Chapter 1 - Introduction to Information Security

**Distinguish between vulnerability, threat, and control**

Threat is a set of circumstances which can cause harm.

Vulnerability is a weakness that could be exploited to cause harm.

Control is a measure that prevents threats from exercising vulnerabilities.

**List three kinds of harm company might experience from theft of computer equipment**

The company could be damaged in through character of harm: integrity, availability & confidentiality. Theft of computer equipment would result in compromization of mainly availability and confidentiality. If the loss is not known and the equipment is e.g. copied, fabricated or modified and then put back, the company would also suffer from integrit problems.

By loosing the computer equipment, the company could suffer a financial loss in:

* Buying a new PC (direct cost)
* Setting up a new PC (direct cost in time)
* Downtime (direct cost and cost in time due to disability to work)
* Compromised secrets, data and intelligence (indirect cost)

**List at least three kinds of harm company could experience from electronic espionage or unauthorized viewing of confidential company materials.**

Private emails could be read. Essential information about the core business such as a secret reciepe or a secret business operation could be revealed. These type of harm could be crucial to the existence of certain businesses and could result in a massive financial loss indirectly.

Credentials could be attained though espionage and unauthorized viewing, putting the user of those credential to risk and the account connected to those credential would be at risk as a subject of compromization.

If a customer plan is revealed, a competitor may act faster and result in a loss of marketing shares and ultimately, large financial losses.

**List at least three kinds of damage a company could suffer when the integrity of a program or company data is compromised.**

Compromised Integrity:

* Integrity of e.g. a file could imply many different thing. For example it can mean that the file has been changed, replaced or fabricated. So, the content of the file cannot be ensured to be the same as before the integrity change.
* in certain systems, an integrity error, or integrity compromize can make a system completely useless.
* If a register is dependent of the modification date, we will have a faulty indexing following the modified file.
* In safety critical system especially, integrity problems can make data completely useless. If integrity of a system cannot be ensured its behavior cannot be relied upon.
* An example is if a binary file has changed, it will for a normal user be hard to check what has caused the change, what the change is and what the change implies when execuring or using the binary file.

Compromised company data:

* Financial loss in terms of revelation of secrets, credentials or other secret agreements.
* Time loss in terms of lost key files, blueprints and recipees, resetting systems, redoing work.

**List at least three kinds of harm a company could encounter from loss of service, that is, failure of availability. List the product or capability to which access is lost, and explain how this loss hurts the company.**

Failure of availability as a result of loss of service can happen for most service.

* Failure 1: Bank customers cannot access their website due to an DDoS attack. The bank suffer from a financial loss in terms of withheld bank transaction and other financial activity. The bank suffer from customer irritation and may take reputational damage in terms of frustration and the fact that the service is down. Customer themselves may suffer from financial loss in terms of withheld payments, debt and downtime. When customer are affected financially, tha bank is too.
* Failure 2: If an important electronic design document or file is lost, a business operation and project might be crippled. The loss may require creating a new document, dropping the project or halting the project until it is retrieved to its normal state. In a project, many people might depend on a document.
* Failure 3: Connection problems. If an ISP suffer from physical or logical DoS in any of their main systems, many customers may be affected. This will cause irritation, stress and financial loss for customers. Such a situation may cause a number of customers to change ISP provider cause a financial loss also for the current ISP provider. The ISP problem owners of the DoS may have to spend a lot of resource on diagnosis of the network, the specific error and in exhausted customer support channels.

In short, is the loss of service is happening in a non-critical environment such as music streaming or similar, the effects are also short term (mostly irritation, frustration, stress etc).

However, if the loss of service is in a critical environment, such as in a hospital or a traffic light system, lifes are at stake. Here, there is a higher risk of permanent damage and more long term financial losses in terms of reputation, results and safety assurance.

**Describe a situation in which you have experienced harm as a consequence of a failure of computer security. Was the failure malicious or not? Did the attack target you specifically or was it general and you were the unfortunate victim?**

For example, a sports fantasy management website became popular ish 10 years ago. This site was based on profiles of thousands of players. The profiles were created by the managers of the teams and data was uploaded under verbal consent / agreement. A few years back (after GDPR), I stumbbled across my profile on Google showing a profile with name, picture, age and description. I wanted to take it down, but I did not have any login. I tried to take it down through mail-contact with the business, but the picture is still cached in googles servers somewhere.

**Describe two examples of vulnerabilities in automobiles for which auto manufacturers have instituted controls. Tell why you think these controls are effective, somewhat effective, or ineffective.**

An example is the amount of software used in todays automobiles. It requires all range of microcontrollers along with engine control unit, infotainment, and control systems. This makes automobiles in general more prone to vulnerabilities and effective control of such. Another example is the expensive hardware integrated and mounted on automobiles which must be protected from theft. Automobile industry have had less experience in cybersecurity compared to the computer science fields and thus, there has been a lack in security awareness embedded into the development lifecycle. Dealing with security patching.

An example of vulnerabilities in an automobile is the Controller Area Network. This is bus network used in safety-related communication. Real world attacks has been implemented against ECUs connected through this type of network.

In the CAN case, an attacker can use sniffing to learn about other network nodes to perform e.g other attacks. DoS attacks can also be done on the network itself and directly towards ECUs. Spoofing can be done, this is when an attacker is sending data to a node falsifying to another node in the network. This is pften performed as a replay attack where sniffed data (earlier authentication) is sent to a subject. There are also attacks where the payloads has been forged by the attacker, called masquerade attacks. For example IA-CAN has 2 step authentication and uses cryptography to randomize an identifier.

**One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?**

Use of a version control system (VCS) like for example bitBucket, gitHub or Serena Dimensions CM. Any changes can continously be added, committed and pushed to a remote repository (cloud storage) and easily be fetched or pulled to the same or another machine. The cost is only as expensive as the changes since your last push (update) which should only be minutes if you're doing something time consuming and important.

**On your personal computer, who can install programs? Who can change operating system data? Who can replace portions of the operating system? Can any of these actions be performed remotely?**

I (the admin) can change operating systems data and install programs. None of these actions can be performed remotely. A guest user does not exist, the default for guest user is to be able to install any program in his/her home directory. Potentially, they could install malicious programs if such a profile is created and no password is given.

**Suppose a program to print paychecks secretly leaks a list of names of employees earning more than a certain amount each month. What controls could be instituted to limit the vulnerability of this leakage?**

When the program sends data (transmits data) or stores data, encryption can be implemented. This way even though the data (paycheck) leaves the enterprise and other controls can easily be circumvented, the data cannot be read. If the information is not encrypted, it is hard to control the leakage once the information has left the enterprise. An extreme control could be to install a honeypot, generating fake profiles in order to disorient an attacker. Inside the enterprise itself, least privalege should be used so the list of users that can benefit from the printing shall be short and gone through. If there are no limits on e.g. a printer or such devices, an audit trails should be implemented tracing back to the specific user ID. So we have an access control on the device & the program, and we have a least privalege policy on the program itself. If the program is correctly implemented, credentials should be used to activate the process.

If the leakage is found and the problem is reoccuring, an organization would have to reinstate the standard access controls, least privalege reset, patch the security problem (if any) and start reusing it.

**Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four? That is, is any of the four equivalent to one or more of the three? Is one of the three encompassed by one or more of the four?**

Interruption, interception, modification and fabrication is a state or a cause. it may be seen as a methods from an attackers perspective or a vulnerability from a subjects perspective.

* Interruption may cause availability problems.If a communication is cut for a few seconds (interrupted), a service connected / related to that communication might not be available is there are no backup communication.
* Interception may cause confidentiality problems. If a communication is wiretapped / eavesdropped or sniffed a user's data is subject to unauthorized viewing. Confidentiality and privacy is violated and the data (or intelligence) is compromised. Private data or the private communication is not private anymore.
* Modification & Fabrication may cause integrity problems. If a binary file is modified, one cannot be sure before analysis what has been changed or what effects it might have. If data has been fabricated, it may create an illusion to the user, tricking it into a certain behavior. Fabricated files could also trick database systems, operating systems or networking systems. Integrity problems is especially important in safety-critical application where some files can never change. Modification and fabrication can also be done to implant malicious code into a program or file.

**Do you think attempting to break in to (that is, obtain access to or use of) a computing system without authorization should be illegal? Why or why not?**

Attempting to break into a system should be legal. Stealing something or leveraging the intrusion of some sort shall be illegal. This way we maximize the level of penentration testing and good-will hacking both for hobby individuals, researchers and professionals (industry people). The legal break in will create a strong force and incentment to create more secure systems from the beginning and to continously update and patch existing solutions. Criminals would not stop due to making an act illegal since that is the definition of a criminal (someone who oversteps the law). Making a break-in illegal would put criminal hackers and terrorists in an empty room with the target (an application not as secure). Making intrusion legal, also forces / puts pressure on businesses to patch their systems instead of postponing it due to financial reasons.

If something is unauthorized viewed, stolen or blocked, of course, theses acts shall be illegal.

**Describe an example (other than the ones mentioned in this chapter) of data whose confidentiality has a short timeliness, say, a day or less. Describe an example of data whose confidentiality has a timeliness of more than a year.**

Confidentiality with short timeliness:

* A weekly email can have a timeliness of just a day or less.
* An upcoming event plan can have a timeliness of just a day or less.
* An auto generated security token through the Federal Identity Manager Google Auth or Microsoft Auth.

Confidentiality with long timeliness:

* Marketing or product plans
* Medical records
* Tax returns
* A secret password
* A secret question
* A creditcard number and its CVC code

**Do you currently use any computer security control measures? If so, what? Against what attacks are you trying to protect?**

Windows defender – To update against the latest security threats, vulnerabilities and harm all over the world. As a reference monitor to check downloading files, internet traffic, and operating system processes. As a patcher to update Windows Firewall policies and rules. As a virus scanner to detect malicious or suspicious code.

Windows firewall – To avoid certain traffic, patterns and data from the network both for outcoming and incoming traffic. Based on standard security rules following a robust set of policies based on historical events and known identifiers.

Network Modem/router – Another security constrol before the actual PC. Acts as a first firewall, configured to detect and filter out certain traffic and traffic patterns.

ISP Network subscription - A known Internet Service Provider which internallt have blacklisted traffic, and filters out some traffic. Registers known problems , known threats and harms.

Addblocker – To avoid popup site, fishing, click jacking, imitation and driveby downloads.

VPN – To encrypt my communication on the internet. To keep my internet activity private and protect myself against eavesdropping, sniffing and other network-based / internet-based attacks. Fool the browser and other programs that I am connecting from another location etc.

TOR – To keep my network activity confidential by using the necryption provided through TOR. Both the source and the destination IP address is encypted between all routers. The routing path can be set depending on what level of security one wishes and it jump randomly using an existing TOR directory. The TOR directory hands out routes to the TOR client which decrypts a message the requested number of time. When a message arrives at the routes it is decrypted and the message (still decrypted) is sent to the next router which does the same. Ultimately, the message unfolds as a peeled onion (therefore the onion browser) and the final destination recieves the message in plain text, if the message itself is not encrypted aswell.

Duckduckgo – To prevent addware, spyware, webpages to track my browser activity. Prevent me from using the mostly used browsers and prevents them from tracking me. i have control over my activity and what tracksI am leaving after.

Incognito/private browser mode – Cookies is not saved, history is not saved, no other data is saved and information is not collected or displayed based on earlier activity.

Knowledge – I only visit known and trusted website to avoid attacks. When using login-credentials I often use a two-factor method with an out-of band alternative communication such as SMS, e-mail or regular mail.

**Describe an example in which absolute denial of service to a user (that is, the user gets no response from the computer) is a serious problem to that user. Describe another example where 10 percent denial of service to a user (that is, the user’s computation progresses, but at a rate 10 percent slower than normal) is a serious problem to that user. Could access by unauthorized people to a computing system result in a 10 percent denial of service to the legitimate users? How?**

Absolute denial of service is a critical harm when the user is in an emergency and must perform a certain operation on that computer.

10 % slower computation than usual may become a serious problem when the user application is safety critical.

If many unauthorized people are accessing the same system, depending on the system design, it may delegate resources to those users resulting in a potential 10 % denial of service to legitimate users.

**When you say that software is of high quality, what do you mean? How does security fit in your definition of quality? For example, can an application be insecure and still be “good”?**

All software contains bugs, but software of higher quality contains less bugs and have solutions on how to recover, avoid or mitigate a bug. A software can definently be useful and not take any important security meassures. It may provide some kind of function or tool for users at the same time as putting them to risk.

A software is of high quality when all aspects of quality is covered. This includes security IF, there is a requirement that the application must be secure (that is if the application can be used to cause any harm). If a system is insecure, the system obviously has some requirement of being secure and the security is thus of lower quality affecting the overall quality of the software.

**Developers often think of software quality in terms of faults and failures. Faults are problems (for example, loops that never terminate or misplaced commas in statements) that developers can see by looking at the code. Failures are problems, such as a system crash or the invocation of the wrong function, that are visible to the user. Thus, faults can exist in programs but never become failures, because the conditions under which a fault becomes a failure are never reached. How do software vulnerabilities fit into this scheme of faults and failures? Is every fault a vulnerability? Is every vulnerability a fault?**

A fault is a problem that developers can see by looking at the code. Failures are problems such that systems crash or invokes the wrong function (visible to users).

Not all faults results in a failure, but some could potentially become a failure. If a failure impact the users negative, it is a vulnerability. In fact, a failure is always a vulnerability. A fault is not always a vulnerability since not all fault can be exploited to be negative to users. For example a fault may remain a fault only for the developers. For some fault we need a condition for it to become a failure, this condition may never be reached. Not every fault is a vulnerability but every vulnerability is some kind of fault.

A vulnerability is a fault which may be used to cause a failure. Not every fault is a vulnerability, nor the opposite. Even though it is likely that a vulnerability is a fault, there might be external factors creating a vulnerability. A vulnerability can potentially lead to a failure of functionality or usage overall.

**Consider a program to display on your website your city’s current time and temperature. Who might want to attack your program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**

if the website displays the current time and temperature, the website may have some traffic to it. It is also a failry simple website which witness of little implemented or though through security controls and security design. One motive could be to spread confusion, another could be to take over the site, a third could be to advatage the user traffic to the site spread malicious code, misleading content, or to obtain user information.

The simple site could be advantaged for website defacement, residing in a similar domain (1 letter anamoly) or redirect users to the other site. This way the user thinks they are visiting a legit site but under the hood, there might be malicious activity going on. For example,activity can be traced, links can be hidden. The visiting users could be subject of a clickjacking attack, where they are tricked into a certain input and e.g. a download is masked. Taking over the site, the attacker might append misleading content, change the information or install drive-by downloads which is trigger only on requesting a page. Many attacks can be performed using cross-site scripting which is similar to buffer overflow. if the site implements databse requests, SQL injections might be possible to create problems in the database or retrieve information other than the temperature and current time.

An attacker could have the motive to make the website insignificant to redirect traffic to another website. Another motive could be to spread confusion among the public. A third motive would be to track traffic or display adds to make a financial benefit. They may want to put down the site. They might want to modify the site. They might want to fabric the site. They might want to surveillance the traffic.

**Consider a program that allows consumers to order products from the web. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**

Ordering a product involves a lot of customer information and possible payment credentials. These can be of high value for a hacker. If they can steal that information they could sell it or use the payment credential. If the site is huge and the business depend on the sales from it, one can argue the importance of having it online or if it could be a subject of a DoS attack to interrupt the access and disable it for a few minutes, hours or days. For example, putting a service out could be used in blackmailing attempts. Also, the items and their information could be chaged or manipulated by the attacker, thus integrity issues arise.

A webshop could be attacked with a dot-dot-slash attack where a lot of entries and URL's are tested. If access is granted through one of the entries, wrong information may be public to the attacker.

Most likely, the webshop uses some database to list all its projects and its information. This database could possibly be an SQL database. So the input fields in the webshop could be manipulated to perform a SQL-injection attacks if inputs checks and database input is not checked and sanitized.

Cross-site scripting.

A competitor who want an advantage in sales. An activists who interest are not inline with the companies. A government secret service, if the site is used to steal user and payment credentials and information.

They might cause financial loss, time loss etc.

The attackers may use e.g. denial of service. Loading the product system to much making an interruption long enough to making an impact on the sales, reputations and customers.

The attackers may use a fishing email, imitating the interface of the web interface, stealing customer information.

Attackers may use other malware to steal customer or company information.

**Consider a program to accept and tabulate votes in an election. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**

A program that accepts votes could be a high target for hacking attacks since the output/result of manipulating the input to the website or the website itself could manipulate the result. First of all, the program or website could be substituted with a fakewebsite resulting in that credentials are stolen and that the actual vote is not registered. The website or program could be attacked with injected links and scripts in storage, inputs and other vulnerabilities to generate a certain input from the clients running it. If an add-on, or other program is installed on the client's browser it may manipulate the result of that website or program. It could be attacked with cross-site scripting, SQL-injection attacks to manipulate the input or the stored result. It would be valuable to colellect all kinds of user information in the votes since this is a valuable asset and could be sold. To download the program, some kind of distribution is needed. If this distribution is hacked e.g. a website, an attacker may replace the program download with a malicious download (A Trojan).

Government supported hackers, criminal networks, political organizations. They may want to change the outcome of the election by flipping the tabulate votes.

They might use vulnerabilities in social networks, creating fake profiles spreading misinformation and propaganda.

**Consider a program that allows a surgeon in one city to assist in an operation on a patient in another city via an Internet connection. Who might want to attack the program? What types of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?**

Government/regime supported hackers, technical competitors, someone who wants to cause harm or blackmail for money. Ransomware.