Aarni Ylitalo

2584582

**Week 3**

Task 1

Lock-ins can be divided into 2 sub-groups, monopolistic and non-monopolistic. Monopolistic meaning if a single vendor has a monopoly for a technology or method. These can be for example patents. Non-monopolistic and collective lock-ins are called as technology lock-ins. These kind of lock-ins are society level lock-ins which are controlled by the masses who stick to use a certain technology. Example of this is QWERT keyboard layout. Monopolistic, collective and non-collective lock-ins are known as vendor lock-ins. Monopolistic and collective lock-in is when a company has a product so dominant, people are afraid to switch from it. These are often locked behind a patent. Apple is in my opinion good example of this with their products linking with each other seamlessly and specifically iMessage and FaceTime. The collective aspect comes from people fearing that they will miss out if they can’t FaceTime or do some else Apple only thing with their friends.  
  
Sources

Wikipedia

Task 2

Phishing is when someone creates an email, post on social media or a link on a website that for example leads to page asking for your login credentials or other personal information. Effectiveness comes from multiple factors; there are no laws about it, peoples general knowledge about them is limited, its easy to do and human nature of naively to believe what they are told. Example of phising attack is a legitimate looking email from Google or Apple or some website to change your password and link to change it. For the attacker its relatively easy to get the data how these companies emails and websites look making it quite a task for an average joe to tell if its real or not. When the victim clicks the link and gives the information the data goes to the attacker and possibly giving confirmation for the victim that password is changed even when its not.

Social engineering is basically using manipulation to gain sensitive data or access. It is considered to be more effective than technological methods due to human error. Social engineering is used in emails, text messages, chats, forums, phone calls and face-to-face. Text based social engineering usually utilizes peoples emotions such as fear, concern, joy or happiness. With some information about the victim it can be tailored to victims life situation e.g. marital status, finance etc.. In-person social engineering takes advantage of peoples attention and awareness. These include shoulder surfing where attacker peeps others PIN or password when they are not aware of it. Other types of in person attacks are claiming to be an employee and getting access to companies network from the inside by implanting malware with usb or other device.

Password is recommended to be at least 12 characters long, containing upper and lowercase letters, numbers and symbols. Password should be also something that can not be found on dictionary not be name of anything.(Microsoft) This is something that people tend to have hard time to when creating account for websites or apps. Maybe the biggest sin is that humans use same password on multiple platforms and it also tends to be weak e.g. Password123. Reason for that is our finite memory or possibly even more our laziness to create unique passwords for each service.

PGP (Pretty Good Privcy) is an encryption method which uses public-key and symmetric-key encryption to protect confidential messages. The public-key is meant to be visible for everyone and the private-key to be strictly sent only to recipient. With the private-key and public-key combination the message could be decrypted. Problem with this lies in the symmetric part of the private-key, it is always the same for specific sender. Another problem is that PGP is challenging to use. Trading PGP keys takes a lot of time and is not simple process. Integration with different programs is a time consuming process. Lastly PGP does not have forward secrecy. That means if key is compromised it can be used to read encrypted messages from the past.

Malware is a term for software which is designed to harm on contaminate a device. Its purpose may be to steal sensitive information through keystrokes for example. Usually it spreads by duplicating its self and going through network on its own. I may stay inactive for a while and activate its payload remotely on due to a some action. How malware gets to its first destination is through email, websites or apps, usually requiring to download something. When downloading it may even have the app or data the person needs but also the harmful payload.

Sources

<https://powerdmarc.com/why-is-phishing-so-effective/>

<https://blog.knowbe4.com/human-behavior-is-what-makes-phishing-attacks-so-successful>

<https://clearinsurance.com.au/what-is-social-engineering-and-why-is-it-so-effective/>

<https://powerdmarc.com/cyber-attackers-use-social-engineering-attacks/>

<https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

https://www.raconteur.net/sponsored/why-do-we-have-such-a-hard-time-with-passwords-heres-the-answer

<https://skiff.com/blog/pgp-dead-what-next>

https://www.michigan.gov/ag/consumer-protection/consumer-alerts/consumer-alerts/id-theft-telemarketing/malware

Task 3A

Intellectual property is way to protect invention and works by legal methods. These methods include patents, copyright, trademarks patents and non-disclosure agreements (NDA).

Patent is right to use an invention. It has to be applied and granted and it is country specific. Patents cover the invention for unauthoried commercial use, manufacturing, distribution, importing or selling. If someone uses the patented method/technology/etc. it can be forced by law to compensate for the losses caused by the unauthorized use. Patented technologies can be used by a third party if they make a licensing deal. Example of a patents can be found from <https://ppubs.uspto.gov/pubwebapp/> and searching 11770062. This gives Apples patent for Liquid Heat Exchanger For Electronic Device.

Copyright is used mainly for artistic work, from music and literature to computer programs and technical drawings. Its main purpose is to protect expression and not ideas. Copyright applies to majority of countries and it does not require applying, meaning its obtained automatically. There are some countries where voluntary registration is possible, which may ease any problems in the future.

Trademark is a protection for goods and services. It can be gotten by application process and paying some fees and its also country specific.

Non-disclosure agreement is legally made agreement between two or more entities who agree to not to share information obtained from each other.

Digital watermarks are markers in files like audio, video or image. These can be seen/heard but are usually somewhat minimal or transparent. Main use for watermarks are for tracking copyright infringements.

Software license is a legal way to use copyrighted software. It can be split into free/open and non-free. Free/open licenses vary form giving all rights to forbidding proprietization. Non-free licenses go from giving noncommercial use to no public information.

Digital Rights Management (DRM) is the way to control copyrighted material. Its main purpose is to protect copyrights holder’s rights and prevent any misuse of their copyrighted medium.

Software protection dongles are used to unlock data and software restrictions with hardware. Sound kinda sketchy.

Sources

<https://www.wipo.int/about-ip/en/>

<https://en.wikipedia.org/wiki/Digital_watermarking>

<https://en.wikipedia.org/wiki/Software_license>

<https://en.wikipedia.org/wiki/Software_license>

<https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm>

https://cpl.thalesgroup.com/software-monetization/software-licensing-basics/dongles