



CSCI 415: Computer and Network Security
Sample Questions for Final
Dr. Nazli Hardy

My Advice:

Read your notes (if you missed a class, connect with a classmate and also look online for slides)
Practice– write out/ draw key concepts
Form a study group

Overview

The test will consist of:

True/False
Multiple Choice
Diagrams/ Label
Short Answers

My Expectations

Be concise, clear, and concrete in your answers

Note: the following are sample questions so that you have a feel for the types of questions that can be asked. **Do not limit your studying to only these questions.**

Intro to Cryptography

The differences between symmetric and asymmetric keys – also advantages and disadvantages of each

Why is hashing useful and important – give an example

Transpositional Encryption

Difference between bit-level encryption and character-level encryption

Which 2 organizations are responsible for DES

What is AES and what is DES?

Cryptography II

If people know the algorithm, how is the ciphertext not deciphered by everyone?

Relation between encryption and decryption algorithms

What are the 2 requirements for the secure use of symmetric encryption?

What is a message authentication code (mac)

What is an alternative to mac

Steganography

What are some ways in which messages can be hidden in digital media?

What are carrier files? (know some examples of these)

Cryptography III

Show your understanding using labeled DIAGRAMS – digital envelope, digital signature, digital certificate, SSL

SSL/ IPsec / S/MIME

What are the 2 services for SSL connections (SSL Record Protocol Services)

IPv4, IPv6 – a differences between them in terms of security

IP-level security encompasses what three functional areas

Some benefits of IPsec

A benefit of S/MIME (it is implicit that you know what S/MIME is)

Some functions of S/MIME

Kerberos

What is Kerberos?

What is the most common algorithm used with Kerberos

The 2 main parts to Kerberos (ans. AS and TGS)

Ethics and X.509

What is the X.509 Standard?

What is a CRL?

Be familiar with some ethics bodies – so you can recognize them

Why do you think the emphasis of the ethics code in CS is on people rather than on machines?

Forensics I

Computer vs. network forensics

- Typical nature of corporate forensic cases – some of the measures that are taken (e.g. electronic copies of emails (header data))
- email server logs – or the server that houses back ups
- .pst files (Outlook)

Forensics II

Motives

3 C's of evidence

Chain of custody

Preservation of data (how is this done)

Forensic copy (what is this, what is the significance)

Mirror image, slack, residual data

Forensics III

4 ways to spot a doctored image

Types of graphics files

Forensics IV

Why is it hard to carry out forensic analysis on PDAs

What makes smartphones gems for forensic analysts

What do email headers contain that help out forensic experts

Software Security I & II

What is an example of buffer overflow – and what would be a solution to this problem?

What is an example of is sql injection – and what would be a solution to this problem?

What is an example of is cross-site scripting – and what would be a solution to this problem?

What is command injection?

What are metacharacters?

Security Management and Control

Risk appetite

Some considerations is risk treatment alternative (risk acceptance, risk transfer etc.)

3 main classes of control

What is a risk treatment

What are some factors that have to be taken into account in cost-benefit analysis

Why is it important to keep personnel involved in the security policy of a company

Have an understanding of a risk register

Clear, Concise, Concrete