A28438 *No Calculator permitted in this examination*

UNIVERSITY OF
BIRMINGHAM

School of Computer Science

First Year – MSc Computer Science
First Year – MSc Computer Security

06 23900

Network Security

Summer Examinations 2013

Time Allowed: 1:30 hours

[Answer ALL Questions]

Turn Over

1. TCP is stateful protocol. Establishing a TCP connection involves the use of sequence numbers.

   (a) What security properties should sequence numbers have? Justify your answer briefly. **[2%]**

   (b) Describe any three attacks that can be carried out when sequence numbers do not have the necessary security properties? Discuss the probability of success in each case. **[3x3=9%]**

   (c) Propose and describe the design of a covert channel based on TCP sequence numbers. **[7%]**

   (d) Describe any two security flaws in the design of the Border Gateway Protocol (BGP). What impact do they have on routing security? **[6%]**

2. Consider the following protocol which is proposed for wireless transmission: it relies on a 40-bit secret key K shared between two communicating parties to protect the data of each transmitted frame. K is a permanent key which never changes its value. When the user A wants to send a frame of data to B, he/she proceeds in the following 3 steps:

   - CRC encoding: Given an n-bit message M (n is a constant), A computes the 32-bit parity check $L(M)$, where L is a linear function that does not depend on K (Note that the linear property of the function L satisfies $L(X \oplus Y) = L(X) \oplus L(Y)$ for any X, Y). The plaintext is $(n + 32)$-bit $P = M||L(M)$ where $||$ means concatenation.
   - Encryption: A encrypts P with the stream cipher RC4 using the secret key K and a 24-bit initial vector IV assigned to each frame. The ciphertext is $C = P \oplus RC4(IV, K)$.
   - Transmission: A sends (IV, C) in clear to B over the radio link.

   (a) The organisation that proposed this protocol advertises that the protocol encryption enforces a total of $40 + 24 = 64$ bits of security strength. Critically assess this statement; is it true? Justify your answer. **[4%]**

   (b) Explain how the receiver B uses K to extract the original message M upon receipt of (IV, C). **[4%]**

   (c) Suppose the 24-bit IV is assigned at random to each frame. Consider a file sharing application where A and B are exchanging files at the rate of several MB per second. Show that it leads to a serious security problem. Propose a better solution. **[8%]**

   (d) Assume that an attacker sitting in-the-middle has intercepted one frame of traffic data (IV, C) from A destined for B. Show that attacker can compute a valid C' where $C' \neq C$, such that he/she can send the modified data (IV, C') to B without fear of detection. How many different choices of such C' does he/she have? **[8%]**

3. For each of the following, reply **True** or **False** along with a two line justification for your answer. No marks will be awarded where answers are not justified. **[11x2=22%]**

   (a) Malware spread can be completely independent of the payload it executes on each system it infects. Justify with an example.

   (b) A fundamental property of malware spread is that they generate random Internet addresses and then probe those to find new victims.

   (c) A common approach for creating polymorphic malware uses encryption technology.

   (d) There are malware that have compromised more than 10000 systems connected to the Internet in less than an hour.

   (e) It is fundamentally harder to create a detector with low false-positive rate than with low false-negative rate.

   (f) An advantage of anomaly detection over signature-based detection is the ability to potentially detect novel attacks.

   (g) Signature-based techniques have the attractive property that it's easy to share the signatures between different parties.

   (h) Apache webservers can instruct browsers to store a given cookie for many years.

   (i) There are techniques that can be used to track what text you cut-and-paste from certain web pages.

   (j) In a secure decentralised chat system involving many participants, it is a good idea to use a unique cryptographic key for each hop that a given messages takes through the network.

   (k) It is a good idea to require companies to notify users upon breaches of stored personal information.

4. (a) List any three security risks posed by insider attacks in P2P networks. **[3%]**

   (b) Briefly describe any two key-revocation schemes for defending against insider attacks. **[10%]**

5. Consider an attack scenario where the attacker can observe (but not manipulate) network traffic between a victim's computer and a bank's webserver. Further, consider that the attacker can launch some Javascript code within the victim's browser. The javascript code can send arbitrary requests to the bank's webserver. The browser will send these requests with the user's cookie for that bank. The goal of the attacker is to discover the cookie value. Note that the attack javascript is not allowed to communicate with any other server.

   SSL/TLS optionally supports data compression. When compression is used, it is applied on all the transferred data, as a long stream. In particular, when used with HTTPS, compression is applied on all the successive HTTP requests in the stream, header included.

   Propose a design for the javascript attack code that can enable the passive adversary on the network to deduce the value of the cookie. Your answer should make use of the fact that SSL/TLS supports optional data compression and once enabled is used for the duration of a session. Give a detailed working example that demonstrates how your attack would be carried out using sample values in each step. **[17%]**