Exam 2012, Questions and answers rn

Information Security (University of Queensland)

COMS3000: 2012 exam answers

Question 1. [25 marks] Complete a Risk Register showing Greenfield Risk (no controls), Current Controls, Current Risk (before any new controls), and Residual Risk (after new controls), including all necessary items, such as consequences, mitigation, and likelihood, for the following THREE items:

1. Despite your excellent vulnerability patching program (new patches are applied within hours of release), a university student guesses your root password is toor (root backwards) and defaces your public website, which doesn't affect your current business but you cannot attract new business until you fix the defacement.

2. You need the administrative password to apply a critical patch to your stock market application before the market opens in 45 minutes or the company will be bankrupted - and the whole IT department (the only 6 personnel who know the administration passwords) were hijacked while flying to Ruxcon in Melbourne on AN487 - the plane left Australian airspace has not been seen since. [Only answer for this particular situation, do not generalise into all the other risks this raises.]

3. A meteor strikes your data centre (which is not currently located in an underground bunker specifically hardened to withstand meteor impacts) destroying all your computer systems and the company is unable to recover.

You must include the QUALITATIVE risk matrix that explains your risk ratings with consequences and likelihoods. It must not be less than a 3 x 3 matrix or larger than a 5 x 5 matrix. [Note it is not required to be a square matrix - 3 x 5 is perfectly acceptable]

You must choose your own ratings of consequence and likelihood at each stage (greenfield, current, and residual), based on your knowledge of threats, vulnerabilities, and controls, across the various domains of information security, including risk management, access control, personnel security, and physical security.

[Hint! Start this question on a new double-page opening in the answer booklet. You may break this up into three risk registers (greenfield, current, and residual) if you prefer.]

No controls

Risk name	Probability	Impact	Risk score
Root password guessed	Likely	Catastrophic	Extreme risk
Everyone who knows the password	Unlikely	Catastrophic	High risk

is unavailable			
Meteorite strike	Rare	Catastrophic	Moderate risk

Current controls

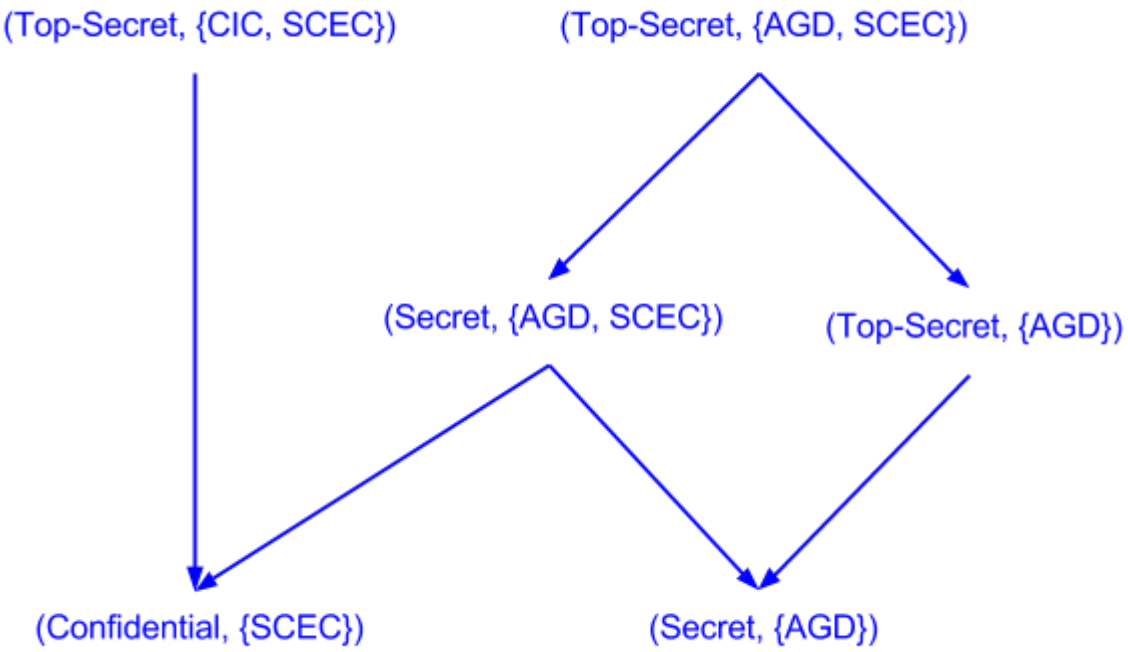
Risk name	Probability	Impact	Risk score
Root password guessed	Likely	Catastrophic	Extreme risk
Everyone who knows the password is unavailable	Unlikely	Catastrophic	High risk
Meteorite strike	Rare	Catastrophic	Moderate risk

New controls

Risk name	Probability	Impact	Risk score
Root password guessed	Rare	Catastrophic	Moderate risk
Everyone who knows the password is unavailable	Rare	Catastrophic	Moderate risk
Meteorite strike	Rare	Minor	Low risk

Question 2. [12 marks] Consider a Lattice Model with the levels "Top-Secret" (highest), "Secret", and "Confidential" (lowest) 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})



Question 3. [8 marks] You work for Australian Widget Makers Pty Ltd, a small Brisbane company. Like many small businesses, Widget Makers wants to utilise the cloud to get big business economies in their small business. However Widget Makers data is a trade secret and their competitive advantage. The business servers (to move to the cloud) directly interrogate the factory historian servers on the factory SCADA networks (no factory servers will move to the cloud) and load it into the business database (to move to the cloud) for subsequent data mining. How are you going to ensure the security of Widget Makers information and systems when you move them to the cloud?

1. This answer will depend somewhat on what type of cloud service as responsibilities differ between SaaS, PaaS and IaaS, therefore it is important to fully understand the contract and responsibilities of all parties
2. Use encryption (eg. SSL) for all communication between factory and cloud servers, in particular for management and administration interfaces
3. Separate duties so that no individual has access to all layers, also put measures in place to detect abuse and escalation of privilege
4. Ensure that SLA is balanced, binding and sufficient

Question 4. [25 marks] The following ciphertext:

PMITZTMGCEQLILWTZTBGDKACTZTSSUE

was produced with a Vigenère cipher using only one of the following 20 keys:

APPLE GATE AN TENT FAIR MOTOR BIKE FRED CIPHER KNIGHT ASP PRIME

BUY BAKER ANT TOOLS BY HEROES IN ELF.

a) [10 marks] Demonstrate the most efficient method to decrypt the ciphertext with only the resources you have available to you in this examination.

1. Find repeated string
2. Count offset for the starting letter of each repetition
3. Calculate the differences between the offsets in each occurrence
4. Find GCD of these differences
5. Use the GCD as the length of the key to narrow key options down
6. Assess key options based on frequency analysis

P M I **T Z T** M G C E Q L I L W **T Z T** B G D K A

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

C **T Z T** S S U E

24 25 26 27 28 29 30 31

Offsets = 4, 16, 25

Offerences = 16 - 4 = 12, 25 - 16 = 9

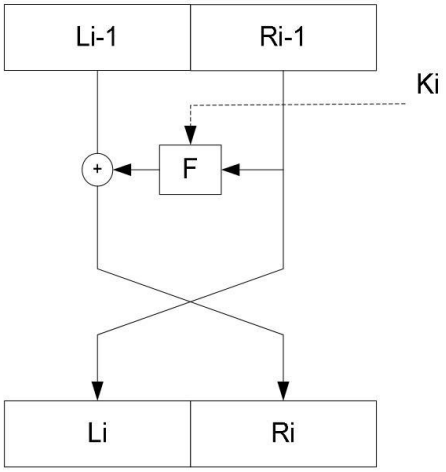
GCD(12, 9) = 3

Therefore key is either ASP, BUY, ANT or ELF

b) [15 marks] Correctly decrypt the ciphertext using any method. A Vigenère table is provided below.

Trying ASP as the key decrypts to “putthemoneywiththebookinthesafe” or “put the money with the book in the safe” so this is clearly the key.

Question 5. [15 marks] 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 subjected 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) [10 marks] 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 01011001; and

1001 = 1001 xor (0101 xor k)

1001 xor 1001 = 0000

0000 = 0101 xor k

0101 xor 0000 = 0101

b) [1 marks] Therefore what is the 4-bit key being used here?

k = 0101

To test:

1001 xor (0101 xor 0101)

= 1001 xor (0000)

= 1001

c) [4 marks] What is the result of the second 8-bit Feistel round?

[1001] [0101 xor (1001 xor 0101)]

= [1001] [0101 xor 1100]

= [1001] [1001]

= 1001 1001

Question 6. [8 marks] A biometric system has the following parameters: FRR = 0.03, FAR = 0.05. 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.)

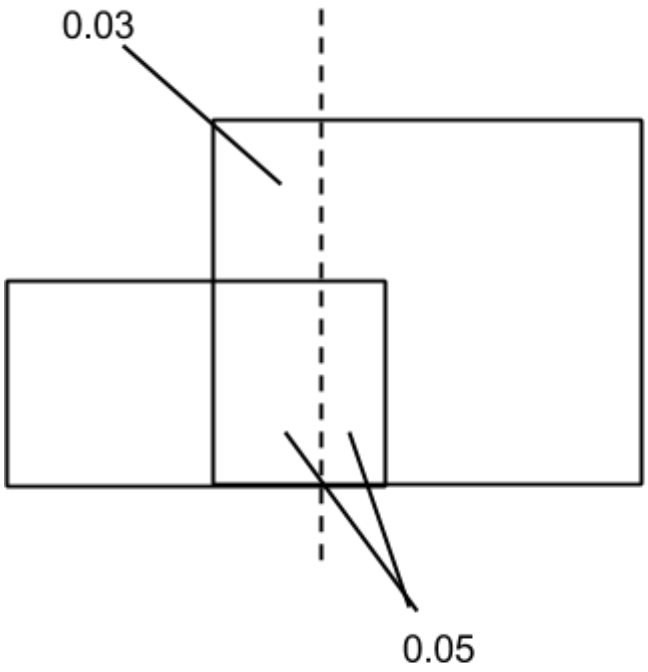
~~Of 2% "imposters", 5% will get in, therefore 0.02 x 0.05 = 0.001~~

~~Therefore 1 - 0.001 = 0.999 or 99.9% of users **inside** the system should be genuine~~

Let A be accepted.
Let G be Genuine.

The FRR is the probability that a genuine user is not accepted. So:
FRR = P(~A|G) = 0.03
∴ P(A|G) = 1 - P(~A|G)
= 0.97
The FAR is the probability that a NON-genuine user is accepted. So:
FAR = P(A|~G) = 0.05
∴ P(~A|~G) = 1 - P(A|~G)
= 0.95
P(G) = 0.98 (As stated in question)
∴ P(~G) = 1 - P(G)
= 0.02

To Find the probability that the accepted user is genuine or the P(G|A), we use:
P(G|A) = P(G && A) / P(A) *where && is the intersection of.
Now.
P(G && A) = P(G) x P(A|G)
= 0.98 x 0.97
= 0.9506
Now.
P(A) = P(A|G) x P(G) + P(A|~G) x P(~G)
= 0.97 x 0.98 + 0.05 x 0.02
= 0.9516
So.
P(G|A) = 0.9506 / 0.9516
= 0.9989 or 99.89%



98% x 0.05 = 0.049
98% x 0.03 = 0.294
1 - 0.049 - 0.294 = 0.9216 = 92.16%

Question 7. [2 marks] What is the purpose of a CA in a PKI?

To prevent man-in-the-middle attacks where the public key is substituted by an eavesdropper. The public key for a CA is embedded in a PKI implementations, and when a CA issues a certificate they encrypt a hash of it with their private key. The user can then decrypt the signature to produce the hash with the CA's public key and use the hash to be sure no one has altered the public key of who they're trying to contact.

A CA issues public key certificates to trusted parties. The CA must trust all parties it issues certificates to. This allows users to trust the parties because they trust the CA via transitive trust.

Question 8. [2 marks] What is the purpose of SOAP for Web services?

Question 9. [4 marks] Describe the security mechanisms available in the original IEEE 802.11 WLAN standard.

Question 10. [6 marks] Describe the main MAC security enhancements provided in the IEEE 802.11i amendment.

Question 11. [2 marks] Are "Level 3" merchants required to be PCI DSS compliant?

Explain.

Yes. Anyone who stores, transmits or processes “account data” (ie. PAN, Name, Expiry, etc.) must be PCI DSS compliant. The “level” only affects the requirement for compliance to be validated, rather than the necessity of compliance which is always required. Level 3 merchants are only required to “self-assess” compliance, rather than having an on-site review.

Question 12. [4 marks] Describe and explain the difference between IDS and IPS in network security.

IDS = intrusion detection system

IPS = intrusion prevention system

IPS is an extension of an IDS, it is able to detect intrusions like an IDS, however it also has the ability to intercept and potentially block traffic. It therefore must be “inline” with traffic, rather than just observe it.

Question 13. [5 marks] This is an actual field from the /etc/shadow file of a Linux system "**1UsR3x$PoS92oabFjdCSp/0H/a2so**" the "$" are separators, the first "1" means MD5 the next "**UsR3x**" is called the salt.

What is the rest "**PoS92oabFjdCSp/0H/a2so**" of the field in this entry and how and why is the "**UsR3x**" used?

The salt is used to prevent two identical passwords from producing identical hashes. This makes a database of common passwords and their corresponding hashes (ie. a rainbow table) less effective.

The rest of the entry is the hash, which includes both the salt and the password. When a password is verified a process similar to the following would occur: Does md5(UsR3x + password) = PoS9…

Question 14. [2 marks] 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, a key is something you have and a go-card is also something you have. The factors of authentication are something you are, something you have and something you know. Therefore a proximity card and a key would not be considered two-factor authentication.