CSE 473 – Introduction to Computer Networks

Quiz 5 Solution

11/12/2013

1. (4 points). Consider a block cipher with a block size of 8 bits that is used to encrypt English text, represented by ASCII characters. Assume we augment this with cipher block chaining. So, the first byte is xor-ed with an 8 bit initialization vector before encrypting it and each subsequent byte is xor-ed with the previous ciphertext byte before encrypting it.

   Explain the purpose of cipher-block chaining.

   Cipher block chaining is intended to prevent an attacker from exploiting statistics to help it break a cipher. Specifically, it keeps different instances of a given plaintext block from having the same ciphertext value. That prevents an intruder from looking for the most commonly occuring ciphertext byte and concluding that it corresponds to the letter 'e', for example.

   Describe how you could break this encryption system. Be specific.

   There are at most 256 different ciphertext blocks. This means that a given ciphertext value will appear repeatedly in a long stream of ciphertext. If we pick one such ciphertext value and find all its occurrences in the ciphertext, all the characters that immediately follow these positions are xor-ed with the same value. So, we can analyze the statistics of the characters in these positions in order to break the code, with respect to the characters in that position. The process can be repeated for other ciphertext values.

2. (6 points) In a typical SSL session between a client and a remote server, how does the client verify that it is communicating with the desired server, rather than some intruder? Be specific.

   The server sends the client a certificate containing its public key that has been signed by a certificate authority. The client uses its copy of the CA's public key to check that the certificate was signed by the CA. If the signature matches and is not on the CA's revocation list, it accepts it.

   Suppose that an intruder removed a record from an SSL packet sent from the server to the client. How would the client's SSL software detect that something is wrong? Be specific.

   Records in an SSL session are numbered, starting at the beginning of the session. The sequence numbers are included in the MAC calculation used to verify each record, so if a record is removed, the SSL software will detect a mismatch in the MAC.

   Suppose an intruder sent a TCP FIN packet to the server that looked like it came from the client. Would this cause the TCP connection to be closed? If so, how would the SSL software detect that something was wrong. Be specific.

   The connection would be closed. Each SSL record has a type field. The last record of a session has a special type value, so if the connection is closed before the client sends its last record, the SSL software could detect it by just checking the type field of the last record received.