EECE 571B, Spring 2012

Quiz #1 Key

March 6, 2012

This quiz consists of 11 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: _____

Your Given name: _____

Your student ID: _____

Name of your left neighbor: _____

Name of your right neighbor: _____

#	Points	Out of
1		5
2		5
3		5
4		5
5		5
6		5
7		5
8		5
9		5
10		5
TOTAL		50

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. **What are the four most prominent characteristics of malicious Sybils in Renren OSN, that were used for detecting them? Briefly describe each characteristic, i.e., how that characteristic was different for malicious Sybils vs. legitimate accounts.**

1) Invitation frequency: Sybils were much more aggressive in sending friendship requests than non-Sybils.
2) Outgoing requests accepted: Regular users had much higher acceptance rate than Sybils.
3) Incoming requests accepted: Sybils were nearly uniform in accepting all incoming friendship requests.
4) Clustering coefficient: non-Sybil users had cc values orders of magnitude larger than Sybils.

2. **Based on finding of Monarch authors, how are e-mail spam and tweet spam compared?**

- They overlap little in the features
- E-mail spam is marked by much shorter lived features compared to tweet spam
- Tweet spam uses URL redirects much more often than e-mail spam.

3. **a) What are the main differences between the approach in the adaptive password-strength meter (APSM) proposed by Castelluccia et al. and such meters as the one by Microsoft?** (Hint: this question is about the difference in the ideas, rather than characteristics of the approaches.)
   b) List advantages and disadvantages of the above two approaches, as compared to each other.

a) The approach by Castelluccia et al. outputs the password's score that approximates the guessability of the password in relation to the other passwords in the password database, that is, the frequency of password's n-grams in the dataset comprising n-grams from the database. Whereas, password strength meters, like the one by Microsoft, only check if the password meets the pre-set rules, independently of the other passwords used in the system.

b) Microsoft's meter:
   i) Easy to implement as a dowloadable JavaScript without the need to communicate with the server.
   ii) Does not require knowledge of the other passwords in the system or their characteristics.
   iii) Has no risk of system passwords being compromised because of the server compromise.
   iv) Can flag hard to guess passwords as weak and easy to guess passwords as strong, thus confuse/annoy the users.

   APSM:
   i) Has non-negligible risk of helping the adversary to guess passwords in the system, if the dataset with password n-grams is compromised.
   ii) Is much more (than Microsoft's) precise in assessing the easy of a password candidate being guessed by a rationale adversary, thus provides better feedback to the users, when they pick new passwords.

4. **List the key differences between the original Encrypted Key Exchange (EKE) proposal by Bellovin and Merritt and the original SRP proposal by Wu.**

   1. EKE suffers from plaintext-equivalence, i.e., it is vulnerable to off-line attacks on the password database if it's leaked from the server and SRP is not.

   2. EKE uses symmetric and public key cryptography and SRP does not.

5. **a) Define "detection rate" and "Bayesian detection rate" in the context of intrusion detection.**
   b) Based on the findings of Axelsson (i.e., "The base rate fallacy …" paper), what's the main factor limiting the performance of an IDS?

   a) Detection rate is $P(A|I)$, i.e., the rate of true positives. Bayesian detection rate is $P(I|A)$, i.e., the rate of alarms that really indicate an intrusion.

   b) The factor limiting the performance of an IDS is not the ability to identify behavior correctly as intrusive, but rather *its ability to suppress false alarms.*

6. **Summarize the pure fragmentation attack from "The Final Nail in WEP's Coffin" paper that allows an adversary to decrypt any packet on a WEP-protected network, when it's connected to the Internet.**

    1. The attacker eavesdrops one data packet and recovers eight bytes of keystream because the first eight bytes of clear-text are known and the cipher-text has been intercepted.
    2. The attacker uses 802.11 fragmentation for transmitting data of up to 64 bytes. IP fragmentation may be used on top for sending larger packets.
    3. The attacker eavesdrops the encrypted packet of interest.
    4. She then uses IP fragmentation to simply prepend an additional IP header to the front of the eavesdropped packet and send the result to the host on the Internet controlled by her.
    5. Upon reception, the AP will decrypt both the new header and the original packet x, and reassemble them into a single packet. If the new header contains an Internet address, the AP will send the packet there in clear-text
    6. If the attacker controls the Internet host the packet was sent to, he can recover the clear-text of x.

7. Describe the adversary model in the fragmentation attack from the previous problem.

The adversary's objective is to decrypt eavesdropped packets in a WEP-protected WiFi network connected to the Internet.

Adversary's capabilities:

Before the attack:

1. Knows content of the first 8 bytes of packets sent in the network,

During the attack:

2. Eavesdrops packets in the network,
3. Sends packets to the network,
4. Controls a host on the Internet reachable from the target WiFi network,
5. Knows the IP address of the outside host, which it controls,
6. Knows or can obtain the router's MAC address.

8. a) Summarize the idea of the countermeasure that the authors of the *optimistic* acknowledgment (opt-ack) DoS attack ("Misbehaving TCP Receivers …") propose.

b) Explain why it does not harm much the communications with benign clients and helps detect malicious clients.

a) They propose that the server randomly *skip* sending the current segment, and instead send the rest of the current window.

b) A benign client that actually gets all of the packets, except the skipped one, will start re-ACKing for the lost packet, thereby invoking the fast retransmit algorithm. Given that most modern TCP stacks implement selective acknowledgments, this solution is very efficient. The only penalty applied to a conforming client is a single round trip time in delay. On the other hand, a malicious client cannot tell the difference between an intentionally dropped packet and a packet dropped in the network by congestion. Thus, an attacker will ACK the skipped packet, alerting the server to the attack.

9. a) Define acronyms MAC and HMAC and explain the difference(s) between MAC and HMAC, as applications of hash functions. No need for exact HMAC formula.

b) Explain how one can use public key crypto to sign a message and to verify a signed message.

a)
MAC – message authentication code
HMAC – hash-based MAC

MAC(m) = h(m)
For computing HMAC, one has to provide to the hash function not only the message m but also a (presumably secret) key K.

b)
To sign a message m with private key K_D, one produces tuple (m, s), where $s = E_{K_D}(m)$.
To verify signature s for message m, one computes $m' == E_{K_E}(s)$ and compares m' with m, where K_E is the corresponding public key.

10. List the 10 principles of designing secure systems that were discussed in the security bootcamp.

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Duty
7. Least Common Mechanism
8. Psychological Acceptability
9. Defense in depth
10. Question assumptions