# Midterm Exam – Spring 2011, CSCI 530

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**P**oints: \_\_\_\_\_\_\_\_\_\_\_/**100**

1. **(3 pts)** Define what is vulnerability and what is exploit. What effect can exploit have on a system?

**Vulnerability: Bug in software or misconfiguration that makes an application or OS behave in unexpected manner.**

**Exploit: Input/code that exercises the vulnerability**

**Effects: Crash the system, give attacker access (root or user level), slow down the system – pretty much any effect that the creator did not desire**

1. **(5 pts)** Explain what is tragedy of commons. Why do we say that most problems in cyber security suffer from tragedy of commons phenomenon?

**Def: Case when there’s a shared resource and if a few people increase their use of resource they benefit but if everyone does that the resource gets depleted.**

**Because most problems require solutions in places where people don’t have economic incentive to solve them.**

1. **(4 pts)** Describe how a homophonic cipher works. Then describe how a polymorphic (polyalphabetic) cipher works.

**Homophonic: cipher symbols chosen randomly from a set. Frequency of symbol in plaintext determines size of set.**

**Polyalphabetic: Multiple mappings for symbols, one chosen for each symbol and then we advance to next mapping.**

1. **(10 pts)** Define what is a block cipher and what is a stream cipher. What modes of operation exist for a block cipher (it is enough to just list the modes).

**Block cipher maps groups of plaintext symbols (blocks) into sequences of cyphertext. Stream cipher maps each symbol into a symbol of cyphertext.**

**ECB, OFB, CFB, CBC**

1. **(10 pts)** Explain how linear feedback shift registers work
   * + **Each step one bit is shifted out out of the register and becomes part of keystream**
     + **One bit is added to the register by combining the bits that were there originally**
     + **Primitive polynomials show us which bits to combine to cover the entire space of the register values**
2. **(8 pts)** Alice wants to send message M to Bob. How can she ensure the following properties, using asymmetric cryptography:
   1. **(2 pts)** Confidentiality

**Encrypt M with Bob’s public key**

* 1. **(2 pts)** Integrity but not confidentiality

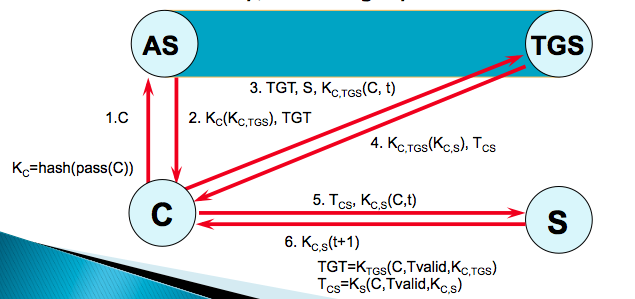
**Calculate H(M) and then post it somewhere or she can encrypt H(M) with her private key and send along with the message**

* 1. **(2 pts)** Confidentiality and integrity

**Encrypt M with Bob’s public key and Encrypt H(M) with either Bob’s public key or Alice’s private key**

* 1. **(2 pts)** Confidentiality, integrity and non-repudiation

**Encrypt M with Bob’s public key and Encrypt H(M) with either Alice’s private key**

1. **(10 pts)** Describe how Kerberos works. Make sure to show all the steps needed for a client to access a server.
2.  **(10 pts)** Explain how cookies can be used for authentication. What are the advantages and disadvantages of such authentication approach?
   * + **Cookie: username and pass or session ID**
     + **Server stores cookie in browser cache on successful login and each time client visits the server the browser hands the cookie back to the server**
     + **Cookie is deleted on log out and session is closed at server**

**Adv: It’s easy for users**

**Dis: Cookies can remain on machine if user doesn’t log off. They can also be sniffed since they are sent in clear**

1. **(10 pts)** Our company is implementing Bell-Lapadula model for access control. Below are the access control matrix and the classifications of various objects and people. After going through them answer the following questions. Make sure to show the decision process that lead to your answer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bob | Chris | Amy | Laura |
| Salaries | write, read |  | write, read | read |
| Vacations |  | write, read |  |  |
| Building map | read | read | read | write, read |
| Orientation | read | read | write, read |  |

Salaries is a top-secret file

Vacations is a secret file

Building map and Orientation are unclassified

Bob and Chris have secret clearance

Amy has top-secret clearance

Laura has confidential clearance

* 1. **(2.5 pts)** Which files can Bob read?

**Bob has secret clearance. He can read at that level or below so he should read BM, Orient and Vac. But ACM only gives him read privs for BM and Orien.**

* 1. **(2.5 pts)** Who can read Building map?

**Everyone has read priv in ACM and BM is unclassified so everyone can access it.**

* 1. **(2.5 pts)** Who can write Vacations file?

**Chris is the only one that has write access in ACM and he has secret clearance which is the same level as the file’s classification.**

* 1. **(2.5 pts)** How can we grant to Laura permission to read the Vacations file?

**Either increase Laura’s clearance to secret or demote Vacation file to confidential AND give Laura read access in ACM**

1. **(10 pts)** What kind of traffic would attacker need to generate to learn:
   1. **(2 pts)** All the DNS information about a network

**DNS zone transfer**

* 1. **(2 pts)** Live machines within a network

**Ping sweep**

* 1. **(2 pts)** Services within a network

**Send service requests to commonly open ports (TCP and UDP)**

* 1. **(2 pts)** Vulnerabilities in installed applications within a network

**Vulnerability scan using existing tools**

* 1. **(2 pts)** Network topology

**Traceroute to multiple (all) dsts in network**

1. **(10 pts)** Describe how stack overflow works. Then list at least two defenses from stack overflow attacks.

**Apps store on stack return address, frame ptr, arguments to function and local variables for each function call**

**If the attacker provides too long an input for a function’s local variable that input can overwrite the return address on the stack**

**Usually the return address is overwritten to point back to the input which contains malicious code**

**Using safe functions**

**Checking app inputs**

**Forbidding exec from stack**

**Forbidding writes on stack**

**Saving return address elsewhere**

1. **(10 pts)** Describe how ARP poisoning works. Now describe how DNS poisoning works and contrast this with ARP poisoning.

**In ARP poisoning the attacker sends a reply mapping his MAC address to someone’s IP address. The switch takes it.**

**In DNS poisoning the attacker has to wait for a request or elicit a request and then send the reply back faster than the authority. The reply must match the query ID from request.**

**ARP works on same subnet and DNS works remotely**

**ARP – unsolicited replies; DNS – must have a request go out to auth, attacker must be faster than auth and match the query ID**