CS458 - Assignment 3

Name: Lawson Fulton
UserId: ljfulton
Student#: 20381453

Written Answers

1. a) If an adversary controls both the first and last hop in a tor circuit then it may be possible to use a timing attack for deanonymization. This works because the entry node has the ips of people connecting to the network, and the exit node can see the raw data and where it is going. It is then possible to correlate the size and timing of messages entering and leaving nodes to determine if a tor user connecting through the entry node is forwarding data through to the exit node.

b) A relay operator may prefer to run a non-exiting relay because it could be a legal risk operating the node that is sending the unencrypted data to its final destination. If a crime is committed by a tor user through an exit node, the operator of that node is potentially the only person verifiably linked to that crime, regardless of whether they committed it.

c) The data leaving an exit node is unencrypted (except for potentially application level encryption like https). This would allow an exit node operator to snoop on that data and potentially steal passwords or banking information. Researchers could study the type of data coming through the network and the types of websites being accessed.

d) Although the remailer can remove timing and ordering information, along with completely changing the contents of the message through encryption, it is still possible to try and correlate messages based off of their size. If you see a very large message entering the node along with many small messages, and then you see many small messages leaving along with one large message, it is very likely the two large messages correspond to the same email.

2. d) Fingerprints are important in GnuPG for the purpose of verifying public keys. If Alice sends me their public key over an insecure channel like email, there is a chance that the key could be compromised. I could try to verify the key securely over the phone, but it would be much to laborious due to its length. The solution is to use the key fingerprint which is short enough to be verified over the phone.
If this procedure is not followed properly, a adversary could launch a man in the middle attack to intercept Alice's public and replace it with their own. If the adversaries key is then used to encrypt the message, they would have full access to its contents.
Another issue is that if the hash function used for the fingerprint is not second pre-image resistant, it may be possible for an attacker to create a public key that hashes to the same value as Alice's key.

3. a)
i) CREATE VIEW aliceview AS SELECT * FROM Accounts
WHERE CustomerName = Alice

GRANT SELECT ON TABLE aliceview
TO Alice

ii) GRANT SELECT (CustomerName, AccountNumber, Balance), UPDATE (Balance)
ON TABLE Accounts
TO Clerk

iii) GRANT SELECT, INSERT, UPDATE (CreditRating)
ON TABLE Accounts
TO Manager

b) Consider the view created in 3a.i) where Alice can only read accounts with her own name. If she had the ability to update the CustomerName field, she could change the name to Bob, causing the entry to disappear from her view, since the view must only contains entries with her name.

4. a) Another type of patient who may be significantly at risk of a loss in privacy is one that is under the care of a large number of providers. For example, someone who is having a major surgery with perhaps even 20 or 30 people involved. This type of patient would be at risk simply because of the large number of people who could argue to have reason for viewing the patient's health records. The more people who have that information, the more likely a loss of privacy could occur.
Another type of patient at risk would be someone very high profile, such as a politician, where speculation about their level of health could significantly impact their career. This could provide incentive for someone working at the hospital to view the health record information and potentially leak it to the press.

b) The need for a patient to provide explicit consent before allowing a doctor or nurse to view their health records poses two major problems. One, if the patient is unconscious, or otherwise incapacitated, it would not be possible for the provider to view potentially life saving information in a timely manner. Second, consider a patient who is delusional and distrustful that refuses to give consent to any request. Under the law, the doctor or nurse would not be allowed to look at the patient's health records, even if the patient before falling ill would have allowed such access.

c) One way that computerized health records rather than paper could endanger a patient's privacy is that it is potentially harder to restrict access to records by certain individuals. This is because the access rights are very broad on electronic records to allow quick access in an emergency situation. Another is that with paper records, it is possible to have someone evaluate a reason for accessing records on the spot, rather than retroactively investigate with an audit of the access logs.

d) The first issue that allowed the patient's privacy to be breached was that the initial complaint filed was treated as security issue rather than privacy one. The patient's husbands' department supervisor rather than department manager was notified. This resulted in the CPO not being notified, so no VIP flag was set on the file.
The second issue was that even after the CPO was notified after the first breach of privacy, no action was taken to actually prevent further access to the records. A VIP flag was set on the patient's file that gave a warning, but it did little to stop the nurse from viewing the record at least 9 more times.

5. The average case complexity in terms of oracle calls is 2048N where N is the number of 16 byte blocks in the cipher text. The worst case complexity is 4096N. In either case it is O(N).

6. The main issue is that the server tells the attacker when a cookie has an invalid padding. A solution would be to simply return an error for *any* invalid cookie. That is, any cookie that was not generated by the server. This would be possible if every cookie was given a MAC or digital signature by the server, and the server rejected any cookie without a valid signature / MAC.

7. In section 3.1 the only difference would be in the case that the valid padding found was not 1, this is done on line 5.b. Instead of outputting **r_b-n+1 ^ n … r_b ^ n** we should output **r_b-n+1 ^ 1, r_b-n+2 ^ 2, … r_b ^ n** in order to match our padding scheme (where ^ is xor). In section 3.2 we have to change line 1 from xor-ing **b - j + 2** to xor-ing **b - k + 1** and similarly on line 5 change **b - j + 2** to just **1**.