

ISA662 Section 1

Homework 4 (Due April-25)

(Note: Please keep your answers short. It is strongly recommended that you use a text editor, such as Notepad or Word, for the homework. If you submit homework through emails, make sure you get a receipt message from me the following day.)

1. In practice, many users use the same password on multiple servers (credit card accounts, bank accounts, etc.). Explain why they do this, and why this is a bad idea in terms of security? (Hint: consider dictionary attacks, phishing, etc.)

2. Assume an attacker has compiled a dictionary of 10,000 entries for an off-line dictionary attack on a server with 100 users.

If the server does not use salt, and the attacker's goal is to get a particular user Bob's password. How many hash values will the attacker compute in the worst case?

If the attacker's goal is not to get a particular user's password, but to get as many passwords as possible, what is your answer then?

How do your answers to the above **two** questions change if the server is using salt?

Is salt helpful in an online dictionary attack? Explain if your answer is yes.

3. Suppose a server is using Lamport's scheme, and the current value on the server is $h^{100}(k)$. If an attacker somehow knows the value $h^{40}(k)$, then at most how many times can he logon?

4. If the class discussion forum were using the Encrypted Key Exchange (EKE) protocol (which is not the case), then you definitely don't want to use the same password for the class discussion forum and for your online bank. Explain why.

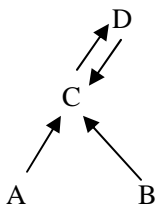
5. Explain why the Crowds anonymity mechanism is **not** vulnerable to an attack where the first and last Jondo collude (the first Jondo will be the one next to the sender, and the last Jondo the one next to the server).

6. Suppose you know X can have values: 0 with probability 0.5, 1 and 2 with probability 0.25, respectively. Compute the entropy $H(X)$.

Suppose now you know that $X \leq 1$. Compute the entropy again.

Did the entropy decrease or increase? What does this change mean?

7. Transform the following non-lattice, transitive policy into a lattice using the method taught in class.



8. How can an anonymizing network defeat the VoIP tracing method? (Hint: the tracking method depends on a covert timing channel, so your goal is to close or at least mitigate it.)