University of Maryland
CMSC414 — Computer and Network Security
Professor Jonathan Katz

Review for the Final Exam

Note: This is a high-level summary of topics for the final. I have tried to be comprehensive below, but unless stated otherwise *everything covered in class is fair game.*

Lecture 1 I want you to understand why security is hard, why security is always a trade-off, and why there is more to security than computer security. You should understand the broader point of the "Trusting Trust..." article.

Lectures 2–10 (Cryptography and cryptographic pitfalls)

- Why are definitions and proofs important? Understand Kerchoffs' principle and why "security through obscurity" is not a good idea.
- Understand the differences between the private- and public-key settings, instances when each might be appropriate, and their relative advantages. Understand private-key encryption, message authentication, block ciphers, hash functions, public-key encryption, and digital signatures, and appropriate applications of each of these primitives. You should know names of schemes used in practice for each of these, and the basic constructions we went over in class.
- Understand the security guarantees provided by various definitions. When (and why) must encryption be randomized? Does encryption guarantee integrity? What is the difference between chosen-plaintext security and chosen-ciphertext security? Why is chosen-ciphertext security important?
- What is the one-time pad? What are its limitations? What does computational security mean?
- You should know ECB, CBC, and CTR modes, understand whether (and why) they are secure against chosen-plaintext attacks, and why they are insecure against chosen-ciphertext attacks.
- You should understand how Diffie-Hellman, El Gamal, and (secure versions of) RSA encryption and signature schemes work. You should understand the weaknesses of "textbook RSA" encryption and signatures. You should know what hybrid encryption is and how it works.
- Understand why cryptography does not solve all security problems. You should also generally be aware of the standard crypto mistakes that tend to be made.
- You should understand the WEP attacks as discussed in class and the two papers assigned for lecture 10. You are *not* responsible for the details of the padding oracle attack (though you should understand that this is a type of chosen-ciphertext attack), or for the other papers assigned for lectures 9 and 10.

- You should understand things like side-channel attacks at a high level, and how a cryptosystem could be attacked in the real world even if it is proven secure.

Lectures 11–16 (Network security)

- We spent a fair amount of time talking about different forms of authentication (keys, passwords, biometric data), as well as various key exchange and mutual authentication protocols. All of this makes for good exam questions.
- Understand certificates, certificate chains, and certification authorities. You should be aware of different forms of public-key infrastructure (PKI).

Lectures 17–19 (System security)

- Understand the distinction between policy and mechanism.
- Know and understand the Saltzer and Schroeder principles, as covered in class. For each principle, can you think of things we covered in class illustrating that principle?
- Understand the distinction between authentication and authorization.
- Understand the different access control mechanisms (ACLs, capabilities, and access control matrices) and their tradeoffs. Understand the different access control policies (MAC, DAC, RBAC) and different flavors thereof (Bell-LaPadula, Biba).

Lectures 20–24 (Programming-language security)

- Understand buffer overflows and how they can be exploited in detail. Be prepared to identify potential buffer overflows in code snippets I provide.
- Understand the methods for protecting against buffer overflows that were discussed in class.
- Understand SQL-injection, XSS, and CSRF attacks, and be prepared to identify potential attacks in code I provide. Also understand the defenses against these attacks, as discussed in class.

Lecture 25 (Database privacy)

- Know different mechanisms for database privacy, and their relative advantages. You should be able to recognize and find attacks like those shown in class.

Lectures 26–28 (Network security in practice)

- You should understand the network stack model, and the different tradeoffs for implementing security at various layers of the stack.
- You should know what SSL, IPsec, and IKE are at a high level. You do not need to memorize any details of the protocols, however I may present you with various pieces of these protocols and ask you to explain what they do, what would happen if some modification is introduced, etc.
- You should be familiar with the difference between signature-based and anomaly-based IDS, and the advantages/disadvantages of host-based IDS vs. network-based IDS. You should also know Bayes' law and how to use it.