CS458 Assignment 3

Name: Darren Poon
Userid: dyhpoon
Student number: 20311433

Question 1

a) Patients that have records that could be unauthorized accessed by employees at that hospital are at risk of a loss in privacy, because their personal health information can be accessed by any employees (nurses) even if nurses do not provide any health care to them.

Also, patients in other hospitals are also at risk of a loss in privacy. Since clinical information systems are connected, and designed to provide broad access to personal health information. Therefore, no technical features for restricting access are used, and can be easily access by employees who work in hospitals.

b) If patient’s explicit consent is necessary before any doctor or nurse, it may pose problems. The reasons are delay in patients’ health care treatments and providing incorrect treatments to patients who are allergic to foods/medicines.

c) Since computer systems are vulnerable to many different attacks, attackers can exploit these vulnerabilities which may endanger to patient’s privacy. For example, the health information is vulnerable in hospitals, where patients’ records can be unauthorized access by nurses.

Using computerized health records have more serious threats than paper records. Even if patients’ information got stolen, paper records are more difficult to be spread to the public (internet). In the article, the complainant’s information can be accessed on ten known occasions, and was used and disclosed for illegal purposes.

d) One of the problems in the hospital’s response to the privacy breach is that the determination of adding the VIP flag on patients’ record is very bad. Even though the complainant asked for her information protected, no VIP flag was added on her record, therefore, nurses can access to her record anytime without monitored.
The other problem is that hospital’s clinical information systems give a broad access privilege to nurses. Even a nurse does not provide any health care to a patient; she can still access that patient’s health information. It is important that the hospital to address this problem and restrict the access privilege to the level they should have.

Question 2

a) Approximately 2500 relays were on 1/1/2012, and about 800 were volunteered to be Exit relays. Since Exit relay is the last relay that Tor traffic passes through before it reaches its destination, so the IP address of the Exit relay will be interpreted as the source of the traffic. In other words, if there is a malicious user launching some attacks, then Exit relay is responsible to take the blame. Therefore, some relays may not volunteer to be Exit relay.

b) The number of Tor users from China on 1/11/2009 was about 9200 users, and there were only about 500 users on 1/1/2010. It shows that the number of Tor users dropped rapidly from 11/2009 to 1/2010, it is because of the Great Firewall of China which Chinese government wanted to monitor the network and blocked Tor. However, average Tor users in China can switched to non-public relays, called bridges.

c) Since Tor's traffic is bouncing through relays, and bottlenecks and latency is present among volunteers' computers while transferring data. Furthermore, Tor does not always choose the best path, it pick one of the Tor nodes arbitrarily to send packets.

Question 3

a) If Eve wants to confirm her guess, she could just compute the c by herself. To be more specific, she could use {m1, m2, m3} to compute (m^e) mod n, and check if any of her new c values are same as the c which was sent to Bob from Alice. If yes, then Eve is correct to her suspicion, otherwise, she is wrong.

b) We could do the similar way in part a. Eve can still be able to compute the c' by herself. Since r is a random number from 000 to 999, Eve only needs to compute "*c' = (m || r) ^e mod n*" by substituting r from 000 to 999 for each m1, m2, and m3. If any of c' that Eve computes is the same as the one that Alice sent, Eve can verify that message is an encryption of m1, m2, or m3.

c) Using the method I described in part b, we first need to convert m1, m2, and m3 into decimal number (m1 = 2212500180913, m2 = 1905121200180913, m3 = 815120400180913). Then, we can try to find c = (m || r) ^e mod n, where r = {000, …, 999}. If any of c is same as c', we can verify that Eve suspicion is correct.
The result shows that c' is an encryption of m3 with r = 649 (m||r = 815120400180913649).

d) Alice can learn m by running the challenge-response model using c = (m ^ e) mod n, where m = random value(s) from Z_n. If Bob abort the protocol, Alice can learn that this is the m that was sent.
Given the ciphertext that observed by Alice, Alice should create a new c' by using m = c (so Alice ciphertext is c' = c^e mod n), this can make sure that Alice can compute a new unique ciphertext, and Bob will not abort the protocol.

Question 5

a) Both confirm.ps and authorize.ps have the same hash value of "3621e20ce4dd5eb07b1b2597e15d440f".

b) Given these two files, an attacker can learn the algorithm or pattern in order to change the content of other files, but have the same MD5 hash value. To be more specific, he could perform collision attacks (Man-In-The-Middle Attack) by replacing/modifying the content of files, but these files will have the same hash value. And the recipient would not be noticed that files have been changed.