CMPT 542
Midterm Exam
Spring 2015
April 21st, 2015

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 from the cryptography slides.

Write your answers on this exam. You may use both sides of the page.

When answering questions that request an explanation, keep your explanation short and correct. Explanations containing incorrect information will be marked wrong, even if correct information is also included.

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. (20 points) The current public key infrastructure for HTTPS relies on a system of trusted authorities to verify identities and sign public keys associated with a domain name. Recently, investigations have shown that there are well over 250 trusted certificate authorities worldwide. This is causing researchers to consider the need for designing a PKI system for HTTPS that does not rely on trusted central authorities. Is the Perspectives system a suitable replacement? Why or why not?

Solution: There are many possible answers to this question. A good solution will have the following characteristics:

- Recognizes that perspectives still has a trusted authority, namely the notaries. (But this is different from trusting 150 different CAs.)
- Demonstrate a good understanding of how Perspectives works by discussing the notaries, the fact that the binding of a key to host is based on network observations, and that the client can make its own trust decisions based on the information.
- Demonstrate a good understanding of how the traditional PKI model works for HTTPS, based on a CA making the key to hostname binding decision.
- Making sound, reasoned argument for their answer to the question.
- Not including incorrect information.

Grading was in the following ranges:

- 19-20: Excellent understanding of Perspectives and the existing model. Excellent discussion of why Perspectives is or is not a good replacement. No factual errors or crucial omissions. Mention that Perspectives does have centralized trust in some ways.
- 16-18: Similar to above, but with some minor factual errors or omissions.
- 13-15: Similar to above, but with some major factual errors or omissions.
- Lower: Lack of basic understanding of either Perspectives or the existing model.

2. (20 points) In *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds* the authors present a key stroke timing attack in section 8.4, but they fail to demonstrate that such an attack is practical on real systems. Do you think that publishing an unproven attack like this is a good idea or a bad idea? Give 3-5 reasons that justify your answer.

Solution: There are many possible answers to this question.

Grading was in the following ranges:

- 19-20: Three very strong, or five moderately strong points. All points should be without factual errors and relevant to the question.
- 16-18: Similar to above, but without strong enough points or some minor factual errors or omissions.
- 13-15: Similar to above, but without strong enough points and/or some minor factual errors or omissions.
- Lower: Lack of basic understanding of the question topic.

3. (25 points) Imagine you are writing the proposal for the structure of a development team tasked with designing a secure DRE voting system. Write an essay discussing how open you should be with the design process. Discuss the positives and negatives of being open, and make recommendations for how open you think the process should be. Be sure to back up your recommendations with a discussion of the specific problem domain (DREs and electronic voting) as well as a references to the criteria for openness developed by Bruce Schneier in *Secrecy, Security, and Obscurity*.

Solution: There are many possible answers to this question. A good solution will have the following characteristics:

- Discusses potential downsides of openness such as attackers being able to analyze the system, how it is used, etc. (Includes specific examples related to voting.)
- Discuss potential upsides of openness such as experts being able to verify the design of the system as whole, the cryptography (which is hard to get correct), etc. (Includes specific examples related to voting.)
- Makes justified recommendations for what should really be done.

Grading was in the following ranges:

- 23-25: Excellent discussion of upsides and downsides without any factual errors or obvious omissions. Makes excellent, well reasoned recommendations.
- 20-22: Similar to above, but including some minor errors or weaknesses.
- 17-19: Similar to above, but including some major errors or weaknesses.
- Lower: Lack of basic understanding of the question topic.

4. (35 points) Write a letter to the developers/designs of the Diebold voting system discussed in *Analysis of an Electronic Voting System*. In your letter, summarize for them the relevant results from *Why Cryptosystems Fail* that you believe should have better informed their design and implementation decisions. In addition, give them a list of recommendations that they should use going forward in designing future DRE systems.

Solution: There are many possible answers to this question. A good solution will have the following characteristics:

- Provides an overview of relevant points from *WCF*, including things like design of cryptography by experts, evaluating the system with the people who will actually use it, etc.
- Provides recommendations for the future or DRE systems, such as bringing in experts to design the cryptography, evaluating the system with actual poll workers and voters, etc.

Grading was in the following ranges:

- 32-35: Excellent answers addressing the above points without any errors.
- 28-31: Good answers with only minor errors or omissions.
- 25-27: Reasonable answers with some errors or omissions.
- Lower: Lack of basic understanding of the question topic.

End of Exam.

Don't write anything in here.

Page	Points	Score
1	20	
2	20	
3	25	
5	35	
Total:	100	