CS 458 A2

Tom Yan

Intelligent Agents of Intelligence fight for Intelligence

1. (i) read access
   (ii) neither
   (iii) both
   (iv) read access
   (v) neither
   (vi) read access
   (vii) neither
   (viii) write access

2. (a) Lowest: (Handler, $\{\alpha, \gamma, \delta\}$), Highest: (Director, $\{\alpha, \gamma, \delta, \eta, \lambda\}$)
   (b) Lowest: (Handler, $\{\alpha, \beta, \delta, \eta\}$), Highest: (Handler, $\{\alpha, \beta, \gamma, \delta, \eta, \lambda\}$)
   (c) Cyril is the better option since the lowest clearance level Cyril must hold allow her read access to the file while the lowest clearance level Ray must hold doesn't.

3. When modifying, add empty string so integrity level gets updated. Take the following steps:

   (i) read F129, I(Barry): (Agent, $\{\alpha, \beta, \gamma, \eta\}$)
   (ii) read F676, I(Barry): (Agent, $\{\alpha, \beta, \gamma\}$)
   (iii) read F513, I(Barry): (Agent, $\{\beta, \gamma\}$)
   (iv) modify F123, I(F123): (Agent, $\{\beta, \gamma\}$)
   (v) read F369, I(Barry): (Support, $\{\beta\}$)
   (vi) modify F123, I(F123): (Support, $\{\beta\}$)
   (vii) read F101, I(Barry): (Unclassified, $\emptyset$)
   (viii) modify F123, I(F123): (Unclassified, $\emptyset$)

Securing password authentication

1. This scheme is not secure since it is still susceptible to brute force attacks of a particular user if the attacker does not have a password file. A standard cryptographic hash is relatively easy to compute.

2. They can improve this scheme by using a MAC that mixes in a secret key to compute the password fingerprint.

3. The SHA-1 hash function could have produced this hash. The password that hashes to this value is petunia. I determined it by using a reverse hash calculator online that has a database of pre-compiled hash values.

4. A better option is to use an iterated hash function that is expensive to compute such as bcrypt. This way it will take much longer to brute force a password and it will slow down a guessing attack significantly.

Firing up the Firewall

1. This is not a good strategy since future attacks might not be in the blacklist of IP addresses. A better option would be to maintain a whitelist as it is generally better to use the strategy of ”forbid everything unless explicitly allowed” in firewalls.

2. Denial of service or some other attack with IP address spoofing. A firewall with packet filtering can be used to defend against it since it can drop spoofed traffic. The attack is originating from outside the company network yet the IP is in the CIIS IP adress range. The firewall can be set up to drop the spoofed traffic.

3. - ALLOW all => 32.23.11.0/25 FROM PORT 80/443 to all BY BOTH
   - ALLOW 32.23.11.25 => all FROM PORT 443 to all BY TCP
   - ALLOW 32.23.11.0/25 => all FROM PORT 22 to all BY TCP
   - ALLOW 53.16.71.12 => 32.23.11.0/25 FROM PORT 1551 to 5000/5100 BY BOTH
   - ALLOW 32.23.11.10 => 32.23.11.0/25 FROM PORT 3223 to all BY TCP
   - ALLOW 32.23.11.10 => 9.19.11.217 FROM PORT 3223 to all BY TCP