CMPT 542
Final Exam
Spring 2015
June 9th, 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. Cryptography Short Answer

   Provide short answers to the questions below. You answers should be **1-2 sentences at most**.

   (a) In Section 6.1 of *How to 0wn the Internet in Your Spare Time* the authors propose an improved worm that uses public key cryptography to validate commands sent from the bot master.

      i. (4 points) Why would this make a worm more powerful than one that doesn't include signed commands?

      > **Solution:** It would prevent other people from being able to send commands to the worm, because they can't sign their commands with the correct key.

      ii. (2 points) Why use public key cryptography for the signing instead of symmetric key cryptography?

      > **Solution:** If you use symmetric key signing, then someone could analyze your worm, extract the key, and use it to send valid commands.

   (b) (4 points) Why is it important that Tor incorporates Perfect Forward Secrecy into its design? (In other words, what attack does PFS stop.)

   > **Solution:** If a Tor router is compromised, the keys it knows can't be used to decrypt past traffic.

2. (25 points) Discuss how the techniques from *Tor* could be used to enhance the security of the *Perspectives* system. Be sure to emphasize exactly which aspects of Perspectives could be improved with specific Tor technologies and how those improvements would improve the security of Perspectives as a whole.

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

- Tor is about anonymity. Primarily anonymity for the client from the server, but also possible anonymity of the server (hidden services).
- There are two connections in Perspectives between a client and the perspectives system: Client → Notary Authority and Client → Notary Server.
- Tor could provide privacy for a user by making sure that the NS can't tell which clients are looking up certs for which domains.
- Tor could provide privacy for a user by making sure that the NA can't tell which clients are using the system.

Grading:

- 5 points for each point above properly addressed.
- 5 points for the overall quality of arguments.

3. (25 points) *Why Cryptosystems Fail*, published in 1993, gave us tremendous insight into security failures in the banking industry as well as recommendations for how to avoid those failures in the future. 20 years later, the same author published both *Why Payment Systems Fails* and *Chip and Skim: cloning EMV cards with the pre-play attack*.

   Write an essay discussing how well the advice given in WCF was taken by the financial industry in the design of EMV. Be sure to discuss ways in which the advice was taken *and* ways in which it was not.

Solution: This answer has two important parts:

1. A discussion of WCF recommendations that were taken.
2. A discussion of WCF recommendations that obviously weren't taken.

Grading:

- 10 points for the discussion of taken recommendations.
- 10 points for the discussion of not-taken recommendations.
- 5 points for the overall organization and clarity of the essay.

4. (25 points) In *Chip and Skim* the authors layout the technical requirements for two types of attacks. However, to really pull off the attacks would involve both technical issues and social engineering. Discuss the social engineering components that would be required for a real attacker to pull off each type of attack.

Solution: This answer has two important parts:

1. A discussion of social engineering techniques required to pull off the preplay attack with back UNs. (Implementation flaw.) This could discuss things like how to find machines with predictable UNs, how to harvest auth requests from valid cards, etc.
2. A discussion of social engineering techniques required to pull off the preplay attack that involves altering the UN in transit between the terminal and the bank (Protocol flaw.) This mainly includes discussing how to get access to perform the MITM attack.

Grading:

- 10 points for the discussion of social engineering required for the preplay attack with bad UNs.
- 10 points for the discussion of social engineering required for the protocol flaw.
- 5 points for the overall organization and clarity of the essay.

5. (15 points) Describe three significant ways that your understanding of security and security research has been impacted as a result of the readings you did for this course. Be specific in your answers, and cite relevant papers when discussing what you have learned.

Solution: Here I am just looking for three well reasoned things learned that are properly cited and discussed in the papers we read. This question is really testing how well the student can articulate and backup what they learned.

Grading: 5 points per way. (The question asked for three ways the student has been impacted.)

End of Exam.

Don't write anything in here.

Page	Points	Score
1	10	
2	25	
5	25	
8	25	
11	15	
Total:	100	