IT Security - Midterm Test

Total points 61/75

Practice questions translated from Hungarian.

✓ 1.) What is the **hash-and-sign** paradigm? * 1/1

○ Reduces efficiency if you sign the message hash instead of the message.

● Increases efficiency by signing the hash of the message instead of the message. ✓

○ Increases efficiency if it duplicates the message hash.

○ Reduces efficiency if it duplicates the message hash.

✓ 2.) What is the purpose of the **cryptographic hash function**? * 1/1

● A hash function is a function that records arbitrary long messages to long outputs (n-bits). ✓

○ It stores the data in a hash table.

○ Accelerates password identification.

○ Slows down password identification.

✓ 3.) What is the difference between **risk minimisation** and **risk optimisation**? *1/1

● Risk should be optimized by spending as little as possible on it, i.e. the value of the minimisation is reduced. ✓

○ They mean the same thing.

○ Minimizing should be supported by all possible resources.

○ Optimisation should be supported by all possible resources.

✓ 4.) What does the **open design principle** say? * 1/1

○ Safety through obsecurity.

○ Outsiders can have a say in the design, they can make the changes themselves.

● Software security should not depend on the secrecy of the design. ✓

○ Not only to be used by a closed community.

✓ 5.) How are you protected for **long-term storage** on iOS? * 1/1

○ Keys used for encryption are only saved in iCloud for backup restoration.

● Data is cryptographically bound to the device. ✓

○ Data is immediately deleted if decryption fails.

○ Data is only accessible after successful fingerprint authentication.

✓ 6.) What type of attack is possible if the key space is small? * 1/1

● Brute Force attack. ✓

○ Trojan attack.

○ Malware attack.

○ Any of the options.

✓ 7.) What is a certificate chain? * 1/1

○ Issued certificates are stored in a certificate chain.

○ Revoked certificates are stored in a certificate chain.

● Each end-user certificate can be verified by verifying a certificate chain (root to user). ✓

○ Intermediate certificates are stored in a certificate chain.

✓ 8.) What is a **stack frame**? * 1/1

○ A pair of memory addresses representing the top and bottom of a stack.

○ The programming framework of the stack.

● When a function is called, the area on the stack that the function handles. ✓

○ The memory area pointed to by the stack pointer.

✓ 9.) Which factor **does not** determine the IT Security risk? * 1/1

● Repair. ✓

○ Threats.

○ Countermeasures.

○ Vulnerabilities.

✓ 10.) What is **stretching**? * 1/1

○ Hash depends not only on the password but also on a random value.

○ Hash computation time is accelerated by optimisation.

● To artificially increase the hash counting time. ✓

○ The password hash can be randomly long.

✓ 11.) What do we mean by **key space** in encryption? * 1/1

○ On the backing store, the place where the key can be safely stored.

○ The area indicated by the key pointer.

○ There is no location for the key.

● The key space of the algorithm is the set of all possible permutations of the key. ✓

✓ 12.) What is **not** a definition **nor** characteristic of stack overflow? * 1/1

○ A special form of buffer overflow.

○ Occurs when a procedure copies user-controlled data into the local buffer stack without checking the size.

○ User-controlled data overwrites other values in the stack, including the potential return value.

● The stack indexing is incorrect, resulting in an overflow. ✓

✓ 13.) What is a **MAC**? * 1/1

○ The name of certain apple products.

○ The hash function is located at the address pointed to by the MAC.

● Can be seen as a hash function with an additional input (the key). ✓

○ Unique identifier.

✓ 14.) Which is **not** one of the hacker groups? * 1/1

○ Terrorist organization

○ Computer crime organization.

○ Disgruntled employee.

● Computer scientists. ✓

✓ 15.) Which characteristic does **not** describe the White/Grey box? * 1/1

○ Much more efficient, but high cost of entry.

○ Generates inputs that trigger new code paths.

● Verification where we have only minimal prior knowledge of the system -> only inputs and outputs are examined, we do not know the inner workings. ✓

○ Aims to maximize code coverage.

✓ 16.) How does public key binding to an authorized user work? * 1/1

○ The public key is assigned to the user by specifying the private key.

○ The user can choose the public key that suits him/her.

● The name and the public key are linked to the digital signature of an authenticated authenticator. ✓

○ The user ID and the public key are automatically generated together.

✓ 17.) What is the **birthday paradox** and how does it relate to the hash function? * 1/1

○ Chooses an arbitrary date as a birthday, nothing to do with the hash function.

○ Choose an arbitrary date as birthday and extend it with a hash function.

○ Randomly drawing elements from a set of N elements, it can be stated with 100% probability that it will not meet sqrt(N).

● If you randomly draw elements from a set of N elements, a repeating element has a high probability of being encountered after sqrt(N) choices. ✓

✓ 18.) How can we ensure key freshness? * 1/1

● With time stamps, time windows. ✓

○ A nice refreshing cocktail.

○ Calendar synchronisation.

○ Timers.

✓ 19.) What is the average complexity of an exhaustive key search attack on a k-bit key? *1/1

○ (k-1)

○ 2^(k-1) * 10^10

○ (k-1)^2

● 2^(k-1) ✓

✓ 20.) What type of information is **not** useful to collect before the attack? * 1/1

○ System architecture.

○ Used security mechanism.

○ Access rights.

● Geological location. ✓

✓ 21.) The **Caesar Cipher** is easy to crack because a fixed number is the size of the key space. What is this number? *1/1

○ 22

○ 64

○ 67

● 25 ✓

✓ 22.) What is not the key size of AES? * 1/1

○ 128

● 64 ✓

○ 192

○ 256

✓ 23.) How many steps does it take to crack a complete system? * 1/1

○ Attacks consist of 5 steps.

○ Preparation, execution, cryptographic verification, debugging.

○ Always one big bug causes the compromise of the whole system.

● Usually a combination of several attacks building on each other and several different vulnerabilities. ✓

✓ 24.) What programming error can lead to SQL injection? * 1/1

○ The system is not connected to the network, so cannot be checked by the application.

● Data from the client side is processed by the application without verification, malicious code can be executed on the system. ✓

○ No direct access to the application and the database created from known malware.

○ Non-programming error leads to SQL injection.

✓ 25.) Which risk is **not** relevant for IT Security? * 1/1

○ Unauthorised access

○ Loss of confidentiality or availability of information.

○ Attacks against services provided by different systems.

● Technical or hardware damage to the machine during a storm. ✓

✓ 26.) Which of the following is **not** an advantage of cloud computing? * 1/1

○ Increases system reliability and user-friendliness.

● Increases risk in terms of security, privacy and confidentiality. ✓

○ IT systems easy to deploy, operate and maintain.

○ Efficient for service providers.

✓ 27.) What is the difference between **MAC** and **DAC**? * 1/1

○ For Mac, the reference monitor must check all access, for DAC this is set by the user.

○ For MAC, untrusted users can grant access rights, for DAC not possible.

● With DAC, untrusted users can grant access rights, not possible with MAC. ✓

○ Access protection is discrete for DAC, continuous for MAC.

✓ 28.) Which **protocol** is used to securely access web pages? * 1/1

● HTTPS ✓

○ HTTP

○ Google Chrome

○ Mozila FireFox.

✓ 29.) What does the term "**MAC function**" mean? * 1/1

○ Medium Access Control protocol.

○ Mandatory Access Control based access protocol.

● Message Authentication Code calculation. ✓

○ Key generation on Apple MacBook computers.

✓ 30.) Which is **not** true for Android? * 1/1

○ Least code running with root privileges.

○ At startup, each component assumes that the underlying components are sufficiently secure.

● Application signatures allow developers to be verified. ✓

○ Ability to exploit security capabilities of some processors despite processor independence.

✓ 31.) What can be overwritten other than the return address during a stack overflow attack? * 1/1

○ Controllable data.

● Non-controllable data. ✓

○ Return address only.

○ The contents of the entire stack.

✓ 32.) What is a certificate revocation list (CLR)? * 1/1

○ List of certificates revoked after expiration.

○ A sequence of steps to follow when revoking a certificate.

● List of certificates revoked before expiration. ✓

○ List of certificates about to expire.

✓ 33.) What is the use of storing the hash of the password in the control table instead of the password? *1/1

○ It is not useful to store a hash instead of a password.

○ Because of the hash, it takes 1000 years to crack the password.

● The hash cannot be used to decrypt the password, but it can be used to compare whether the password is correct. ✓

○ Instead of a hash, a fraction of the password is stored.

✗ 34.) Which does **not** increase security risks? * 0/1

○ Threats

○ Vulnerabilities

● Countermeasures ✗

○ Short passwords

Correct answer

● Short passwords

✓ 35.) What is the AES block size? * 1/1

○ 32 bits.

○ 64 bits.

● 128 bits. ✓

○ 256 bits.

✓ 36.) What is a difficult mathematical problem related to the security of the Diffie-Hellman protocol? * 1/1

○ Factorization.

● Discrete logarithm calculation ✓

○ Decoding linear codes.

○ Factorization modulo a large prime number.

✓ 37.) How does **Caesar Encryption** work? * 1/1

○ Substitutes plaintext letters from a set of real numbers.

● Replaces the letters in plain text with letters of the alphabet at a specified distance from it. ✓

○ Complements the letters in plain text with the letters in the real number set.

○ Complements the letters in plain text by one letter of the alphabet spaced at a given distance from it.

✓ 38.) What hard math problem does the RSA system pose? * 1/1

● Key-Pair generation algorithm. ✓

○ Discrete logarithm.

○ Taylor polynomial.

○ Differential calculus.

✓ 39.) Return-to-LibC attack... * 1/1

● Specifies a LibC in-memory function as return address parameterized by malicious code. ✓

○ On boot, the machine will no longer load the op. system because the op. system will be infected with LibC.

○ No such attack, Return-toLibC is a valid assembler instruction.

○ Overwrite the LibC library with a long NOP sled which is terminated with a RET statement.

✓ 40.) What should not be logged? * 1/1

○ Allow resource access.

○ Unsuccessful system call.

○ Location information (geolocation).

● Password. ✓

✓ 41.) How can we measure the strength of a randomly chosen password? * 1/1

○ H = L * logN 2

○ H = L * log2 L * N

● H = L * log2 N ✓

○ H = L * logL N

✓ 42.) What is **security**? * 1/1

○ Antivirus protection for your computer

○ Protects against accidental hardware failures.

● Focuses on the risks from deliberate attacks by intelligent attackers (malware). ✓

○ Tries to minimize the damage caused by accidents.

✓ 43.) What is not in a DMZ layout / DMZ topology? * 1/1

○ Server.

○ Packet filter.

○ Application proxy.

● Direct connectivity between the internal network and the DMZ. ✓

✓ 44.) Which approach is **least effective** against XSS? * 1/1

● Blacklist. ✓

○ HTTP - only cookie.

○ CSP.

○ Whitelist.

✓ 45.) What is usually the first step in a web-server attack? * 1/1

○ Lock out the user.

● Maximize the attack surface. ✓

○ Redirect important data.

○ Implement strong security measures.

✓ 46.) Developing secure software is difficult. Which reason is **not** supported? * 1/1

○ Security testing is difficult.

○ Developers face time, functionality and resource constraints.

● Attackers have a much easier time than developers. ✓

○ Security is difficult to measure.

✓ 47.) What is a CVE (Common Vulnerabilities and Exposures)? * 1/1

○ An online platform for critical vulnerability testing.

○ A parameter in the operating system to check the virtualized environment currently in use.

○ A technique to exploit vulnerabilities in electric cars.

● A database containing all known vulnerabilities, i.e. a publicly available database containing all vulnerabilities. ✓

✓ 48.) What is the best performance for fingerprint matching? * 1/1

○ High FA and low FR rate.

○ High FA and FR rate.

● Low FA and FR rate. ✓

○ Low FA and high FR rate.

✓ 49.) Software detects corrupted input data, what should it do? * 1/1

○ The software must still perform the programmed calculations.

● The input data must be rejected and the event logged ✓

○ The software should attempt to recover the corrupted data.

○ The software shall log the corrupted data.

✓ 50.) What is the Kerckhoffs principle? * 1/1

● Assume that the encryption algorithm is known to the attacker. ✓

○ Assume that the encryption algorithm is not known to the attacker

○ Assume that the encryption algorithm is known to the user.

○ Assume that the encryption algorithm is not known to the user.

✓ 51.) What is **not** the purpose of the OWASP project? * 1/1

● To distribute the best security software on the market. ✓

○ To raise funds for security awareness training.

○ To gather the best experts to develop OWASP materials.

○ To serve as a checklist for developers with the TOP 10 list.

✓ 52.) Why to use automated vulnerability checking software? * 1/1

○ They find all bugs, even the unknown ones.

○ No need to spend any time on manual testing during penetration testing.

○ IDS systems are also detected.

● They can look through a lot of bugs quickly, a great help for manual testing. ✓

✓ 53.) What is nonces? * 1/1

○ Single use keys.

○ Set of single-use viruses.

● Unpredictable real numbers. ✓

○ Co-domain of single-use keys.

✓ 54.) What is safety? * 1/1

● Focuses on risks from accidental failures, accidents and natural disasters. ✓

○ Helps to protect against viruses received by correspondents.

○ Protects against malware in case of unsafe downloads from various torrent sites.

○ Protects against operating system failures.

✓ 55.) What does buffer overflow exploit? * 1/1

○ The program has a memory leak, it does not release all the buffers it has reserved.

○ The program refers to an already freed buffer area.

● The program does not check how much data is written to a given buffer size. ✓

○ The program increments the buffer index until it turns negative and thus flushes out the buffer.

✗ 56.) What are the characteristics of a targeted attack? * 0/1

○ The target is innocently chosen: the attack tools used are not customised

● The target is randomly selected. the attack tools used are customized. ✗

○ The target is not randomly chosen, the offensive tools used are customized.

○ The target is not randomly selected. the offensive devices used are not customised.

Correct answer

● The target is not randomly chosen, the offensive tools used are customized.

✓ 57.) What are the characteristics of a script kiddie? * 1/1

○ Limited technical capabilities, Limited information retrieval capabilities, Significant resources.

● Limited technical capabilities, Limited information retrieval capabilities, Limited resources. ✓

○ Variable technical capabilities, Advanced information retrieval capability, Significant resources.

○ Advanced technical skills, Advanced information gathering skills, limited resources.

✗ 58.) What is the purpose of authentication? * 0/1

● To define the set of privileges of a (already logged in) user. ✗

○ To log the operations performed (or intended to be performed) by users, together with their context.

○ To decide whether a given (logged in) user X can perform a given operation Y on a given object Z.

○ The disclosure and credible proof of identity of a user who intends to use the system.

Correct answer

● The disclosure and credible proof of identity of a user who intends to use the system.

✗ 59.) What is a security incident? * 0/1

○ Malfunction caused by an accidental error.

● System compromise caused by an intentional attack. ✗

○ System compromise caused by an intentional attack that has been detected.

○ Malfunction caused by accidental failure and detected.

Correct answer

● System compromise caused by an intentional attack that has been detected.

✓ 60.) Which statement is false? * 1/1

○ Attacks usually exploit vulnerabilities in IT systems.

● Security mechanisms usually make it impossible for attacks to take place. ✓

○ Security mechanisms try to eliminate vulnerabilities in IT systems.

○ Successful attacks can lead to the compromise of IT systems.

✗ 61.) Which of the following can Siri send information from an iOS device to the cloud while it is running? *0/1

○ The current battery charge level.

● The user's Apple ID. ✗

○ Music library information.

○ Data from the accelerometer sensor.

Correct answer

● Music library information.

✓ 62.) Which of the following is the most commonly used two-factor authentication method in practice? *1/1

○ Using a fingerprint and a mobile token generator.

● Using a password and a mobile token generator. ✓

○ Using a password and a trust question.

○ Using a password and a PIN.

✗ 63.) Why is penetration testing important? * 0/1

○ Because it helps to deal with incidents faster.

○ Because it can provide feedback on system security in the early stages of development.

○ Because it can be used to demonstrate what an attacker would need against a live system.

● Because it can be used to train developers in security awareness. ✗

Correct answer

● Because it can be used to demonstrate what an attacker would need against a live system.

✗ 64.) Which method is not a possible defense against buffer overflow? * 0/1

○ Formal proof of the correctness of the code base.

○ Implement security testing to find bugs.

○ Restricting user rights.

● Using a memory-safe programming language. ✗

Correct answer

● Restricting user rights.

✗ 65.) Which of the following is not a typical target for security incident management? *0/1

○ Identify and report the attacker who caused the incident.

● Collect data in a way that it can be used as evidence in forensic proceedings. ✗

○ Restoring the system to its original state.

○ Finding out the cause of the incident in order to avoid similar incidents in the future.

Correct answer

● Identify and report the attacker who caused the incident.

✓ 66.) In practice, which of the following is the least likely to be the basis of an attack against a crypto system? *1/1

● Hacking the cryptographic primitive used. ✓

○ Side channel attack against the implementation.

○ Weak key management.

○ Protocol failure.

✓ 67.) Which is typical for a worm attack? * 1/1

○ Has a very long, straightforward code structure.

○ Uses polymorphic code that cannot be detected by antivirus programs.

● Can spread automatically by exploiting vulnerabilities, fast. ✓

○ It relies on user interaction and therefore spreads slowly.

✓ 68.) One of the main objectives of the "**Duqu**" malware scan was.... * 1/1

○ ...to identify the adversary.

○ ...to find out how much data was lost.

○ ...to determine how vulnerable the system is.

● ...to restore normal workflow and understand who, why, how and with what they were attacking. ✓

✗ 69.) Security mechanisms can be preventive, which seek to prevent attacks, or detective, which seek to detect successful attacks. Which of the following statements is true? *0/1

● ASLR (Address Space Layout Randomization) is a detection mechanism. ✗

○ Cryptography is a detection mechanism.

○ Security awareness is a preventive method.

○ Message authentication code (MAC) is a preventive security mechanism.

Correct answer

● Security awareness is a preventive method.

✗ 70.) What is not a typical purpose of security incident handling? * 0/1

○ Finding out the cause of the incident to prevent similar incidents in the future.

● To collect data in such a way that it can be used as evidence in forensic proceedings. ✗

○ To restore the system to its original state.

○ Identify and report the attacker who caused the incident.

Correct answer

● Identify and report the attacker who caused the incident.

✓ 71.) What is a short password certificate? * 1/1

● A digitally signed data structure that inseparably shares the public key with its owner. ✓

○ The signature created with the public key O c. The private key associated with the public key.

○ Private key associated with the public key.

○ A digitally signed data structure that inextricably links the public key to the private key.

✗ 72.) What is an advantage of an anomaly-based iDS? * 0/1

○ It never commits a false positive error.

○ It can detect unknown attacks.

○ Significantly reduces the administrator's load.

● Never commits false negative detection. ✗

Correct answer

● It can detect unknown attacks.

✗ 73.) What is pseudo-anonymisation? * 0/1

● Removal of sensitive attributes. ✗

○ Generalisation of quasi-identifiers.

○ Removal of all attributes from the database that are quasi-identifiers.

○ Removal from the database of all attributes that are direct identifiers.

Correct answer

● Removal from the database of all attributes that are direct identifiers.

✗ 74.) What is the purpose of a cryptographic hash function? * 0/1

○ Message authentication.

○ Integrity protection.

● Fast search in cryptographic data. ✗

○ Message impression calculation.

Correct answer

● Message impression calculation.

✗ 75.) Which of the following is not really a system compromise from a security perspective? *0/1

○ Someone obtains the administrator's password and then uses it to log in and intentionally perform operations that bring a distributed database into an inconsistent state.

● Someone inadvertently obtains the administrator's password and then uses it to log in and execute random commands in a random manner, resulting in an inconsistent state of a distributed database. ✗

○ An accidental power outage causes servers to shut down, resulting in a distributed database being in an inconsistent state.

○ Someone intentionally causes a power failure, which causes servers to shut down, resulting in a distributed database being inconsistent.

Correct answer

● An accidental power outage causes servers to shut down, resulting in a distributed database being in an inconsistent state.