College of Computing

Georgia Institute of Technology

CS 6262: Network Security: Spring 2009

Quiz II

There are 12 questions and 8 pages in this quiz booklet (including this page). Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If I can't understand your answer, I can't give you credit! There are three pretty challenging questions (clearly marked); you may want to look through the whole quiz and save those for last.

Use the empty sides of this booklet if you need scratch space. You may also use them for answers, although you shouldn't need to. *If you do use the blank sides for answers, make sure to clearly say so!*

Note well: Write your name in the space below AND your initials at the bottom of each page of this booklet.

THIS IS AN "OPEN NOTES, OPEN PAPERS" QUIZ.
LAPTOPS ARE ALLOWS, BUT NETWORKING IS NOT.
NO ENCRYPTED WIRELESS TRAFFIC.
MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!

Initial here to indicate that (1) you've read the instructions and (2) you agree to abide by the Georgia Tech Honor Code:
The last page has easy bonus questions, which you can answer outside of the allotted time. Rip the last page off of your quiz for some bonus points and turn it in (anonymously if you like). You won't get the points if you don't tear off the page (this is to make certain you've read this far!).

Do not write in the boxes below

1-5 (xx/20)	6-10 (xx/28)	11-12 (xx/14)	Bonus (3/3)	Total (xx/65)

Name:

I Warmup

1. [4 points]: Which of the following is true about a WEP-encrypted wireless channel?
(Circle ALL that apply)

- **A.** Without knowing or recovering the WEP key, an attacker can send arbitrary messages on the wireless channel.
- **B.** WEP's use of a CRC checksum makes it more vulnerable to replay attacks.
- **C.** WEP's reuse of initialization vectors makes it more vulnerable to known plaintext attacks.
- **D.** Without knowing or recovering the WEP key, an attacker can masquerade as any other sender on the wireless channel.
- **E.** None of the above.

Answer 1 The answer is: (A), (C), (D). ■

2. [4 points]: Which of the following is true about DNS cache poisoning?
(Circle ALL that apply)

- **A.** A cache poisoning attack requires the attacker to correctly guess the transaction ID for the DNS query.
- **B.** The Kaminsky DNS cache poisoning attack allows an attacker to poison the records for an arbitrary second-level domain in the local resolver's cache.
- **C.** Setting shorter TTL values on NS records and A records on valid DNS responses makes it more difficult for an attacker to mount a cache poisoning attack.
- **D.** Randomizing the source port of the DNS queries from the local resolver makes it more difficult for an attacker to mount a cache poisoning attack.
- **E.** None of the above.

Answer 2 The answer is: (A), (B), (D). ■

3. [4 points]: To maximize the likelihood of being able to mount a man-in-the-middle attack against some IP prefix $130.207.0.0/16$ using BGP route hijacking, which of the following route announcements should the attacker announce?
(Circle ALL that apply)

- **A.** Two route announcements for $130.207.0.0/17$ and $130.207.0.128/17$.
- **B.** One route announcement for $130.207.0.0/16$.
- **C.** One route announcement for $130.207.0.0/15$.

Initials:

D. One route announcement for 0.0.0.0.

E. None of these will ever be effective.

Answer 3 The answer is: (A). ■

4. [4 points]: Which of the following is true about various traffic monitoring techniques?
(Circle ALL that apply)

A. Flow monitoring technology such as Cisco NetFlow provides sufficient statistics about traffic flows to detect a traffic flooding attack.

B. SNMP counters on routers are typically sufficient to detect a traffic flooding attack.

C. SNMP counters on routers count packets per flow.

D. A attack flood of small packets could cause the router to generate more traffic as a result of flow reports than the attack itself.

Answer 4 The answer is: (A), (B), (D). ■

5. [4 points]: Which of the following is true about cross-site scripting (XSS) attacks?
(Circle ALL that apply)

A. All XSS attacks can be prevented by disabling Javascript.

B. All XSS attacks can be prevented by never echoing user input back to the browser in a script.

C. An XSS attack might trick a client browser into divulging a user's authentication token to a third-party site.

D. A user might fall victim to an XSS attack simply by visiting a page, without ever even clicking on a link or entering data into a form.

E. All of the above.

Answer 5 The answer is: (B), (C), (D). ■

Initials:

II Potpourri

6. [4 points]: In S-BGP, route attestations from AS A to AS B include a signature for the AS path that includes B. For example, if AS A wishes to announce a route with AS path `X Y Z` to AS B, the route announcement will include an attestation for the path `X Y Z A B`.

Why does the route attestation need to include B? Describe in detail some attack that is possible if the route attestation did not include B.

(Answer legibly in the space below.)

Answer 6 An attacker could omit some ASes from the AS path by dropping some of the other route attestations. It could also insert additional ASes on the AS path between A and B. ■

7. [4 points]: George Burdell observes: "Since sending spam requires the spammer to complete a three-way handshake with the receiving mail server, we can simply maintain a list of known bad IP addresses and automatically reject any mail received from those IP addresses."

A. Does completion of a three-way handshake imply that the source IP address for the TCP connection is not forged? Why or why not?

B. Give two reasons why IP addresses in George's list might become stale.

(Answer legibly in the space below.)

Answer 7 Completion of a three-way handshake does not imply that the source IP address is not forged (*i.e.*, the source address could still be forged). For example, in class, we discussed a BGP route hijacking attack whereby an attacker hijacks a BGP route for some prefix and steals IP addresses contained within that IP prefix. In such a case, an attacker could complete a three-way handshake from a stolen IP address. ■

8. [6 points]: Recall from lecture that *fast flux DNS* is a common technique for hosting scam infrastructure on a botnet.

A. Explain the difference between single flux and double flux.

B. Fast-flux domains have been observed to return DNS A records for IP addresses across many more distinct $/24$ subnets than legitimate domains. Why might this be the case?

C. Studies have observed that IP addresses in scam hosting infrastructure may change roles over time. Why might an IP address that was a spammer suddenly switch to a different role, such as hosting authoritative DNS?

(Answer legibly in the space below.)

Answer 8 A single-flux network changes the DNS `A` record mappings to allow an attacker to re-map the IP address where a DNS name is hosted. Typically, single-flux is implemented with a bullet-proof DNS hosting service to host the authoritative nameservers. A double-flux network, on the other hand, typically uses bots/zombies themselves to implement the changing DNS record mappings. So, the authoritative nameservers themselves would be hosted on a botnet, and double-flux would remap the NS records (and possibly the IP addresses of the NS records).
An IP address that was a spammer might suddenly switch to a different role if it showed up on a blacklist. For example, even if a spamming IP address is listed on a spam blacklist like SpamHaus, it might still be used for other purposes (*e.g.*, hosting the authoritative nameserver for a scam domain). ■

9. [6 points]: Recall that in Problem Set 2, you implemented a fast exponentiation method. Suppose that you wanted to compute 3^{2051} using this method. (Usually such an operation is part of modular exponentiation, but please ignore the operation of taking a modulus for this problem.)

A. How many multiplications would you need to perform this computation? (Feel free to show your work.)

B. Public-key cryptography methods such as RSA rely on modular exponentiation with large exponents. Describe an attack that would be possible on RSA if encryption were performed with a small exponent.

(Answer legibly in the space below.)

Answer 9 An answer of $\lg(2048) + 3 = 14$ receives most credit (2 points). Answers that recognize that some of the computations in the initial fast exponentiation could be cached and re-used to reduce this further receive full credit.
There are a few small exponent attacks on RSA, but here is one:
`http://www.usna.edu/Users/math/wdj/book/node45.html`. ■

Initials:

10. [8 points]: Suppose a Web server on a network you are operating has suddenly come under a massive flooding-based denial-of-service attack 2^{20} distinct IP addresses. Each IP address is sending a packet stream of 1024-byte packets at a rate of 2 packets per second. In other words, you are seeing low-rate streams from a very large number of attackers.

A. What is the overall traffic rate of the attack, in gigabits per second?

B. You would like to enumerate all IP addresses in this attack. However, the only monitoring capability you have is flow monitoring, which generates a flow records based on a sampled packet stream, which samples each packet with sampling probability of $1/1000$. Suppose traffic flows all arrive roughly uniformly, and that you observe traffic for 30 minutes.

How many distinct IP addresses are you likely to capture? About how long might you have to wait to capture about 95% of all of the IP addresses in the attack? (Hint: If you know about "coupon collector" problem from your discrete math classes, that idea might help you here.)

C. Give one reason why filtering traffic from all of these IP addresses might be difficult in practice.

(Answer legibly in the space below.)

Answer 10 The overall traffic rate is $2^{20+10+3+1}$ = 16 gigabits per second.
The second part can basically be solved by applying the coupon collector idea. The first IP address will be captured in the first packet with probability 1. The second unique IP address will be captured with probability $(n-1)/n$, where $n = 2^{20}$, so the expected time to capture the second IP address is $n/(n-1)$. The expected time to capture the third packet is $n/(n-2)$, and so on. So, an acceptable way of formulating this answer would have been as follows:

$$\sum_{i=0}^{0.95n} \frac{n}{n-1}$$

One reason that filtering traffic from these IP addresses may be difficult in practice is that each individual IP address may require a separate filtering rule. In these cases, the number of filtering rules could quickly exhaust a router's resources. ■

Initials:

III Design Question: Covert Channels

After finishing CS 6262, George Burdell decides that it is time to travel to faraway lands. Because George plans to visit lands where access to various sites on the Internet might be filtered, he decides to set up a system to ensure that he is able to continue to make voice over IP calls back to his parents in the United States.

George's first design is to set up a proxy that his voice client can connect to while he is traveling. "All of my outbound calls will be encrypted and routed through my proxy in Atlanta." George writes the following function to encrypt each packet:

```
// initialization vector
char init[] = "imcovert";

// randomization
srand(0);

void* encrypt(char *plain, char *cipher, int len, char *key) {

  // copy initialization vector into IV
  strcpy(IV, init, 8);

  for (i=0; i < len; i+=8) {

     // produce 64-bit cipher block
     rc4.encrypt(plain[i], cipher[i], IV);

    // Update IV
    IV = (int)IV & (rand() % 255);
  }
}

void *sendPacket(char *buf, int socket) {

   // send ciphertext, plus initial IV in the clear
   sprintf(buf, "%s%s", init, buf);
   send(fd, buf);
}
```

Initials:

11. [6 points]: Eve Dropper says that, even if the channel between his client and the proxy is encrypted with a symmetric key known only to him and the proxy, a censor may still be able to determine when George is calling the same person repeatedly, even without knowing the key. Is she right? Why or why not?

(Answer legibly in the space below.)

Answer 11 She is correct. The encryption proceeds with the same initialization vector each time a new message is initiated, so this re-use of IVs could result in a known plaintext attack. ■

12. [8 points]: George decides that instead of relying on an encrypted channel, he will embed the packets for his voice calls into a stream of TCP traffic to a proxy, which will then extract the data from the TCP stream and send it to the destination.

George decides to use the last two bits of the TCP timestamp as a covert channel, and to delay the sending time of each packet in the stream by up to 3 seconds to achieve the correct lower two bits.

A. George designs his system to send voice traffic *in the covert channel* at about 64 kilobits per second. Given that each packet in the visible traffic stream can send two bits, and assuming that each packet in the cover traffic is 1500 bytes, what must the average rate of the visible traffic stream be, in kilobytes per second?

B. George notes that this traffic stream is rather high, and might not be entirely deniable (not to mention that it might not even be possible to send at such a high rate while on his travels). He figures that if he sends 64-byte packets in his TCP stream, he could achieve a much higher rate for his covert channel. What is the problem with this approach?

C. *Open-ended.* George thinks that he can introduce TCP sequence number gaps to send additional bits in his channel. Can you suggest a way?

(Answer on the back.)

Answer 12 At 2 bits of cover per packet, George will need to send $2^{16}/2 = 2^{15}$ packets per second to generate enough cover traffic. At 1500 bytes per packet, this is approximately 4.8×10^4 kilobytes per second.
64-byte packets may not be deniable cover traffic.
Various options here include artificially injecting losses, forcing retransmissions, etc. (various answers are acceptable). ■

Initials: