Exam 2010, Questions and answers rn

Information Security (University of Queensland)

COMS3000: 2010 exam answers

Q1. [2 marks] 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. The client must accept the attackers certificate.

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

Q2. [16 marks] 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's; then the first eight characters are converted using the binary using the following code:

A = S001	G = 0110	M = s100	S = 1010
B = S010	H = 0101	N = s001	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 = S1101	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) [1 mark] What is the salt used for?

To introduce a protection against "rainbow table" attacks, that is a table containing a hash of all common passwords.

b) [2 marks] What does the password "ZuluDawn" get recorded as for a salt of 0'?

ZULUDAWN

SULUDAUU~~N~~

0 (salt) 1010 (S) 1110 (U) 0001 (L) 1110 (U) 0100 (D) **0**001 (A) **1**110 (U) 1110 (U)

Answer: 0AE1E41EE

c) [2 marks] What does the password "Zu1uDawn" get recorded as for a salt of 1'?

1 (salt) 1010 (S) 1110 (U) 0001 (L) 1110 (U) **1**100 (D) **1**001 (A) 1110 (U) 1110 (U)

Answer: 1AE1EC9EE

d) [1 marks] User Alice has password entry "1A2A4A95D". Someone attempts to login as Alice and gives the password "BobIsThe14me" will this validate correctly against "l A2A4A95D" and allow access?

Yes - there is a collision (Using only the first 8 characters and a Salt of 1)

BobIsThe14me -> BOBISTHE -> 1010 0010 1010 0100 1010 1001 0101 1101 -> **1**A2A4A95D

Yes, collision hashing to the same salted password so it will allow access.

e) [10 marks] Using the password "AliceForever", which hashes to "O11-4356AD" 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.)

Sttrong resistance - not capable of getting any values x1, x2 such that h(x1) = h(x2) (read up on birthday paradox). weak resistance - given x1, able to get an x2 such that h(x1)=h(x2) and x1 != x2

Weak Collision Resistance: *"LLDJHGSV"* hashes to 0116AD435

AliceForeverIsYellow will also hash to the same, remembering it only uses the first 8 letters

Strong Collision Resistance: "*hellothere!*" and "*hellothere!123*" both hash to 05511A955

Q3. [2 marks] Given two inputs x1 = 11111 111 and X2 = 11101111 to an ideal ("random 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?

8? ← Pretty sure it is 4, as each bit has a 50-50 chance of being the same. As the hash of x1 and x2 should be random (as per the "random oracle model") then we would expect half of the bits to be the same. ?

8 bits -> 256 combinatons -> probability of a collision is 1/256 = 0.39%
Expected number it differs by should by 0.39% x 8 bits = 0.03125 bits. ← nope. first, collision probability has nothing to do with it, and your answer doesn't even make sense - assume 0.03 bits

Commented [1]: What is the difference between strong and weak collision resistance? +burningfly@gmail.com

Commented [2]: strong resistance - not capable of getting any values x1, x2 such that h(x1) = h(x2) (read up on birthday paradox). weak resistance - given x1, able to get an x2 such that h(x1)=h(x2) and x1 != x2

Commented [3]: Check this

Commented [4]: I think it's 4

Commented [5]: I'm not too sure on the blue bit,
Just thought i'd have a squiz at it,
Lemme know what you think,
And i'll try and fix zit,

Commented [6]: Sorry was trying to rhyme, but that seems to have failed - Does what I did sound valid at all? Just thinking that as the question stands, its way too easy

Commented [7]: What's the consensus on Q3?

Commented [8]: It's 4..... obviously...

Commented [9]: I dont know who commented on the thing, but keep it civil - its not a bloody war, if you wanna go ape at people, get outta here

Commented [10]: well, is there anyone who can provide evidence otherwise?

Commented [11]: How does that justify replying like a prick? A simple, I dont think so + explanation would've sufficed instead of talking like a stuck up prick

Commented [12]: i dont think i replied "like a prick" i explained (twice) the reason, but hey, if you dont like 3 words in caps, go rage. maybe think about your answer a bit next time.

Commented [13]: Compare your response with all the other answers/replies - they're alot more civil/explanatory without downgrading anyone in the process

Commented [14]: Sorry to everyone else, this document's meant to help people - not downgrade

Commented [15]: not sure how bringing IT rep into this helps. look, you dont like it, change it, or just live with it, really, life is not so bad. next time explain why someones answer is wrong instead of stating an answer with some bogus answer like you know what your doing.

Commented [16]: I commented on the side saying I didnt know if it was correct, I can guarantee there'd be alot more people wondering how to do that - with a similar idea, simply saying no thats not correct, rather than wording a response ...

Commented [17]: I don't think its very downgrading at all. i had already explained how to it, above! If you don't like it, ...

Commented [18]: wow this is a long comment.

Commented [19]: Soooo... what was the result of the checking? :)

Commented [20]: Yes.

Commented [21]: sometimes.

Commented [22]: i am as sure as i am that 7 bits are in a byte. ie. very sure.

Commented [23]: If the output was 64-bits, then 32 would be expected to be the same?

Commented [24]: yeh

rounds down to 0 bits - therefore you are expecting x1 and x2 to be *EXACTLY THE SAME* (0 bits different). Read the lecture slides on it. It is 4. basicly, for a [New] input, flip coins to determine the bits being 0 or 1. With only 2 combinations, the answer is 1/2*n which is 8/2 = 4. Trust me.

Q4. [4 marks] Describe the latest Wireless enhancements provided in the IEEE 802.11w amendment.

Protects some of the data management packets, for those packets it provides provides mechanisms that enable; data integrity, data origin authenticity, replay protection, data confidentiality

Which in turn protects against injection attacks, Disassociation attacks and Fake APs

Q5. [3 marks] 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

Q6. [3 marks] 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.

Two factor means – using a combination of something you have, or are, or know.

The RSA token acts as something you HAVE, together with a password to gain remote access which is something you KNOW, you can implement two factor authentication./

Q7. [6 marks] Classify each of the following controls from the PCI DSS as a Preventative, Detective or Reactive measure [3 marks] and explain Why each is so classified [3 marks]:

PCI DSS Requirement 10.6: "Review logs for all system components at least daily."

Detective - it will not help prevent vulnerabilities being exploited, but may help detect an intrusion

PCI DSS Requirement 12.6: "Implement a formal security awareness program to make all employees aware of the importance cardholder data security."

Preventative - this reduces the risk and therefore helps prevent compromised security.

PCI DSS Requirement 12.9: "Implement an incident response plan."

Reactive - after an incident, the threat has already been realised, and therefore a response can be prepared ahead of time, but it does not reduce risk or detect compromises.

Q8. [8 marks] 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

Q9. [4 marks] 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.

An arbitrary unique amount of bits used to sign a cryptographic message. It is used in order to stop replay attacks. It means that the attacker cannot record a message, play it back and have it be valid. A nonce is a number used once, and once only, never to be used again. The purpose of a nonce is to prevent replay attacks, the number is used once by the client and server, and so if the server receives the number again, it will know it's a replay and deny access.

Commented [25]: i dont think 'sign' is the correct word. isnt it added into the hashing process like "h(salt, h(pass))"?

Commented [26]: That's what I thought...

Commented [27]: from the lecture slides, the server keeps plain text passwords, and the nonce (not salt, sorry), is used like so: h(nonce || pass) (|| = concatenate) so that prevents replay, but server stores plaintext, which is a little silly.

Q10. [1 mark] Explain the difference between quantitative risk analysis and qualitative risk analysis.

What differentiates qualitative risk assessment from quantitative risk assessment is that in the former one does not try to assign hard financial values to assets, expected losses, and cost of controls. Instead, one calculates relative values.

Quantitative – Assigning probabilities to loss events and/or quantifying the cost/impact of loss events i.e. 56% ARO. Relating to, measuring, or measured by the quantity of something.

Qualitative – Assigning ranks to loss events, such as 'low','medium'.Relating to, measuring, or measured by the quality of something rather than its quantity: "a qualitative change in the curriculum".

Q11. [15 marks] The ciphertext "QCDXIMWSOMIAJBRXIMVVEOQXXIMWMOM" was produced with a Vigenére 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) [7 marks] Demonstrate the most efficient method to decrypt the ciphertext with only the resources you have available to you in this examination.

Working out: http://i.imgur.com/L9WeG.jpg

First, you need to find the pattern in the ciphertext. This will be a repeated string of characters (in this

Commented [28]: Why not use Kasiski test? for tri-gram "XIM", distances are 4, 16, 24. These have GCD of 4, thus key length is most likely 4.

Commented [29]: Yeah that's a good way of doing it. However, the repeated phrase way (i.e. the way in the image) will still work too, by that reasoning?

Commented [30]: yes but kasiski test is a more formal and probably better way of putting it.

example, “XIMW”; see the image above). The length of this repeated string will also be the length of the cipher key. So, look at the available keys and pick the key which matches the derived key length. In this case, the only key with a length of 4 characters is BIKE.

Note: If there were other alternatives, we would need to decrypt using all possible keys and try to determine which one makes the most sense (we most likely won’t have to do this because it’s brute force).

Because we have a key length of 4, we need to split up the ciphertext into four-character blocks and align the key “BIKE” with each of them (see image). Next, we use the Vigenere table to decrypt each of the characters individually to form the decrypted string. Each key character represents one of the alphabet columns in the Vigenere table. See image in part B for a guide on how to use the table.

Work from left to right (or right-to-left, if you really want to). Find the alphabet column for the key character you’re dealing with (so we start with “B”). Now take the current cipher character (“Q”) and scan down the key’s alphabet column until you find it. Now look across to the far left column, which will always be the “normal” (A-Z, 0-26) alphabet. The decrypted character is therefore “L”.

Now repeat the procedure. Key “I”, cipher “C”, result “U”. Key “K”, cipher “D”, result “T”. Key “E”, cipher “X”, result “T”. Now move on to the next cipher block. Key “B”, cipher “I”, result “H”. And so on.

b) [8 marks] Correctly decrypt the ciphertext using any method. A Vigenére table is provided below.

Example of how to use the table: http://imgur.com/4QmFF

Result: PUTTHEMONEYWITHTHEMANINTHEMINE

Q12. [9 marks] 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) [3 marks] Given this information, What is the ARO and ALE?

SLE (Single Loss Expectancy) = (16k+8k+12k)/3 = 12k

ARO (Anualized Rate of Occurrence) = 3 / 5 = 60%

ALE (Annualized Loss Expectancy) = SLE * ARO = 12000 * 0.6 = $7200/year

b) [6 marks] A vendor has 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.

Assuming (a) is correct, the loss without antivirus is 7,200
in (b) with antivirus:
ALE = AV Cost + Damage done by Virus’ even with AV
ALE = 4200 + (1/9 x 12,000) = $5, 533

Q13. [10 marks] Consider a language considering only of the following Words with the corresponding probabilities:

a p=0.25

b P=0.10

c P=O.20

d P=0.05

e p=0.40

a) [5 marks] What is the Shannon Information per word of text in this language?

H(X) = 0.25 x -log(0.25) + 0.1 x -log(0.1) + 0.2 x -log(0.2) + 0.05 x -log(0.05) + 0.4 x -log(0.4)

= 2.0414461

b) [2 marks] The following binary encoding scheme is used for the above language.

b=1, e=00, c =010, a = 0110, d = 0111

Encode the following Words of the language into a continuous bit stream: b d a b e

Is this encoding unambiguous? (Explain why.)

1011 1011 0100

It's not ambiguous as there are no digits that could be taken as the incorrect letter (amazingly). All prefix free codes.

c) [2 marks] What is the average number of bits required to encode a word using this encoding scheme?

(0.1 x 1) + (0.4 x 2) + (0.2 x 3) + (0.25 x 4) + (0.05 x 4) = 2.7 bits

[Taking into account the relative weights of each symbol (0.1, 0.4, etc) and the number of bits for each character (1,2, etc) lets you calculate the average.]

d) [1 mark] How much redundancy does a code Word contain on average?

Using more bits for messages than their Entropy (absolute minimum) is called Redundancy

Absolute Minimum/Entropy = 2.041425 bits

Current Scheme Information = 2.7 bits

Redundancy = 2.7 - 2.041425 = 0.658575

Q14. [5 marks] The ciphertext "EHZDUHWKHLGHVRIPDUFK" was produced with a "Caesar cipher" using Julius Caesar's historical key (according to Suetonius) and our modem 26-letter alphabet. Correctly decrypt the cipheflext using any method.

BEWARETHEIDESOFMARCH

Q15. [2 marks] Explain the difference: between a CP and a CPS in a PKI?

CP – Certificate Policy – A document listing the types of certificates a certification authority issues. A certificate policy is a document which aims to state what are the different actors of a public key infrastructure (PKI), their roles and their duties.

CPS – Certification Practice Statement – A document that details the identity verification process for issuance of certificates by a certification authority. A statement of the practices which a certification authority employs in issuing certificates.

According to X.509, a certificate policy is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security

requirements."

Q16. [2 marks] What is the Discrete Logarithm of 6 to the base 5 if We are calculating modulo 7, i.e. $\log_5 6 \bmod 7$

$\log_5 6 \bmod 7$ can be found by calculating each of 5^x mod 7:

$5^1 \bmod 7 = 5$
$5^2 \bmod 7 = 4$
$5^3 \bmod 7 = 6$

-> $\log_{-5} 6 \bmod 7 = 3$

Q17. [2 marks] Name two OASIS standardised Security Tokens approved for use with WSSecurity.

Username Tokens

REL Tokens

SAML Tokens

Kerberos Tokens

X509 Tokens

(Lecture 2, slide 34)

Q18. [6 marks] 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

Q19. [4 marks] 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 (A1ice's and Bob's) to compute the shared secret key that will be established between Alice and Bob.

N=p=11

A=g=3

Alice – x = 3

Bob – y = 4

Version 1 (Lecture)

Alice	Bob
Gy = 3^4 = 81	gx = 3^3 = 27
Gxy mod p = 813 mod 11 = 9	Gxy mod p = 274 mod 11 = 9

Version 2 (Tutorial)

Alice	
x = 3	y = 4
X = gx mod p = 33 mod 11 = 5	Y = gy mod p = 34 mod 11 = 4
Y = 4	X = 5
43 mod 11 = 9	54 mod 11 = 9

Q20. [3 marks] What are the steps in a SAML Browser Artifact Profile to obtain web single signon from one web site to another?

Logs on,

requests to go to another page withing single signon

Given artifact

gives artifact to second page

second page asks the artifact's generator if it's legit

if it is the user stays signed in

Q21. [9 marks] 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 HMACSHA1.

a) [1 mark] How many bits are in a 64 hexadecimal character key?

64*4 bits = 256 bits

b) [1 mark] What is the total entropy of a truly random 64 hexadecimal character key?

Truly random suggests equally weighted (not biased)

Log2 256 = 8 bits of entropy

Commented [31]: doesn't this imply there are only 256 possible outcomes? a 64 bit hex key will have 2^256 possible values, hence log2(2^256) = 256?

c) [1 mark] How many bits are in 63 printable ASCII characters'? (There are 95 possible different printable ASCII characters.)

63*7 bits

each character actually needs less than 7 bits as 95 < 128 (6.57 to be more accurate), so this could be represented in log(base 2)95 * 63 = 6.57 * 63 = 413.9 bits

d) [3 marks] What is the total entropy of a truly random 63 printable ASCII characters?

Truly Random, means equally weighted

Log2441 = 8.785 bits of entropy OR

log(base 2)413.9 = 8.6931, depending on which of the above is used.

e) [3 marks] 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

Log2182 = 7.5078

Commented [32]: Absolutely no clue about this - wild guess at doing something

Commented [33]: This question seems very ambiguous...

Q22. [4 marks] Consider an RSA system with the following parameters:

p=3, q=5, n=q*p=15

a) [1 mark] Find a valid parameter (public key) e, other than e=3.

e must have no common factors with z. So we need to find z:

z = (p-1)(q-1) = (3-1)(5-1) = 8

Therefore, e could be 5 or any number that has no common factors with z.

b) [3 marks] Use the above RSA system with parameter to encrypt the following three plaintext messages: m1=2, m2 = 4, m3=7

$C_{m1} = m^e \bmod n = 2^3 \bmod 15 = 8$

$C_{m2} = m^e \bmod n = 4^3 \bmod 15 = 4$

$C_{m3} = m^e \bmod n = 7^3 \bmod 15 = 13$

SUK A BORTZ