Name: Leng Sopharot

Generation: 18

Gender: M

**16.11.2020**

**Final exam**

**Professional ethic in ICT**

**Questions (Total 40 pt)**

**Answer**

1. Threat is a negative event that can lead to an undesired outcome, such as damage to, or loss of, an asset. Threats can use—or become more dangerous because of—a vulnerability in a system. In common usage, the word Threat is used interchangeably (in difference contexts) with both Attack and Threat Actor, and is often generically substituted for a Danger.

* **Threat Actors**

Once we know what threats are it’s pretty straightforward to see what Threat Actors are. They’re simply the person, actor, entity, or organization that is initiating the given scenario.

This is generally reserved for human-driven scenarios, such as hack attempts. It doesn’t usually make sense to talk about threat actors when the event is a flood or an earthquake, for example. And if it does you probably have a book deal in your future.

## Vulnerabilities

Vulnerabilities are simply weaknesses in the system, and are not as commonly confused as other terms. Vulnerabilities are what make Threats possible and/or more significant.

### Examples

Common examples of Vulnerabilities include:

* Lack of proper building access control
* Cross-site Scripting (XSS)
* SQL Injection
* Clear text transmission of sensitive data
* Failure to check authorization to sensitive resources
* Failure to encrypt sensitive data at rest

Vulnerabilities are the weaknesses that are taken advantage of by Threat Actors to do what they’re trying to do.

## Risks

Risks are most commonly confused with threats, but they’re different in a crucial way.

A risk, in plain language, is a chance of something bad happening combined with how bad it would be if it did happen.

Let’s unpack that—it’s a **chance** of something bad happening…combined with **how bad** it would be if it happened. It’s essentially the combination of Probability and Impact, and in fact the most common equation for risk is the following:

Risk = probability x impact

The cause of confusion with Threats and Risks is that most people use both terms interchangeably a substitute for scenarios, without understanding the difference, e.g.:

We need to protect against these risks.

…or…

We need to protect against these threats.

…which are both the same as…

We need to protect against these scenarios.

It’s true that both refer to scenarios: the difference is that a Threat is a negative event by itself, where a Risk is the negative event combined with its probability and its impact.

## Summary

* **A Threat** is a negative scenario you want to avoid
* **A Threat Actor** is the agent that makes a Threat happen
* **A Vulnerability** is a weakness that can be exploited in order to attack you
* **A Risk** is a negative scenario you want to avoid, combined with its probability and its impact
* The difference between a Threat and a Risk is that a Threat is a negative event by itself, where a Risk is the negative event combined with its probability and its impact

1. **There are three type of hackers:**
2. **. Black Hat**

Black hat hackers are normally responsible for creating malware, which is frequently used to infiltrate computerized networks and systems. They’re usually motivated by personal or financial gain, but can also participate in espionage, protests, or merely enjoy the thrill. Black hat hackers can be anyone from amateurs to highly experienced and knowledgeable individuals looking to spread malware steal private data, like login credentials, along with financial and personal information. Upon accessing their targets and depending on their motives, black hat hackers can either steal, manipulate, or destroy system data.

1. **. White Hat**

Also known as “ethical hackers,” they’re often employed or contracted by companies and governmental entities, working as security specialists looking for vulnerabilities. While they employ the same methods as black hat hackers, they always have permission from the system’s owner, making their actions completely legal. White hat hackers implement strategies like penetration tests, monitor in-place security systems, along with vulnerability assessments. Ethical hacking, the term used to describe the nature of a white hat hackers’ actions, can even be learned through independent sources, training, conferences, and certifications.

1. **. Grey Hat**

As the name suggests, these individuals utilize aspects from black and white hat hackers, but will usually seek out vulnerabilities in a system without an owner’s permission or knowledge. While they’ll report any issues they encounter to the owner, they’ll also request some sort of compensation or incentive. Should the owner not respond or reject their proposition, a grey hat hacker might exploit the newfound flaws. Grey hat hackers aren’t malicious by nature, but do seek to have their efforts rewarded. Since grey hat hackers don’t have permission to access the system by its owner, their actions are ultimately considered illegal, despite any alarming findings they might reveal.

1. [Malware](https://www.crowdstrike.com/epp-101/malware/) is malicious software that enables unauthorized access to networks for purposes of theft, sabotage, or espionage. There are many types of malware, and many attacks use a combination of several types to achieve their goals.

**Malware** is usually introduced into a network through [phishing](https://www.crowdstrike.com/epp-101/what-is-phishing/), malicious attachments, or malicious downloads, but it may gain access through social engineering or flash drives as well.

* **6 types of malware with example**

### 1. Ransom ware

[Ransom ware](https://www.crowdstrike.com/epp-101/what-is-ransomware/) is software that uses encryption to disable a target’s access to its data until a ransom is paid. The victim organization is rendered partially or totally unable to operate until it pays, but there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly.

* **Ransom ware Example:**

This year, the city of Baltimore was hit by a type of Ransom ware named [[MobbinHood](https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/)](https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/), which halted all city activities, including tax collection, property transfers, and government email for weeks. This attack has cost the city more than $18 million so far, and costs continue to accrue. The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million.

### 2. Fileless Malware

Fileless malware doesn’t install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell or WMI. Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software — and because these attacks are stealthy, they are up to [ten times more successful](https://www.csoonline.com/article/3227046/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html) than traditional malware attacks.

* **Fileless Malware Example:**

[Astaroth](https://www.zdnet.com/article/microsoft-warns-about-astaroth-malware-campaign/) is a fileless malware campaign that spammed users with links to a .LNK shortcut file. When users downloaded the file, a WMIC tool was launched, along with a number of other legitimate Windows tools. These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners. Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server.

### 3. Spyware

Spyware collects information about users’ activities without their knowledge or consent. This can include passwords, pins, payment information and unstructured messages.

The use of spyware is not limited to the desktop browser: it can also operate in a critical app or on a mobile phone.

Even if the data stolen is not critical, the effects of spyware often ripple throughout the organization as performance is degraded and productivity eroded.

* **Spyware Example:**

[DarkHotel](https://www.wired.com/2014/11/darkhotel-malware/), which targeted business and government leaders using hotel WIFI, used several types of malware in order to gain access to the systems belonging to specific powerful people. Once that access was gained, the attackers installed key loggers to capture their targets passwords and other sensitive information.

### 4. Adware

Adware tracks a user’s surfing activity to determine which ads to serve them. Although adware is similar to spyware, it does not install any software on a user’s computer, nor does it capture keystrokes.

The danger in adware is the erosion of a user’s privacy — the data captured by adware is collated with data captured, overtly or covertly, about the user’s activity elsewhere on the internet and used to create a profile of that person which includes who their friends are, what they’ve purchased, where they’ve traveled, and more. That information can be shared or sold to advertisers without the user’s consent.

* **Adware Example:**

Adware called [Fireball](https://www.wired.com/2017/06/hack-brief-dangerous-fireball-adware-infects-quarter-billion-pcs/) infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and track web activity. However, the malware had the potential to become more than a mere nuisance. Three-quarters of it was able to run code remotely and download malicious files.

### 5. Trojan

A Trojan disguises itself as desirable code or software. Once downloaded by unsuspecting users, the Trojan can take control of victims’ systems for malicious purposes. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.

* **Trojan Example:**

[Emotet](https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/) is a sophisticated banking Trojan that has been around since 2014. It is hard to fight Emotet because it evades signature-based detection, is persistent, and includes spreader modules that help it propagate. The Trojan is so widespread that it is the subject of a [US Department of Homeland Security alert](https://www.us-cert.gov/ncas/alerts/TA18-201A), which notes that Emotet has cost state, local, tribal and territorial governments up to $1 million per incident to remediate.

### 6. Worms

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, worms can be used by malicious actors to launch DDoS attacks, steal sensitive data, or conduct ransom ware attacks.

* **Worm Example:**

[Stuxnet](https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/) was probably developed by the US and Israeli intelligence forces with the intent of setting back Iran’s nuclear program. It was introduced into Iran’s environment through a flash drive. Because the environment was air-gapped, its creators never thought Stuxnet would escape its target’s network — but it did. Once in the wild, Stuxnet spread aggressively but did little damage, since its only function was to interfere with industrial controllers that managed the uranium enrichment process.

1. **Social engineering** is a broad term used to describe a range of techniques to trick people into giving fraudsters what they want. **Phishing** is a specific technique designed to gain personal information, usually via email.

**Examples of** [social engineering](https://terranovasecurity.com/what-is-social-engineering/) range from [phishing](https://terranovasecurity.com/what-is-phishing/) attacks where victims are tricked into providing confidential information, vishing attacks where an urgent and official sounding voice mail convinces victims to act quickly or suffer severe consequences, or physical tailgating attacks that rely on trust to gain physical access to a building.

#### Confidentiality , Integrity, Availability

#### Confidentiality

Confidentiality measures protect information from unauthorized access and misuse.  Most information systems house information that has some degree of sensitivity. It might be proprietary business information that competitors could use to their advantage, or personal information regarding an organization’s employees, customers or clients.

#### Integrity

Integrity measures protect information from unauthorized alteration.  These measures provide assurance in the accuracy and completeness of data.  The need to protect information includes both data that is stored on systems and data that is transmitted between systems such as email.  In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to alter.

#### Availability

In order for an information system to be useful it must be available to authorized users.  Availability measures protect timely and uninterrupted access to the system. Some of the most fundamental threats to availability are non-malicious in nature and include hardware failures, unscheduled software downtime and network bandwidth issues.  Malicious attacks include various forms of sabotage intended to cause harm to an organization by denying users access to the information system.

1. Symmetric and asymmetric and different

* **Cryptography** is the science of protecting information by transforming it into a secure format. This process, called [encryption](https://techterms.com/definition/encryption), has been used for centuries to prevent handwritten messages from being read by unintended recipients. Today, cryptography is used to protect [digital](https://techterms.com/definition/digital) data. It is a division of [computer science](https://techterms.com/definition/computer_science) that focuses on transforming [data](https://techterms.com/definition/data) into formats that cannot be recognized by unauthorized users.

**Example:** of basic cryptography is a encrypted message in which letters are replaced with other [characters](https://techterms.com/definition/character). To decode the encrypted contents, you would need a grid or [table](https://techterms.com/definition/table) that defines how the letters are transposed. For example, the translation grid below could be used to decode " 1234125678906" as "techterms.com".

* **Symmetric encryption** uses a single key that needs to be shared among the people who need to receive the message while
* **Examples** of symmetric encryption algorithms include:
* AES (Advanced Encryption Standard)
* DES (Data Encryption Standard)
* IDEA (International Data Encryption Algorithm)
* Blowfish (Drop-in replacement for DES or IDEA)
* RC4 (Rivest Cipher 4)
* RC5 (Rivest Cipher 5)
* RC6 (Rivest Cipher 6)

AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers. RC4 is stream cipher.

* **Asymmetrica**l encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
* **Examples** of where symmetric cryptography is used are:
* Payment applications, such as card transactions where PII needs to be protected to prevent identity theft or fraudulent charges
* Validations to confirm that the sender of a message is who he claims to be
* Random number generation or hashing

1. **Cyber law** investigates crimes perpetrated in the physical world but enabled in cyberspace. For example, organized crime syndicates using the internet to distribute illegal substances may face prosecution under cyber laws.

• Regulation is a rule or order issued by an executive authority or regulatory agency of a government and having the force of law.

•Legal Compliance simple means to comply with all the necessary laws and regulations applicable.

1. Secure Email Sever:

• Scan email attachments for malware.

• Turn off the preview feature and change download settings in email clients.

• Create junk email filter in email clients.

• Digitally sign your mail messages.

• Avoid unwanted emails using filters

• Create and use strong passwords.

• Provide alternate email address for mail recovery.

• Check for last logging activity.

• Use HTTPS for browser connection.

• Disable/unselect Keep Me Signed In/Remember Me functions.

• - Network Communication:

• Client: A process that requests services on the network.

• Server: A process that responds to a request for service from a client.

• Datagram: The basic unit of information, consisting of one or more data packets, which are passed across an Internet at the transport level.

• Packet: The unit or block of a data transaction between a computer and its network. A packet usually contains a network header, at least one high-level protocol header, and data blocks. Generally, the format of data blocks does not affect how packets are handled. Packets are the exchange medium used at the Internetwork layer to send data through the network.

1. What is firewall, IPS/ IDS, network firewall, endpoint firewall?

• firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

• Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies – any other traffic attempting to access the network is blocked. Network firewalls sit at the front line of a network, acting as a communications liaison between internal and external devices.

• endpoint firewall is a firewall that runs within the application. It’s aware of the software used inside the website and understands how it’s built.

• IDS is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems.

• IPS is part of your network to detect and stop potential incidents.

* 1. Give example of attacking to ICT via TCP and via UDP?
  2. Please give definition and example of ICT policy, ICT procedure, ICT standard, and ICT guideline?

• ICT policy (The Information and Communications Technology and Security policy): is a formal statement of the rules and guidelines applied by the Municipality which must be adhered to by people utilizing and managing the ICT facilities.

• ICT procedures refers to the development or acquisition, testing and implementing applications and databases to support the department's business needs to capture, store, retrieve, transfer, communicate, and disseminate information through automated systems.

• ICT standards play an essential role in achieving interoperability of new technologies and can bring significant benefits to both industry and consumers. They help ICT markets remain open and allow consumers the widest choice of products.