UNIVERSITY
OF
JOHANNESBURG

**FACULTY OF SCIENCE**

**ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING**

|  |  |
|---|---|
| **MODULE** | **IT00217 / IT28X17**<br>INFORMATICS SECURITY RISK ANALYSIS |
| **CAMPUS** | **APK** |
| **EXAM** | **NOVEMBER 2014** |

|  |  |  |  |
|---|---|---|---|
| **DATE** | 19 November 2014 | **SESSION** | 08:30 - 10:30 |
| **ASSESSOR** |  | DR WS LEUNG |  |
| **EXTERNAL MODERATOR** |  | DR R PIDERIT<br>*(UNIVERSITY OF FORT HARE)* |  |
| **DURATION** | 120 MINUTES | **MARKS** | 100 |

1. Answer ALL questions.
2. Keep all answers relevant to the field of Information Security Risk Analysis.
3. Note the mark allocation for each question: if a question is worth 20 marks, ensure that your answer contains at least twenty facts.
4. Do NOT write in pencil.
5. Write neatly and legibly - if the work cannot be read, it cannot be marked.
6. Non-programmable calculators may be used
   - All working out must be shown in the answer.
   - DO NOT ROUND OFF values until the final answer.
7. This question paper consists of 6 (including this cover page) pages.

## Case Study

John Riley is a Fortune 500 media house executive who was recently the victim of a series of fraudulent transactions in which close to R250 000 was charged to his EMV ("Chip and PIN") credit card. According to statements accessible via Internet banking, several of the transactions were for payments to online stores located overseas while the majority were actually cash withdrawals from an ATM located at the food court that Mr Riley frequents.

Several days after reporting the fraud to the Machiavellian Bank, Mr Riley was informed that the bank would not be refunding him his lost money, citing the following reasons:

- For all online transactions, Mr Riley was further authenticated through an online verification system that sends him an OTP via SMS to his registered mobile phone.
- For all ATM withdrawals, a PIN was entered to authenticate Mr Riley as the authorised owner of the card. Furthermore, it is not possible to clone EMV cards.
- The Machiavellian Bank prides itself on being a progressive bank that puts the power to manage everyday aspects of banking (such as setting daily withdrawal limits, contact details, passwords, PINs, etc.) in the hands of their clients. All of this is made possible through the Internet banking site. To gain access to the site, customers will need to provide a username, an online PIN, and a password. As an additional level of security, changes regarded as being "sensitive" require the input of an OTP that is sent via SMS to the registered mobile phone.
- Despite being advised not to share his Internet banking credentials, logs show that Mr Riley has clearly provided them to YourPersonalFinancesGuru.com, a website that logs into a subscriber's Internet banking account to extract various financial information to provide reporting on spending habits.

Needless to say, Mr Riley is furious with the Machiavellian Bank's response. He has hired the services of your company, UJ Security Risks Advisory (UJ SecuRA) to conduct a risk assessment of his current practices to prove that banks are irresponsible to shift blame onto their innocent customers.

To that end, he has granted you full access to his office (which has an open door policy) and to inspect his desktop computer, his mobile phone, and his iPad (Wi-Fi only) which he uses whenever he is on the road (which is often). Should you require any of Mr Riley's passwords, Harold, his personal assistant, has been advised to provide you with them.

## QUESTION 1

You believe that Mr Riley is in for a surprise when you complete your investigation and will likely require more than just the results of the risk assessment. Prepare a report for Mr Riley in which you:

a) Explain why the results of a risk assessment alone are insufficient in addressing any risks identified by illustrating the generic requirements of risk management, identifying the four stages of the risk management cycle (4) and give a brief description of the role each stage plays (4). (8)

b) Identify assets that should be reviewed in the risk assessment. For each identified asset, explain **how** you will carry out the examination of the asset (i.e. what must you do to gather the necessary information about the asset). Your answer should be limited to only assets that Mr Riley is responsible for and can thus modify if necessary. ***Your answer should not include any "findings" you may have made.*** (12)

**[20]**

## QUESTION 2

The Machiavellian Bank has approached UJ SecuRA for assistance with allegations that a serious vulnerability exists with its ATM machines, resulting in potential pre-play attacks that would be indistinguishable from if a card had indeed been cloned. Allegedly, there exists an implementation flaw with the way in which ATMs generate a nonce for authentication purposes. As a result, attackers who are able to guess what the nonce will be, are able to harvest what appear to be legitimate authorisation requests for usage later (Bond, Choudary, Murdoch, Skorobogatov, and Anderson; 2014).

a) Provide a brief description of the three broad classes of ineffective random number generation that should be considered in your investigation. (6)

b) Taking into consideration that you have the backing of Machiavellian Bank, describe the scientific approach you would employ to prove or disprove that a weakly-implemented random number generator can possibly enable pre-play attacks on ATMs. (10)

c) Assuming that Machiavellian Bank is successful in patching all its ATMs, thus improving the way the nonce is generated, why will you advise them that pre-play attacks are still possible with the way that EMV transactions are processed? Describe two possible scenarios. (4)

**[20]**

## QUESTION 3

Management at Machiavellian Bank have realised that their attitude to risk has been outdated for quite some time (they believe risk is defined as population). They have retained your services to assist them with the updating their readiness for tackling risk.

a) How has the definition of risk evolved over the years? Your answer should include the various factors that are considered to increase or decrease risk. Your answer should further unpack these factors into contributing elements. (10)

b) Explain how Cressey's Fraud Triangle hypothesis would assist you in coming up with the bank's security policies to reduce the risk of the organisation. Your answer should demonstrate how (if) the various elements of the Fraud Triangle link to the occurrence of risk. Use a diagram to aid you in your answer. (10)

**[20]**

## QUESTION 4

Machiavellian Bank would like you to provide them with a single attack tree diagram that will provide them with the following information:

a) The various ways in which threat actors are able to commit fraudulent transactions on customers' accounts. You should include the various elements required by the threat actor to carry out the attack. *Make use of the case study provided and any other additional information from Questions 1 and 2.* (5)

b) The most likely approaches (taking possible and impossible attacks into consideration). (3)

c) Two **appropriate** countermeasures that could be deployed to address potential attacks. (2)

**[10]**

**THIS PAPER CONTINUES ON THE FOLLOWING PAGE**

## QUESTION 5

Machiavellian Bank customers are also able to access the various features of Internet banking via an app that is installed on their mobile phones. The Chief of Innnovation had originally proposed the introduction of a "mobile wallet" feature to the app that would effectively allow customers to link the phone to the funds in their bank account. The feature is meant to allow customers to pay for goods with merchants that support the payment option simply by swiping their phone.

However, due to the recent problems with the ATMs, plans were put on hold with upper management being very concerned with introducing potential security issues. Assist the Chief of Innovation by providing a misuse case that details the following:

a) At least five use cases along with appropriate actors (5)

b) At least three misuse cases with appropriate actors (3)

c) At least two measures that could be seen to mitigate threats identified (2)

**[10]**

## QUESTION 6

In light of this whole debacle, YourPersonalFinancesGuru.com has approached you to conduct an analysis of their system. They are particularly concerned with the following assets and their associated vulnerabilities:

- Asset A: Third-party information aggregation partner user database
  - Value Score of 98
  - Estimated accuracy of assumptions & data: 65%
  - Vulnerabilities:

| Vulnerability | Likelihood | Risk handled by current control |
|---|---|---|
| AV1 | 0.2 | No current control |
| AV2 | 0.6 | 75% |

- Asset B: Web server
  - Value Score of 95
  - Estimated accuracy of assumptions & data: 90%
  - Vulnerability:

| Vulnerability | Likelihood | Risk handled by current control |
|---|---|---|
| BV1 | 0.7 | 65% |

Prioritise the above vulnerabilities in order of highest to lowest risk, given the information provided. Be sure to show your full working out of the answer.

**[7]**

## QUESTION 7

Due to poor economic figures (and the fact that its services is offered for free), the management of YourPersonalFinancesGuru.com needs to embark on a cost-cutting exercise that involves optimising the costs of securing the organisation's network.

a) By means of a cost-benefit analysis, determine whether the countermeasure currently in use (an Intrusion Detection System (IPS)) can be justified by considering the following facts provided. Show your full calculation. (8)

- An asset valuation estimated the following values:
  - Web server: R900 000
  - Each desktop on the network (there are 16): R13 000 each.
- Prior to the implementation of the IPS:
  - Logs showed two (2) attacks occurred in the previous year.
  - On average, damage to the system was 47%
- The countermeasure has a base cost of R750 000 per annum with an additional R25 000 support fee per month.
- After the implementation of the IPS:
  - Logs show one (1) attack during the year.
  - Damage to the system was 5%.

b) Assume that the efficiency of the current countermeasure (Option A) is 95%. (5)

After some investigation, YourPersonalFinancesGuru.com has managed to source a possible alternative (Option B) from Secure Network Solutions which costs R1 050 000.00 per annum. Initial tests suggest that the system is 91% effective.

Is Option B more cost-effective than Option A? Show how you have worked out the answer.

**[13]**

***— END OF EXAMINATION ☺ —***

**GRAND TOTAL [100]**