CS 458 – A2

Name: Dweep Shah
U.W. ID: dm2shah
Student Number: 20511868

1. Mail of various colours

   a. Let the sensitivity level of the contact be x. Then, $C(x) \geq_{dom} C(B)$ and $C(B) <_{dom} C(x)$ since contact can read Document D001 but not write to it. Also, $C(x) <_{dom} C(S)$, and $C(S) \geq_{dom} C(x)$ since the contact can write to Document D002 but not read from it. Therefore the sensitivity level S $>_C$ B, and sensitivity level S is more dominant then sensitivity level B.

   b. According to the Bell-LaPadula model, my contact has:
   i) read access
   ii) neither
   iii) read access
   iv) neither
   v) read access
   vi) write access

   c. An application proxy firewall might be used to not allow highly sensitive documents from ToqToq's network. This is because an intercepting proxy would make it transparent for clients retrieving the documents. The proxy would have full knowledge of the document permissions, and can do sophisticated processing.

   d. Step 1: write to D401
   D401: (Management, {5, 8})
   Step 2: read from D118
   Contact: (Consultant, {5})
   Step 3: write to D401
   D401: (Consultant, {5})
   Step 4: read from D340
   Contact: (Customer Support, {})
   Step 5: write to D401
   D401: (Customer Support, {})
   Step 6: read from D276
   Contact: (Unclassified, {})
   Step 7: write to D401
   D401: (Unclassified, {})

2. Adding salt to an open wound

   a. A popular hash function that could have been used to generate this hash is SHA1, since this hash function produces a 160bit hash value which is rendered as a 40-digit hexadecimal number. The hash shown is a 40-digit hexadecimal number. A popular hash function that definitely did not produce this hash is MD5 since it produces a 128 bit hash value which is a 32 digit hexadecimal number. Since the hash show is a 40 digit hexadecimal number MD5 is not definitely not the hash function.

b. An attack that could be used to try and crack the above hash is to use an online password guessing attack by using data collected from social engineering to create a dictionary of the most common passwords and their corresponding hashes. This table of map between the brute forced list of passwords and their hash value can be used to crack the hash from D401.

c. The purpose of the salt is to have two users with the same password to have two different hash values from the hashing function, so it is harder to execute a password guessing and brute force attack. If the string salt is appended to each password in D401 before hashing then the hashing function will produce the same output for two users with the same password, and hence salting would be pointless.

d. Their argument that standard, non-iterated cryptographic hash functions are pointless is because they still do not completely guard against guessing attacks. It only slows down the attacker slightly, and the attacker can still generate rainbow tables to crack the hash and determine the password using common password guessing methods with previously gathered data. Using an iterated cryptographic hash function makes cracking the hash much more difficult using guessing attacks.

3. Going viral

a. I would think ToqToq might be using a packet filtering gateway to filter packets based on the header data. Since the source of the packet is not from an expected IP it gets blocked from being sent.

b. The firewall might not block me this time since I would be sending the requests from within the company premises, and my source IP address would be of the form accepted by the firewall. Since the packet filtering gateway checks my source address to be of the correct form, I am not blocked by the firewall.

c. The intrusion detection system is likely blocking the upload of objects with a malicious signature is likely what is blocking me from uploading the virus. The network based IDS uses heuristics and anomalies to detect upload of a file with a malicious signature based on previous behavior.

d. To get the virus on the ToqToq network, the attack can be changed so that the signature is allowed by the intrusion detection system. A polymorphic worm can be used to develop a virus that passes through the IDS eventually by collecting data and eventually passing through the IDS with the correct signature.