Exam 2011, Questions and answers - COMS3000 PAST EXAM QUESTIONS rn

Information Security (University of Queensland)

COMS3000 PAST EXAM QUESTIONS

Definitions

*Describe and explain the difference between **Authorisation**, **Authentication** and **Identification**.*

Identification is determining the identity of someone, whereas authentication is VERIFYING that identity (making sure they are who they say they are) and authorisation is determining whether to allow that person access to a certain resource based on the authenticated identity.

*Define each of the components of the **CIA-triad** and give an information security example of a failure of each.*

Confidentiality: fails if an attacker can get access to the content of a secure message (e.g. can access company financial information through a compromised password)..

Integrity: fails if an attacker can change the content of a secure message (e.g. has write access to a secure database).

Availability: fails if an attacker can prevent normal access to a secure message (e.g. denial of service).

Hashing

A password system uses the "Slapdash Hashing Algorithm 9" (SHA-9) that works as follows: All punctuation, numerals, special characters and whitespace are discarded; all remaining text is converted to uppercase; all 'W's are converted to 'UU'; all 'Z's are converted to 'S'; then the first eight characters are converted to binary using the following code:

A = S001	*G = 0110*	*M = s100*	*S = 1010*
B = S010	*H = 0101*	*N = s011*	*T = 1001*
C = S011	*I = 0100*	*O = s010*	*U = 1110*
D = S100	*J = 0011*	*P = s001*	*V = 1101*
E = S101	*K = 0010*	*Q = s110*	*X = 1100*
F = S110	*L = 0001*	*R = s101*	*Y = 1011*

Where S is the salt (0 or 1) and s is the inverse of S.

The result is output as nine hexadecimal characters consisting of the salt (0 or 1) followed by the 32-bit hash output as eight hexadecimal characters.

e.g. Password "password" may be recorded as "091AAEEAD" or as "119AAEE25"

***a)** What is the **salt** used for?*

Guards against multiple users having the same password. They will all have a different hash since they all have different salt's, so the attacker cannot break more than one password at a time.. Also, I'm pretty sure the salt has to be saved with the password, so if the attacker gets the password, they'll get the salt. So it doesn't make it harder for the attacker to crack a single password. Guards against pre-image attacks since the attacker will not know the salt beforehand, so they cannot pre-compute hashes

b) *What does the password "ZuluDawn" get recorded as for a salt of 0?*
ZULUDAWN
SULUDAUU
1010 1110 0001 1110 S100 S001 1110 1110
1010 1110 0001 1110 0100 0001 1110 1110
0AE1E41EE

c) *What does the password "ZuluDawn" get recorded as for a salt of 1?*
ZULUDAWN
SULUDAUU
1010 1110 0001 1110 S100 S001 1110 1110
1010 1110 0001 1110 1100 1001 1110 1110
1AE1EC9EE

d) *User Alice has password entry "1A2A4A95D". Someone attempts to login as Alice and gives the password "BobIsThe14me" - will this validate correctly against "1A2A4A95D" and allow access?*
BOBISTHE
S = 1
1010 0010 1010 0100 1010 1001 0101 1101
1A2A4A95D, so yes

e) *Using the password "AliceForever", which hashes to "0114356AD" for salt "0", using only letters and ignoring case, demonstrate two different breaks, one each of BOTH the strong collision resistance and weak collision resistance of this hash* ***and clearly identify which is which.*** *(You should only use the above password and hash in one of your two demonstrations.)*
Weak collision:
With salt "0" SHA9("LliceForever") == SHA9("AliceForever")
Strong collision:
Because the hash only uses the first 8 digits of the password, SHA9("infosecurity") == SHA9("infosecuritysucks")

*Describe the difference between the "****Strong Collision Resistance****" and the "****Weak Collision Resistance****" of cryptographic hash functions?*
Strong: There is no two inputs which will produce the same hash
Weak: it is infeasible to find two inputs which produce the same hash.

*Describe the difference between the "****pre-image resistance"*** *and the "****2nd-pre-image***

***resistance**" of cryptographic hash functions?*
The resistance against finding a value *x* that hashes to an existing hash *h* is pre-image resistance. The resistance against finding two values *x* and *y* that hash to the same hash *h*, where *x* != *y* is 2nd-pre-image resistance.

*This is an actual field from the /etc/shadow file of a Linux system "**1UsR3xSPoS02oabFjdCSp/0H/a2so**" the "$" are separators, the first "1" means MD5 and the next "**UsR3x**" is called the salt. What is the purpose of the rest ("**PoS02oabFjdCSp/0H/a2so**") of the field in this entry and how and why is the "**UsR3x**" used?*
The rest of the field is the salted hash of the password. The salt is used to prevent two users using the same password from having the same hash stored. The hash is calculated like so H(X) = H(salt || password) where || means concatenation. The salt also adds extra security by making rainbow table attacks (Hashes of common passwords can simply be pre-calculated and then used as a reverse lookup table) much more difficult, as a hash would need to be stored for each possible combination of password and salt value. For a large enough salt space, this makes pre-calculation infeasible, forcing passwords to be cracked once the salt is known.

*Given two inputs x1 = 11111111 and x2 = 11101111 to an ideal ("r**andom oracle model**") cryptographic hash function h() with an 8-bit output, what is the expected number of bits in which h(x1) and h(x2) differ?*
Ideal = each output bit equally likely → two possible outputs for each bit (0 or 1), so 50% chance of each occurring → for every bit in output of x1, 50% chance the bit will be different from the output of x2 → 8 bits x 0.5 = 4 bits

Risk Analysis

The ABC company has suffered three extensive virus outbreaks on its internal networks in the last five years. These three events cost ABC a total of $16000, $8000 and $12000, respectively, in lost time and effort to recover, in the last five years.

***a)** Given this information, what is the ARO and ALE?*

ARO (Annualised Rate of Occurrence) = 3 viruses / 5 years = 0.6
SLE = ($16000 + $8000 + $12000) / 3 = $12000 (average)
ALE (Annual Loss Expectancy) = ARO * SLE = 12000 * 0.6 = $7200

b) *A vendor proposed a new anti-virus solution that will cost $4200 per annum in licence and maintenance fees and is estimated to reduce the probability of a virus outbreak to just one in nine years - provide the figures to show if this is or is not a more cost-effective solution*
New ARO = 1/9 = 0.1111
SLE = still $12000
ALE = $12000 * 0.1111 + cost of antivirus = $1333 + $4200 = $5533 which is less than $7200 so it is a more cost-effective solution

The ABC company's existing firewall and IPS solution stops most attacks on their Web server. The typical cost of a successful attack is $34, 000 (losses and repairs). The estimated cost in fees and wages maintaining the current firewall+IPS solution is $39,250 per annum. The equipment has no remaining residual value. Over the last five years, there have been nine successful attacks on their webserver.

a) *Given this information, what is the current ALE?*
ALE = SLE * ARO
ARO = 9/5 = 1.8
SLE = $34,000
ALE = 34000 * 1.8 = $61,200

b) *A vendor has proposed a replacement firewall+IPS solution that will cost $57,000, with a five-year lifetime, plus $9,520 annual licence and maintenance fees and would also require $12,000 of a system administrator's time to maintain, but will reduce the ARO for a successful Web server attack to 1.5 - provide the figures to show if this is a more cost-effective solution.*
Cost of current firewall+IPS plus ALE of attack = $39,250 + $61200 = $100,450
If sysadmin time is 12000 / year → Solution cost per year = 57000/5 + 9520 + 12000 = $32,920
If sysadmin time is 12000 /5 years → solution cost per year = 57000/5 + 9520 + 2400 = $23,320

New ALE = 34000 * 1.5 = $51,000
Cost of new solution + cost of attack per year = 51000 + 23320 = $74,320 which is less than $100,450 so it is more cost effective

What is Residual Risk?
The risk remaining after security measures have been applied.

Explain the difference between quantitative risk analysis and qualitative risk analysis.
Quantitative risk analysis assigns a specific monetary value to loss incurred from an information security breach and numerical probability to how often such a breach is likely to occur.

However this is often difficult to estimate, so qualitative risk analysis can be used instead to assign likelihood and impact ratings such as high, medium, low etc to events.

PCI DSS

PCI DSS Requirement 8.3 *states "Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties." Explain how I can use an RSA SecurID token to achieve this.*
Using a username, password and token provides both 'something you have' and 'something you know' to authenticate, thus providing two-factor authentication.

Classify each of the following controls from the PCI DSS as a Preventative, Detective or Reactive measure and explain why each is so classified:
PCI DSS Requirement 1.1.6*: "Review firewall and router rule sets at least every six months. "*
Reactive

PCI DSS Requirement 3.6.8*: "Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities."*
Preventative - Key custodians have acknowledged that this is their responsibility.

***PCI DSS Requirement 10.6**: "Review logs for all system components at least daily."*
Detective - Reviewing the logs will reveal any suspicious activity after the fact, and most likely include usernames/IP addresses of the culprits. Does not prevent attack or specify what action should be taken upon attack detection.

***PCI DSS Requirement 12.6**: "Implement a formal security awareness program to make all employees aware of the importance of cardholder data security"*
Preventative - Aims to prevent attacks by increasing awareness and hopefully reducing data security holes.

***PCI DSS Requirement 12.9**: "Implement an incident response plan."*
Reactive - An incident response plan specifies how to behave in the event of a breach, which neither prevents nor detects attacks.

Are "Level 3" merchants required to be PCI DSS compliant? Explain.
Yes, they simply have reduced audit requirements. The requirements to be compliant are unchanged.

Cryptography/Key Exchange

*The ciphertext "QCDXIMWSOMIAJBRXIMWEOQXXIMWMOM" was produced with a Vigenere cipher using only **one** of the following 20 keys:*
PRIME SHE AN GUY TEN FAR MOTOR BY CIPHER ELF KNIGHT BIKE TOOLS BAKER BY HEROES EXTEND MIGHT LOCAL.

***a)** Demonstrate the **most** efficient **method** to decrypt the ciphertext with only the resources you have available to you in this examination.*
QCD**XIMW**SOMIAJBR**XIMW**EOQX**XIMW**MOM
XIMW occurs at distances 4, 16, 24 → gcd = 4 = most likely key length
Only 4-letter key provided is BIKE

QCD**XIMW**SOMIAJBR**XIMW**EOQX**XIMW**MOM
BIKEBIKEBIKEBIKEBIKEBIKEBIKEBI

***b)** Correctly decrypt the ciphertext using **any** method. A Vigenere table is provided in the Quick Reference Guide.*
Decipher: first letter, Q, key = B
1) Look down the first column for the key (B)

2) Look along the row of the key, until you find the ciphertext (Q)
3) Look at the top of that column for the plaintext (P)

PUTTHEMONEYWITHTHEMANINTHEMINE

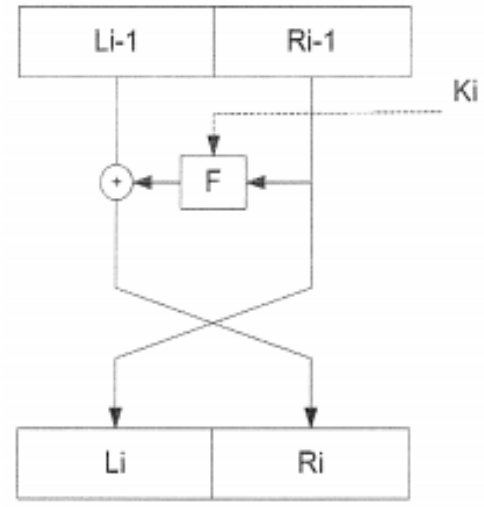
*The ciphertext "EHZDUHWKHLGHVRIPDUFK" was produced with a "**Caesar cipher**" using Julius Caesar's historical key (according to Suetonius) and our modern 26-letter alphabet. Correctly decrypt the ciphertext using any method.*

Traditional Caesar cipher = shift of 3:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

BEWARETHEIDESOFMARCH

*The figure below shows a **single round** of a particularly weak 8-bit **Feistel cipher** with a **reversible** function F. This function F simply performs a bit-wise Exclusive-OR (XOR) of the right-hand side with a **constant** 4-bit key. Because the function being used here is reversible this particular implementation is easily subject to cryptanalysis:*



All logical operations are performed bitwise. Disregard any initial or final permutations of an overall algorithm implementation - consider only the individual Feistel rounds.

***a)** Explain and demonstrate **how** you can leverage this reversibility of the function F() to*

determine the 4-bit key being used, if the input was 10010101 and the output was 01010110; and

Input: 10010101
Output: 01010110

Input gets split into two 4 bit halves → 1001 0101
Right half goes to left half of output
1001 is XOR'd with key to get 0110
XOR is reversible by simply XOR'ing the right half of output and the left half of the original input
1001
0110
1111

b) *Therefore what is the 4-bit key being used here?*
1111
c) *What is the result of the second 8-bit Feistel round?*
Input: 01010110
Split in two → 0101 0110
Right half goes to left half of output → output so far is 0110 xxxx
F(0101) = 0101
1111
1010
Output = 01101010
*Consider an **RSA** system with the following parameters:*
p=3
q=5
*n=p*q = 15*
a) *Find a valid parameter (public key) e, other than e=3.*
z = (p-1)(q-1) = 2 * 4 = 8
e can't have common factors with z
e = 5

b) *Use the above RSA system with parameter e=3 to encrypt the following three plaintext messages: m1 = 2, m2 = 4, m3 = 7*
$c = m^e \pmod{n}$
$m1 = 2^3 \pmod{15} = 8$
$m2 = 4^3 \pmod{15} = 4$
$m3 = 7^3 \pmod{15} = 13$

*Alice and Bob are using the **Diffie-Hellman protocol** to establish a shared secret key. They agree on the public parameters n = p = 11 and a generator a = g =3.*

Alice chooses a random number x =3 and Bob chooses a random number y =4.

Show the two different ways (Alice's and Bob's) to compute the shared secret key that will be established between Alice and Bob.

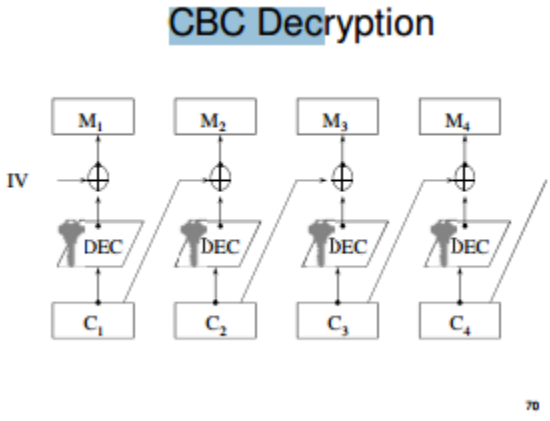
Alice

Alice computes $X = g^x = 3^3 = 27$ and sends it to Bob
Alice receives Y = 81 from Bob
Alice computes $K(AB) = Y^x \bmod p = 81^3 \bmod 11 = 9$

Bob

Bob computes $Y = g^y = 81$ and sends it to Alice
Bob receives X = 27 from Alice
Bob computes $K(AB) = X^y \bmod p = 27^4 \bmod 11 = 9$

*Draw a block diagram of a block cipher in **Cipher Block Chaining (CBC)** mode for decryption. Due to a transmission error, a ciphertext block (say C2) has a single bit error in the first bit of the block. How does this affect the plaintext blocks after decryption at the receiver?*



A single bit error in C2 would cause M2 to be completely garbled, and M3 to have a single bit error. CBC is self-recovering from bit errors.

Biometrics

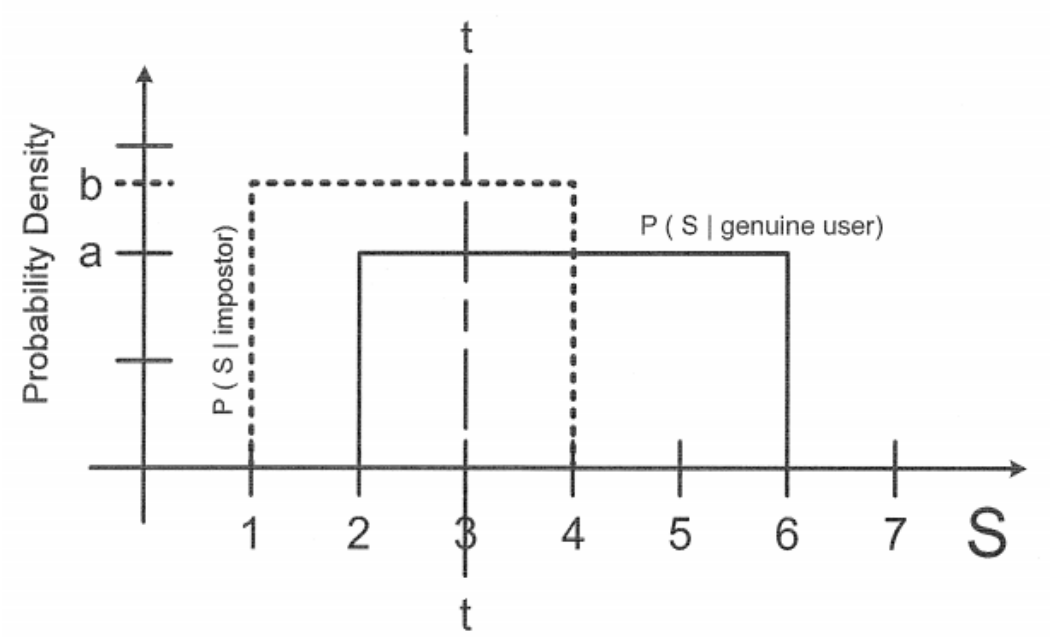
A biometric system has the following parameters: FRR = 0.05, FAR = 0.01. We further know that in 98% of all cases, genuine users are trying to use the system, and in 2% of the cases we have an impostor trying to circumvent the system.

Given the system has accepted a user, what is the probability that this user is genuine and not an impostor? (Hint: Carry at least four significant figures in all calculations)

Let A be Accepted
G be Genuine
FRR = 0.05 => P(~A|G) = 0.05 so P(A|G) = 0.95
FAR = 0.01 => P(A|~G) = 0.01 so P(~A|~G) = 0.99
P(G)=0.98 => P(~G)=0.02

TO FIND: P(G|A) Probability that the accepted user is genuine.
P(G|A) = P(G && A)/P(A)
Now, P(G && A) = P(G)*P(A|G) and P(A) = P(A|G)*P(G) + P(A|~G)*P(~G)
P(G && A) = 0.98*0.95 = 0.931 and P(A) = 0.95*0.98 + 0.01*0.02 = 0.9312
So, P(G|A) = 0.931/0.9312 = 0.999787 = 0.9998
Answer: 0.9998

Consider a biometric system with the following (somewhat unrealistic) conditional probability density functions for the matching score S for an impostor and a genuine user:



a) *Calculate the parameters FAR and FRR*
Calculate b: (4-1) * b = 1 so b = ⅓
Calculate a: (6-2) * a = 1 so a = ¼
FAR - False Accept Rate (imposters allowed in) = (4-3) * b = ⅓ = 33.3%
FRR - False Reject Rate (genuine users locked out) = (3-2) * a = ¼ = 25%

b) *What is the minimum realistic operational threshold t for which FAR = 0? What is the corresponding FRR for this value of t?*
FAR = 0 = 1/3 x (4-t) = 4/3 – t/3 = t/3 = 4/3 -> t = 4
FRR = ¼ x 2 = 0.5

c) *You are asked to adjust the system so that FAR=5%. Where do you need to set the threshold t to achieve this? What is the resulting FRR?*
FAR = 0.05 = 1/3 x (4-t) = 4/3 – t/3 -> .15 = 4 – t -> t = 3.85

t = 3.85
FRR =1.85/4 = 0.4625

d) *What is the Crossover Error Rate of the system?*
Crossover occurs when FAR = FRR
1 - ((t-1) / 3) = (t - 2) / 4
1 = (t-1)/3 + (t-2)/4
12 = 4(t-1) + 3(t-2)
12 = 7t - 10

t = 22/7
CER = (t - 2) / 4 = 0.28

Access Control/Authentication

For the PCI DSS, explain whether you would consider the need for the use of an electronic proximity card (like a Translink "GO-card") and a separate lock needing a physical key, as ***two-factor authentication*** *to gain physical access to a data centre?*
No, both rely on the 'something you have', so using both doesn't add any extra security.

Explain why general purpose filesystems (such as in Windows, UNIX, Linux, OSX, etc.) are not considered ***Mandatory Access Control (MAC)****? What term is used to describe this paradigm for access control?*
They are not considered MAC because access rights to files are typically defined by the owner of the file, rather than through a system-wide policy. This paradigm is known as Discretionary Access Control.

Describe and explain the difference between three different factors of ***authentication mechanisms****.*
Something you KNOW
something you HAVE
something you ARE

something you know, such as a password, something you have, such as a keycard or something you are, such as a physical characteristic of you, these three things give you, three different ways in which you can authenticate a person, using them in a combination of one another is recommended.

Public Key Certificates/Trust

*Explain the difference between a **CP** and a **CPS** in a **PKI**?*

Certificate Practice Statement (CPS) is a publication by a CA specifying the details of their identity verification process. Certificate Policy (CP) is a publication detailing the different types of certificates the CA issues.

*Outline the structure of an **X.509 version 3 digital certificate** noting carefully where the various names, keys and algorithms are; and which components are included in the hash, which components are signed, which key is used to create the signature and which key is used to verify the signature.*

The structure of an X.509 v3 digital certificate is as follows:

- Certificate (This section is hashed then encrypted with the subject's private key)
    - Version
    - Serial Number
    - Algorithm ID
    - Issuer
    - Validity
        - Not Before
        - Not After
    - Subject
    - Subject Public Key Info
        - Public Key Algorithm
        - Subject Public Key
    - Issuer Unique Identifier (optional)
    - Subject Unique Identifier (optional)
    - Extensions (optional)
- Certificate Signature Algorithm
- Certificate Signature

*Explain, with an example, the concept of **transferred** (or **transitive**) **trust**.*

Transitive trust allows two parties who have never met to establish a trust between them, through a mutually trusted third party.

If Bob trusts Jane and trusts Jane's decisions on who is trustworthy, then Bob implicitly trusts anyone that Jane decides to trust. If Jane decides to trust Adam, then Bob also trusts Adam via transitive trust.

Shannon Information

Consider a language consisting only of the following words with the corresponding probabilities:
***Γ**: p = 0.25*
***Δ**: p = 0.10*
***Ξ**: p = 0.20*
***Σ**: p = 0.05*
***Θ**: p = 0.40*

***a)** What is the Shannon Information per word of text in this language?*
0.25 * (-log 0.25 / log 2) + 0.1 * (-log 0.1 / log 2) + 0.2 * (-log 0.2 / log 2) + 0.05 * (-log 0.05 / log 2) + 0.4 * (-log 0.4 / log 2)
= 0.5 + 0.332 + 0.464 + 0.216 + 0.529
= 2.041

***b)** The following binary encoding scheme is used for the above language:*
***Δ** = 1*
***Θ** = 00*
***Ξ** = 010*
***Γ** = 0110*
***Σ** = 0111*

*Encode the following words of the language into a continuous bit stream: **Δ Σ Γ Δ Θ**. Is this encoding unambiguous? Explain why.*
1 0111 0110 1 00
Yes, no combination of words can result in a bitstream that can represent any other set of words.

***c)** What is the average number of bits required to encode a word using this encoding scheme?*
sum each word: freq * length
0.25 * 4 + 0.1 * 1 + 0.2 * 3 + 0.05 * 4 + 0.4 * 2
2.7

***d)** How much redundancy does a code word contain on average?*
Average number of bits per word - number of bits of information per word
= 2.7 - 2.041 = 0.659

WPA *and* ***WPA2 Pre-Shared Keys*** *may be entered as either the 64 hexadecimal characters for the actual binary key or otherwise as a passphrase of 8-63 (but not 64) printable ASCII characters which are then hashed using the SSID as the salt and 4096 rounds of HMAC-SHA1.*

a) *How many bits are in a 64 hexadecimal character key?*

4 bits per hexadecimal character

64 * 4 = 256 bits

b) *What is the total entropy of a truly random 64 hexadecimal character key?*

Truly random = each character is equally likely to be included

$\log_2$(number of bits in key) = $\log_2(256)$ = 8 bits of entropy

c) *How many bits are in 63 printable ASCII characters? (There are 95 possible printable ASCII characters.)*

63 * 7 = 441

d) *What is the total entropy of a truly random 63 printable ASCII characters?*

$\log_2$(number of bits possible) = $\log_2(441)$ = 8.78 bits of entropy

e) *What is the total entropy of an English phrase of 63 printable ASCII characters?*

English Phrase Consists of 26 letters.

ASCII has 63 printable letters.

Proportion of English:ASCII is 26/63 = 0.4126

ASCII has 441 bits, 41.26% of this belongs to English -> 182

Log_2182 = 7.5078

Attacks

*Describe the steps involved for a **Man-In-The-Middle attack** to occur during an SSL handshake.*

Ultimately there are two connections made. The client connects to the intruder, and the intruder connects to the server. The intruder passes on the information. Therefore from a server or client point of view, the information is being passed, but cannot see that it is going through a third party.

[Note, attacker already has a valid session with the server - this is the Renegotiation attack?]

1. Client sends supported cipher suites, and Client Nonce to Attacker
    1a. Attacker sends supported ciphers suites, and Attacker Nonce to Server
2. Server sends cipher suite choices, and Server Nonce to Attacker
    2a. Attacker sends cipher suite choices, and Attacker Nonce to Client
3. Server sends Server's public key and certificate to Attacker
    3a. Attacker sends Attacker's public key and certificate to Client
4. Client sends PMK encrypted with Attacker's key to Attacker
    4a. Attacker sends PMK encrypted with Server's key to Server

Attack is successful if:

Attacker has a way to redirect client request → DNS poisoning, ARP spoofing
Client fails to verify Server certificate

*Describe an authentication **Replay Attack** and how a challenge-response authentication protocol can prevent an authentication Replay Attack, and explain under what condition such an attack would still be possible with a challenge-response authentication protocol.*

Replay Attack

Server has username and password of Client stored.
Client sends username and password to Server in order to login.
Attacker eavesdrops on message exchange and learns username and password.
Attacker can then login as Client.

Challenge-Response

Client requests login.
Server sends challenge integer c to Client.
Client calculates hash of password and c and sends hash to Server.
Server calculates hash of password and c, and if the hash matches the Client response, authenticates the user.
Attacker can eavesdrop on communication and obtain hash, but cannot determine password from it.
Attacker can still perform replay attack if the same challenge integer is used, as the same hash result would be required, which the attacker could have eavesdropped from earlier communication.

Describe how a wireless station may be forced to disconnect from a legitimate

access point in an attempt to get it to use a "Fake AP" and how can this be averted.
By sending out a fake “disassociate” signal, and then spoofing as the ap when they try to reconnect.

Prevent by encrypting all send information rather than just data packets this can be prevented.

Network Security

*Describe the latest wireless security enhancements provided in the **IEEE 802.11w** amendment.*

- (Some) protected management frames
- Provides mechanisms that enable
    - data integrity
    - data origin authenticity
    - replay protection
    - data confidentiality

(for selected management frames)

- Provides protection against:

- Injection attacks
- Disassociation attacks
- Fake APs

*What are the three security functions provided by **WS-Security** to a **SOAP** message?*
Sending security tokens to assert user identity
Signing data to ensure data integrity and verify sender
Encrypting data to ensure confidentiality of data

*What is the purpose of the **WS-SecurityPolicy** standard?*
A standard set of extensions which can be used when building secure web services to implement integrity and confidentiality

*What is a **nonce**? What is the purpose of a nonce in a **challenge-response authentication** protocol? Describe how a nonce can be used to achieve this.*
A nonce is a number that is used only once. It's purpose is to prevent replay attacks by forcing the calculations to be done fresh every time, requiring all the original information.

*Describe when and how nonces are used in the **TLS handshake**.*
Nonces are sent in the first communication to and from the client. They are used in the calculation of the shared secret key.

*Name two **OASIS** standardised **Security Tokens** approved for use with **WS-Security**.*
Username token
X.509 token
Kerberos token
SAML token
*Compare and contrast a **WPA 4-way handshake** to a **WPA2 4-way handshake**.*
The both have 4 key messages in the handshake.
WPA Handshake cannot establish a connection however with the handshake alone, it must perform a GTK handshake immediately after.
Messages 1,2,4 are the same in both.
Message 3 is different – WPA2 includes the GTK in the message passed.
WPA uses TKIP for pairwise and groupwise
WPA2 provides TKIP and CCMP
WPA doesn't do pre-authentication

*What are the steps in a **SAML Browser Artifact Profile** to obtain web single sign-on from one*

web site to another?

1. Browser requests SSO (Single Sign-on) from Identity Provider
2. Identity Provider generates artifact.
3. Identity Provider re-directs user with artifact to Service Provider Artifact Receiver Service
4. SPARS verifies artifact with Identity Provider over mutually authenticated SOAP back-channel
5. Once verified SPARS redirects browser to target page.

*What is the purpose of **WSDL**?*
Describes the interface of a web service. Serves as a contract between the client and the server specifying what functions will be provided.

*Describe how a WLAN using TKIP can be **either** a **TSN** or an **RSN**? What is the difference in each of these scenarios?*
TSN - Transition Security Network - if using WEP
RSN - Robust Security Network - if WEP is disallowed

*Briefly describe two types of **Security Tokens** that can be attached to a **SOAP** message using **WS-Security** (WSS).*
Username token
Kerberos Token

*Describe what is meant by the terms **SaaS**, **PaaS**, and **IaaS** and state who is typically responsible for securing which components for each.*
SaaS: Software as a service, the cloud provider will be giving you access to a specific set of software, It is your responsibility to follow security policy provided by them in order to maintain a secure environment.

PaaS: Platform as a service, you will be provided with a working operating system, it is your responsibility to secure all incoming and outgoing traffic along with all applications you install.

IaaS: Infrastructure as a service, the Cloud provider will ensure the physical hardware is secure, aside from that it is up to you to ensure you are running a secure service.

*Give an example of an information security control for each of the domains of the **Certified Information Systems Security Professional Common Body of Knowledge***

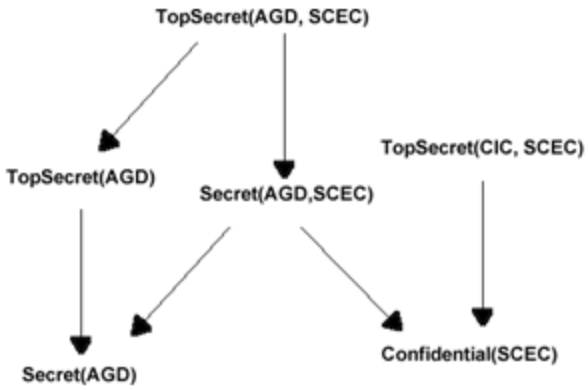
"Common Body of Knowledge" – 10 domains:

- Information Security and Risk Management → information security policies
- Security Architecture and Design → Biba integrity model
- Access Control → passwords
- Application Security → database vulnerabilities
- Legal, Regulations, Compliance and Investigations → computer forensics
- Physical (Environmental) Security → diesel generators
- Operations Security → change control management
- Business Continuity and Disaster Recovery Planning → building crisis management plans
- Cryptography → known plaintext attack
- Telecommunications and Network Security → TCP

Lattice

Consider a Lattice Model with the levels "Top-Secret", "Secret" and "Confidential" and the compartments "CIC", "AGD" and "SCEC". Draw a ***lattice*** *with only the following nodes:*

(Secret, {AGD})
(Confidential, {SCEC})
(Top-Secret, {AGD, SCEC})
(Top-Secret, {CIC, SCEC})
(Secret, {AGD, SCEC})
(Top-Secret, {AGD})



General

For each of the following information security topics state which the various domains of the CISSP CBK they belong to:

a) *Copyright* - Legal, regulations, etc.
b) *SABSA, Zachman or TOGAF* - Security architecture and design. ?
c) *The AES* - Cryptography.
d) *The different types of fire extinguishers* - Risk Management.
e) *Software patching* - Operations security.
f) *Bell-LaPadula* - Security architecture and design. ???
g) *Stream-based ciphers* - Cryptography.
h) *Internet Protocol Security (IPsec)* - Telecommunications and Network security.
i) *The deterrent effects of various fence heights* - Physical security.
j) *Role-based access control (RBAC)* - Access control.

*Describe the top level of the "**SABSA Matrix**", called the "**Contextual View**" and then detail the*

content of each of the cells in this layer of the security architecture.
Contains the context in which each motivation is described.
Business Decisions:
Business Risk:
Business Processes:
Business Governance:
Business Geography:
Business Time Dependence:

*What is the **Discrete Logarithm** of 6 to the base 5 if we are calculating modulo 7, i.e. $\log_5 6 \bmod 7 = ?$*
5^x mod 7 = 6
5^1 .. = 5
5^2 .. = 4
5^3 .. = 6
answer: 3