Quiz 2

Fall 2013 – EECE 512 – UBC

October 24, 2013

Candidate's name:
Candidate's student number:
Candidate's signature:

Remarks

1. No books, notes, or any other devices with text storage or communication capabilities are allowed.
2. Be brief and to the point.
3. **There are four questions on this quiz. Each question is 5 points.**
4. The maximum score possible on this quiz is 20.
5. *The duration of this quiz is 45 minutes.*

This page left intentionally blank.

1. **Name at least three ways of evading bot classification proposed in "Detecting Automation of Twitter Accounts . . . " and briefly explain the difficulties an adversary would face while evading the classification scheme using those ways?**

   Sample Answer:

   - An adversary can use a "manual" device for twitting but this is impractical for automated tweets.
   - A bot can increase timing entropy at the expense if tweeting frequency.
   - A bot could intermix spam with ham tweets to dilute spam density.

   □

2. **Explain the main difference between attacks reported in "The final nail in WEP's coffin" and "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication". Particularly, what was done new in the latter work that was not done in the former one?**

   Sample Answer: The main difference between the two, is that the attack on WPA Enterprise Authentication used multiple layers, including the WiFi UI on commodity OSs.

   □

3. **Explain the intuition behind the two breaches of privacy (from "New Privacy Issues in Mobile Telephony …"), which expose a subscriber's identity and allow an attacker capable of sending and receiving messages on the air to identify the presence of a target mobile phone in a monitored area, or even track its movements across a set of monitored areas.**

   Sample Answer:

   - **IMSI Paging Attack**: The possibility of triggering a paging request for a specific IMSI allows an attacker to check a specific area for the presence of mobile stations of whom he knows the identity, and to correlate their IMSI and TMSI.
   - **AKA Protocol Linkability Attack**: An active attacker just needs to have previously intercepted one legitimate authentication request message sent by the network to the victim phone. The captured authentication request can now be replayed by the adversary each time it wants to check the presence of the phone in a particular area. On reception of the replayed authentication challenge and authentication token (RAND, AUTN), the victim phone successfully verifies the MAC and sends a synchronization failure message. However, the MAC verification fails when executed by any other mobile station, and as a result a MAC failure message is sent.

□

4. **What are the main four contributions claimed by the author of “Analyzing an Anonymized Corpus of 70 million Passwords”?**

Sample Answer:

(a) Formalization of improved metrics for evaluating the guessing difficulty of a skewed distribution of secrets, such as passwords, introducing α-guesswork as a tunable metric which can effectively model different types of practical attack.

(b) A novel privacy-preserving approach to collecting a password distribution for statistical analysis. By hashing each password at the time of collection with a secret key that is destroyed prior to our analysis, we preserve the password histogram exactly with no risk to user privacy.

(c) Adaptation of techniques from computational linguistics to approximate guessing metrics using a random sample. The paper parametrically extends the approximation range by fitting a generalized inverse Gaussian-Poisson (Sichel) distribution to the data.

(d) An application of the above methods the analysis of a massive corpus representing nearly 70 M users, the largest ever collected, with the cooperation of Yahoo!. The authors analyzes the effects of many demographic factors.

□