Name:
Surname:
Student ID:

Introduction to IT security
Exam: Friday, 22nd of January 2021

1. RSA

    a. Explain the logic of public-key cryptography

    b. Could you explain a pros and cons of asymmetric encryption and symmetric encryption?

    c. What is role of the hash functions?

to encrypt a message M the sender:
obtains **public key** of recipient PU={e,n}
computes: C = M^e mod n, where 0≤M<n
n = 187; e = 7

Use the additional coding: transform your message into numbers by replacing each letter with its rank in the alphabet (for example, A is 01, B is 02, c is 03, D is 04…)

    d. Give the cyphertext of the following word using RSA encryption:

2. Firewall

    a. The following table shows a sample of a packet filter firewall rule set for an imaginary network of IP address range 192.168.1.0 to 192.168.1.254 (:182.168.1.0/24). Describe the effect of each rule.

	Source address	Source port	Dest address	Dest Port	Action
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow

7	Any	Any	Any	Any	Deny

b. Rules creation

In this exercise, you are given a set-up scenario from which you must determine how firewall rules would be written

- Outbound rules explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers. Because outbound traffic is allowed by default, you typically use outbound rules to block network traffic that you do not want.
- Using the blank template below, please write OUTBOUND firewall rules for the following:
    - Assume you have a small network at 169.64.98.0/24 subnet
    - Your web/e-mail server is at address 169.64.98.12
    - You don't want anyone on your network to access Facebook at all
    - You want to allow all ICMP messages sent out by your network
    - You don't want anyone on your network to be able to send any messages to DePaul

Rule #	Protocol	Accept/ Reject	Source IP	Source Port	Destination IP	Destination Port

c. Rules creation
In this exercise, you are given a set-up scenario from which you must determine how firewall rules would be written

- Outbound rules explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers. Because outbound traffic is allowed by default, you typically use outbound rules to block network traffic that you do not want.
- Using the blank template below, please write OUTBOUND firewall rules for the following:
  - Assume you have a small network at 169.64.98.0/24 subnet
  - Your web/e-mail server is at address 169.64.98.12
  - You don't want anyone on your network to access Facebook at all
  - You want to allow all ICMP messages sent out by your network
  - You don't want anyone on your network to be able to send any messages to DePaul

Rule #	**Protocol**	**Accept/ Reject**	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**

3. Confidentiality, Integrity and Availability

Explain the following terms:

- Vulnerabilities and Attacks
    - system resource vulnerabilities may
        - be corrupted
        - become leaky
        - become unavailable
    - attacks are threats carried out and may be
        - passive
        - active
        - insider
        - outsider

4. Risk management: Case Study: Silver Star Mines

This case study involving the operations of a fictional company "Silver Star Mines", the local operations of a large global mining company. It has a large IT infrastructure used by numerous business areas. Its network includes a variety of servers, executing a range of application software typical of organizations of its size. It also uses applications that are far less common, some of which directly relates to the health and safety of those working in the mine. Many of these systems used to be isolated, with no network connections between them. In recent years they have been connected together, and connected to the company's intranet to provide better management capabilities. However, this means they are now potentially accessible from the Internet, which has greatly increased the risks to these systems.

A security analyst was contracted to provide an initial review of the company's risk profile, and to recommend further action for improvement. Following initial discussion with company management, a decision was made to adopt a "combined approach" to security management. The analyst was then asked to conduct a preliminary formal assessment of their key IT systems to identify those most at risk, which management could then consider for treatment.

The first step was to determine the context for the risk assessment. Being in the mining industry sector places the company at the less risky end of the spectrum, and consequently less likely to be specifically targeted. Silver Star Mines is part of a large organization, and hence is subject to legal requirements for occupational health and safety, and is answerable to its shareholders. Thus management decided that they wished to accept only moderate or lower risks in general.

Next, the key assets had to be identified. The analyst conducted interviews with key IT and engineering managers in the company. A number of the engineering managers emphasized how important the reliability of the SCADA (Supervisory Control and Data Acquisition) network and nodes were to the company. They control and monitor the core mining operations of the company and enable it to operate safely, efficiently, and most crucially to generate revenue. Some of these systems also maintain the records required by law, and which are regularly inspected by the government agencies responsible for the mining industry. Any failure to create, preserve and produce on demand these records would expose the company to fines and other legal sanctions. Hence, these systems were listed as the first key asset. A number of the IT managers indicated that a large amount of critical data was stored on various file servers either in individual files, or in databases. They identified the importance of the integrity of this data to the company. Some of this needed be available for audits by government agencies. There were also data on production and operational results, contracts and tendering, personnel, application backups, operational and capital expenditure, mine survey and planning, and exploratory drilling. Collectively, the integrity of stored data was the second key asset. These managers also indicated that three key systems: the Financial, Procurement, and Maintenance/Production servers, were critical to the effective operation of core business areas. Any compromise in the availability or integrity of these systems would impact on the company’s ability to operate effectively. Lastly, the analyst identified e-mail as a key asset, as a result of interviews with all business areas of the company. E-mail is given greater importance than usual due to the remote location of the company. Hence the collective availability, integrity and confidentiality of mail services was listed as a key asset.

Having determined the list of key assets, the analyst needed to identify significant threats to these assets, and to specify the likelihood and consequence values. The major concern with the SCADA asset is unauthorized compromise of nodes by an external source. These systems were originally designed for use on physically isolated and trusted networks, and hence were not hardened against external attack to the degree that modern systems can be. Recognizing that the SCADA nodes are very likely insecure, these connections are isolated from the company intranet by additional firewall and proxy server systems. The second asset concerned the integrity of stored information. These assets could be compromised by both internal and external sources. All indications are that such database security breaches are increasing, and that access to such data is a primary goal of intruders. These systems are located on the company intranet, and hence are shielded by the company’s outer firewall from much external access. However, should that firewall be compromised, or an attacker gain indirect access using infected internal systems, compromise of the data was possible. The availability or integrity of the key Financial, Procurement, and Maintenance/Production systems could be compromised by any form of attack on the operating system or applications they use. Although their location on the company intranet does provide some protection, due to the nature of the company structure a number of these systems have not been patched or maintained for some time. This means at least some of the systems would be vulnerable to a range of network attacks if accessible. The last asset is the availability, integrity and confidentiality of mail services. Without an effective e-mail system the company will operate with less efficiency.

Given that externally sourced attacks are increasing, and known cases of attacks on SCADA networks exist, the analyst concluded that whilst an attack was very unlikely, it could still possibly occur. Thus a likelihood rating of Rare was chosen. The consequence of successful attack could have serious consequences as it could affect the safety of personnel in the mine, and the financial impact could be. A consequence rating of Major was selected. This results in a risk level of High. For integrity of stored information, a likelihood rating of Possible was chosen. Discussions with IT managers revealed that some of this information is confidential and may cause financial harm if disclosed to others, as well as the possibility of serious legal consequences if personal information was disclosed, or if the results of statutory tests and process information were lost. Hence a consequence rating of Major was selected. This results in a risk level of Extreme. For availability or integrity of the key Financial, Procurement, and Maintenance/Production systems a likelihood of Possible was specified. Discussions with management indicated that the degree of harm would be proportional to extent and duration of the attack. An attack would have a detrimental impact on the efficiency of operations. Consequence ratings of Moderate and Minor respectively were selected, resulting in risk levels of High or Medium. For availability, integrity and confidentiality of mail services, a likelihood rating of Almost Certain was selected in recognition of the wide range of possible attacks, and the high chance that one will occur sooner rather than later. Discussions with management indicated that whilst other possible modes of communication exist, they do not allow for transmission of electronic documents. Since compromise would not have a large impact, a consequence of Minor was selected. This results in a risk level of High. The information was summarized and presented to management, with the final result of this risk assessment process is shown in this Table.

Asset	**Threat/ Vulnerability**	**Existing Controls**	**Likelihood**	**Consequence**	**Level of Risk**	**Risk Priority**
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Could you propose the next steps and how you will mitigate the risks?

5. Explain the differences between symmetric and asymmetric cryptography. What is role of the hash functions?

6. What is a DOS attack and a Flooding Attack?

Name:
Surname:
Student ID:

7. Explain SSL and IPSEC. What are the differences between the 2?

8. Explain what is a risk analysis (in the security risk management)?

Name:
Surname:
Student ID:

Introduction to IT security
Exam: Monday, 31st of January 2022

1. Asymmetric and symmetric encryption

   a. Explain the logic of public-key?
   b. Could you explain a pros and cons of asymmetric encryption and symmetric encryption?
   c. What is role of the hash functions?
   d. What is the difference between cryptanalytic and the brute-force attacks?

Name:
Surname:
Student ID:

2. RSA Algorithm

to encrypt a message M the sender:

obtains **public key** of recipient PU={e,n}

computes: C = M^{e} mod n, where $0 \le M < n$

n = 187; e = 7

Use the additional coding: transform your message into numbers by replacing each letter with its rank in the alphabet (for example, A is 01, B is 02, c is 03, D is 04…)

Give the cyphertext of the following word “IT” using RSA encryption (Explain the RSA logic)

3. Permissions

Consider the following setting:

- There are 5 doctors (d1 . . . d5), 3 nurses (n1 . . . n3) and a patient (p1).

- Users can have roles medicalStaff, doctor, pediatrician, pediatricSurgeon, surgeon, nurse, pediatricNurse, patient, visitor.

- The permissions that can be assigned to the roles are readMI, updateMI, leadSurgery, assistSurgery, giveMedication, giveMedicationToChild

This setting can be formalized as follows:

- U = {d1 , d2 , d3 , d4 , d5 , n1 , n2 , n3 , p1 }

- R = {medicalStaff , doctor , pediatrician, pediatricSurgeon, surgeon, nurse, pediatricNurse, patient , visitor}

- P = {readMI , updateMI , leadSurgery, assistSurgery, giveMedication, giveMedicationToChild}

The setting has the following assignments:

User-to-role assignment: Permission-to-role assignment:

UA = { (d1 , doctor),
(d2 , surgeon),
(d3 , pediatricSurgeon),
(d4 , pediatrician),
(d5 , doctor),
(n1 , nurse),
(n2 , pediatricNurse),
(n3 , nurse),
(p1 , patient)
}

PA = { (pediatricSurgeon, leadSurgery),
(surgeon, leadSurgery),
(surgeon, assistSurgery),
(doctor , updateMI),
(medicalStaff , readMI),
(pediatricNurse, giveMedicationToChild),
(nurse, giveMedication)
}

The roles obey the following role hierarchy tree:

RH = { (pediatricSurgeon, surgeon),
(pediatricSurgeon, pediatrician),
(surgeon, doctor),
(pediatrician, doctor),
(doctor ,medicalStaff),
(pediatricNurse, nurse),
(nurse,medicalStaff)
}

Finally, we have the following constraints:

- Someone who is assigned the doctor role may never be assigned to the nurse role

- There should be at least one pediatricSurgeon:

(a) Suppose we introduce a permission “examinePatient” and we explicitly give this permission to doctors: PA := PA ∪ {(doctor , examinePatient)}. Does a pediatrician have this right now too? Explain your answer.

(b) Introduce a new permission “deleteMI” and adjust the setting such that all doctors and surgeons and pediatricians and pediatricSurgeons have this new permission.

Name:
Surname:
Student ID:

4. Firewall

The following table shows a sample of a packet filter firewall ruleset for an imaginary network of IP address range 192.168.1.0 to 192.168.1.254 (:182.168.1.0/24). Describe the effect of each rule.

	Source address	Source port	Dest address	Dest Port	Action
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

Why the latest rule (the number 7) must be always present?

5. Confidentiality, Integrity and Availability

Explain the following terms:

- Vulnerabilities and Attacks

    - system resource vulnerabilities may
        - be corrupted
        - become leaky
        - become unavailable

    - attacks are threats carried out and may be
        - passive
        - active
        - insider
        - outsider

6. What is a DOS attack and a Flooding Attack?

7. Explain SSL and IPSEC. What are the differences between the 2?

8. Explain what is a risk analysis (in the security risk management)?