CS 491/591 Security and Privacy Spring 2010 Lab 3b

80 points (30 for the hypothesis testing, 30 for OpenOffice forensics, and 20 for your thoughts on Roger's talk). Lab 3a was 20 points of lab 3.

Assigned: 16 April 2010

Due: Monday, 3 May 2010, at 11:59pm

The purpose of this lab is to explore the nature of information and the trails and clues it leaves behind.

You will turn in a single *.pdf with all three parts as part of the same document (divided into sections). This lab is an individual effort, you may talk about it with your classmates at a high level only.

Part I: Hypothesis testing (30 points)

I will provide you with the sanitized data (no identifying information, other than your handwriting) from lab 3a for students that were willing to share their submissions. I'll give you the *.pdf's and a text file with the numbers transcribed. Your job is to identify the cheaters. You need to use statistical hypothesis testing (unless you want to argue for a different technique). Imagine that you'll need to testify to a jury and convince them that the cheaters cheated. Furthermore, the jury will need to hear a specific statement like "There's a 97.4% chance that these numbers were completely made up by the defendant."

In your writeup, you should write at least a half a page for this section. You should state clearly what your null and alternate hypothesis is and include equations. Identify the cheaters by number. You should have at least one paragraph about your thoughts on this type of digital forensics (which is used by, *e.g.*, the IRS to detect when people are making up numbers). What if the cheater knows the technique you will use? Does this make the technique totally useless and not worth forensic analysts to even learn about?

Part II: OpenOffice forensics (30 points)

I will install an OpenOffice XML dump tool on shasta and give you instructions on how to use it. We will also discuss some examples of how inconsistencies in OpenOffice metadata could be used for forensics.

Your job is to come up with an example of part of a lab for next year's security and privacy class. **I.e.**, you'll need to create one or more OpenOffice documents with some story behind them, and show how

the metadata would either confirm or refute the story in court if you were a forensics expert. The story need not be a legal one, the context could be cheating on a homework assignment or international espionage, whatever you like---don't be afraid to be creative.

Depending on the story, you may need multiple configurations of OpenOffice or perhaps OpenOffice in a virtual machine where you're allowed to change the system time, configuration, etc. All CS lab machines have OpenOffice and VNC. If you need help with additional setup (virtual machines, OpenOffice on a variety of OSes, etc.) please let me know and I'll be happy to help.

Your writeup should be at least half a page of text and contain plenty of pictures (screencaps of OpenOffice or snippets of metadata are highly encouraged in your writeup). You should tell me how you would assign what you came up with as an assignment, *i.e.*, what you would tell students up front, what they'd need to figure out on their own, what the basic story they as forensics analysts would be tasked with confirming or refuting, *etc.*

Part III: Ethics and anonymity/anti-censorship software (20 points)

Suppose you're on a team that is making a Tor-like software distribution for cell phones. Your aim is to create peer-to-peer Bluetooth network software that protesters can use to share pictures and text messages when the Internet and cell phone towers have been shut down (as occurs often during protests in many countries). The software allows protesters to broadcast their images and thoughts in a peer-to-peer fashion over Bluetooth (which has a range of maybe 50 feet), and then vote on the images and thoughts of others to have the most popular/impactful messages spread throughout the network.

Your team is moving ahead rapidly on development and marketing (it's free software, but you're planning on a marketing campaign to get cell phone users to download and use it so you can save the world ASAP). Nobody on your team is discussing the ethical issues regarding the forensic capabilities of the governments of countries where you expect the software to be used. Your teammates are very enthusiastically looking forward to disseminating the software in particular countries where they feel governments are oppressing protests. Technical meetings contain many comments where team members express desire to undermine particular governments around the world. You feel like they are rushing the release of the software and misrepresenting the protections the software provides, especially regarding the threat of protesters' cell phones being physically confiscated.

Write a one-page (at least) memo to your teammates describing what you feel is a discrepancy between what protections the software provides and what protections the marketing campaign promises. You should focus on forensics issues and the threat of cell phones being physically confiscated, but you can certainly discuss other issues, too, if you wish. You should also include a paragraph describing what you believe the role of people developing software such as this should be. Is it necessary to remain apolitical? To what degree are you and your teammates responsible when protesters are jailed or worse as a result of using your software (either directly or indirectly)? Is writing technical papers about the limitations of your software and releasing it as open source enough, or do you have a greater responsibility to educate less technical folks about your software and what it will and will not do? Feel free to make up any specific facts you like as long as you follow the basic storyline.