CMPT 542
Midterm Exam
Fall 2016
November 7th, 2016

Instructions: Read carefully through the entire exam first, and plan your time accordingly. Note the relative weights of each segment.

This exam is partially open-note. You may refer to printed copies of the assigned research papers as well as print-outs of your summaries.

Write your answers on this exam. You may only write on one side of the page.

Make sure that your answers are of sufficient depth to justify 30 minutes of work per question. Answers without sufficient depth will not receive full credit.

When you are done, present your completed exam to the instructor at the head table. If leaving before the exam period is concluded, please leave as quietly as possible as a courtesy to your neighbors.

Name:

Student ID Number:

Signature:

1. (30 points) [Mandatory]

   Discuss how the results obtained in "Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem" by Cangialosi et al. support or refute the conclusions drawn by Ross Anderson in "Why Cryptosystems Fail". Make sure your discussion is very specific to those papers and includes specific examples from both.

Solution: There are a variety of possible answers here. A good answer will...

- Demonstrate a good understanding of both papers, meaning that incorrect information is not included.
- Make sound, reasoned arguments that are well justified by referencing points made in the papers.
- Discuss the fact that WCF was about highlighting an incorrect threat model, and PFS demonstrates a real scenario of the threat model being different than expected.
- Make note of the fact that in PKS it seems that the outsourcing actually improved security. This point could tied into WCF in two different ways: It refutes the WCF idea that outsourcing your security is a bad idea; it supports the WCF idea that having experts involving in your security is a good idea.
- Not include incorrect or unclear information.

Grading:

- 27-30: Excellent understanding of both paper. Excellent discussion of the ways that PKS supports or refutes WFS, with at least two major points and a few minor points. No factual errors or crucial omissions.
- 24-26: Similar to above, but with some minor factual errors or omissions.
- 21-23: Similar to above, but with some major factual errors or omissions or demonstrated misunderstandings of the core papers involved.
- Lower: Lack of basic understanding of the papers, the question, etc.

2. (30 points) [Mandatory]

In cryptography, we design algorithms using Kerckhoffs principal: Namely the algorithm is made publicly available and should be peer-reviewed, but the key is kept secret. Discuss how the principals discussed by Bruce Schneier in "Secrecy, Security, and Obscurity" should or should not be applied to Steganography.

Solution: There are a variety of possible answers here. A good answer will...

- Demonstrate a good understanding of both papers, meaning that incorrect information is not included.
- Make sound, reasoned arguments that are well justified by referencing points made in the papers.
- Not include incorrect or unclear information.
- Discuss some of the differences between cryptography and steganography that are relevant to the argument. One example is that steganography has the stated intention of ensuring no one knows it is there, while crypto does not.
- Discuss the specifics of Schneier's arguments that are and/or are not valid for Steganography. For example, two good points could be about:(1) Whether or not there is a body of experts able to evaluate the work; and (2) Whether or not there are others working on the same side that would benefit from learning from the mistakes of others.
- Justify the main argument in a coherent way.

Grading:

- 27-30: Excellent understanding of both paper. Excellent discussion of how and why Schneier's arguments about crypto do or don't apply to steg. No factual errors or crucial omissions.
- 24-26: Similar to above, but with some minor factual errors or omissions.
- 21-23: Similar to above, but with some major factual errors or omissions or demonstrated misunderstandings of the core papers involved.
- Lower: Lack of basic understanding of the papers, the question, etc.

3. (30 points) [Optional: You must answer *either* Question 3 **or** Question 4]

   Imagine that a major local bank hires you as a consultant to help them improve the security of their users' passwords. Based on the results found in "The science of guessing: analyzing an anonymized corpus of 70 million passwords", what would you recommend the bank do in order to help their users increase the security of their passwords? Each of your recommendations should be justified by the paper's results.

Solution: There are a variety of possible answers here. An answer should demonstrate knowledge of the following:

- Demonstrate a good understanding of the paper's results.
- Make sound, reasoned arguments that are well justified by referencing results in the paper.
- Not include incorrect or unclear information.

Grading:

- 27-30: Makes 3-5 really good recommendations that are strongly and explicitly justified by the paper. No factual errors or crucial omissions.
- 24-26: Similar to above, but with some minor factual errors or justifications that could be justified by the paper, but weren't in the essay.
- 21-23: Similar to above, but with some major factual errors or recommendations were not justified by the paper.
- Lower: Lack of basic understanding of the papers, the question, etc.

4. (30 points) [Optional: You must answer *either* Question 3 **or** Question 4]

   In "Secure Ranked Keyword Search over Encrypted Cloud Data" the threat model is a modified version of the threat model used by other works on searchable encryption. Write a discussion of this new threat model: In what ways is the threat model different from the related work, why were the changes made, and how did the authors justify those changes? Do you think that changes are legitimate? Why or why not?

Solution: There are a variety of possible answers here. An answer should demonstrate knowledge of the following:

- Discuss the threat model of SSE, namely an honest but curious server who is able to see the search patterns.
- Discuss the changes to the threat model, namely that under ranked SSE the server also sees the rankings of the encrypted results.
- Discuss that the changes were necessary in order to add the functionality of ranking, which is exactly how the authors justified them.
- Gives a well-reasoned opinion of whether the changes are legitimate.

Grading:

- 27-30: A strong argument (see above) with no factual errors or omissions.
- 24-26: Similar to above, but with some minor factual errors or omissions.
- 21-23: Similar to above, but with some major factual errors or omissions or demonstrated misunderstandings of the core paper involved.
- Lower: Lack of basic understanding of the papers, the question, etc.