10.txt, file20.txt, …, file50.txt.
3. Enter "abcde" in file10.txt; enter "12345" in file30.txt. Save these files.
4. Generate hash code for all the files in "testfolder" using the SHA256 encryption algorithm, and keep them under protection. What is the generated hash code for these files?
5. Now you are an unauthorized user. Add a new line "you are hacked" on the second line of file10.txt. How can you detect this edit?

Question 2

Advanced user—Verification of user-specified files

Assume that some new files are added to the folder. All the file names in the folder are in this form: fileXY.txt, where XY is a two-digit integer. Now you wish to monitor all the

files between file20.txt and file40.txt. For example, the files to monitor could be file20.txt, file40.txt, file355txt, file 28.txt, and so on. How can you make this configuration on FileVerifier++? Hint: use "Advanced Processing" on the "Operations" menu and a regular expression.

Question 3

Let's hack—Modify files without alerting the file owner

1. As the owner of file20.txt, protect this file using SHA256. Then, save the protection status in "status.csv" on the desktop via "File -> Save Results…" and exit Fileverifier++. You will come back tomorrow morning and fully rely on Fileverifier++ to check if anyone has modified the file at night.
2. Switch your role to that of a hacker. You have secretly logged on to the computer and found out that the protection status was saved in "status.csv". Add a new line "you are hacked" to file20.txt.

How can you erase any evidence of your unauthorized actions so that the owner will not find out what you did using Fileverifer++?

Answer 1

1. Right-click on the desktop and select "New -> Folder" to create a new folder and name it "testfolder".
2. Double-click the folder, right-click on the folder widow, and select "New -> Text Document" to create a new TXT file. Name it file10.txt. Repeat this step to create file20.txt to file 50.txt.
3. Double-click each of these TXT files to edit them in a text editor. Enter the strings required by Question 1, step 3, and save.
4. Start Fileverifier++: enter "FileVerifier++" on the search bar and select "Fileverifier++" on the Best Match.
5. Click "Algorithms" on the menu bar and choose "SHA256" on the drop-down menu.
6. Click the "Dirs" button and choose the "testdir" folder. The files in "testdir" will appear on the screen. The path, hash code, and some other information are displayed, as shown in Figure 1.

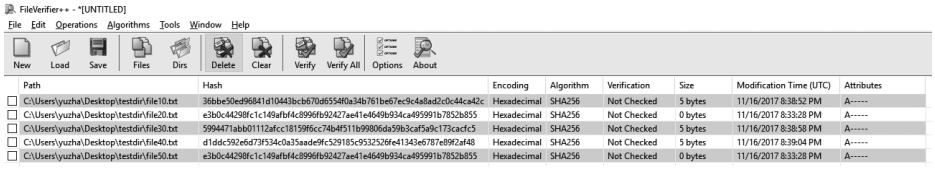

Figure 1. FileVerifier++

7. Open file10.txt and add "you are hacked". Save the file.
8. Verify the integrity of the files: Switch back to FileVerifier++. Click the "Verify All" button, and click OK on the "Check Tree" window.
9. You can see that the item for file10.txt is colored red. This means FileVerifier++ has detected the edit from step 7.

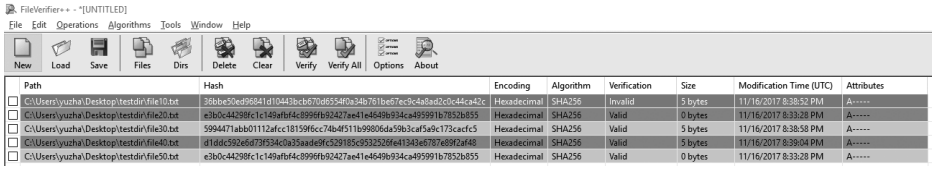

Figure 2. FileVerifier++

Answer 2

1. Select the "Operations" menu and choose "Advanced Processing…".
2. On the "Advanced Processing" window, click the "Browse…" button and select the "testfolder" you created.
3. Choose "Files matching regular expression:" and enter the regular expression "file[2-4][0-9]\.txt", as shown in Figure 3. Click the button "Add to list" and then "OK".
4. All the files between file20.txt and file40.txt will appear on the list.

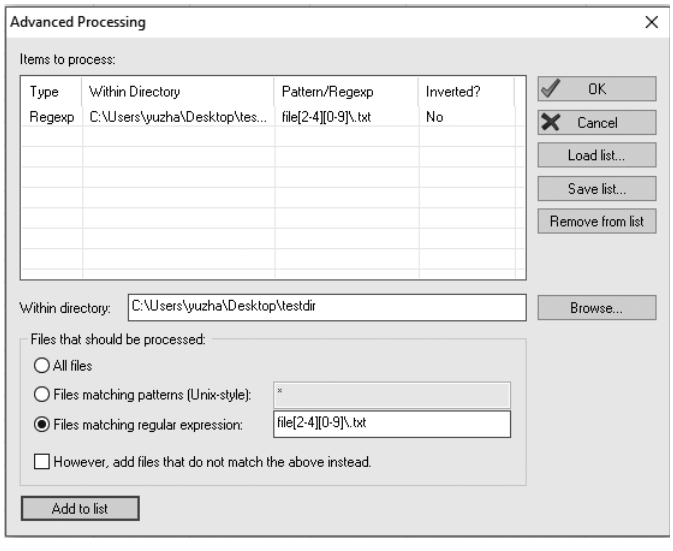

Figure 3. Advanced processing

Answer 3

1. As an owner: Click the button "Save" and choose the desktop as the save location. Enter "status" as the file name and choose "(.CSV)" as the file type. Click "OK" to save the protection status.
2. Close FileVerifier++.
3. As a hacker: Open "file20.txt" in "testfolder" and enter "you are hacked" on a new line. Save the file and close the editor.
4. Start FileVerifier++ and click the "Files" button. Select "file20.txt", which you just edited, and click "OK".
5. Choose "Algorithms->SHA256" as the Hash algorithm. Click "Verify All" and then "OK". The file "file30.txt" should appear green on the file list.
6. Follow step 1 to save the current protection status. This time, save the status in "status_hacker.csv" on the desktop. Close FileVerifier++.
7. Open "status.csv" and "status_hacker.csv" on the desktop. Comparing the content of the files, you can see that the information of "file30.txt" is different on these status files.
8. To clean up any evidence of your unauthorized edit, select and copy the line for "file30.txt" on "status_hacked.csv". Delete the line for the same file on "status.csv" and paste what you copied from the "status_hacked.csv". This should result in something like in Figure 4. Exit FileVerifier++.
9. To further clean your footprints, delete "status_hacker.csv".
10. As an owner: Routinely check if anyone edited your protected files. To do this, start FileVerifer++. Load the protection status you saved last time by clicking the "Load" button and selecting "status.csv" on the desktop. Click "Verify All" and "OK". Now, all three files should be colored green, meaning that the software failed to detect the new line added by the hacker.

```
testdir\file20.txt,0,11/16/2017 20:33:28,A-----,SHA256,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
testdir\file30.txt,21,11/17/2017 04:52:36,A-----,SHA256,8c51799b61e206ddf60842fd572cb68d20f8eff89f2fb9c7ddba304505209a3b
testdir\file40.txt,5,11/16/2017 20:39:04,A-----,SHA256,d1ddc592e6d73f534c0a35aade9fc529185c9532526fe41343e6787e89f2af48
```

Figure 4. Advanced processing

Discussion Questions

Critical Infrastructure Protection

As communities become more reliant on information technology, they are also becoming susceptible to attacks. In particular, critical cyber infrastructures are at risk. However, because of the interdependence of the critical infrastructures, there is a pressing need to develop a group centric (involving different infrastructures) framework, which can help improve threat management and incident response.

1. Discuss if it is possible to develop such a framework.
2. What formal methods can be modified or developed further to ensure critical infrastructure protection.
3. Consider a scenario, such as health care, and suggest how such a framework could be used.

Points to Consider

There are no right or wrong answers. Students will have to apply abstract concepts to real issues. More discerning students will possibly consider the classic models and evaluate their applicability to the world of interconnected cyber infrastructures. Some students may use utility companies as an example.

Instructors may find the following article useful: W. Zhao and G. White, "Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security," in Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS) (New York: IEEE, 2014), pp. 1987–96.

Formal Methods and Their Applicability

There is some controversy surrounding the use of formal methods in cyber security management. Most researchers consider formal methods to be highly successful in the context of safety-critical systems. There are claims that much of this success comes from the deployment in regulated industries. With this in mind:

1. Discuss if formal methods are more well-suited in highly regulated environments (e.g., military, health care, or not).
2. Evaluate if assurance through formal methods is more of a compliance issue or that of self-governance.

Points to Consider

As noted previously, there are no right or wrong answers. Students will have to apply abstract concepts to real issues. Instructors may find the following article interesting and useful: J. Voas and K. Schaffer, Whatever Happened to Formal Methods for Security? Computer, 49(8; 2016), 70. (Also available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5120363/.)