Net ID:

# University of Illinois at Urbana-Champaign
# Department of Computer Science

Midterm 1 – Answers and comments
CS461/ECE422 – Computer Security I
Fall 2008
Wednesday, October 8, 2008

## *Multiple Choice – 2 points each*

1. The key generation technique used by Schneier's Solitaire encryption scheme that we studied in class is an example of what style of key generation.
    a. Electronic Codebook (ECB) mode
    b. Cipher Feedback (CFB) mode
    c. Book cipher
    *d. Output Feedback (OFB) mode*

2. Which asymmetric key algorithm is used for securely generating common secrets in commonly used network security protocols?
    a. RSA
    b. AES
    c. Bin packing
    *d. Diffie-Hellman*

3. What style of risk analysis uses exact values for probabilities of a risk and values of assets?
    a. Qualitative risk analysis
    b. Coordinated risk analysis
    *c. Quantitative risk analysis*
    d. Cooperative risk analysis

4. Which algorithm would be most appropriate for storing a message integrity code or message authentication code with a network packet?
    a. CRC
    b. SHA-256
    c. MD5
    *d. HMAC-SHA1*

5. Which of the following measures can aid in discovering the period of a Vigenere's cipher?
    *a. Index of coincidence*
    b. Avalanche effect
    c. Birthday paradox
    d. Totient function

6. What technique is effective in deterring an online (type 2) password attack?
    a. Adding salt to the complementation information.
    *b. Backoff or increasing delay between failed password attempts*
    c. Eliminating access to the L function.
    d. Adding a trusted path.

Net ID:

## *Short answer*

7. (12 pts) Below is a list of policies and mechanisms.
    a. Mark each element as a policy or a mechanism.
    b. Create pairs of policies and the mechanism that could implement that policy. There are an odd number of items in the list, so there will be one spare.

| **Index** | **Type** | **Matching Pol or Mech Index** | **Value** |
|---|---|---|---|
| 1 | *Mech* | *10* | The company login page must store unique images for each customer and present that image upon login. |
| 2 | *Policy* | *5* | Only members of the executive council (and their direct representatives) should have access to sensitive business plans. |
| 3 | *Mech* | *11* | At registration, all parents must show a deed or bill showing their name and current address. |
| 4 | *Mech* | *7* | When purchasing a book online, the customer must provide their residential zip code. |
| 5 | *Mech* | *2* | All network communication to and from the critical access servers must be encrypted using at least AES 256 encryption. |
| 6 | *Mech* | *8* | Access to any educational computing resources must be authenticated by a University netid and a bluestem password. |
| 7 | *Policy* | *4* | Online and mail order vendors are responsible for collecting the sales taxes levied by the locality of the purchaser. |
| 8 | *Policy* | *6* | Only University of Illinois students may use the student computing labs. |
| 9 | *Mech* | *No match* | All communication on the network must include message authentication codes constructed from HMAC-SHA. |
| 10 | *Policy* | *1* | All customers must be able to distinguish the company's true login web page from similar pages not hosted by the company. |
| 11 | *Policy* | *3* | Only residents of Urbana may enroll their children in Unit 116 schools. |

8. (14 pts) You have received a X.509 certificate C2<<Bob>> (Bob's certificate signed by C2). Your certificate authority is C1. The certificate infrastructure uses RSA keying information.
    a. What certificate should you already have to protect yourself against a man-in-the-middle attack?

*You should have the certificate for your certificate authority C1*

    b. What certificate do you need to fetch to verify the certificate you just received?

*You need to fetch the C2 certificate.*

    c. What do you need to verify? What information will you use to complete this verification?

*You need to verify Bob's certificate, the C2 certificate, and any other certificates that fill in the chain from C2 to C1.*

    d. Show the equations you would use the verify one certificate.

*Not many folks got this section.*

*Assume you had Certificate C with hash value C.hash and signature C.signature and signer S. Say the signer's public key is (S.pub.e, S.pub.n).*

$\{C.signature\}^{S.pub.e} \bmod S.pub.n = C.hash.$

    e. If you (or your system) do not perform this verification, what attack are you opening yourself to?

*If you do not verify a signature, your opponent could perform a man-in-the-middle attack and pass of his own certificate as the requested certificate.*

9. (6 pts) Use the text from question 10 and the Vigenere's tableau at the end of the exam (if needed) to decipher the following phrase using the book cipher technique.

```
BLRBH YPLPY HLVVD
```

```
IENJO YCIPH ERING
or I ENJOY CIPHERING
```

*A lot of folks tried to used the table to encrypt the message again. You needed to use the key to select the row, find the ciphertext in the row and then follow that back up to the column header to get the plaintext. You needed to perform the ciphering step backwards.*

10. (10 pts) The standard Unix access control encoding of permissions in the user/group/other triplet approximates the expressibility of the full access control list model.
    a. Give an example of a scenario that could be expressed in a full access control list that cannot be expressed by the Unix user/group/other model.

*Consider file f. User U1 has read R access. User U2 has W access. User U3 has X access. User U4 has RX access. Could model three groups with U1 as owner, U2 as a member of a group, and U3 as other. But you cannot distinguish U3 and U4.*

*A number of folks brought up that Unix only supports a fixed number of rights, e.g. no copy rights or transfer rights. While this is true, there is nothing structural about the Unix access control triplet that would prevent this.*

    b. Show the protection state of your example from part a in an access control matrix.

| | *F* |
|---|---|
| *U1* | *R* |
| *U2* | *W* |
| *U3* | *X* |
| *U4* | *RX* |

11. (8 pts) You have discovered an efficient algorithm to factor large numbers. How does this affect the effectiveness of RSA? Given Bob's public key **(e,n)**, private key **d**, and an encrypted message **{m}(e,n)** from Alice to Bob, show specific equations to illustrate how your algorithm could be used to discover **m**.

*Say you can compute p and q from n. n = p*q. Then you also know the totient of n (p-1)*(q-1).*

*Remember e*d mod totient(n) = 1. You can find the inverse efficiently over a modulus. In fact Bob had to do this to pick d initially. Given e and totient(n), compute d.*

*Now with Bob's private key, you can decrypt the message Alice encrypted for Bob.*

Net ID:

12. (12 pts) Your boss wants you to compute how long a password would need to be to ensure that an adversary capable of testing 18,000 passwords per second will only have a 40% probability of breaking any randomly selected password in 9 months.
    a. Over the basic latin alphabet (a-z).

*P = TG/N  N = TG/P = (.75*365*24*3600)*18000/.4*
*N = 1,064,340,000,000  Find n such that 26^n > N*

*n = 9 gives us  26^9 = 5,429,503,678,976 which is greater than N.  So the passwords must be 9 characters long.*

    b. Over the set of phonemes (440 phonemes).  Each phoneme is represented by approximately 3 characters.

*N = 1,064,340,000,000  Find n such that 440^n > N*

*440^4 = 37,480,960,000*
*440^5 = 16,491,622,400,000*

*Passwords should contain 5 phonemes or approximately 15 characters.*

    c. Which alphabet would you suggest using for randomly generated passwords and why?

*I would go with the phonemes even if they are a bit longer in terms of numbers of characters.  Random passwords that can be pronounced are easier to remember.*

    d. How accurately do you feel that your computations model how quickly a real attacker will take to break passwords?  Why is this a good model?  Or what are the weaknesses?

*Since the passwords are randomly generated, the Anderson equation fairly accurately models how quickly an attacker will work through the space.  The weaknesses remain in the assumptions of how quickly an attacker can process guesses.*