CS2107 handout

Mu Changrui

2021

1 Terms

1.1 vulnerability

The weakness of a system, which can be exploited to cause loss or harm

1.2 threat

Different to threat, it's a set of circumstances that has potential to cause loss or harm.(threat itself may not be weakness)

1.3 control

A control is an action, device, procedure, or technique that removes or reduces vulnerability. A threat is blocked by control of vulnerability.

1.4 C-I-A triad

Confidentiality: the ability of a system to ensure that an asset is only viewed by any authorized parties.
Integrity: the ability of a system to ensure that an asset can only be modified by authorized parties.
Availability: the ability of a system to ensure that an asset can be used by authorized parties.

1.5 authentication

The ability of a system to confirm the identity of sender

1.6 nonrepudiation /accountability

the ability of a system to confirm that a sender cannot convincingly deny having sent something

1.7 CVE

common vulnerabilities and exposures(CVE) list: dictionary of publicly known security vulnerabilities and exposure(a baseline index point for evaluating coverage of security tools and services)

1.8 advanced persistent therat

attack comes from organized, well financed, patient assailants
related terms: spear phising

1.9 attack surface

the system's full set of vulnerabilities: actual or potential(p28)
include: physical hazards,malicious attacks by outsiders, stealth data theft by insider, mistkaes, and impersonations

1.10 identification

the act of asserting who a person is(public)

1.11 authentication

the act of proving that asserted identity: that the person is who she says she is(private)

1.12 subject

two sides of identification or authentication in security

1.13 rainbow table

A list of concealed forms of the common passwords.
There is shortcoming: the same passwords will turn out to be the same concealed passwords

1.14 salt

An extra data field different for each user to make the concealed password different among users(even the key is the same)

1.15 received operating characteristic(ROC)

a graphical representation of the trade-off between the false negative and false positive rates

1.16 federated identity management

a union of separate identification and authentication systems
The authentication is performed in one place and separate processes and systems determine that an already authenticated user is to be activated

1.17 Access modes

Access modes are any controllable actions of subjects(people) on objects(system or target) including but not limited to read, write, modify, delete, execute, create, destroy, copy, export

1.18 Granularity

The fineness or specificity of access control.

1.19 Reference Monitor

A combination of hardware and software that:

1. always invoked
2. immune from tampering
3. assuredly correct

1.20 Access control directory

A machanism that works like a file directory, every file has unique owner who possesses control access rights and to revoke access of any person at any time

1.21 Access control matrix

In access control matrix, two lists are needed for per connection, we need a list to record who can visit certain objects, also need a list to record which object a certain subject can visit, hence a matrix can be made to combine the two information

1.22 nonce

In cryptography, a nonce is an arbitrary number that can be used just once in a cryptographic communication.

1.23 DDH

The decisional Diffie–Hellman (DDH) assumption is a computational hardness assumption about a certain problem involving discrete logarithms in cyclic groups. It is used as the basis to prove the security of many cryptographic protocols, most notably the ElGamal and Cramer–Shoup cryptosystems.

1.24 HSM

Hardware security module A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. A hardware security module contains one or more secure cryptoprocessor chips

1.25 covert channel

covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

1.26 Password-authenticated key exchange/agreement

In cryptography, a password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password. An important property is that an eavesdropper or man-in-the-middle cannot obtain enough information to be able to brute-force guess a password without further interactions with the parties for each (few) guesses. This means that strong security can be obtained using weak passwords.

1.27 primality test

A primality test is an algorithm for determining whether an input number is prime. Among other fields of mathematics, it is used for cryptography. Unlike integer factorization, primality tests do not generally give prime factors, only stating whether the input number is prime or not.

Factorization is thought to be a computationally difficult problem, whereas primality testing is comparatively easy (its running time is polynomial in the size of the input)

1.28 Self-signed certificate

A self-signed certificate is an identity certificate that is signed by the same entity whose identity the certificate certifies. It is signed by the stated entity’ s private key. It is commonly used by root certificate authorities. It is also used by developers in the early stages of development when a valid certificate of a host is not available yet.

1.29 Malleability

An encryption algorithm is ”malleable” if it is possible to transform a ciphertext into another ciphertext which decrypts to a related plaintext

1.30 Kerckhoffs’ Principle

Kerckhoffs’ Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

1.31 Post-Quantum Cryptography

This generally refers to PKC that are secure against quantum computer.

1.32 Lattice-based cryptography

Based on this hard problem– Given the “basis” of lattice, it is computationally hard to find the shortest (or approx) lattice point. Many proposals, no clear winner yet.(Just hypothesis, no standard yet)

1.33 Multivariate polynomial

Given a multivariate polynomial, it is difficult to find the solution (under modulo p). No secure construction yet.(Just hypothesis, no standard yet)

1.34 blind signature

In cryptography a blind signature, as introduced by David Chaum, is a form of digital signature in which the content of a message is disguised before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature(Applied with the homomorphic prperty of RSA)

1.35 Jacobi symbol

Related to the one-bit leak of RSA
The Jacobi symbol is a generalization of the Legendre symbol, which can be used to simplify computations involving quadratic residues. It shares many of the properties of the Legendre symbol, and can be used to state and prove an extended version of the law of quadratic reciprocity.

1.36 RC4

In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a stream cipher. While it is remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure.[3][4] It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used. Particularly problematic uses of RC4 have led to very insecure protocols such as WEP

1.37 stream cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation is an exclusive-or (XOR).

1.38 HRNG

In computing, a hardware random number generator (HRNG) or true random number generator (TRNG) is a device that generates random numbers from a physical process, rather than by means of an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random ”noise” signals, such as thermal noise, the photoelectric effect, involving a beam splitter, and other quantum phenomena. These stochastic processes are, in theory, completely unpredictable, and the theory’s assertions of unpredictability are subject to experimental test.

1.39 QRNG

Quantum random number generator: it will use quantum entanglement to generate true mathematical randomness.

1.40 Authenticated encryption

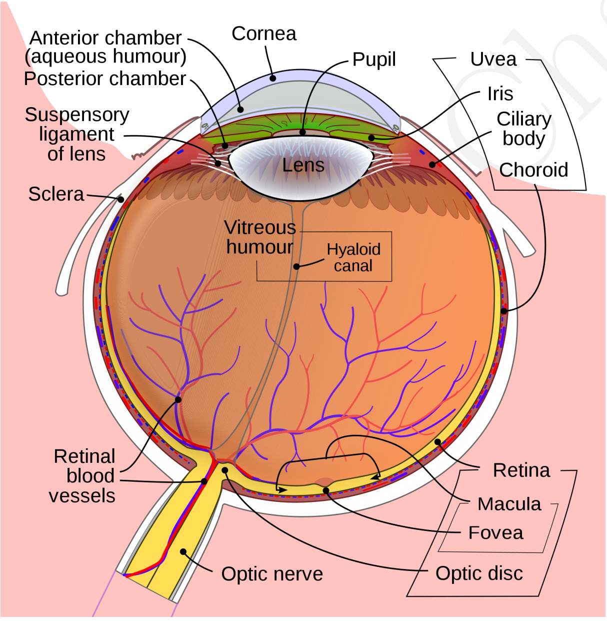
Authenticated encryption (AE) are forms of encryption which simultaneously assure the confidentiality and authenticity of data.

1.41 retinal scan

A retinal scan is a biometric technique that uses unique patterns on a person's retina blood vessels.

1.42 iris scan

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance. The discriminating powers of all biometric technologies depend on the amount of entropy[1][circular reference] they are able to encode and use in matching. Iris recognition is exceptional in this regard, enabling the avoidance of ”collisions” (False Matches) even in cross-comparisons across massive populations.[2] Its major limitation is that image acquisition from distances greater than a meter or two, or without cooperation, can be very difficult.



1.43 Graphical password

A graphical password or graphical user authentication is a form of authentication using images rather than letters, digits, or special characters. The type of images used and the ways in which users interact with them vary between implementations.(e.g.Image sequence, image generated text, facial recognition, draw-a-secret)

1.44 End-to-end encryption

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers –including telecom providers, Internet providers, and even the provider of the communication service –from being able to access the cryptographic keys needed to decrypt the conversation. In many messaging systems, including email and many chat networks, messages pass through intermediaries and are stored by a third party, from which they are retrieved by the recipient.

1.45 Cryptology

Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis

1.46 Cryptanalysis

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.

1.47 Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

1.48 NSA

The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT).

1.49 NIST

The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

1.50 Cryptography back-door

A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device (e.g. a home router), or its embodiment (e.g. part of a cryptosystem, algorithm, chipset, or even a ”homunculus computer” —a tiny computer-within-a-computer such as that found in Intel’s AMT technology).

1.51 Key escrow

Key escrow (also known as a ”fair” cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees’ secure business-related communications, or governments, who may wish to be able to view the contents of encrypted communications (also known as exceptional access).

1.52 Decryption order

Decryption order: legislation that requires individuals to surrender cryptographic keys to law enforcement.

1.53 Whitfield Diffie

Whitfield Diffie: an American cryptographer and one of the pioneers of public-key cryptography.

1.54 Ron Rivest

:a cryptographer and an Institute Professor at MIT.

1.55 Alice, Bob, Eve, Mallory, Trent

1. Alice and Bob: The original, generic characters. Generally, Alice and Bob want to exchange a message or cryptographic key.
2. Eve: Evesdropper, who is usually a passive attacker. While she can listen in on messages between Alice and Bob, she cannot modify them.
3. Mallory: A malicious attacker who is active and who can modify messages, sub- stitute messages, or replay old messages.

4. Trent: A trusted arbitrator, who acts as a neutral third party.

2 Attacks

2.1 chosen-plaintext attack (CPA)

A model for cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme.

2.2 Skimming

Use of a device to copy authentication data surreptitiously and relay it to an attacker. ATM machines are particularly vulnerable to the skimming attacks: small machine can be set to the ATM machine to copy and retain the information recorded on the magnetic stripe on your bank card and small camera to get the name.

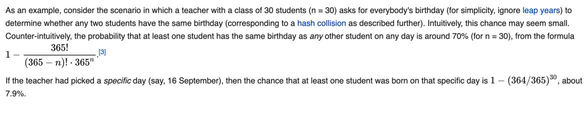
2.3 replay attack

A form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a spoofing attack by IP packet substitution. This is one of the lower-tier versions of a man-in-the-middle attack

2.4 birthday attack

A birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes). With a birthday attack, it is possible to find a collision of a hash function in $\sqrt{2^n} = 2^{n/2}\sqrt{2^n} = 2^{n/2}, with 2^n 2^n$being the classical preimage resistance security.

2.4.1 birthday problem



As an example, consider the scenario in which a teacher with a class of 30 students (n = 30) asks for everybody's birthday (for simplicity, ignore leap years) to determine whether any two students have the same birthday (corresponding to a hash collision as described further). Intuitively, this chance may seem small. Counter-intuitively, the probability that at least one student has the same birthday as *any* other student on any day is around 70% (for n = 30), from the formula $1 - \frac{365!}{(365-n)! \cdot 365^n}$.[3]

If the teacher had picked a *specific* day (say, 16 September), then the chance that at least one student was born on that specific day is $1 - (364/365)^{30}$, about 7.9%.

2.5 DNS spoofing

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

2.6 Insider attack

The attacker is from the entity or has access to some of resources

2.7 Typosquatting

Typosquatting, also called URL hijacking, a sting site, or a fake URL, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typos made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).

2.8 brute-force attack

1. Offline attack: the attacker has access to encrypted material or password hash, and can try different keys without risk of discovery and interference; To defend offline attack, at least 128 bits, 256 bits would be consider safe

2. Online: the attacker should interact with a target system. In this case, the system can counteract with the attacker by,

   (a) limiting the number of attempts,

   (b) add dalay between each successive attempt

   (c) requiring a CAPTCHA answer

   (d) verification code sent to a cell phone

   (e) locking accounts out after reaching a threshold of unsuccessful logon attempts.

   (f) Introducing the second factor of authentication

   To defend online attack, 30-40 bits are enough

2.9 replay attack

During the authentication, if Bob uses repeated nounce, the eavesdropper can know the cyphertext and personate Alice to communicate with Bob

2.10 side-channel attack

Side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs).

2.11 Cryptojacking /malicious cryptomining

uses the machine's resources to "mine" forms of online money known as cryptocurrencies.

2.12 Ransomware

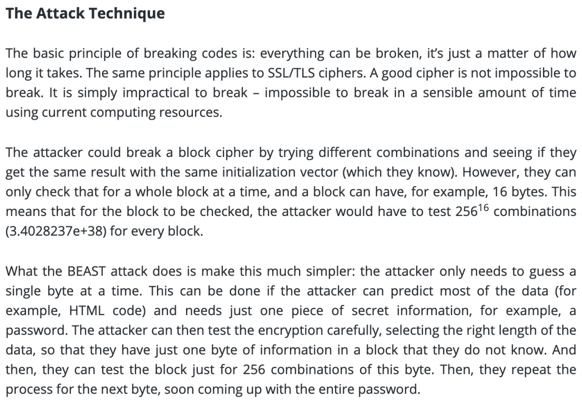
A type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

2.13 IoT(Internet of things) attack

The IoT attack surface is the sum total of all potential security vulnerabilities in IoT devices and associated software and infrastructure in a given network, be it local or the entire Internet

2.14 BEAST attack

BEAST stands for Browser Exploit Against SSL/TLS. It is an attack against network vulnerabilities in TLS 1.0 and older SSL protocols.
The Transport Layer Security (TLS) protocol is a successor to Secure Sockets Layer (SSL). Both are cryptographic protocols that let you use different cipher suites to encrypt the communication between a web browser and a web server.



The Attack Technique

The basic principle of breaking codes is: everything can be broken, it's just a matter of how long it takes. The same principle applies to SSL/TLS ciphers. A good cipher is not impossible to break. It is simply impractical to break – impossible to break in a sensible amount of time using current computing resources.

The attacker could break a block cipher by trying different combinations and seeing if they get the same result with the same initialization vector (which they know). However, they can only check that for a whole block at a time, and a block can have, for example, 16 bytes. This means that for the block to be checked, the attacker would have to test 256^{16} combinations (3.4028237e+38) for every block.

What the BEAST attack does is make this much simpler: the attacker only needs to guess a single byte at a time. This can be done if the attacker can predict most of the data (for example, HTML code) and needs just one piece of secret information, for example, a password. The attacker can then test the encryption carefully, selecting the right length of the data, so that they have just one byte of information in a block that they do not know. And then, they can test the block just for 256 combinations of this byte. Then, they repeat the process for the next byte, soon coming up with the entire password.

2.15 active attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

2.16 masquerade attack

The intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.

2.17 Mirai attack

Mirai (Japanese: 'future') is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers

2.18 Glitching attack

A attack that results in the system hardware fault by manipulating certain environment of the server: eg. interrupt power, temperature sensor and signal to make CPU or other process component goes wrong

2.19 Github DDos Attack 2015

parts of the attack seems to be coordinated through h code, originating on Baidu's server; there is a piece of java script code is injected into Baidu's supplied tracker. When user uses Baidu, injected code cause their browser to constantly load two pages

2.20 Heart bleed attack

OpenSSL cryptography library related bug. Improper implementartion of input validation in the implementation of TLS heart beat extension
The heart beat is a periodic signal generated by hardware or software to indicate normal iperation or to synchronize other parts of computer system
it's considered as a kind of buffer over-read attack In other words, it's like a side-channel because it exploit the implementation rather than the algorithm itself

2.21 Buffer over-read

: a program, while reading data from buffer, overruns the buffer's boundary and reads adjacent memory

2.22 XSRF or CSRF

Cross-site request forgery: attacker tricks victims into making a request the victim did not intend to make after the user is being authenticated by the server
This exploit the server's trust to client

2.23 Mirai attack

mirai took advantage of insecure IoT, it scans ,large blocks of the internet for open telnet port(which is used to remotely control host), and then attemp to login with default passwords. In this way, it makes a mass botnet army

2.24 WannaCry attack

It's basically a kind of ransomware attack, target at computer running microsoft OS by encrypting data and demanding ransome payment in Bitcoin

2.25 Perya

It's similar to wannaCry, also ransomware attack, it locks the hard drive's file system table and precent windows from booting

2.26 Stuxnet

A malicious computer worm(combine multiple zero-day), targets supervisory control and data aquisition(SCADA) systems and is belioeved to be responsible for causing substantial damage to the Nuclear system in Iran

2.27 Conficker/Downup

Computer worm targetting Microsoft Windows OS
Applies the flaw of Windows and dictionaery attack administrator, which creates administrator login and further creates botnet army

2.28 Privilege escalation

Privilege escalation refers to the action of exploiting a hole or flaw in a software problem to gain elevated access to resourcrs that is normallly protected from and application or user

2.29 Resolution attack/DNS hijacking/DNS spoofing

DNS queries are incorrectly resolved in order to unexpectly redirect users to malicious sites

2.30 Reflection attack

For system that uses the same protocol in both direction for challenge-response authentication system
Using target to authenticate its own challenge

2.31 Relay attack

Attacker records the signal of cars seeking for key(assumue key is located remotely
The other attacker send the recorded seeking signal to key, and record the signal sent by the key and then play the recorded signal of key in a place near the car to open the car

2.32 Amplification attack

A kind of DDos Attack
Normal DNS queries, the response is 5 times longer than the requests. So response/request amplification factor is 5 or more
During the attack, attacker craft DNS requests in a way that substantially amplifies the size of response(or instead of request for 1 site's IP, it requests for whole domain)

2.33 Non-invasive and Invasive attack

Non-invasive attack: the attack won't change the target hardware
Invasive attack: the attack will change the target hardware

3 SIM card attack

SIM card and server use DES encrypted and mac to communicate with a shared key

1. DES is vulnerable to bruteforce
2. The attacker can send a disallowed message to the SIM card and will recieve an error feedback from the SIM card, this feedback's plaintext if fixed, the error message is sent in clear followed by the mac; So can brute force the key(known plain-text)

4 Defense

4.1 Control to a system

Not just the name and password,also time and place (non-working time or not in company or personal pc are prohibited)

4.2 Security through Obscurity

To hide the disign of the system in order to achieve security
Which is just a trick but not strategy: The RC4 is initially secret traded but was anonymously postly publicly later

4.3 ASLR

Address space layout randomization: make the the position of the base address of executable randomly. The position of libraries, heap stack in the process's address is also randomized

5 Vulnerability

5.1 Propagation of access rights

A propagate access right to B, if B propagate access to C, in this case, A may not know that C's access exists. It's very dangerous.

5.2 Non-padding RSA

some people call RSA library with parameter-"NO Padding"

6 threats classification

6.1 other

natural disasters:fire,flood, electrical power, failure of communication cable, processor chip or disk drive

6.2 human

benign(nonmalicious)

malicious(random and directed) random attack: the attacker wants to harm any computer or users(e.g. mailicious code posted on public website
directed attack: the attacker intends harm to specific computer(organization, indivisual, particular product such as the attack between antivirus softwares)

7 vulnerability classification

procedure
design
implementation
weak authentication
lack of access control
error in programs
finite or insufficient resources
inadequate physical protection

8 control

8.1 philo

1. prevent: blocking the attack or closing the vulneability
2. deter: making the attack harder but not impossible
3. deflect: making another target more attractive
4. mitigate: making its impact less serve
5. recover from its effects
Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm

8.2 method

1. physical control: using something tangible, such as wall and fences, locks,human guards, sprinklers etc
2. procedural control: command or agreement(laws,regulations, policies, copyrights)
3. technical controls:passwords, program/os access control, network protocols, fierewalls, encryption, network traffic flow regulators.

9 three security tools(frequent)

1. authentication
2. access control
3. cryptography

10 authentication mechanism

10.1 something the users knows

password, PIN numbers, pass phrases, secrethandshake, mother's maiden name

10.2 something the users is

biometrics(physical characters of the user): fingerprint, pattern of a person's voice, or a face

10.3 something the user has

identity badges, physical key,s, a driver's license, uniform

11 The first 12 steps when trying to break a password

1. no password
2. the same as the user ID
3. is, or is derived from. the user's name
4. on a common word list
5. contain a short college dictionary
6. contained in a complete English word list
7. contained in common non-English-language dictionaries
8. contained in a short college dictionary with capitalizations or substitutions
9. contained in a complete English dictionary with capitalizations or substitutions
10. contained in common non-English dictionaries with capitalization or substitutions
11. contained by brute force, trying all possible combinations of alphabetic characters
12. contained by brute force. trying all possible combinations from the full character set

Every password can be guessed; password strength is determined by how many guesses are required.

12 Some attack to password

12.1 Dictionary attacks

The basic vision is that the password is purely composed of English words, the COPS[FAR90], Crack[MUF92], and SATAN[FAR95] allows web sdministrator to scan a system for weak passwords also allow attackers to do the same.
A advanced vision is replace some characters in the word, such as 0 for O, 1 for I or l, 3 for E or

@

12.2 Inferring passwords likely for a User

Mostlikely, a password of someone has something meaningful to her.

12.3 Defeating concealment

Operating systems store passwords in hidden(encrypted) form so that compromising the id-password list does not give immediate access to all user accounts
But the conceal in the OS sometimes is just scrambling, rather than real encryption; or sometimes it's just restricted form for encryption.
Because people often use one of a few predictable password: the interceptor can create what is called a rainbow table: a list of concealed form of the common passwords
A threats of the conceal passwords is that, the same passwords will be convealed to the same string; On the other hand, if we sea two person used the same concealed passwords, it;s reasonable to think that they are both using some common passwords, and hence rainbow table can be applied
To counter the two threats, some systems use an extra pice called the salt
A salt is an extra data field differenmt for each user, perhaps the data the account was created or is transformed by concealment

12.4 Exhausive attack

also called brute force attack, just tries all possible password in some automated fashion
A password 26 chars A-Z and can be anylenth from 1 to 8 characters: 26^1+...+$26^8 \approx 5 \times 10^{12}$, which takes common computer 150 years, but computer cluster just two month

12.5 good password

characteristics of good password:
1. long enough
2. chosen from a large set of characters
3. do not appear in dictionaries

12.6 security questions

Some system ask some questions that only the authenticated subject knows
However, some information is easy to be got from other media(e.g. use facebook public info to crack email and use email to crack facebook

13 Biometrics authentication

e.g:
1. fingerprint
2. hand geometry
3. retina and iris(parts of eye)
4. voice
5. handwriting, signature, hand motion
6. typing the characteristics
7. blood vessels in the finger or hand
8. face
9. facial feature

usually false acceptance must be much smaller than rejection false
usually reduction of false acceptance will increase false rejection(over correlation)
False positive: incorrectly confirming an identity
False negative: incorrectly denying an identity

13.1 false acceptance and false rejection

	Is the person claimed	Is not the person claimed
Test is Positive	True Positive = a	False Positive = b
Test is Negative	False Negative = c	True Negative = d

Sensitivity = $a/(a+c)$: tells the degree to which the screen selects those whose names correctly match the person sought
Specificity = $d/(b+d)$: tells the proportion of nagative result among who are not sought
Accuracy=$(a+d)/(a+b+c+d)$: the degree to which the test flags the condition
Prevalence=$(a+c)/(a+b+c+d)$: how common a certain condition is
Sensitivity and Specificity are statistical negatively related, unless add more samples, increase one will decrease the other

13.2 attack against biometric：biometric forgeries(fake product)

Artificial fingerprint

14 Authentication based on tokens: something u have

14.1 Active and passive token

Passive tokens do not change.
Active tokens communicate with a sensor

14.2 static and dynamic token

Static token remains fixed: keys.identity card. passports, credit and other magnetic-stripe cards and radio transmitter cards
Dynamic tokens has computing power on the token to change their internal state (even if it is heared, doesn't matter, it will be changed)

15 Effective policy implementation

15.1 Check every access

we should aim to check every access by a user to an object, and revoke user's privilege to access if in need

15.2 Enforce least privilege

Least privilege states that a subject should have access to the smallest number of objects necessary

15.3 Verify acceptable usage

checking that the activity to be performed on an object is appropriate

16 Authentication

1. Entity authentication: with connection

2. Data authentication:

   (a) Connectionless

The data-origin authentication implies integrity

16.1 Strong authentication and weak authentication

1. vulnerable to replay attack

2. sniff during the process cannot be used to impersonate user

17 Pass word caching

The password is cached in some public server or host

18 Password Hashing

Not feasible to recover its value from hashed V during the authentication because of the one-way property of hash
The authentication process: hash the user-inputted value and compare with the hash value in the password file
IMPORTANT: shoud not let two password has the same hash value(hacker can compare and guess replay attack), every user should have a salt, which is randomly generated and stored in the password file. (salt make it harder to pre-comput a list of encrypted password

19 Legacy system

In computer science, a legacy system is an old method, technology, computer system or software program

20 DEP

Data execution prevention: prevent data in heap, stack, from execution

21 Cryptosystem

A system for encryption and decryption

22 Cryptography

the practice of using encrypotion to conceal message

23 Crypto analysis

The study of encryption and decryption in order to recover hidden message In some way, the cryptography and cryptoanalysis are against each other

24 Authentication made by symmetric key system

Symmetric key system can also provide authentication, because only legitimate sender can produ e a message that will be decrypted properly with the key, e.g. MAC
However, the symmetric key cannot be used for verification, because ther are at least two party holds the key, i,e. it's not non-reputable

25 Comparation between RSA and AES

RSA is considered much slower than AES(10000 TIMES), 128-bit AES is key equivalent to 3072-bits RSA
Therefore, RSA is not usually applied to encrypt huge file, a common practice to encrypt huge file is

1. Select a AES key, say k
2. use the k to AES encrypt the big file, i.e. AES(k,p)
3. use the public key of the receiver to encrypt the k, i.e. RSA(key_public,k)

4. send AES(k,p)$\|RSA(key\_public, k)$

26 Requirement for good hash

1. Pre-image resistant or one-way: given an integer c, it's hard to find a integer m, such that c=h(m)
2. second pre-image resistant: given an integer m, it's hard to find a integer m2, such that m1≠m2 and h(m1)=h(m2)
3. Collision-free: it's hard to find two integer m1 and m2 such that m1≠m2 and h(m1)=h(m2)

4. Arbitary length to fixed length

For cryptographical hash(mac or signature), it's also required that it's hard to forge a mac without the key

27 HMAC

see the notes, makes it harder to extend the hash

28 Why apply hash before signature

1. Hash is unique representation of data
2. hash is shorter and fiexed-length, so more efficient

29 SIEM

Security information and event management; it's a set of tools that provide a holistic view of the information security of an organization

30 SOC

security operation center: centralized facility where there are teams of information security worker who monitor and analyze an organization's security posture on an ongoing basis

31 CISO

Chief information security officer: a senior level executive within an organization reponsible for

- enterprise vision
- strategy
- program

32 Instrusion detection system

A device or software application that monitor and protects network system from malicious activity or policy violation

33 SOP, Same Origin Policy

Web browser allows script contained in the first web page to access data in the second web page but only if both the web page share the same origin

34 Exposure

A software error that allows attackers to break into system

35 MD5

1. Extensive vulnerabilities
2. Collision attack can be conducted within secends now

36 Semantic Security

Semantic security is one that only negligible information can be feasibly extracted from ciphertext

37 End-to-end encryption

A communication system where only the communication users can read the msg

38 Drive-by download

Drive-by download refers to unintentional download of virus or malicious software

39 The right of root user

root user can read, write, delete any file regardless or the access setting. However, it cannot execute any file
i.e. A file can only be executed by the root user only if it has the execute permission granted

40 How to check whether a certificate is revoked or not

check with online CRL distribution point or OCSP responder

41 RigiNotor/Turktrust

Two examples where CA is compromized

42 Abused CA

Tustware, subordinate root certificate

43 Scam baiting

Attacker applies false promise to invoke victim's greed or curiosity, which lure victivm to a trap that steals their personal information or inject malware in victim's computer

44 DAC and MAC

- DAC:
  - User can give the ownership of one object to another user
  - User can decide the access type of other user
- MAC:
  - System-enforced
  - both subjects and objects are ruled with label set by system