CSCI 362 Computer and Network Security
Midterm Exam 3 Study Guide

• Review your assigned readings from the textbook and handouts.
• Go through the activities and the homework assignments. Make sure that you have a solid understanding of the topics they address.
• Go through the self-check list below and make sure that you are able to answer these questions.
• Note that this document doesn’t mean to give an exhaustive coverage of what might appear in the exam!
• This is a comprehensive exam. The all the material in the study guides for the first two midterm exams apply to this one as well.

1. Goals in Security
   • Confidentiality
   • Authentication
   • Integrity
   • Availability
   • Non-repudiation (*)
   • Authorization
   • Freshness (*)
   • Scalability (*)

   (a) Understand the security goals in the list above so that you are able to identify when a security technology or product is capable of meeting each goal.
   (b) Given a scenario or product, identify which of these goals is desirable.
   (c) Construct a scenario where one or more of these goals is desirable.
   (d) Be particularly mindful of the goals marked with an asterisk, as these haven’t been covered in previous exams.

2. Authentication for Humans

   (a) What makes a good password?
   (b) Dictionary attacks: Describe the sequence of steps that must be followed to implement such an attack. Suggest measures that can be taken to help a password system be more resistant to dictionary attacks.
(c) Describe the mechanics of a birthday attack. Be prepared to explain why this attack works better than brute force in terms of run-time asymptotic complexity. (You don’t have to be able to explain the Birthday Paradox, but it won’t hurt to spend some time studying it.)

(d) Identify what can be done to make an online, password-based authentication system more resistant to brute-force attacks. (Hint: S&M page 217 discussion on exponential backoff and blacklisting.)

(e) Discuss the effectiveness of a password authentication system that expires passwords every X months and that does not allow users to reuse any of the last Y chosen passwords.

(f) Discuss the good and the bad consequences of imposing a set of rules for the construction of passwords.

(g) Discuss the consequences of false positives and false negatives in authentication systems based on biometrics.

(h) Reflect on how Linux authenticates users through /etc/passwd and /etc/shadow. Explain why the first file is world readable and why this does not invite disaster. Explain why the second file is only readable to root and why this is not an inconvenience.

3. Authentication Protocols

(a) Given the ladder diagram for an authentication protocol, demonstrate how one can orchestrate known plaintext attacks, chosen ciphertext attacks, oracle session attacks, parallel session attacks, or offset attacks.

(b) Given a set of requirements, construct an authentication protocol that uses the minimum number of flows and cryptographic operations.

(c) Contrast the suitability of symmetric-key and public-key cryptography in a given authentication protocol.

(d) Analyze whether a given authentication protocol implements one-way or two-way authentication.

4. Certificates and PKI

(a) Reflect on the amount and on the type of information that was required of you to request the creation of a personal certificate for e-mail. Is it sufficient to determine that the user making the request is indeed the owner of the purported identity?

(b) Discuss who should generate and store public and private keys in a PKI issued certificate.
(c) Describe the mechanics of setting up email encryption/decryption based on certificates issued by a PKI. What are the steps the each party must complete in order to be able to exchange secure email? Reflect on the experience of using your personal certificate to digitally sign and/or to encrypt email.

(d) Compare the Web of Trust model used by a certificate authority to the Web of Trust model that motivates key signing parties. Identify advantages and disadvantages of each.

(e) Describe the mechanics of a key signing party and explain what needs create motivation for them.

(f) What purpose do X.509 certificates serve? What kind of information does they contain and how could they be used by Internet applications such as e-mail or web browsing? Identify applications that can benefit from the use of X.509 certificates. Identify the limitations and/or difficulties associated with the use of certificates.

(g) Identify the roles of the Certificate Authority (CA) the Registration Authority (RA) in the implementation of a PKI.

(h) Construct solutions to make PKI scalable so that is can serve large populations of users.

5. Modern Cryptography

(a) Consider the practical issues in the implementation of the RSA encryption algorithm. What kind of support is needed for the mathematical operations involved? How does one encipher a long message (say, a thousand bytes) using RSA? It is based on blocks? It is a stream cipher?

(b) Contrast RSA with a symmetric-key cryptosystem. Identify the advantages and the disadvantages of each.

(c) Consider the Diffie-Hellman algorithm. Identify the problem that this algorithm solves. Identify any operational issues that might arise in the use of this algorithm and propose solutions to address them.

(d) Given a cipher, can you identify to what kinds of cryptanalytical attacks it is vulnerable?

(e) When is a cipher most vulnerable to frequency analysis attacks? What kind of statistics can be used in a frequency analysis attack to a ciphertext? Under what conditions can a frequency analysis attack be successful?

(f) What are the characteristics of an ideal cipher? What makes the one-time pad an unbreakable cipher? What are the difficulties in implementing a one-time pad? Why isn’t a one-time pad widely used?

(g) Contrast a stream cipher to a block cipher. What are the keys to each cipher like? How does each kind of algorithm process plaintext?
(h) Consider the block cipher modes we studied. Can you explain why ECB is insecure and why CBC is secure? Why can we say that OFB and CTR produce stream ciphers from a block cipher?

(i) Compare the concepts behind symmetric-key and public-key ciphers. What are the advantages, disadvantages, and difficulties of using symmetric key or public-key ciphers? Consider implementation issues and run-time performance in your analysis.