Stony Brook University

CSE331: System Security Fundamentals

Assignment 5: Side Channels & Steganography

This assignment includes a series of Capture the Flag (CTF) challenges. Each task involves performing analysis on a toy file. In each task, your goal is to extract a secret flag.

Notes

- You will need to provide documentation on how you solved each task.

Task 1: Find the encoded message in 1.bmp

Hint: Look for two null bytes.

Task 2: Find the encoded message in 2.wav

Hint: Did you know you can visualize sound?

Task 3: Find the encoded message in 3.bmp

Hint: Look at pixels more carefully.

Task 4: Find the encoded message in 4.gif

Hint: You should be able to find the password in the end.

Task 5: Find the encoded message in 5.wav

Hint: SOS . . . - - - . . .

Task 6: Find the encoded message in 6.jpg

Hint: Bacon is delicious, unless it's a cipher.

What to submit

Submit a tarball to Blackboard, using your student ID number as its name (e.g. "123456789.tar.gz"). The tarball should contain:

- A report, describing your codes and how you accomplished each task in PDF format titled "**report.pdf**".
- a folder titled "**code**", which includes all the codes you developed to accomplish each task. Code file names should start with "**task[N]-**" (e.g., task1-solver.py, task2-reader.py, task2-code.py) where N is the task number the code is used on. **Unlike the previous homework, it's not mandatory to develop code for each task.**
- Shell script to run each of the tasks you have code for. These files should be named "taskN.sh" where N is the task number (e.g., "task1.sh").
- A text file titled "**flags.txt**". The text file should include 6 lines of text, each containing the flag for the associated task.

Lateness

Assigned work is due on 11:59PM on the dates listed in the class calendar. We strongly recommend that you get started early. Late submissions will be penalized by 10% of the maximum attainable score, plus an additional 10% every 4 hours until received. The instructors may grant individual extensions, but only under extraordinary circumstances.

Collaboration

Acts of cheating, plagiarism, and unacceptable collaboration will be reported to the Academic Judiciary. Cheating is when you copy, with or without modification, someone else's work that is not meant to be publicly accessible. Plagiarism is the practice of taking someone else's work or ideas and passing them off as one's own without providing attribution. Unacceptable collaboration is the knowing exposure of your own solutions, or the use of someone else's answers or solutions.

At the same time, we encourage students to help each other learn the course material. As in most courses, there is a boundary separating these two situations. You may give or receive help on any

of the concepts covered in lecture. You are allowed to consult with other students about the conceptualization of a project, or the general approach for solving problems. However, all work, whether in scrap or final form, must be done by you.

If you have any questions as to what constitutes unacceptable collaboration or exploitation of prior work, please talk to an instructor right away. You are expected to exercise reasonable precautions to protect your own work, including not posting solutions publicly.