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

Review for Final

Note: This is a high-level summary of topics you should know for the final. I have tried to be comprehensive below, but unless stated otherwise *everything covered in class or in an assigned reading 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 2–7, 9 (Cryptography) (Lecture 8 will not be covered on the final.)

- Why are definitions and proofs important? Kerchoffs' principle and why "security through obscurity" is not a good idea.
- Understand the differences between the private- and public-key settings, and their relative advantages. Understand private-key encryption, message authentication, block ciphers, hash functions, public-key encryption, and digital signatures, and the appropriate applications of each of these primitives. You should know names of schemes used in practice for each of these.
- Understand the security guarantees provided by various definitions. When (and why) must encryption be randomized? Does encryption also 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 the security requirements for hash functions, and the relevance of "birthday attacks".
- You should understand how Diffie-Hellman, El Gamal, and RSA work. You should understand the weaknesses of "textbook RSA" encryption and signatures. You should know what hybrid encryption is and how it works.
- You do not need to know about the JCA.

Lectures 9–11 (Cryptography pitfalls)

- Understand why cypto not solve all security problems. You should also generally be aware of the standard crypto mistakes that tend to be made.

- You should understand things like side channel attacks, and why a cryptosystem can be attacked even if it was proven secure.
- You are *not* responsible for the papers assigned for these lectures.

Lectures 12–14 (System security)

- Understand the distinction between policy and mechanism.
- Understand the Saltzer and Schroeder principles, as covered in class, and where they apply. For each principle, can you think of things we covered in class that illustrate that principle?
- Understand the distinction between authentication and authorization.
- Understand the different access control mechanisms: ACLs, capabilities, and access control matrices. Understand the different access control policies: MAC, DAC, RBAC. Understand the distinction between identity-based access control and code-based access control.
- Bell-LaPadula and Biba models, etc.
- Trusted computing.

Lecture 15 (Database security)

- You are responsible for the assigned paper by Sweeney.
- Understand the different mechanisms for database privacy, and their relative advantages. You should also be able to come up with attacks like those shown in class.

Lecture 16 (Anonymity) (You *are* responsible for this material on the exam.)

- Understand anonymity: Why is it important? Why is it different from privacy? Why isn't anonymity trivially achieved by using encryption?
- You should understand the basics of the TOR protocol, as described on the slides from that lecture.
- You are not responsible for anything in the assigned papers, except for what is covered on the lecture slides.

Lectures 17–19 (PL security)

- Understand buffer overflows and how they can be exploited. Understand HW3, and be prepared to identify potential buffer overflows in code snippets I provide.
- You are not responsible for the "Smashing the Stack..." paper.
- You should be aware of some basic methods for protecting against buffer overflow attacks, as discussed in class.
- Understand SQL injection attacks, and be prepared to identify potential attacks in code snippets I provide.
- Understand XSS and XSRF attacks, and be prepared to identify potential attacks in code snippets I provide.

Lectures 20–27 (Network security)

- We spent a fair amount of time talking about key exchange and mutual authentication protocols, and all of this makes for good exam questions. Please *make sure to read the assigned sections of the book* (as listed on the course syllabus).
- You are responsible for the paper "Do strong passwords accomplish anything?"
- Understand PKI, certification authorities, etc. You should read the paper by Ellison and Schneier.
- Firewalls and IDS will only be covered at a high level. You should, however, know Bayes' law and how to use it.
- You should understand the network stack model, and the different tradeoffs for implementing security at various layers of the stack.
- You do not need to memorize any details of SSL, IPsec, or IKE. 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.

Lecture 28 (Privacy) You are *not* responsible for this material on the exam.