Computer Security

Exam checklist

Version: February 20, 2017, 09:54

- This list can be used as a tool when studying for the exam. It is a collection of the topics that have been discussed during the lectures. The topics are listed by chapter in the course book, but note that some things are not covered in the course book (most notably time-memory-tradeoff attacks). The topics have been divided into three classes; *most important*, *less important* and *least important*. Note that topics covered by the course book but not by the lectures are automatically placed in the class called *least important*.
- There is no guarantee that *all* exam problems are covered by information given in this document. Exam questions can often be based on the fact that you understand some concept rather than just remember it. These questions are hard to relate to a specific topic from the lectures since they may cover several chapters. However, studying the topics below will make you well prepared for also these questions.

Several of the following topics WILL show up on the exam. Consider these as most important:

Chapter 3
□ Terms like confidentiality, integrity, availability, authentication, nonrepudiation, accountability.
□ Difference between data and information.

Chapter 4
□ Spoofing attacks.
□ Password recovery using brute force, dictionary and time-memory-tradeoff attacks.
□ You should know the idea behind the time-memory-tradeoff attack, but no details. You should know the tradeoff given by $N^2 = M^2T$ and $P = N$ and how a table is constructed.
□ The idea behind rainbow tables and when they are useful, but no details.
□ The purposes of salts in password hashing.
□ How the system can help protecting against password compromise.
□ Biometric systems, the terms FRR, FAR and EER and how they relate, assuming FTA is zero.

Chapter 5
□ Discretionary vs. mandatory access control.
□ The difference between capabilities and ACLs.
□ How powersets can be used in access control.
□ Least upper bound and greatest lower bound in lattices. Mathematical details are not needed but if you see a Hasse diagram you should be able to locate least upper bound and greatest lower bound for two nodes.

Chapter 6
□ The difference between reference monitor, security kernel and the trusted computing base (TCB).
□ The concept of reference monitors and their purpose.
□ Controlled invocation.

Chapter 7
□ Difference between real and effective UID in Unix.
□ Difference between crypt, MD5 crypt and bcrypt in terms of performance and security. You do not have to know the details of the algorithms or exactly where they are used.
□ Purpose of /etc/shadow file and the type of information stored in this file (no details).
□ How access control works in Unix (read,write,execute,owner,group,other).
□ Setuid in Unix.
□ You do not have to remember what is in an inode, but if you see an inode you should be able to locate the important information in it.
□ Use of umask in Unix.
□ Usage and potential problems with searchpath in Unix.
□ How hosts.allow and hosts.deny are used to determine access control to network services in Unix.

Chapter 8
□ The problem with the LM hash and how the NTLM hash is better. You do not have to know the exact details of how they work.
□ What are access tokens and what do they contain?
□ The concept of privileges.
□ What are security descriptors and what do they contain?
□ The concept of DACL, how access control lists are searched and what consequences does the search have? The difference between Windows and Unix is important here.
□ The purpose of the SACL.
□ How access control on the network differs from access control on the computer.
□ Access control for a restricted token.

Chapter 9
□ How a general tracker can be used to derive sensitive information in statistical databases.

Chapter 10
□ You should understand how buffer overflow attacks on the stack work and how they can be prevented and detected. This includes canaries, W$\oplus X$ and ASLR.
□ You should understand the idea behind SQL injection attacks how they can be prevented.

Chapter 11.1-11.2, 12.1-12.3
□ In Bell-LaPadula you should know the ss-property, the *-property and the ds-property.
□ Tranquility in Bell-LaPadula.
□ Conceptual difference between Bell-LaPadula and Biba models.
□ How new integrity levels are computed after reading/writing to an object in the case of dynamic integrity levels in Biba?
□ You should know the fact that Clark-Wilson focuses on integrity.

Chapter 13
□ Strengths and limitations of security evaluation.
□ Difference between Orange Book, ITSEC and Common Criteria in terms of functionality and assurance for products.
□ Classification of products in Orange Book, ITSEC and Common Criteria, but not the details of the different classes or evaluation levels.

Chapter 14
□ Empirically, provably and unconditionally secure.
□ Kerckhoffs' principle.
□ Relation between stream ciphers and OTP.
□ Stream ciphers vs. block ciphers.
□ Block cipher modes ECB, CBC and OFB.
□ Symmetric vs. asymmetric cryptography and which types of algorithms belong to which group.
□ You should be able to compute a toy RSA example, which means that you should know the RSA algorithm.
□ Defining properties of hash functions and the additional properties preimage resistance, second preimage resistance and collision resistance.
□ Birthday paradox. You do not have to know how to derive it but you should know its meaning and consequences.
□ Properties of MAC functions.
□ Digital signatures and how they differ from MAC functions.
□ You should know that El Gamal is based on the discrete logarithm problem.

Chapter 15
□ The terms key transport, key agreement, implicit key authentication, key confirmation and explicit key authentication.
□ Replay attacks.
□ Man-in-the-Middle attacks □ Certificates and certificate chains. You do not have to know every field in a certificate, only the most important ones.
□ The Diffie-Hellman protocol (how it works) and the main problem with the protocol.
□ How STS solves the problem in Diffie-Hellman.
□ For AKEP2, EKE, Needham-Schroeder and Kerberos you should only remember the most important things about them, e.g., the problem with Needham-Schroeder and how Kerberos solves this problem. You should be able to understand them when you see them, but not remember the details by heart.

Chapter 16
□ Traffic analysis.
□ The SSL handshake when RSA is used.
□ Purpose of random numbers in SSL.
□ Basics of IPsec.
□ The difference between the 4 ways of using IPsec, {AH, ESP}× {Transport, Tunnel}.

Chapter 17
□ The difference between packet filters, stateful packet filters and application level proxies.
□ Idea behind anomaly detection and misuse detection for an IDS, and the differences.
□ Purpose of Honeypots.

Chapter 19
□ How authentication and key agreement works in GSM.
□ The important improvements made to the authentication and key agreement

in UMTS compared to GSM.
□ The fact that the encryption algorithm in GSM is a stream cipher and in UMTS a block cipher in a stream cipher mode of operation.
□ CRC-32 problem, IV size problem and authentication problem in WEP.
□ The fact that WPA2 uses AES and is completely different from WEP and WPA.

Very few of the following topics will show up on the exam. These should be studied after you know everything above. The list is sorted but not divided into chapters. Consider these as less important:
□ Setgid for directories, sticky bit.
□ File copy and links (cp and ln) in Unix.
□ Race conditions.
□ Mounting file systems in Unix.
□ TCP wrappers.
□ The Windows registry. No details.
□ Groups in windows.
□ Mandatory access control in Windows Vista.
□ Primary keys, foreign keys and integrity rules in databases.
□ Individual trackers in database inference.
□ Database views and how they can simplify access control.
□ Cascading authorizations in databases.
□ Invocation in Biba model.
□ Clark-Wilson security model.
□ Chinese Wall security model.
□ One time signatures.
□ Security associations in IPsec.
□ SSL handshake when Diffie-Hellman is used.
□ SSL record, alert and change cipher spec protocols.
□ Difference between WEP and WPA.

The following topics will NOT be covered by the exam, but if you are interested in the topic and have lots of time left you can look at it. The list is sorted but not divided into chapters. Consider these as least important.
□ Strings of integers with prefix as partial ordering.
□ The generic access rights in Windows.
□ The access mask in Windows.
□ Unicode and UTF-8 encoding.
□ Heap based buffer overflow attacks.
□ Integer overflows.
□ Federal Criteria.
□ Details of El Gamal signatures and El Gamal encryption.
□ Key management in IPsec.
□ Computations of master secret and key in SSL.
□ The SQL language details.
□ How the A5/1 algorithm works.
□ Name of functions and how they are computed in UMTS.
□ Encryption algorithm in UMTS.
□ Variant of CBC-MAC used in UMTS.
□ How the RC4 algorithm works.