1 Definitions

a. What is a security policy?

b. Which steps are involved to define one?

c. How can attack trees help for defining a security policy [www.schneier.com/paper-attacktrees-ddj-ft.html]? 

d. Use an attack tree to define the possible attacks you could perform to get access to your friend’s facebook account. Please do this using your page in landscape mode to make it easy to read.

e. Besides attack trees, which framework could help for narrowing down a threat model?

f. Describe two policies of your choice (possibly those seen in the course), their pros and cons

g. What are DAC and MAC? Pros and cons?

h. Describe MLS, Biba, High-water mark, Low Water-Mark Mandatory Access Control (LOMAC), Clark-Wilson, Chinese Wall, Decentralised Information Flow Control (DIFC), Type Enforcement (TE), Least Privilege Principle.

2 DNS

Explain the security concerns with the Domain Name System (DNS) in terms of confidentiality, integrity, authenticity, etc. and briefly outline a threat for each.

3 Security policy models

Suppose you are planning a surprise birthday party for a friend. You have decided to implement some of the security policies discussed in class while planning the party. For simplicity, assume you’ve set up a website hosting a single text file with information about the party.
a. What relevant security classifications are there for people with regards to access to data about the party?

b. What information flows are allowed between these classes of people?

c. Which security model is most relevant here? Bell-LaPadula, Biba, Lattice, or some combination?

d. Explain why, in the real world, it is very difficult to enforce the desired policy. In particular, what scope of user actions must be controlled by the security policy in order to gain high assurance?

4 Social networks (2010 Paper 8 Question 11)

Social networking sites are becoming ever more popular, and many other sites now let users add each other as friends. Discuss the effect that social context has on

a. phishing;

b. inference control;

c. the market for privacy;

d. community detection.

In what ways might social context be used to protect against harm online?

5 Phishing (2007 Paper 7 Question 3)

A rapidly-growing online crime is *phishing*, in which victims are lured by an e-mail to log on to a website that appears genuine but that actually steals their passwords. You have been hired by a bank to help them harden their online banking service against phishing attacks. Explain briefly the strengths and weaknesses of the following four possible countermeasures:

a. SSL/TLS client certificates issued to each customer;

b. a handheld password calculator issued to each customer;

c. displaying a unique picture to each customer during the login process;

d. requiring that large payments, or payments to new recipients, be authorised by telephone or SMS as well as online.
6 Covert channels

If the Bell-LaPadula system is fully implemented, a malware process which acquires root privileges will be able to read all files on the system, but not be able to write to any files which regular users can read. However, there are many other ways of conveying information. For each of the following possible covert channels, discuss how a signal process (high privilege) might communicate secret bits to an untrusted spy process, the rough efficiency of the channel, and what steps the system might take to eliminate or narrow the covert channel. Propose two other covert channel mechanisms you can think of; and present mitigation techniques.

a. Network traffic volume
b. Power consumption
c. Processor cache contents
d. File system fragmentation

7 Double Entry Bookkeeping

You and your roommates have had trouble keeping track of how much money is owed to whom, so you decide to build a computer system to keep track. For example, if Aisha pays £5 for Bharat’s lunch, and Bharat pays £5 for Carlos’s concert ticket, your system should allow Carlos to simply pay Aisha £5 and settle all debt. You are so awestruck by the Clark-Wilson security policy model that you decide to incorporate its principles into your system.

a. What invariants should your system protect? How is this similar to the banking systems described in class?
b. What items are unconstrained (UDI’s) and which items are constrained (CDI’s)?
c. Describe a simple transaction procedure (TP) for recording a payment between two people.
d. In the real world, what constraints might you place about which principals (roommates) can edit which UDI’s?

8 Hardware attacks

8.1 Q1

You are attempting to extract a 4-digit PIN from a secure crypto-processor on a smart card. You have reverse-engineering the PIN-verification routine:

```c
if (PINcounter>0) {
    PIN := RequestPIN();
} else {
```
return false;
}
if ( isCorrectPIN(PIN) != true) {
    savePINCounterToNonVolatileMem(PinCounter - 1)
    return false;
} else {
    return true;
}

a. Describe the cheapest hardware attack that can recover the PIN from this card.
b. Is this an attack that a typical bank adversary can afford?
c. Propose a re-factoring of the code that will eliminate this attack.

8.2 Q2

Internally, the PIN verification procedure is coded as follows:

```cpp
bool isCorrectPIN( char[] PIN) {
    correctPIN = loadFromNonVolatileMem();
    for (int i=0; i<4; ++i) {
        if (PIN[i] != correctPIN[i])
            return false;
    }
    return true;
}
```

How would you attack it?

9 Password

Suppose you are a website and you have to store passwords for your users. How would you store them? Compare the security of storing the hash, the hash of the password+salt, bcrypt, scrypt. Detail which attack each of them thwarts, and which attacks are still feasible.