SeungJi Lee (sl136)
CSCI1660

Homework 2

1. Locks
    a. The MACS is used to insure that a key is not stuck inside the lock. If the height difference of a neighbor is too large, then the pin may pin down the key, preventing insertion or removal of the key.

    b. Since the maximum difference is M, we can know that if the next pin cut must be at most M distance away to the top or to the bottom. Thus, we do not need to search all heights.
    In the first pin querying, we do not have any neighbor, and thus need D-1 querying in the worst case. Now, after that first pin, we have neighbor; namely, the pin attacked just before. Thus, the max difference is M. Now, if M < D/2, we have that, at worst case, (P-1)(2M) querying for the rest pins. Then, we have the upper bound of (D-1) + (P-1)(2M). However, if we have M>=D/2, we have P(D-1).
    Now, Let S(n) be the nth pin cut height of the master key and C(n) be the nth pin cut height of the change key. Then, the number of queries are SUM(i=0...n) of 2(S(i)-C(i)).

    c. Assume that the lock uses n pin cuts for creating hierarchical master keying system of n.

    Say we have only one key for the lock. The probability of success is (number of right keys) / (total number of different keys) = 1/(D^P). However, if we add one more layer of pins for the master key, then, the number of right keys becomes 2^P, since for each pin, there is two pin cuts. Then, the probability of success of raking a lock with n hierarchical mater keying system is (n^P)/(D^P). Thus, the probability of successful raking increases fast as n increases. For this reason, the lock manufacturers resist using this technique for hierarchical master keying.

2. $PATH
    a. I could write my own su that stores the username and the password, and put it in the first directory of PATH. If I am restricted in modifying files of the first directory of PATH, I could simply change PATH to make a directory that I have control over to be the first directory.
    b. Check the handed in file: cs166_hw2_su
    c. Check the handed in file: cs166_hw2_su_ext

3. Firewall
    a. Stateless firewalls have many advantages. One of the advantages is that stateless firewalls are faster and perform better under heavy traffic loads, since they do not need to be aware of traffic patterns or data flow. However, stateless firewalls are vulnerable to some specific types of attacks. For example, they are vulnerable to packet spoofing, or ACK scanning attack.
    One example where a stateless firewall would be advantageous is to

implement portknocking protocol as in SynCity project.

b. The advantage of a stateful firewall is that it keeps track of the state of the connections. Thus, the attacks, to which a stateless firewall is vulnerable, are blocked. For example, packet spoofing would not work with a stateful firewall since the connection would not have been established before and thus will be rejected. One of the disadvantages of a stateful firewall is that since it needs to keep track of the states of the connections, it is usually slower under heavy traffics.
One example where a stateful firewall is preferred is to implement FTP.

c. Using the explained technique in the problem, the attacker can send an innocuous packet to pass through the firewall. Then, the attacker can change the source IP address of the previous fragment so that the firewall established a trusted connection with the attacker's source IP address. In stateless firewall, the firewall will add exception with the attacker's source IP address instead of the rightful one, allowing attacker's traffic. In stateful firewall, the attacker could send a SYN packet with the rightful source IP address, then, change the IP address using the technique explained in the problem to make the server handshake with the attacker's source IP address.

4. SYN
   a. Since SYN cookies store all the information necessary for a SYN queue entry in the constructed sequence number, the server side does not to store the information necessary to establish connection in the queue. Thus, however many SYN is received, the queue will not be flooded.

   b. The attacker still can exhaust the server's resources. Since the connection is TCP, once the connection is established, the server needs to keep track of sequence numbers. Thus, the attacker can exhaust the server's resources by successfully opening up large number of connections. The attacker can open multiple connections on one machine using different ports. However, if the server's resources are large enough, the attacker may need to get another IP address to open up the connection. The simple IP spoofing cannot work since the source needs to send ACK to establish the connection.
   The efficiency of the attack decreases significantly since the attacker also needs to use up his resources to maintain the connection.
   This attack also exposes the attacker's source IP address. The server also can block the attacker by inspecting the number of connections a source IP address is establishing.

   c. The attacker needs memory resources to maintain the open connections. Also the attacker may need another IP address assignations to open the large number of connections.

5. WiFi

SeungJi Lee (sl136)
CSCI1660

a. The attacker can simply spoof the IP address of the authorized user and then ARP poison the hotspot’s ARP cache.

b. The administrator can simply create something like TCP. By assigning a random number to each new connection (something like SYN), and adopting handshake and connection protocol similar to TCP, the attack described in a can be prevented.

c. The attacker can come up with his own protocol that does not follow the standard format. Such protocol would put a allowed port number in the field where a regular TCP or other protocol would put the port number. However, when the server and the attacker interpret the packet, they will look at somewhere else to get the port number.