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

Review for Midterm

Note: This is a high-level summary of topics you should know for the midterm. It is *not* comprehensive, but is intended to highlight some basic and fundamental points. Unless stated otherwise, *everything covered in class or in an assigned reading is fair game.* (So please don't ask "is this on the exam?". Unless stated otherwise below, the answer is "yes".)

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 "Trusting Trust..." article, as well as the broader point it is making.

Lectures 2–7, 9 (Cryptography) (Lecture 8 will not be covered on the midterm.)

- Why are definitions and proofs important? Kerchoffs' principle and why "security through obscurity" is not a good idea.
- Understand the difference between the private- and public-key settings, and their relative advantages. Know what are the differences between private-key encryption, message authentication, public-key encryption, and digital signatures. Please get the syntax right: e.g., signing is *not* the same as decryption; verification takes as input a message and a tag/signature; a block cipher is not an encryption scheme, etc. You should know names of schemes used in practice for each of these applications, as well as for hash functions and block ciphers.
- 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? What is a block cipher?
- 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 should know that RSA-OAEP is a standardized scheme that is secure against chosen-ciphertext attacks. You do not need to know the details of RSA-OAEP.
- You should be familiar with those aspects of the JCA that were needed for HW1.

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 are responsible for the required papers assigned for these lectures. You do not need to memorize them, but you should make sure you understand them.
- You should understand things like side channel attacks, and why a cryptosystem can be attacked even if it was proven secure.

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.
- 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 should read 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.