Last Year’s Midterms and Pictures

1. What is a blind SQL injection?

A A helper application for SQL injection developed for the partially sighted

B A type of attack where the result is not directly visible to attacker

C When the attacker is only capable of randomly modifying the SQL query

D When the attacker is only capable of modifying the SQL query with the help of a proxy module

Note: There are 2 different answers in the files we have.

I guess B is correct based on
https://owasp.org/www-community/attacks/Blind_SQL_Injection

2. Interdependent privacy risks for a given user emerge owing to

A Negative externalities of data sharing with third parties

B High fixed costs of ICT services

C Positive externalities of data sharing with third parties

D The data sharing decisions of the given user

3. What is Stuxnet?

A a malware

B An Iranian uranium enrichment plan

C An industrial network standard

D A network of cyber criminal organizations

4. Which of the following solutions can provide protection against ROP attacks?

A ASLR

B Harvard architecture

C DEP

D NX bit

5. Information security is risk management. Assuming that attackers are becoming more skilled over time and other factors affecting the risk of an attack stay the same,

A The likelihood of the attack stays the same, but the risk increases

B The likelihood of the attack increases, hence the risk decreases

C The likelihood of the attack decreases, hence the risk increases

D The likelihood of the attack increases, hence the risk increases

6. What does the design principle “complete mediation” say?

A The amount of shared mechanisms should be minimized

B So\ware should run with the least amount of privileges necessary to complete its task

C Keep it small and simple

D Check every access to every object every time access is requested

7. Which of the following attacks is not relevant for key exchange protocols?

A Replay of protocol messages

B Impersonating a protocol participant

C Exhaustive key search attack

D Man-in-the-middle attack

Note: There are 2 different answers in the files we have.

8. Which of the following risks is not relevant for IT security?

A Denial of services provided by an IT system

B Illegal access to data

C Illegal modification of data

D Random hardware failures

9. What does k-anonymity mean?

A The direct identifiers of an individual match at least k records in the anonymized dataset

B The sensitive attribute values of an individual match at least k, or 0 records in the anonymized

dataset

C The quasi-identifiers if an individual match at least k, or 0 records in the anonymized dataset

D The sensitive attribute values of an individual match at most k records in the anonymized dataset

10. What property of JavaScript makes it dangerous?

A a user generated event is equivalent to a code-based event

B Every object inherits from a global prototype

C The language was developed in about 10 days

D Every variable is in the global scope

Note: There are 2 different answers in the files we have. From the slides I would say both are correct.

11. What is a shell code?

A a particular type of message integrity checksums

B The passcode needed to run the shell

C The program code of the OS shell (e. g. bash or cmD exe)

D Attacker input that aims at opening a shell

12. Which of these is not among the most common attacks against browsers?

A Stack/heap overflow

B Use-after-free

C Integer overflow

D Compromising the ASLR

Note: There are 2 different answers in the files we have.

13. Which of the following properties characterize cyber criminal groups?

A Advanced technical skills, variable information gathering capabilities, rich resources

B Advanced technical skills, advanced information gathering capabilities, limited resources

C Variable technical skills, limited information gathering capabilities, limited resources

D Limited technical skills, limited information gathering capabilities, rich resources

14. Which task is to relay security-related info to the development team?

A Security contact

B Security advisor

C Security team

D Security leadership team

15. What is not among the security goals of Google Chrome?

A Reducing the spreading of exploits

B Reducing the frequency of exposures

C Reducing the window of vulnerabilities

D Reducing the severity of vulnerabilities

16. What is a stack frame?

A Pair of memory addresses referring to the top and the bottom of the stack

B A framework for programming the stack

C Memory area referenced by the stack pointer

D Part of the stack handled by a given function when it is called

17. What does the design principle “least common mechanism” say?

A The amount of shared mechanisms should be minimized

B Software should run with the least amount of privileges necessary to complete the task

C Check every access to every object every time access is requested

D Consider the human in the loop

18. What does salting mean in the case of password hashing?

A Decreasing the hash computation time by optimization

B Increasing the hash computation time artificially

C Computing a hash of random length

D The hash depends on some random input, besides the password

19. Android device encryption feature protects against which of the following attacks?

A Reading user data from the memory of a phone that is tuned on

B Ransomware (since everything is already encrypted)

C Reading user data from the storage of a phone that is turned on, using a data cable disguised as a USB charging cable

D Reading user data from the flash chip of a phone that is turned off

20. Which of the following statements is FALSE?

A Developers are faced with constraints during the development process

B Measuring security is difficult

C Frameworks used during programming do not help the programmer in his/her work

D Attackers only need to find a single vulnerability, while developers have to pay attention to

everything in order for the so\ware to be secure.

21. What is the goal of browser fingerprinting?

A Identify the browser with cookies

B Identify the browser with its persistent attributes

C Identify the user with his/her direct identifiers

D Identify the browser only with its version number

Note: There are 2 different answers in the files we have.

22. Which of these is not a type of XSS?

A Reflected XSS

B Event based XSS

C DOM based XSS

D Persistent XSS

23. What is the main cause that computers can be cracked?

A They contain vulnerabilities

B No antivirus product is installed

C Programmers have strict deadlines

D The appropriate ports are not closed

24. The lemon market for information security is created by

A Information asymmetry

B Low demand

C High fixed costs

D High marginal costs

25. Which of these is performed as a first step during an IOS boot?

A The kernel is initialized

B The Apple root certificate is loaded

C The iBoot code is checked

D The low level bootloader is executed

Note: There are 2 different answers in the files we have.

26. Which of the following actions need a dangerous permission on Android?

A Sending HTTP POST request to the developer's server

B Turning on the vibrator

C Turning on the WIFI

D Sending an SMS

27. What is black-box testing?

A Checking only the input and the output, fuzzing

B A pentest where the ethical hacker has the source code

C A vulnerability testing where we have only minimal information on the target system

D When we use programs for testing that are not known by the developer

28. Why do we hash messages before signing them?

A This allows for shorter signature keys

B This makes the computation of the signature faster

C This ensures that besides signing, the message is also encrypted

D This makes it more difficult to forge signatures

29. Which security service is provided by encryption?

A Confidentiality

B Non-repudiation

C Integrity protection

D Message authentication

30. Zero-day vulnerabilities are…

A Unpublished vulnerabilities which are known to the attacker

B Vulnerabilities that can be identified in less than 1 day

C Vulnerabilities that can be fixed quickly with no effort

D Publicly well-known Vulnerabilities

31. What is a reference monitor in the model of access control?

A a dashboard where we can monitor the operation of our access control system

B An entity that keeps track of the reference to the objects and helps in garbage collection

C An entity that defines the access control rules

D An entity that enforces an access control policy

32. What is “lateral movement”?

A One element of an attack, where attackers go from one infected host to others

B A jump instruction based on memory load instructions

C Protected copy of memory arrays

D Using LM drivers to raise the level of security

33. How does hybrid encryption work?

A The data is encrypted with an asymmetric key cipher whose key is encrypted with symmetric key cipher

B The data is encrypted with a symmetric key cipher whose key is encrypted with an asymmetric key cipher

C We use the DES cipher in an encrypt-decrypt-encrypt mode (i. e. 3DES in EDE mode)

D We compute a MAC besides encrypting the data (like AES-CCM or AES-GCM)

34. What information can be obtained about a website without loading it or communicating with the

server?

A The kernel’s version number

B The version of the webserver, sometimes even the kind of the operating system

C The number of running threads

D The source code of scripts and the security level of the database

35. What is a fingerprint minutiae?

A Special area of the fingerprint (core or delta)

B A global fingerprint pattern (such as whirl, loop, arch)

C The graph defined by the ridge endings and bifurcations

D (Type (ending or bifurcation), position, direction) triplet

Note: There are 2 different answers in the files we have.

36. Which protocol do we use for accessing web pages securely?

A WPA2

B IPsec

C SSH

D TLS

37. A database contains the age, home address, and the list of visited locations of individuals. Which of these attributes do identify an individual the most in this dataset?

A Home address and 2 visited locations

B Age, home address and 2 visited locations

C Home address

D Age and 2 visited locations

38. What happens in case of a stack overflow?

A The computer runs out of stack memory

B Part of the stack is overwritten in an unexpected way

C Too much data is pushed on the stack and it overwrites part of the heap memory

D The return address of a function is overwritten on the stack

Note: There are 2 different answers in the files we have.

39. Which of the following programming languages is sensitive for buffer overflow problems?

A Python

B Java

C Rust

D C/C++

40. What is a reduction proof in modern cryptography?

A When we prove that breaking a given cipher is at least as hard as efficiently solving a hard (or believed to be hard) mathematical problem

B When we prove the security of each component of a cipher, from which it follows that the entire cipher is …

C When we prove that efficiently solving a hard (or believed to be hard) mathematical problem (e.g. factoring) ….. breaking a given cipher

D When we trace back the problem of breaking a given cipher to that of breaking one of its components, or ….. prove that it is sufficient to break that single component to break the cipher.

41. What is a botnet?

A a network designed as a fractal for robust calculations

B Anonymization network with many participants

C A cluster of computers used for distributed computing (hard math problems)

D A network of infected computers (also named zombies) made by attackers

42. Most important properties of worm attacks is

A Needs user interaction and hence spreads slowly

B Exploiting network Vulnerabilities they replicate rapidly automatically

C Very hard to detect by antivirus tools as they use polymorphic code

D Have a very long code structure

43. In fuzzing, the test executor…

A Does not user error reports

B Instruments the analyzed piece of software

C Provides the secure random number generator

D Collects data about the execution

Note: There are 2 different answers in the files we have.

44. The cascade (vienna) computer virus …

A One of the first cyber-physical attacks around 2010

B Infected DEC machines back in the 1970's

C Is one of the first brutal worm attacks in the early 2000's

D Is originating from the 1980's and it made big media coverage

45. What is the purpose of secure Enclave coprocessor?

A Providing a secure boot for the system

B Signature checking for applications

C Recording and storing fitness data

D Handling the Touch ID sensor

46. What are the links NOT encrypted in TOR?

A Between the Entry Onion Router and the Onion Proxy

B Between the Exit Onion Router and the destination

C Between two Onion Routers

D Between the Entry and the Exit Onion Routers

47. Which of the following decisions related to so\ware development must concern itself with the principle of fail-safe defaults?

A Deciding how to document the internal structure of the so\ware in the user manual

B Creation of the user account via which the so\ware can connect to the database

C Designing the buttons on the GUI

D Decision concerning the default configuration values

48. How do we determine the risk?

a. likelihood of successful attacks x their impact

b. attack surface x potential loss

c. potential loss / countermeasures

d. threats x vulnerabilities

Google Forms Quiz

Proof of cancellation

In some applications, it may be useful if the provider can sort the encrypted data (e.g.: the user wants to see the results in an orderly way)

When the computation is outsourced, the user can be sure that the service provider has actually performed the requested task.

Allows keyword searches on encrypted data. The provider cannot learn which words have been searched or what the statistical properties of the encrypted data are.

When a data is stored in the cloud, the user can be sure that the data still exists

When data is removed from the cloud the user can be sure that all copies of it have been deleted.

A countermeasure against side-channel attacks, e.g. to break the link between the leaked information and the confidential data

True

False

What is the hash-and-sign paradigm?

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

What is the purpose of the cryptographic hash function?

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

CAs are typically organized in a hierarchy, where the key of a subordinate CA is attested by another CA at a higher level

True

False

Clocks must be synchronized for nonces (unpredictable real numbers)

True

False

What is the difference between risk minimisation and risk optimisation?

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

What does the open design principle say?

Safety through obscurity

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

How are you protected for long-term storage on iOS?

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

What type of attack is possible if the key space is small?

brute force

Trojan

malware

any

Nonces (unpredictable real numbers) do not require an extra message to be sent

True

False

What is a certificate chain?

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)

What is a stack frame?

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

What factors determine the IT security risk? (Multiple answers are fine)

repair

threats

countermeasures

vulnerabilities

What is stretching?

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

What do we mean by key space in encryption?

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

What is NOT a definition or characteristic of stack overflow?

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

What is a MAC?

the name of certain apple products

unique identifier

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)

Which is NOT one of the hacker groups?

Script Kiddie

Disgruntled employee

Hacktivist group

Terrorist organization

Computer crime organization

State sponsored attacker

Computer scientists

Which characteristic does NOT describe the White/Grey box?

Static analysis

Dynamic analysis with specific inputs

Aims to maximize code coverage

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

Generates inputs that trigger new code paths

Much more efficient, but high cost of entry

Clocks need to be synchronized for timestamps

True

False

The Oracle attack allows an attacker to efficiently decrypt any encrypted CBC ciphertext message with (adaptively) formatted ciphertexts to the server and observe its response

True

False

How does public key binding to an authorized user work?

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

The user ID and the public key are automatically generated together

The user can choose the public key that suits him

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

What is the birthday paradox and how does it relate to the hash function?

choose an arbitrary date as birthday and extend it with a hash function

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

chooses an arbitrary date as a birthday, nothing to do with the 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)

How can we ensure key freshness?

with timestamps, time windows

a nice refreshing cocktail

calendar synchronisation

timers

With homomorphic encryption, the cloud service provider can perform certain operations on the encrypted data and obtain the encrypted result without ever having access to the data

True

False

Global types of fingerprint patterns: swirl, loop, arc

True

False

What is Stretching?

multiple iterations to slow the exhaustion attack

a random number generated by the system to make the pre-compute attack impractical. Adds a long random string to the password before…

What is the average complexity of an exhaustive key search attack on a k-bit key?

(k-1)

2^(k-1) * 10^10

(k-1)^2

2^(k-1)

What type of information is useful to collect before the attack (there can be several good answers)

System architecture

Security mechanism used

Access rights

Geological location

The Caesar cipher is easy to crack because a fixed number is the size of the key space. What is this number?

22

64

67

25

What is the key size of AES? (There can be several good answers)

128

64

192

256

What are the characteristics of a monoalphabetic substitution cipher? (Multiple answers are allowed)

disadvantage: the frequency of letters depends on the language, not on the content of the text e.g. in Hungarian the most common letter is "e"

generalization of Caesar cipher

advantage: takes up little storage space

letter substitution is determined by permutation

disadvantage: very easy to crack with the right technical tools

the key is the permutation, which has an area of 26!

How many steps does it take to crack a complete system?

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

What programming error can lead to SQL injection

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

Which risk is not relevant for IT security?

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

What are the steps for fingerprint matching (multiple answers are fine)

matching the two fingerprints according to the most similar minutia pairs

search for parallel similarity between minutiae

Calculating a global similarity score and making a decision

create a minutia correspondence

Which of the following is NOT an advantage of cloud computing?

Increases system reliability and user-friendliness

Flexible provision of resources

Increases risk in terms of security, privacy and confidentiality

Reduced price for the user

Efficient for service providers

IT systems easy to deploy, operate and maintain

Which can be an effective defense against ROP?

NX bit

DEP

ASLR random addresses -> cannot predict gadaget addresses

Harvard arch

How can we ensure that the established key remains secret?

By encrypting

With RSA

Key exchange protocols

Cannot be kept secret

What are the types of side-channel information?

Timing

network

power consumption

human

In the access protection model, what is a reference monitor?

The entity that enforces the access protection policy

The dashboard interface to monitor the operation of the access control policy

The entity that keeps track of existing references to objects for the garbage collector

The entity that defines the access control rules

In an XSS attack, an attacker successfully executes JavaScript code in the context of another origin

True

False

What is the difference between MAC and DAC?

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

Which protocol is used to securely access web pages?

HTTPS

HTTP

GOOGLE CHROME

MOZILLA FIREFOX

What are the functions of the certification authority? (multiple answers are fine)

publish valid certificates and certificate revocation lists

organizes certificates

issues certificates to users or other CAs

What does the term MAC function mean?

Medium Access Control protocol

Mandatory Access Control based access protocol

Message Authentication Code calculation

Key generation on Apple MacBook computers

Which is NOT true for Android?

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

What can be overwritten other than the return address during a stack overflow attack?

controllable data

non-controllable data

return address only

the contents of the entire stack

Linux implements a non-discretionary access control (DAC) system

True

False

What is a certificate revocation list (CLR)?

A sequence of steps to follow when revoking a certificate

List of certificates revoked after expiration

List of certificates revoked before expiration

List of certificates about to expire

What is the use of storing the hash of the password in the control table instead of the password?

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

Verifiable calculation

In some applications it may be useful if the provider can sort the encrypted data (e.g.: the user wants to see the results in an orderly way)

When the computation is outsourced, the user can be sure that the provider has actually performed the requested task.

Allows keyword searches on encrypted data. The provider cannot learn which words have been searched or what the statistical properties of the encrypted data are.

When a data is stored in the cloud, the user can be sure that the data still exists

When data is removed from the cloud the user can be sure that all copies of it have been deleted.

What is a zero-day vulnerability?

vulnerabilities that are known only to potential attackers

online mail vulnerabilities

vulnerability of the computer's own back-up storage

vulnerabilities that are accidental, not known to anyone

What are the disadvantages of cloud computing?

Increases the risk from security, privacy and confidentiality perspectives

Increases system reliability and user friendliness

Flexible provision of resources

Reduced price for the user

Efficient for service providers

Easy deployment, operation and maintenance of IT systems

Which does NOT increase security risks?

Threats

Vulnerabilities

Countermeasures

Short password

What is the AES block size?

32 bits

64 bit

256 bit

128 bit

Signature errors occur when a variable with a signature is interpreted as a signature or when a signed variable is signed.

True

False

What is a difficult mathematical problem related to the security of the Diffie-Hellman protocol?

Factorization

Discrete logarithm calculation

Decoding linear codes

Factorization modulo a large prime number

Sequence preserving encryption...

In some applications, it may be useful if the provider can sort the encrypted data (e.g.: the user wants to see the results in order)

When the computation is outsourced, the user can be sure that the provider has actually performed the requested task.

Allows keyword searches on encrypted data. The provider cannot learn which words have been searched or what the statistical properties of the encrypted data are.

When a data is stored in the cloud, the user can be sure that the data still exists

When data is removed from the cloud the user can be sure that all copies of it have been deleted.

There is no need to revoke a certificate if there is a change in the personal data in the certificate

True

False

How does Caesar encryption work?

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

Side-channel attacks are based on information caused by the actual execution of the cryptographic algorithm (leaked by the algorithm)

True

False

What hard math problem does the RSA system pose?

key pair generation algorithm

Discrete logarithm

Taylor polynomial

Differential calculus

Return-to-LibC attack?

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

Why do these vulnerabilities occur in practice?

due to shitty BME

connecting to external peripherals

IT systems are increasingly complex, making it difficult to fully cover all possible problems

operating system upgrade

What is Salting?

multiple iterations to slow the exhaustion attack

a random number generated by the system to make the pre-compute attack impractical. Adds a long random string to the password before stacking

What should not be logged?

Allow resource access

Unsuccessful system call

Location information (geolocation)

Password

What does the open design principle say?

The software can be freely developed by anyone later

Design should be open to the community

The number of shared mechanisms should be minimised

The default value should be chosen so that the system remains secure in case of failure

How can we measure the strength of a randomly chosen password?

H = L * logN 2

H = L * log2 L * N

H = L * log2 N

H = L * logL N

What can financial resources be converted into? (there may be several good answers)

increase information gathering skills

deepen technical expertise

renting space with appropriate temperature

access to advanced attack tools and methods

What is security?

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

What is not in a DMZ layout?

Direct connectivity between the internal network and the DMZ

Application proxy

Packet filter

Server

What questions should be answered in the risk optimization process (multiple answers are fine)?

What are the potential threats?

What are the known vulnerabilities/vulnerabilities?

How likely are these vulnerabilities to be exploited by potential threats?

What is the expected loss?

What countermeasures will reduce the risk in a cost-effective way?

The sequence of NOP instructions that slides the CPU instruction execution stream to its final, desired location

True

False

Which approach is least effective against XSS?

Blacklist

HTTP- only cookie

CSP

Whitelist

Which of the following is performed as the first step when booting iOS?

kernel is initialized

low level bootloader

iBoot code verification

apple root certificate is loaded

What is usually the first step in a web server attack?

lock out the user

maximize the attack surface

redirect important data

Developing secure software is difficult. Which reason is NOT supported?

Security testing is difficult

Developers face time, functionality and resource constraints

Attackers have a much easier time than developers

Security is difficult to measure

What is a CVE (Common Vulnerabilities and Exposures)?

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

What is the best performance for fingerprint matching?

High FA and low FR rate

High FA and FR rate

Low FA and FR rate

Low FA and high FR rate

What are the criteria for threat classification? (There may be several good answers)

Motivation

information gathering capabilities

level of technical expertise

level of (resources)

Software detects corrupted input data, what should it do?

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

user authentication = process of verifying the identity of the requested user

True

False

What is the Kerckhoffs principle?

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

The debugging system is a database of errors, which includes information about privacy

True

False

What is NOT the purpose of the OWASP project?

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

Why use automated vulnerability checking software?

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

What is nonces?

single use keys

set of single-use viruses

Co-domain of single-use keys

Unpredictable real numbers

IT security does not deal with ...?

Random hardware failures

Unauthorized modification of data

Unavailability of services provided by the IT system

Unauthorized access to data

What are the two main types of modern corrections?

Flooding/Flow

Overloading

Blocking

Network monitoring

Data ownership verification

In some applications, it may be useful if the provider can sort the encrypted data (e.g.: the user wants to see the results in an orderly way)

When the computation is outsourced, the user can be sure that the service provider has actually performed the requested task.

Allows keyword searches on encrypted data. The provider cannot learn which words have been searched or what the statistical properties of the encrypted data are.

When a data is stored in the cloud, the user can be sure that the data still exists

When data is removed from the cloud the user can be sure that all copies of it have been deleted.

What is one of the key differences between Linux and Windows in terms of access control?

The Linux security system allows a wider range of policies to be written

The Windows security system allows you to describe a wider range of policies

For nonces (unpredictable real numbers), it is enough to measure time locally

True

False

What types of vulnerabilities exist in IT systems? (More than one answer is fine)

technical

physical

personal

operational

What is Stuxnet?

An improved version of the Trojan

New virus scanner

The most threatening Malware in history

A database of viruses

How is the cyber underground organized (who are the players)?

information traders

resource traders

service providers

R&D people, tool makers

criminals, fraudsters and attackers

cashier

In hacking, shellcode is a small piece of code used to exploit a vulnerability in software.

True

False

For time stamps, replay can only work within a small time window

True

False

Searchable encryption...

In some applications, it may be useful if the provider can sort the encrypted data (e.g.: the user wants to see the results in an orderly way)

When the calculation is outsourced, the user can be sure that the provider has actually performed the requested task.

Allows keyword searches on encrypted data. The provider cannot learn which words have been searched or what the statistical properties of the encrypted data are.

When a data is stored in the cloud, the user can be sure that the data still exists

When data is removed from the cloud the user can be sure that all copies of it have been deleted.

What is the function of the Secure Enclave coprocessor?

Application signature verification

Touch ID sensor management

Secure system loading

Secure capture and storage of movement-related data

What is safety?

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

What types of countermeasures exist to reduce the risk? (There may be several good answers)

physical

network

none

technical

What is fingerprint minutia?

Global fingerprint pattern (swirl, loop, ...)

Graph of line endings and branchings

Specific area on the fingerprint, such as core and delta

Triple combination of type (line end or branch), position, direction

What does buffer overflow exploit?

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

What is black-box testing?

A check where even the source code is known to the ethical checker

Testing only input and output, fuzzing

The check uses programs unknown to the developer

Verification where only the minimum prior knowledge of the system is known -> only inputs and outputs are examined, the inner workings are not known

What is the key to Caesar encryption?

an arbitrary number generated when the key is generated

an arbitrary letter from abc

the offset value

a pointer pointing to the encrypted message

01 History of Cryptography

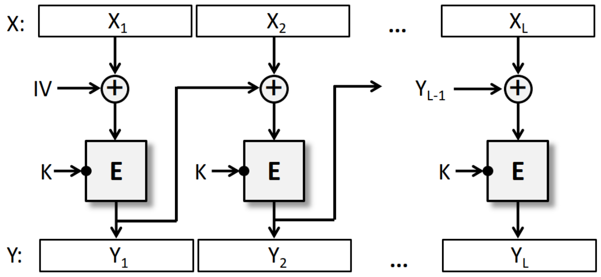
no control questions in the slides, but there are questions about Caesar and Monoalphabetic substitution in the examples.

02 Modern Crypto

How are modern ciphers classified? (types of ciphers?)
Symmetric key ciphers: stream ciphers or block ciphers
Asymmetric key ciphers (slide 5)

What are the block size and the key size of AES?
Block size: 128 bits
Key size: 128, 192 or 256 bits (slide 8)

How does the CBC block encryption mode work?
First, the message will be split into blocks. The first block will be XORed with an initial value (IV) then the block is encrypted using the key K. The next block will be XORed with the encrypted message gained in the step before and then encrypted with the same key K.
(slide 12)



$$\boxed{Y_i = E_K(X_i + Y_{i-1})}$$

Why do we use a hybrid approach for encrypting large messages instead of pure public key encryption?
Public key cryptography is slower than symmetric key cryptography. The hybrid approach can solve that speed problem. (slide 21)

What is a cryptographic hash function?
A function that maps arbitrary long messages into a fixed length output. (slide 23)

What are the desired security properties of hash functions?

- weak collision resistance *(given an input x, it is computationally infeasible to find a second input x' such that H(x') = H(x))*
- strong collision resistance *(it is computationally infeasible to find any two distinct inputs x and x' such that H(x) = H(x'))*
- one-way property *(given a hash value y (for which no preimage is known), it is computationally infeasible to find any input x such that H(x) = y)*
  (slide 24)

What services do MAC functions provide and how?
Message Authentication Codes are used for message authentication and integrity protection. It maps an arbitrary long message and a key to a fixed length output (checksum). If the message is changed during the transmission the MAC value changes too. (slide 25)

What services do digital signature schemes provide and how?
Similar to MAC functions they provide message authentication and integrity protection and in addition non-repudiation of origin. The origin can be proven to a third party for verification. (slide 26)

What is the hash-and-sign paradigm?

The efficiency increases when we sign the hash of the message instead of the message.

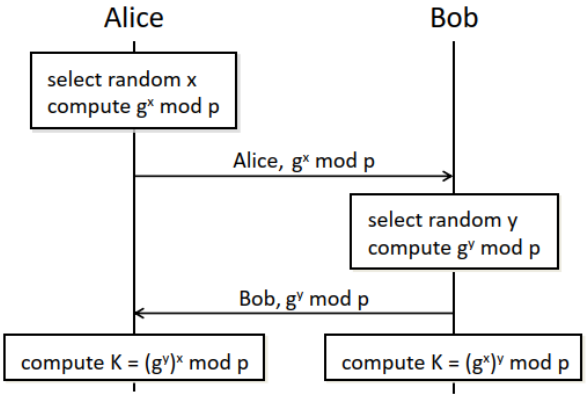
What are the design objectives of key exchange protocols?

- Secrecy of the key
- key authentication
- key freshness
  (slide 32)

What is the difference between key transport and keyagreement?
key agreement: key derived by a function of information provided by both parties. No party can determine the resulting value. They create the key together.
key transport: one party creates the new key and transfers it to the other. (slide 33)

How can we ensure key secrecy, authenticity, and freshness in key transport protocols?
Alice and Bob share long-term keys (K_alice and K_bob) with a trusted party.
secrecy: trusted part creates new K and encryptes it with K_alice and K_bob
authentication: authentication all data with K_alice and K_bob
freshness: provide timestamps or nonces (slide 37)

How does the Diffie-Hellman key agreement protocol work?



(slide 34)

What needs to be added to the basic protocol in practice?
Signing the data transfer, so no attacker can spoof the communication. (slide 36)

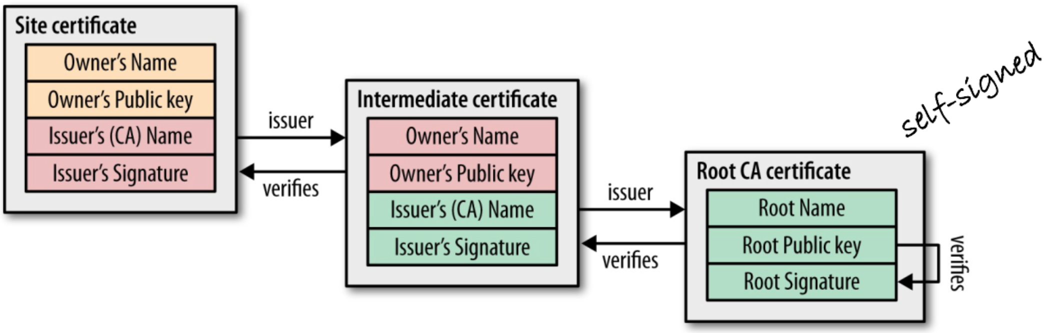
What is a public key certificate? How do we verify it?
Either by encrypting signed keys or by signing encrypted keys. Both parties know the public keys already to verify. (slide 40)

What are the functions of a Certificate Authority?
Binding the public key to an entity, so they can authenticate parties during public key exchanges. (slide 41)

- issue certificates for users
- maintain certificate revocation information
- publish currently valid certificates and revocations lists
- maintain archives (slide 42)

How does a hierarchical PKI look like?
directed tree structure with a root CA. Low-Level CAs are certified by higher-level ones. (slide 43)

What is a certificate chain?
End-users have an authentic public key of a root CA. Starting from the root CA every party can be verified by its predecessor until the end-user. (slide 44)

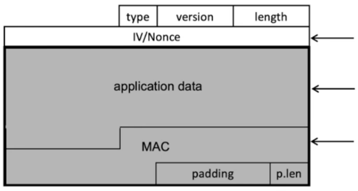


What security services does TLS provide?

Secure connection between the application (browser and server)

- confidentiality
- integrity protection
- mutual authentication of parties
- key exchange
- negotiation of cryptographic algorithms and parameters (slide 47)

How does the TLS Record Protocol work? (message format)



if needed (e.g., CBC mode or authenticated encryption mode)

encrypted payload (confidentiality)

Message Authentication Code (authentication, integrity, and replay protection)

Gray: encrypted (slide 49)

What key exchange methods are supported by TLS? How do they work?

- RSA based
- fixed Diffie-Hellman
- ephemeral Diffi-Hellmann
- anonymous Diffie-Hellman (slide 51)

What are the main reasons for cryptographic systems to fail?

- key management issues (weak random number generators)
- protocol weaknesses (used in wrong ways)
- implementation issues (bugs, side channels)
- human stupidity (using homemade “crypto”) (slide 54)

What do we mean by a side-channel attack? What types of side-channel information do you know?

side-channel attacks are based on information leaked out by the actual implementation of a crypto algorithm, e. g.

- timing information
- power consumption
- any source of extra information that can be exploited (slide 61)

03 Authentication, Authorization

What do the three As in AAA mean?
Authentication (identify), Authorization (check permission), Access control (enforcing the authorization policy), Accounting/Auditing (logging actions) (slide 2,3)

What are the three means of authentication? Give some examples for each.
knowledge-based (password), possession-based (mobile devices, key card, usb-stick), inherence-based (fingerprints) (slide 5)

What is the idea of 2FA/MA? How is it useful?
Using 2 or more authentication methods together to identify. It increases security because attackers need 2 things. (slide 6)

What are three methods of attacking password-protected systems?
eavesdropping, keyloggers, social engineering attacks (slide 8)
brute force, dictionary attacks, hybrid attacks (slide 9)

Why is it better to store password hashes instead of the plaintext passwords?
We can’t get the password from the hash, but we can compare the hash values to verify the password. (slide 12)

What is the purpose of salting?
adding a random value to a password before hashing. So the same passwords will have different hash values. (slide 13)

What is the purpose of stretching?
artificially increasing the time of the hash function to slow down attackers. (slide 13)

Explain how mobile authenticators (mobile tokens) work.
User gets an SMS or a code in his authenticator application to verify that he is in possession of the device. (slide 26)

Describe the model of inherence-based authentication.
The system is trained (samples) to recognize the features. When the user wants to login in he presents his feature and the system verifies it according to the trained known features. (slide 38)

What five requirements must an inherence-based authentication solution meet to be viable?

- Universality (everyone has it)
- Uniqueness (noone has the same)
- Permanence (doesn’t change with time)
- Collectability (can be measured)
- Low possibility of circumvention (can’t be forged) (slide 37)

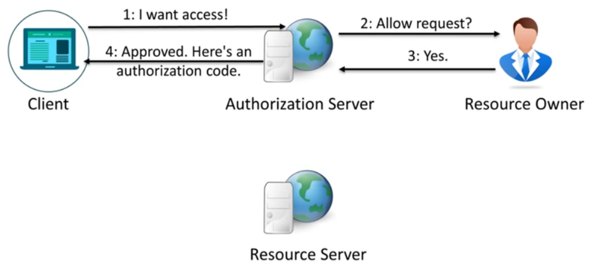
What is the primary purpose of OAuth?

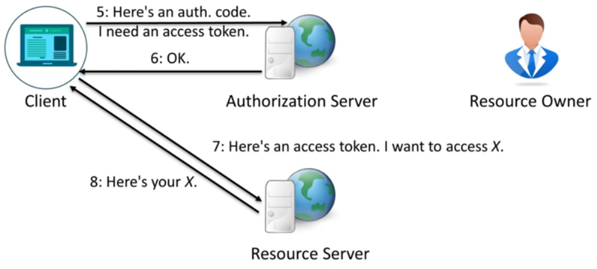
Originally intended to be used for access delegation.
Users can grant access to resources without disclosing their password. (slide 50)

What actors are there in OAuth? Briefly explain the role of each.

- user: person who authorizes a client to access a set of data
- client: application that access the data of the resource owner
- resource server: server that hosts and serves the protected data
- access token: used by the client to access data on the server
- Authorization server: server where the user accept/rejects request for data acces
- refresh token: used to get new access token after expiration
- scope: permission to access data elements (slide 51/52)

Describe the Authorization Code Flow (OAuth).




5: Here's an auth. code. I need an access token.
6: OK.
Client
Authorization Server
Resource Owner
7: Here's an access token. I want to access X.
8: Here's your X.
Resource Server

What are authenticators in FIDO?
Fast IDentity Online.
Bound and Roaming authenticators.
Bound: built into device (fingerprint reader)
Roaming: portable (USB key, NFC card) (slide 41)

What is WebAuthn?
JavaScript API that makes it possible to use FIDO authentication straight from within the browser. (slide 44)

What is the purpose of WebAuthn?
User authentication

What is the purpose of SAML?
Security Assertion Markup Language.
Method of exchanging authentication and authorization information between parties. (slide 62)

What parties are there in SAML? What are their roles?

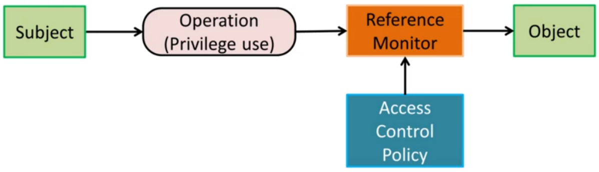
- Identity Provider: authenticates users, performs authorization checks
- Relying Party: accepts the decisions of the Identity Provider (slide 62)

04 Access Control

Explain what Discretionary Access Control is.
Objects have owners and they decide who can access the object.

Explain what Mandatory Access Control is.
Objects and Subjects have security attributes (classes or labels).
The administrator sets a system-wide rule set based on these security attributes. The policy is mandatory.
Example: "Apache is a *web server*", ".php files in /var/www are *web scripts*"
"*web servers* may read and execute *web scripts*" (slide 7)

Describe the typical model of Access Control.



Subject → Operation (Privilege use) → Reference Monitor → Object

Access Control Policy → Reference Monitor

The Subject wants to access (Operation) the Object. The Reference Monitor enforces the Access Control Policy and checks whether the Subject is allowed to access the Object. (slide 4)

What is the job of the Reference Monitor?
Enforcing the Access Control Policy (slide 4)

Where are login data and passwords stored on Linux systems?
/etc/passwd for login data and hashed passwords are in /etc/shadow (slide 9)

How are file permissions on Linux represented?
permissions for owner, group, others. 1+9 characters -rwxrwxrwx (slide 17)

On Linux, a file has -rw-r--r-x permissions and is owned by user1:rndgrp. I am gergo:rndgrp. What can I do with the file?
same group -> can read (slide 18)

The root user sets chmod 777 on the file above. What can I do now?
-rwxrwxrwx -> read write and execute (slide 19)

What Mandatory Access Control implementations do you know for Linux?

- Security-Enhanced Linux (SELinux) (slide 24)
- AppArmor (slide 26)
- Tomyo (not discussed further) (slide 26)
- Smack (not discussed further) (slide 26)

Briefly explain what SELinux is and how it works.

2 modes:

1. Permissive: Everything is allowed but logged
2. Enforcing: Rules are enforced

Has default deny policy -> not explicitly allowed means denied.
It only evaluates checks after general DAC. (slide 24)

Briefly explain what AppArmor is and how it works.

uses the concept of profiles, easier to configure. has 2 modes (similar to SELinux)

1. Complain: Everything is allowed but logged
2. Enforcement: Rules are enforced slide 26)

What is a SID (Windows)?

Security Identifiers (slide 31)

How does Windows store information about its users?

sAMAccountName for Users and Groups and userPrincipalName attribute for domain users (slide 32)
Security Accounts Manager (SAM) is a database encrypted by SYSKEY, but key is stored next to it. (slide 34)
Passwords are hashed (slide 35)

What does permission inheritance mean (Windows)?

Permissions of folders are inherited by files and subfolders if not otherwise specified. (slide 40)

What is the difference between implicit and explicit permissions?

implicit - inherited from somewhere
explicit - explicitly assigned (slide 42)

On a Windows system, I have explicit Allow Read permissions on a file, but I also have an inherited Deny Read + Write permission from a folder above. Can I access the file?

Explicit Deny > Explicit Allow > Implicit Deny > Implicit Allow
Yes, you can. The explicit allow is stronger than the inherited/implicit deny. (slide 42)

How are File Sharing permissions evaluated?
3 Permissions: Read, Change, Full Control
When accessed over the network both ACLs (Access Control Lists) and Share Permissions are evaluated. The effective permission is the intersection of both. (slide 44)

What is the purpose of User Account Control?
Users with Administrator rights get 2 security tokens.

1. with Administrator rights
2. with normal user rights

Usually uses the normal token unless Administrator rights are needed, so programs run on the least required rights. If Administrator rights are needed the authorization is prompted. This prompt runs on a different context (Secure Desktop) and can’t be accessed by malicious programs. (slide 45)

05 Data Privacy

What is privacy?
Privacy is the RIGHT of a person to be able to control how their own personal information is collected, stored, and shared. For example, you can decide with whom you want your personal info to be shared with. (slide 4)

What is the difference between data privacy and security?
Data security involves the protection of said data from threats, and malicious intents.
Data privacy is about responsible handling (storing, collecting, and sharing in accordance to the agreed terms) of the aforementioned data.

What is cookie respawning?
Same values are stored in HTTP and Flash cookies. Flash cookies are permanent while HTTP cookies are deleted after the session. Since the stored values are similar, deleted HTTP cookies can be respawned from Flash cookies. (slide 34)

How can microphones be used for location tracking?
Ultrasound tracking. Apps that have access to the microphone can detect unique ultrasound emitters that are placed in buildings. Such unique sounds can be used to identify a specific location. (slide 44)
Apart from this, the app can intercept voice conversations.

What is pseudonymization?
A rather naive approach to anonymize user data by removing direct identifiers (slide 63)

Is pseudonymous data personal?
Yes, it is possible that several pseudonymous data sets can be used to identify a person (slide 63/64)

Does the combination of multiple k-anonymous datasets preserve k-anonymity? Why?
No, the intersection of to k-anonymous datasets can reveal the identity of a person. The quasi-identifiers of both sets complement each other. (slide 69)

What is browser fingerprinting?
When *mostly* persistent data such as unique identifier of a device, OS, browser version, timezone, screen resolution is queried and collected by websites in order to identify a user. (slide 37)

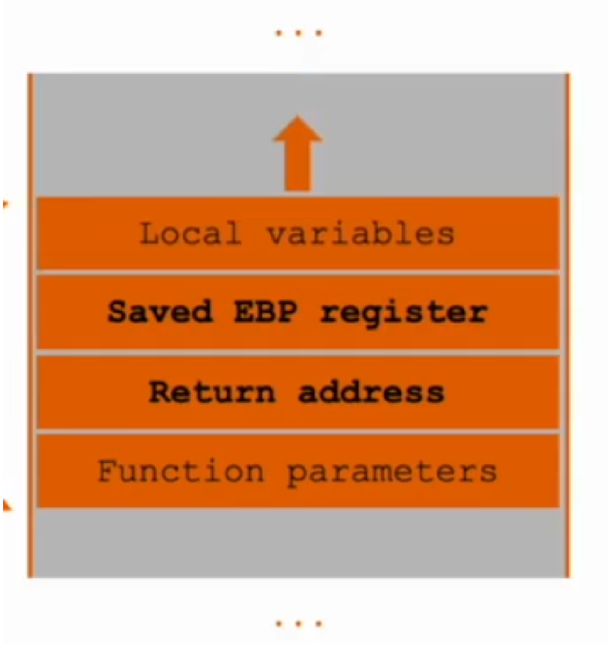
How are the data packets encrypted in TOR?

Each onion router has a RSA key pair. The sender selects a random path through the network and iteratively encrypts the message for each OR. Each OR on the path decrypts one layer of the encryption. Last OR sends the message in clear text to the receiver. (slides 82-90)

06 Memory Corruption

Which programming languages are most affected by the buffer overflow problem?
c/c++ (manual memory management)

What is a stack frame? Where on the stack are function parameters and local variables placed?
Stack frame is a logical structure belonging to a function. (slide 24/25)



What is the main idea of stack overflow?
user-controlled data overwrites other values on the stack. (slide 5)
Happens because size is not verified (slide 30)

Where can the attacker's code be injected in a stack overflow attack?
Shellcode can be injected into the local buffer, environment variables or in the address of a function

What else than a return address can be overwritten in a stack overflow attack?
environmental variables?

Besides stack overflow, what other memory corruption attacks do you know?
integer overflow, NULL pointers and dangling pointers (slide 2)

What is a shell code?
malicious code injected into the stack?

What is a NOP sled? Why is it used?
No Operation. It is used by the attacker to fill up the buffer before the actual malicious shell code. This is useful when the exact size of the buffer is not known. (slide 33)

Why 0x00 bytes should be avoided in shell codes? How to avoid them?
not answered anywhere in the slides

What countermeasures do you know against stack overflow attacks? How do they make the task of an attacker harder?

1. software verification - guarantees bug free code (slide 37)
2. language solution - use languages that are not vulnerable to buffer overflow (Java, Rust) (slide 38)
3. testing - discovering flaws. (slide 36)
   memory safety can be tested indirectly (slide 40)
4. mitigations - checks low level security policies on runtime (slide 41)
    - DEP: separating executable and writable memory locations (slide 42)
    - Canary: 32-bit value between local variable and return address. Is check if changed (slide 44)
    - ASLR: Address Space Layout Randomization
      Memory locations are randomized. Attackers can't guess the location of the shell code. (slide 45)

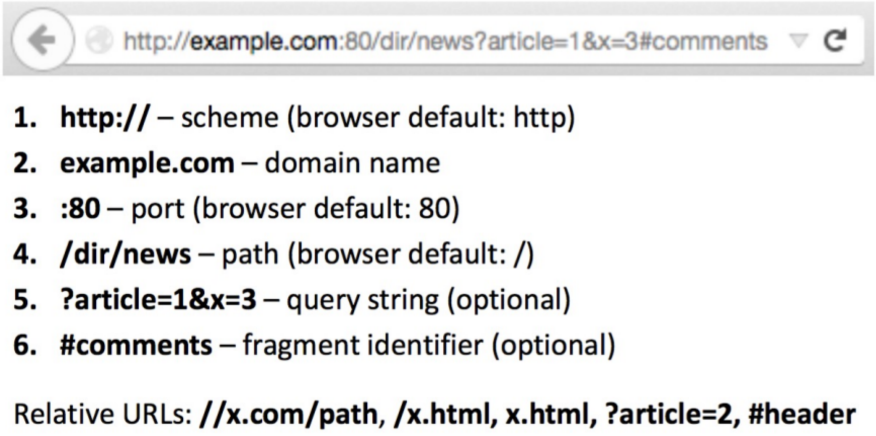
07 Malware

no control questions

08 Web & Browser Security

Web security part

How does the structure of an URL look like?



http://example.com:80/dir/news?article=1&x=3#comments

1. **http://** – scheme (browser default: http)
2. **example.com** – domain name
3. **:80** – port (browser default: 80)
4. **/dir/news** – path (browser default: /)
5. **?article=1&x=3** – query string (optional)
6. **#comments** – fragment identifier (optional)

Relative URLs: **//x.com/path**, **/x.html**, **x.html**, **?article=2**, **#header**

(slide 4)

What are the basic web security problems?

1. Securing transactions between the browser and the server
2. Attacks targeting the client side
3. Attacks targeting the server (slide 10)

What is the OWASP Project?
It is a not for profit organization who’s materials are open source, aimed towards making web security transparent, so that individuals, and companies make informed decisions. (slide 12)

What is usually the first step of an attack against a web server?
Maximizing attack surface (slide 22)

What is the general problem in case of an injection attacks?
Composing an SQL command via string operations by using user input (slide 26)
without input validation.

Show a simple SQL injection example!

*SELECT * FROM users WHERE username=<user> AND password=<pwd>*

- username=a’ #
  (comments out the rest of the query)
- username=a’ union select 1,2,3,* from users #
  (union attack to get information from a more interesting table)
- username=a’; DELETE * from users #
  (query stacking to execute multiple statements) (slides 26-29)

What are the possible countermeasures against SQL injections?

Avoid dynamic SQL

- use static SQL statement text (unless you cannot)
- static SQL statements cannot change at run time, and hence, they are not vulnerable to SQL injection attacks

Filter and sanitize input

- escaping special characters, conforming to naming conventions, …
- best to do automatically: parameterized statements!

Proper setting of access rights to the database

- e.g., allow only SELECT operation, etc… (slide 31)

Client side part

What is the security boundary on the client side?
(slide 36, 38)

The origin.
If a user is accessing multiple sites, and has authentication cookies from some (site A), the other sites (site B) should not be able to read, modify user data on site A. Doing so will allow site B to impersonate the user, and gain read/write access on behalf of the user.

What is the Same Origin Policy?
(slide 38)
Origin = scheme + domain + port combination
Basic principle: **origin = security boundary**
A webpage can only read resources without restriction on its own origin (scheme, domain, port). *Resources on other origins are subject to various access control rules.*

What is limited by the Same Origin Policy when an XMLHttpRequest is sent?
(slide 39)

Reading cookies that belong to other domains.

Where could Javascript code appear?
(slide 46)

- Inline HTML: <script>...</script>
- HTML elements: <img onmouseout="script(this)" … />
- Remote: <script src="example.com/glob.js"></script>
- CSS: body{background:url("javascript:alert('XSS')")}
- Trick: <img src=`javascript:alert("XSS")`>

What could a malicious Javascript do on the client side?
(slide 48)

(within the same origin:)

- Different scripts can access each other’s variables
- Different scripts can redefine each other’s functions
- Scripts can override native methods
- Transmit data anywhere
- Watch keystrokes
- Steal cookies
- User click is equivalent to JavaScript click

What is an XSS (Cross-Site Scripting) attack?

(slide 51)

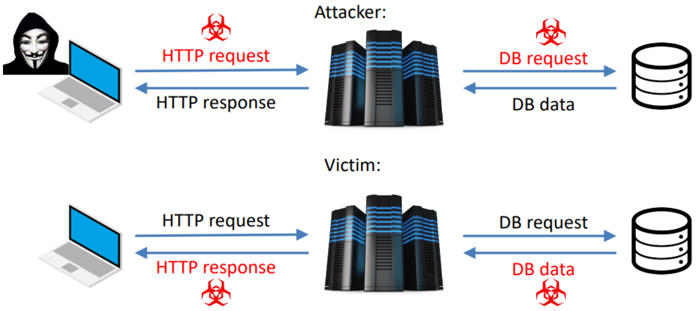
When an attacker manages to run JavaScript code in the context of another origin.
The injected JS code can do anything in the target origin.

What are the types of an XSS attacks?

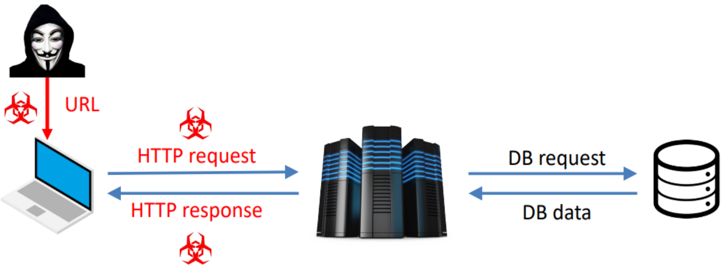
(slide 51, 52, 53)

There are different types of XSS depending on:
– Whether the attacker string is stored on the server
– Where the HTML fragment is assembled

1. Persistent/Stored XSS:
    - Attack JS is stored by the site
    - Examples: comments, messages, user data
    - Trigger: the victim navigates to the containing page



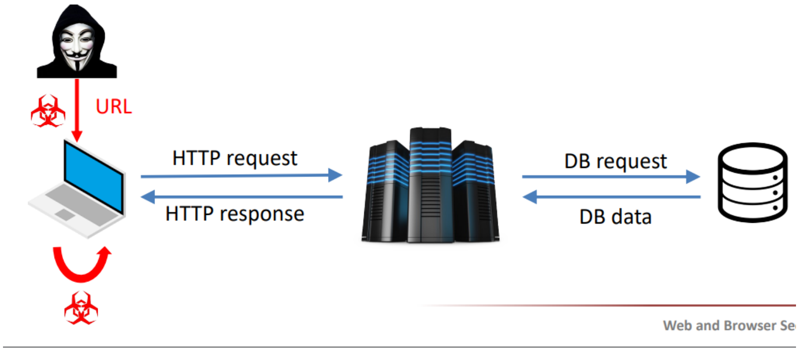
2. Reflected XSS:
    - Attack JS passed as GET/POST parameter
    - Server code "reflects" the parameter in the returned HTML
    - Trigger: user visits malicious site → site redirects to/frames vuln. URL



3. DOM based XSS:
    - The injection does not occur on the server side
    - HTML is created on the client side

```
>> x.innerHTML = attacker_controlled_variable;
```

    - Special case: Client side template based XSS
        >> Client side JS interprets the template
        >> Attacker controlled variable is inserted HTML encoded



What are the mitigation strategies against an XSS attack?

(slide 55, 56)

- User data must be sanitized before inserting into HTML
- The context is important
  - `<p><?php echo $user_comment; ?></p>`
  - `<img src=”...” title=”<?php echo $user_title; ?>”/>`
  - `<script>n= “<?php echo $user_name; ?>”;</script>`
- Blacklist and deleting is not a good solution. Blacklist is **never** complete
- Solution in HTML tag/property context
  - HTML entity encoding
  - PHP: htmlspecialchars()
- **HTTP-only Cookies**
- **Content Security Policy (CSP)**

What is the Content Security Policy?

(slide 56)

Content Security Policy (CSP)

– HTTP header

– Specify the legit sources for resource loading

– Report violations to a specified URL

– By default:

» Don't allow inline script tags

» Don't allow eval()

– Further examples:

» Only load scripts, images and objects from certain domain

» Specify which pages can embed this page in frames

Browser Part

What are the most common browser vulnerabilities?
(slide 62)

memory corruption bugs, e.g.
- stack/heap buffer overflow
- integer overflow
- use after free

Why could URL spoofing be a problem?
(slide 60)

can be used for phishing

What is a Universal Cross Site Scripting?
(slide 61)

Attacks happen to the browser and not to a webpage. JS can be executed in any window opened by the browser, e.g. the settings page.

How is the severity of the vulnerabilities reduced in Chrome?
(slide 65)

- Web content is run within a JavaScript Virtual Machine, to protect the web sites from each other
- Exploit mitigation
- Using an OS-level sandbox

How is the window of the vulnerabilities reduced in Chrome?
(slide 66)

Automatic, frequent update mechanism

09 Securing Software Development

What is the CVE?
(slide 4)

Common Vulnerabilities and Exposures
publicly available database of known vulnerabilities

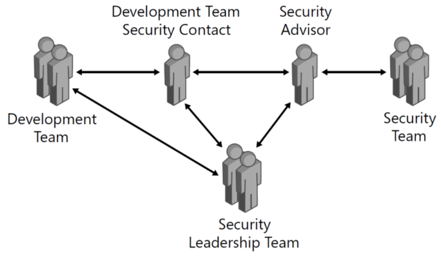
Why is developing secure software difficult?
(slide 9)

1. table is tilted - developers are more (external) constraint (than attackers
2. security testing is challenging - need to test how the system should NOT work
3. weak business motivation - measurement is difficult, no customer enforced competition
4. end-users suffer - developers are not motivated enough

Outline the stages of Microsoft's Secure Development Lifecycle!
(slide 13)

1. Requirements - defining minimum security and privacy criteria
2. Design - follows common principles
    a. Economy of mechanism (KISS)
    b. Fail-safe defaults
    c. Complete mediation
    d. Separation of privilege
    e. Least privilege
    f. Open design
    g. Least common mechanism
    h. Psychological acceptability
3. Implementation - Input validation, error handling, logging
4. Verification - verify that security requirements are met (CIA + 3As)
5. Release - security response plan and incident response plan

What are the tasks and roles of people needed for secure software development?
(slide 15)



Development Team: develop the software
Development Team Security Contact: Receives security related info
Security Advisor: THE security POV
Security Team: dedicated to product security
Security Leadership Team: management of security

What is a bug tracking system? What is required for successful bug tracking?
(slide 20)

- Database about bugs
- Include security/privacy related info as well!
- Required fields: Cause, Effect

What does the design principle "economy of mechanism" say?
(slide 23)

complex software means more bugs. simple/small code is easier to maintain.
BUT small should never be achieved at the expense of simplicity!

What does the design principle "fail-safe defaults" say?
(slide 25)

white-listening -> initially: access is denied
If access is requested, check that it is permitted

What does the design principle "complete mediation" say?
(slide 26)

Check every access to every object

What does the design principle "separation of privilege" say?
(slide 27)

multiple conditions should be met before granting permissions.

What does the design principle "least privilege" say?
(slide 28)

Programs should run with the minimum amount of privilege that is necessary to accomplish the task

What does the design principle "open design" say?
(slide 29)

Don’t depend on the secrecy of the design

What does the design principle "least common mechanism" say?
(slide 30)

Minimize the amount of mechanism

1. common to more than one user, and
2. depended on by all users

What does the design principle "psychological acceptability" say?
(slide 31)

If users do not accept it, they will bypass it

What is the attack surface of the software?
(slide 33)

- All paths for data/commands into and out of the application
- Code that protects these paths
- All valuable data used in the application
- Code that protects these data

Your software detects that the input is corrupted. What should the software do?
(slide 34)

Terminate!

Are the results of arithmetic operations mathematically correct? Why?
(slide 38)

No, because of the boundaries. (arithmetic overflow)

Name 3 examples of improper error handling!
(slide 39)

- Vague error reporting and handling
- Error vs. Exceptions – which one to use?
- No restoration of valid state after exception
- Improper handling (if at all)
- Information leakage

What information is required for logging?
(slide 42)

When, Where, Who, What

What is the importance of logs?
(slide 42)

Logs are the main source for
1. identifying security incidents
2. monitoring policy violations
3. assisting non-repudiation controls
4. incident investigation

What type of data should never be logged?
(slide 43)

Keys, Passwords, Source Code, Tokens, sensitive information in general

When should security testing be performed?
(slide 48)
Throughout the entire development process.

Development lifecycle phase	Activity
Requirements	Security Requirements Study
Design	Security Test Planning
Unit Testing	Static Analysis
Integration Testing	Dynamic Analysis
System Testing	Vulnerability Scanning
Deployment	Penetration Testing
Maintenance	Post-Production Analysis

What is the main characteristic of static analysis?
(slide 49)

Code is not executed only “read” (manual or automated)

Name 4 approaches to static analysis!
(slide 50)

1. Control flow analysis
2. Data flow analysis
3. Code Review
4. Code-based fault injection

What is the main characteristic of dynamic analysis?
(slide 51)

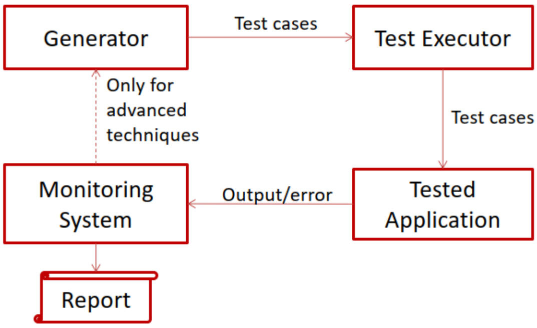
Code is executed.

Discuss the main idea behind fuzzing!
(slide 52)

Random inputs are generated automatically, application is monitored

What are the main components of a fuzzer?
(slide 52)

1. Generator
2. Test Executer
3. Monitoring System



What is the goal of penetration testing?
(slide 54)

Demonstrate how an attacker can gain access to resources without normal means of access

What are the phases of penetration testing?
(slide 54)

1. Reconnaissance - learn about the system
2. Check public databases for vulnerabilities
3. Launch attacks based on collected information
4. Compile the results into a legible format for decision makers

What is the difference between the security response plan and the

(slide 56)

Describes what should be done when a new vulnerability is discovered.

incident response plan?

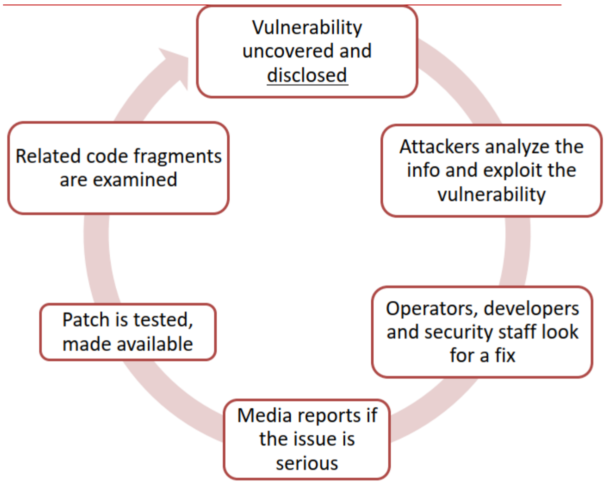
(slide 56)

Describes what should be done when the system is attacked or affected by a vulnerability.

Describe the vulnerability lifecycle!

(slide 58)

1. Vulnerability is discovered
2. Attackers analyze and exploit the vulnerability
3. Developers look for a fix
4. Media reports about it
5. Patch is tested and mad available
6. Related code fragments are examined


Vulnerability uncovered and disclosed
Attackers analyze the info and exploit the vulnerability
Operators, developers and security staff look for a fix
Media reports if the issue is serious
Patch is tested, made available
Related code fragments are examined

What is a security response center? What are its tasks during the Post-SDL Response phase?

(slide 59)

They are responsible for executing the security response plan.

1. Receive and respond to vulnerability reports
2. Analyze report -> *Developers can start working*
3. Manage finder relationships, encourage responsible disclosure
4. Create security bulletin
5. Monitor customer issues and press

What are tasks of the development team during the security response process?
(slide 62)

Implement fix, for variants of original issue as well!

What is the task of the incident response team?
(slide 63)

They are responsible for executing the incident response plan.

1. Scan environment, customer requests, press, etc.
2. Alert and mobilize security response teams -> **security response plan**
3. Assess situation, communicate guidance and workarounds
4. Resolve issue: provide info and tools to restore normal operations

10 Mobile and Cloud Security

Android Part

What operating system kernel is Android built on? Name a few of its low-level security features.
(slide 7)

Linux with the low-level security features:

- XN/NX bit (no execute)
- ASLR (Address space layout randomization)
- SELinux

How are apps isolated on Android?
(slide 8)

isolated in sandboxes with own UID

Name the two most typically used types of Permissions. Give at least one example for each type.
(slide 13/14)

normal permission doesn't pose risk to device or privacy, e.g. VIBRATE, NFC, INTERNET

dangerous permission, READ_CALENDAR, SEND_SMS

How can Dangerous permissions be granted to an app?
(slide 14)

nowadays the application requests the permission at runtime.

Why must applications be signed?
(slide 17)

Yes, otherwise it can't be installed. In case of update the updates must be signed with the same certificate.

Can one install apps from sources other than the Play Store? If so, how?
(slide 18)

Yes. But it must be explicitly allowed.

Why is the Android ecosystem so fragmented? (Hint: think of how updates work.)
(slide)

What are Trust Agents?
(slide)

How does Device Encryption work?
(slide)

Why is it dangerous to set your phone to USB File Transfer mode by default?
(slide)

iOS Part

How does secure boot work in iOS?

(slide 5, https://support.apple.com/guide/security/boot-process-for-ios-and-ipados-devices-secb3000f149/web#:~:text=This%20secure%20boot%20chain%20is,referred%20to%20as%20Boot%20ROM.)

Application processor executes code from Boot Rom, the read-only memory. All secure operations of iOS depend on 'hardware root of trust', an immutable code that is laid down during chip fabrication, and is implicitly trusted. Boot Rom contains the Apple Root CA key, used to verify that the iBoot bootyloader is signed by Apple before allowing it to load.

What is the purpose of the Secure Enclave coprocessor?

(slide)

How is user data security and privacy solved?

(slide)

What are the basic measures of Application security in iOS?

(slide)

How does secure communication through iMessage work?

(slide)

What are the device control options in iOS?

(slide)

Cloud Part

What are the main advantages and disadvantages of cloud computing?
(slide)

What type of service models exist in cloud computing?
(slide)

What type of deployment models exist in cloud computing?
(slide)

What are the main security issues in cloud computing and which of these represent real new challenges?
(slide)

What is the main problem with outsourcing data and processing?
(slide)

What approaches exist to cope with the problem of outsourced data?
(slide)

What is transparent encryption?
(slide)

What is format-preserving encryption?
(slide)

What does homomorphic encryption mean?
(slide)

Why is RSA only a partially homomorphic encryption scheme?
(slide)

What are the main disadvantages of current fully homomorphic encryption schemes?
(slide)

How can the application of trusted hardware help achieve guarantees similar to homomorphic encryption?
(slide)

What real-world examples of trusted execution environments do you know of?
(slide)

What do the following terms mean?

1. **Searchable encryption**
2. **order preserving encryption**
3. **verifiable computation**
4. **proof of data possession**
5. **proof of deletion**

(slide)

11 Network Security (offensive side)

no control questions

12 Network Security (defensive side)

What is the main goal of a firewall?
(slide)

What is the difference between a packet filter and a stateful firewall?
(slide)

How does an application layer firewall work?
(slide)

What is a chain/table in nethooks/iptables?
(slide)

What is the goal of an IDS?
(slide)

What are the main IDS types/detection models?
(slide)

What can be a source for an IDS/IPS/SIEM?
(slide)

What is the difference between an IDS and an IPS?
(slide)

In what problem can a SIEM help us?
(slide)