Cybersecurity

G. Filosofi 2019

Cybersecurity is the process of protecting information by preventing, detecting and responding to attacks

CVE (Common Vulnerability and Exposure): search engine https://nvd.nist.gov/vuln/search
CVE-yyyy-nnnnn: è un modo di classificare le vulnerabilità?

Le vulnerabilità injection vector come si può intuire dal nome, ti permettono di iniettare nel sistema il tuo malware però spesso quel malware è un codice non firmato quindi non è detto che viene eseguito dal sistema per questo caso verrà utilizzato il code signing che serve appunto ad eseguire un codice non firmato.

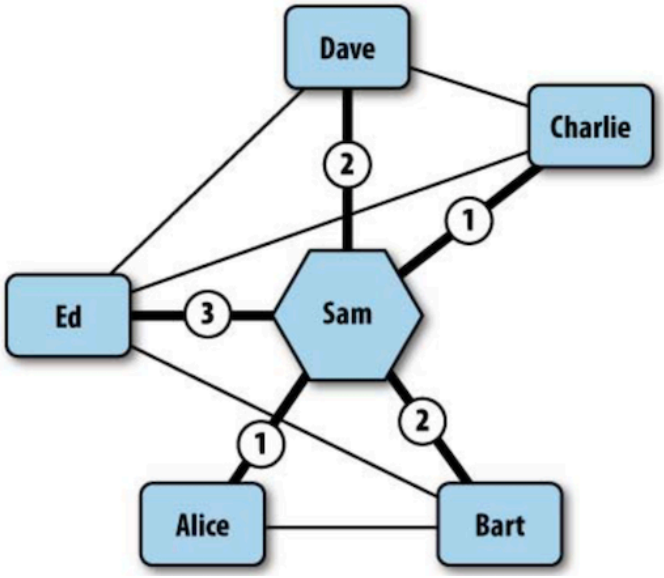
I code-signing certificates sono una delle merci più vendute nei forum della Darknet. Consentono infatti agli autori di malware e virus di firmare il codice affinché il loro malware possa evitare il rilevamento degli antivirus.
I certificati digitali consentono alle aziende e agli autenti di fidarsi del codice sorgente di un software e di verificarne l'integrità. I certificati sono rilasciati dalle autorità di certificazione (CA) e sono concessi alle aziende che producono codice, software o protocolli in modo che possano firmare il loro codice e indicarne la legittimità e l'originalità.
Le vendite di certificati sono aumentate considerevolmente negli ultimi anni da quando i ricercatori di IBM X-Force hanno fornito alcune linee guida per il controllo dei certificati digitali.
Quando un acquirente ordina un certificato, i criminali usano delle identità rubate ad aziende legittime per richiedere alle CA un certificato per un'app o per un sito web fake. I certificati vengono poi utilizzati per firmare il malware.

È consigliabile scaricare i software nei loro siti ufficiali così da avere la certezza che il software è autorizzato; Possiamo comunque fare una scansione del programma sul sito virs total che è un grande database aggiornato con tutti i virus e malware che sono conosciuti.

- IS (Information System): a network of digital hardware and software that people and organizations use to collect, filter, process, create, store and distribute data. Cyber threats to security are among the most serious for private and public critical IS, and stakeholders must enhance the cybersecurity and resilience of such IS
- Security vs Safety: security means keep information private, safety means keep information, people and physical assets safe. With IoT this distinction is more volatile (think to a connected car)
- CIA (Confidentiality, Integrity, Availability): the primary attributes to preserve of a IS
  - Confidentiality (or Security): keep information private, prevent disclosing it to unauthorised people
  - Integrity (or Safety): keep information safe, prevent corrupting it from unauthorised people
  - Availability: keep information or services available to legitimate users
- Hack: a smart, counterintuitive and elegant solution to a problem, a kind of shortcut with respect to the canonical way to solve a problem
- *Opportunistic* vs *Targeted* attacks: *Opportunistic* attacks are attacks in which an attacker has a general idea of what or whom he wants to attack. For example, an attacker going after a Fortune 500 company or HIPAA-compliant company. If the attacker comes across a vulnerability that can lead to exploitation, he will begin to pursue that company. *Targeted* attacks are attacks in which the attacker specifically chooses his target and does not give up until his target is compromised. These determined attackers are the most dangerous and technically advanced. Targeted

attackers choose to target their victims, which are preferably corporate executives (CEO, CFO, COO), because they are the most informed members of an organization, and frequently one of the least technical. An executive's devices, such as a BlackBerry or laptop, may contain information regarding IP, corporate goals and agendas, emails to and from board members, potential acquisitions.

- Mass Fishing vs Spear Fishing
- Network analysis is a good way to identify the circle of trust of a corporate executive. If any of victim's friends share a common friend, referred to as a *commonality*, the friend's line representing the influence to the victim is made thicker and the line is weighted with how many connections the friend shares with the victim. The greatest the weight the greatest the influence on the victim.



- Vulnerability: a weakness in a IS, including human behaviour, that when taken advantage of (exploited) will compromise the CIA (threat). Examples: file inclusion, buffer overflow, race condition, heap overflow, double free, integer overflow, SQL injection
- Exploit (as a noun, read expluá): a coding hack (script, worm or binary software) taking advantage of a vulnerability in a IS to force it to make an unintentional action (e.g. to gain system administrator's or root privileges)
- To exploit a program: to hack a program. Exploitation of a vulnerability: taking advantage of a vulnerability
- Threat modelling: procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent - or mitigate the effects of - threats to the IS
- Buffer Overflow: a vulnerability that bypasses input validation routines to write data into a buffer's adjacent memory. Sometimes that adjacent memory location may be critical to the operation of the targeted program and control of code execution can be obtained through careful manipulation of the overwritten memory data
- SQL injection (SQLi): the act of exploiting a SQL database by a malformed query that bypasses the input validation routines. For example, typing a special strings in the search input field of a web site, a user could get (or change) information pertaining to other users, or produce an undesired content to be rendered in the public web page. SQL injection is a code injection technique that might destroy the database. SQL injection is the placement of malicious code in SQL statements, via web page input. SQL injection is an instance of a more general class of vulnerabilities based on poor input validation and bad design that can occur whenever one programming or scripting language is embedded inside another
- Race condition: a class of error in multi-threaded or multi-tasking environments, where an operation is falsely assumed to be atomic while in fact it depends on a specific sequence of events. If the operation is executed concurrently by two processes, there is some risk the resulting computation not being correct. Altering the sequence of events

may lead to a vulnerability

- File Inclusion: vulnerability of web applications that use the content of a file. An attacker can force the site to include the contents of a file of their choosing
- Vulnerability scan: the act of identifying the signature for potential vulnerabilities by collecting target's data points like OS version, Patch Level, Processore Architecture, Software version, etc.
- Social Engineering: the art of obtaining information from people who don't want to give it
- Sentiment analysis: assessing the sentiment of a given person over time with the intention of abusing the target individual's privacy. This is achieved by tracking in social spaces (Twitter, Facebook, etc.) a word or sentence that expresses positive and negative sentiment. This information can allow the attacker to form social engineering situations. Targeted sentiment analysis may allow attackers in the near future to find out more about someone than that person knows about himself.
- OSINT (Open Source INTelligence): gathering of information regarding an individual from publicly available sources. An update review of OSINT tools is https://osintframework.com
- Malware: any software designed with malicious intent to disrupt normal function, gather sensitive information, access other connected systems when installed and running on a device. The victim must actively download and install the malware. The typical way to protect devices from malware is with antivirus software (AV)
- Worm: virus capable of infecting a device semiautonomously
- Payload: the block of executable code transferred by a malware (like a virus or worm) that is responsible of the harm. It will encrypt or delete your data, or send spam. A different section of code is aimed at the propagation of the virus. Different viruses can carry the same payload
- P2P (Peer-to-Peer): non hierarchical network model. It makes more difficult to identify the control node that initiated an attack
- RAT (Remote Access Trojan): malware that permits to get control of the victim computer remotely. Examples are Netwire, che ha colpito il settore bancario, o Adwind, che dal 2012 ha colpito 500000+ utenti
- Keylogger: come AgentTesla, è un malware capace di intercettare dalla tastiera password e documenti sensibili
- Ransomware: a malware aimed to ask a ransom to unlock resources. Examples are MBR Lock (2012) that locks the OS by replacing the Master Boot Record. Other examples are CTB Locker, TeslaCrypt, WannaCry (2017), GrandCrab (2018)
- Criptojacking: a malware aimed to mine cryptocurrency on PC and smartphone
- Browser Hijacking: a malware that overrides the default functionality of your web browser
- Botnet: network of computing nodes (called Bots, or Zombies) infected by a malware (like Mirai). A hacker, the Bot Herder ("pastore dei bots"), gets control over the bots to synchronize an attack (for example DDoS) against a victim. The malware (the client) forces each bot to connect to a IRC channel (the server) from which they will receive the commands (Command and Control/RAT) to be executed against the victim. The bot herder (attacker) is not directly connected to the victim, making it untraceable.
- Mirai: botnet malware designed to infect IoT devices. It was discovered by MalwareMustDie in 2016. Mirai, whose C source code is available on GitHub, is composed of a virus and a CnC. It scans the internet in search of nodes with active Telnet service, then tries a dictionary based attack. Once infected with the virus, the victim's IP and credentials are communicated to the CnC of the bot herder. No persistent storage is required because, unless the user creates new credentials after a reboot, the device will be reinfected immediately.
- 0-day vulnerability: "Day Zero" is the day on which the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Up until that day, the vulnerability is known as a zero-day vulnerability. Similarly, an exploitable bug that has been known for thirty days would be called a 30-day vulnerability. 0-day vulnerabilities are the most threatening because hackers can use them with maximal likelihood of success

- XSS (Cross Site Scripting) attack: as SQLi, XSS attacks result from improper sanitization of user input, allowing executing code in the context of user's browser session
- In 2017 99% of known malware hit Android e Windows
- La crescita del numero dei malware è esponenziale, anche perché sono entrati in azione tool automatici che generano nuovi malware a partire da quelli noti
- ATP (Advanced Persistent Threat): hacker organizations supported by a government institution. Examples are APT40 (aka Periscope), APT37 (aka Reaper), APT38
- Il kernel Linux è scritto in c e cpp, linguaggi non memory-safe, e in tal senso vulnerabili
- 2FA (Two Factor Authentication): besides the usual account information you have to input an OTP code to get the service
- Hacker: nel 1920 erano gli studenti che nei sotterranei del MIT smanettavano col sistema telefonico (hack = saldare). Dal 1950 i computer hacker modificavano i programmi su TX-0 e IBM 704 con sistemi non ortodossi per migliorarne l'efficienza
- Phone Phreak: someone who loves exploring the telephone system through experiment, specializes in obtaining unauthorized information about the phone system, uses a tool to call long distance without cost
- Software piracy: unauthorized copying and distribution of copyrighted software
- Black hat (aka cracker): an illegal hacker who violates computer security for maliciousness reasons, or for personal gain
- White hat (aka ethical hacker): a legal or ethical hacker that breaks security for non-malicious or illegal reasons
- Grey hat: a hacker that carries out illegal hacking, but not necessarily for their personal gain-often arguing it's for the greater good. Sometimes called hacktivism, it can still be punishable in the eyes of the law
- Hacktivist: an hacker mainly motivated by political reasons. Example: DCLeaks
- Pentesting: diagnostic testing that reveal security weaknesses and vulnerabilities of a IT system
- Pentesters: those who are authorized to perform security tests over a IT system
- Accedere abusivamente a un sistema IT protetto è un reato punito con reclusione fino a 3 anni. Un pentester deve avere un foglio di manleva che lo autorizza a testare la rete
- Gli analisti lavorano sui malware usando macchine virtuali e sandbox
- Website defacement: the act of breaking a website and changing the visual appearance of a website or a web page. Defacers are those who break into a web server and replace the hosted website with one of their own
- DRM (Digital Restriction Management): the science of protecting copyright on applications and digital media contents. DRM must block pirates, users who obtained the application illegally. The simplest (and perhaps oldest) form of DRM, of course, is separating software source code (read by humans), from their compiled binaries (read only by computers)
  Code Signing: a DRM mechanism to authenticate a binary, for being executed only on a specific device, or any other purposes
- Apple DRM policy is based on several means: App Store review process, code signing, sandbox, SIP
- The app runs in a sandbox at a low privilege level to reduce damage they can cause
- Apple introduced the app Code Signing with the App Store. A section of the Mach-O binary is encrypted. Apple or developers can sign applications using their private key.
- Apple developers can sign an app using the FairPlay protocol and provisioning profiles, time-limited files used by the developer and/or by the app
- A hash function is any function that maps data of arbitrary size (the pre image) to data of fixed size (image, hash, or digest).
- Una variazione di 1 bit del file di ingresso deve portare al cambiamento di almeno il 50% dei bit dell'hash
- Cryptographic hash functions. Una funzione di hashing per uso crittografico deve verificare tre condizioni:
- A hash function is *collision-resistant* if an adversary can't find any collision, i.e two different pre-images which result in the same image

- A hash function is *pre-image resistant* if, given an output (image), an adversary can't find any input (pre-image) which results in that output.
- A hash function is *second-pre-image resistant* if, given *one* pre-image, an adversary can't find any *other pre*-image which results in the same image.
- SHA-1 (Secure Hash Algorithm 1) è un esempio di hash function (160bit), introdotto nel 1995. A feb 2017 Google ha effettuato un collision attack, ottenendo una collisione per SHA-1. SHA-1 da deprecato passa a obsoleto. Adesso si preferisce usare SHA-256 (256bit) o SHA-3
- Git uses SHA-1
- Types of attack to hash: collision, pre-image, second pre-image
- Two types of digital signatures: hash-based and asymmetric-crypto-based signatures
- Digital signature: Data that proves that a document (or other piece of data) was not modified since being processed by a particular entity. Generally, what this really means is that anyone who has the right public key can demonstrate which private key was used to sign the data.
- Firma digitale di un documento: Il mittente e autore del documento calcola l'hash su tutto il file, p.es con SHA-2, e poi, con una crittografia asimmetrica, p.es RSA, cripta l'hash usando la sua chiave privata (firma digitale). Il ricevente rimuove la sezione del file contenente la firma digitale, calcola l'hash (sempre SHA-2), poi usa la chiave pubblica per decifrare la firma, e infine confronta i due hash. Se sono uguali allora il documento è autentico
- Talvolta si usa applicare la funzione di hash ricorsivamente più volte su se stesso, in maniera da renderlo più resistente ad attacchi brute-force
- Crittografia + hash: avendo un messaggio in chiaro, diciamo un sw, cifrarlo e basta non é il metodo più sicuro. Infatti, si potrebbe trovare un modo di modificare il messaggio cifrato in maniera tale che, una volta decifrato, il risultato è ancora valido, nel nostro esempio il sw può girare, con magari delle funzioni attive normalmente disabilitate. Infatti per abilitare una funzione anche complessa di un sw basta cambiare un bit. La soluzione è aggiungere al messaggio l'hash del messaggio stesso prima che il messaggio venga cifrato, e poi fare un semplice controllo sull'hash prima di eseguire il sw
- Usare un hash che ammette collisioni è insicuro
- Su sistemi Apple libdyld.dylib (dynamic loader) é la libreria di sistema che ha il compito di decriptare a runtime il programma firmato e caricarlo in una area di memoria controllata dove esso verrà eseguito
- La crittografia in questione è asimmetrica, basata sulla acquisizione e mantenimento del certificato Fairplay sul proprio dispositivo
- Su mac il sistema Gatekeeper filtra le app prima di eseguirle in base all'origine (solo AppStore, anche da developers, oppure qualsiasi). Su iOS il sistema non è bypassabile
- La firma, se non applicata da Apple stessa, deve essere applicata dallo sviluppatore mediante il provisioning profile
- Self modifying code: tecnica usata da molti malware
- Shell code: codice binario eseguibile che viene caricato in Ram a runtime. É uno dei sistemi adottati dai malware
- ROP: Return Oriented Programming, exploit che permette ad un attaccante di eseguire codice anche in presenza di difese. Siccome il sistema impedisce l'esecuzione di codice che venga caricato a runtime in aree di memoria diverse da quelle pre assegnate (ad esempio tramite code injection da parte di qualche sorgente esterna), si cerca di far eseguire al sistema dei comandi che sono già stati caricati in RAM
- DEP (Data Execution Prevention): misura di protezione anti-exploit
- ASLR (Address Space Layout Randomization): misura di protezione contro buffer overrun e exploit che consiste nel rendere (parzialmente) casuale l'indirizzo delle funzioni di libreria e delle aree di memoria. Molto utile contro ROP
- Il code signing marca le pagine di memoria dove il codice puó girare.
- architetture iphone: armv6, armv7, armv7s
- UPnP: universal Plug and Play. Alcune app domestiche devono poter essere accessibili da internet. La porta x del router domestico può essere dirottata verso un ip interno.

- La distribuzione di app al livello di enterprise può essere fatta mediante sito web
- Ogni app ha un URL associato. Una app può aprirne un'altra usando il suo URL
- Un account sviluppatore può installare app su 100 device differenti. Nel suo provisioning profile egli registra i device e poi da Xcode genera le app in formato .ipa da scaricare nei device, tramite iTunes o allegato email.
- AES (Advanced Encryption Standard) is a fast general-purpose block cipher standardised by NIST (the National Institute of Standards and Technology)
- AES-128 and AES-256 are examples of symmetric cryptography
- RSA: Asymmetric algorithm for encryption and digital signatures invented by Ron Rivest, Adi Shamir and Leonard Adleman, based on prime number factorisation. There are two prime numbers p1, p2 (private key) which give the co-prime p1*p2 (public key). RSA-4096, where p1 and p2 are 2048 bit numbers, is considered very secure
- DSA (Digital Signature Algorithm): digital signing based on discrete logarithm inverse
- ECDSA (Elliptic Curve DSA): digital signing based on elliptic curves. We start from a origin point on the curve defined in a p-field (p prime), multiply it by a scalar k (private key) to get another point on the curve (public key). It is able to provide the same security level as RSA with a smaller key and computationally cost. For this reason we use ECDSA for signing on mobile devices. ECDSA-256 is considered secure
- To create a new ssh-key you use the command *ssh-keygen -t <type> -b <size>*, where *<type>* is either of *dsa*, *rsa* and *ecdsa*, and *<size>* is the size in bits of the key
- PRNG: Pseudo Random Number Generator. The number will have the same appearance of a true random number, but it is built in a deterministic way
- CSPNRG: Cryptographically Secure PNRG
- keystream: sequenza di bit casuali generati da un PRNG e da una chiave, che vengono combinati in XOR con un messaggio per ottenere quello cifrato. È una crittografia che opera su un flusso di bit, non su blocchi di bit come AES
- RC2-4–5-6: famiglia di algoritmi di cifratura a flusso. RC4, introdotto nel 1974 alla base di TLS, SSL, WEP e WPA, è stato obsoletato perché violato
- OTP: One Time Pad
- Authentication: the process of verifying that someone or something is the actual entity that they claim to be. Authentication is what happens when you log into a system. It compares your credentials (often user name and password) with a previously established known value such that the system can know that you are who you say you are. For sensitive systems, there is a trend toward using two factor authentication (2FA) which essentially means that users must supply two different secrets, usually one is a password (something they know) and the other is a pin supplied via text (verifying something they have).
- PGP (Pretty Good Privacy): developed by Phil Zimmermann in 1991, owned by Symantec in 2010
- Backdoor: malicious code inserted into a program for the purposes of providing the author covert access to machines running the program
- Certificate: a data object that uniquely binds information about a person or some other legal entity to a public key. The binding is generally done using a digital signature from a trusted third party (a Certification Authority)
- A CA (Certificate Authority) is trusted on behalf of another CA, and so on up to a CA which is trusted by itself (root CA)
- TLS e HTTPS sono protocolli che si basano sulla robustezza della firma digitale (delle cosiddette CA, certificate authorities)
- SSL (Secure Socket Layer): a popular protocol for establishing secure channels over a reliable transport. This protocol has evolved into the TLS protocol, but the term SSL is often used to generically refer to both
- TLS (Transport Layer Security) is the successor to the SSL protocol. In addition to encrypting data over the wire, TLS authenticates a server with a certificate to prevent spoofing
- Fishing: it is the scam conducted via email, with which they try to get confidential information, like passwords
- Sniffing: putting the NIC in promiscuous mode for capturing all messages, regardless

they are sent to you or not

- Spoofing: it is the act of providing a false identity to a network client. It can be conducted at any one of the ISO/OSI layer
- ARP-spoofing: tecnica utilizzabile da un attaccante che prevede l'invio di messaggi ARP su una rete locale generalmente al fine di associare il proprio indirizzo MAC all'IP di un altro host (ad esempio il gateway predefinito) intercettando quindi tutto il traffico ad egli destinato
- ARP-poisoning: listening for ARP broadcast requests, and then responding with the attacker's MAC address. This creates a *race condition* between the valid host attempting to respond and the attacker. This method is inefficient and slow. A much simpler way is to just send out ARP replies to hosts he intends to poison. The victim's machine will update its ARP table.
- By ARP-poisoning two machines A and B on the network, any packet that originally was destined between A and B, and viceversa, will now go to the attacker (MITM). Tipically B is the local gateway, and the attacker awaits for A initiating a SSH session to capture the password exchange
- Cain&Abel: a tool to create and maintain a MITM by ARP-poisoning. A simple interface aids in correlating the captured passwords and sessions to their protocols. Only for Windows ? (ask to mao@oxi.com). A typical scenario is poisoning the victim station and the gateway on the same local network. The victim will initiate a SSH session with a remote peer..
- Media Access Control (MAC) address: unique identifier that is assigned to every network adapter on a network for routing purposes. Consists of two separate parts: the Organizationally Unique Identifier (OUI) and the Network Interface Controller (NIC). The OUI identifies the manufacturer of the network adapter, and the NIC provides a unique identifier for the individual network adapter produced by the manufacturer.

10.151.0.190	0023081587CD	Arcadyan Technology Corp...
10.151.0.2	0018B9E9CBAB	Cisco Systems
10.151.0.70	001EE5E3E1FA	Cisco-Linksys, LLC
10.151.0.75	0004963A8320	Extreme Networks
10.151.0.76	0004963A8310	Extreme Networks
10.151.0.63	001A734B4A78	Gemtek Technology Co., Ltd.
10.151.0.177	00226931F839	Hon Hai Precision Ind. Co., ...
10.151.0.96	001DD94350A0	Hon Hai Precision Ind.Co.,Lt...
10.151.0.13	0013E87E871F	Intel Corporate
10.151.0.42	00215C6D9E51	Intel Corporate

- Sniffing emails: SMTP is a clear-text protocol. This allows an attacker on a network segment to capture emails being sent on the wire. Consider the case where a legitimate user has associated with a wireless network at an airport and sends an email. An attacker who is also using the wireless Internet service at the airport can easily capture this email by using a tool such as mailsnarf:
  host $ mailsnarf
- Spoofing emails: the sender of the email is not authenticated by SMTP
- email backdoor: once the attacker has gained access to the victim's email account, she can plant a backdoor by turning on forwarding options, forwarding all the incoming mail to another attacker-controlled account. This forwarding feature is available on popular web mail accounts and allows the attacker access to the email account, even if the user decides to change his password in the future

- DNS cache snooping: knowing the victim's DNS server, the attacker can discover what DNS records the DNS server has cached. For instance, the attacker can know whether a specific URL (like www.monster.com) has been visited by the employees of an organization that uses dnscache.example.com as DNS server
  home $ dig @dnscache.example.com www.monster.com A +norecurse
  Note: norecurse option tells the server not to attempt to resolve the domain in the case he doesn't know its address (to avoid polluting the cache)
- CFI (Control Flow Integrity): used to prevent ROP like attacks, where chain of gadgets (chunck) of code. Prendiamo il sorgente di tutto il programma e genero il grafo diretto in fase di compilazione e creo dei controlli in forward edge e in backward edge (ritorno). Source e target sono i punti di partenza e di arrivo. CFI controlla che il programma salti sa un source a uno dei target validi per quel source. Purtroppo non sempre si ha tutto il sorgente, ma ci sono librerie, framework, ecc prese da terze parti e non protette da CFI. Un altro sistema è basato su firme. Posso saltare a tutte le funz che hanno una certa firma. Posso applicare il controllo anche in backward. Le prossime generazioni ARM includeranno registri dedicati per CFI backward edge, il return address verrà cifrato in forward e decifrato in backward. Purtroppo i compilatori JIT (come quello del Java) tipicamente non implementano CFI
- Data Only Attack: attraverso particolari dati si forza il programma
- Al livello di sicurezza, i browser sono il punto debole, in quanto devono erigere barriere contro vulnerabilità di vati media files, protocolli di rete, ecc
- Keylogging: sniffing, in hw o sw, dell'input da tastiera
- Steganografia: come veicolare un massaggio nascondendolo in un vettore, p.es un file di testo nascosto e criptato in un file audio o immagine
- Jammer: dispositivo disturbatore di tipo DoS di una rete wireless. Può essere He o Sw
- MITM (Man In The Middle): an attack that creates an alternative route that information should take so that the attacker can capture and alter the data being transmitted. Such attacks alter the way a packet traverses the network by changing the destination of the packet to an alternative location that the attacker controls. After the attacker captures the information, it is sent to the originally intended recipient. This way, the attacker can view and even modify the information that was being sent
- Here is how the attacker can use Hunt (from *http://packetstormsecurity.nl/ sniffers/ hunt/*) to hijack the established Telnet session from client 192.168.1.1 to server 10.0.0.1:
  host $ hunt -i eth0
  …
- MitMo (Man in the Mobile) ..MITB (Man In The Browser)
- Edward Snowden, ex spia NSA
- Fingerprinting: raccolta delle informazioni da uno specifico target
- Shodan, Censys: search engines for discovering vulnerable IoT devices, webcams, routers, servers, SCADA devices, etc. on the internet (https://shodan.io/, https://censys.io)
- Phishing site: to set up a website that looks like another website. The visitor will input her credentials distracted by the site's legitimate-looking logos and visual layout. Typically there is a small window of time (few hours) that phishers have to work with before their websites are discovered and shut down. Low amount of technical skill is required to put up a phishing site. To set up a website that looks like a legitimate website, go to the legitimate website and download the HTML and JavaScript code and the image files. Once you have these resources, you can simply upload them onto a web server. You will also need to set up a server-side script (e.g. php, JS) to capture the victim's submissions and email them to the phisher. A lot of ready-to-use phishing kits are available for every imaginable institution.
- Burp Proxy: local HTTP proxy tool. Can be used to inspect the actual HTTP POST the

browser sends to the web server (available at *http://portswigger.net/proxy/*)
- MobiFish: security software defending against phishing attacks on mobile web pages and apps. MobiFish solves the problem of identity masquerade by comparing the claimed identity extracted from the screenshot of a login interface (OCR) with the actual identity from the URL of a web page or remote server. If these two identities are different, MobiFish alerts the user
- Modding: modification of a product aimed to alter or disable restrictions to functions
- Modchip: small electronic device used to alter or disable restrictions like region coding, DRM, and copy protection of computers or entertainment devices for the purpose of using media intended for other markets, copied media, or unlicensed third-party (homebrew) software
- Proxy anonimizzante: uso di un device connesso terzo (p.es un device IoT) per iniziare un attacco
- Grinder: inspired to the biohacking movement, Grinders are an open community of individuals who implant a piece of hw (NFC, RFID,..) in their body in order to interact with external hw to extend human capabilities, like unlocking a door (see biohack.me, www.dangerousthings.com)

DoS

- DoS (Denial of Service): a massive number of requests saturating the service capability of the victim. Requests can be TCP (e.g. SYN Flooding, where lots of SYN packets will force the victim to reply with SYN ACK packets), UDP (e.g. UDP Flooding, where lots of UDP packets sent to random ports will force the victim to reply with ICMP Destination Unreachable message), or HTTP (HTTP Flooding, where lots of GET/POST will force the victim to process requests)
- DDoS (Distributed DoS): DoS attack that makes use of a botnet
- DRDoS (Reflected DDoS): the attacker sends a large number of requests to servers replacing his source address with the IP address of the victim. All response from all servers will be sent to the victim
- Ransom DDoS: DDoS threats with a ransom

SIP

- SIP (System Integrity Protection): also known as "rootless", it is a access control system where permissions change from user based to process based. SIP is intended to protect system resources integrity, also for the root user. It is a sandbox profile that any processes have to follow. The list of resources can be found in /System/Library/sandbox/rootless.configuration.
- SIP was introduced with OS X El Capitan and prevents potentially malicious software from modifying protected files and folders on your Mac. It also restricts the root user account and limits the actions that the root user can perform on protected parts of the Mac operating system. SIP grants protection of permissions of system files and directories; protection of processes against code injection, runtime attachment and DTrace; protection against unsigned kexts.
- To see which resources are protected use ls -Ol /. For example you can see that /System is a "restricted" folder. You can't change that folder even though using root privileges
- Before SIP, exploiting a system by executing code in kernel space did not add any substantial advantage over taking the root privileges. After SIP it makes sense
- To disable SIP you need to reboot the Mac in Recovery Mode (by holding down the Command+R keys at starts up). From the Utilities menu, select Terminal. Enter *csrutil disable* into the Terminal window and hit the *Return* key to disable SIP. Then Restart. Use *csrutil enable* command in Terminal to re-enable System Integrity Protection. SIP can be also easily disabled from kernel space
- Modificare binari di sistema, installare daemon in certe locazioni di memoria, ecc sono tutte azioni particolari che il kernel consente o meno a un processo sulla base di due fatti: chi ha firmato il processo, gli entitlements dichiarati per quel processo al momento di firmarlo. P.es accedere ai nostro contatto, ottenere la lista dei processi attivi, ecc sono tutti entitlements

RSA

- To use Digital Signalure
  A is going to send a document to B in such a way B is guaranteed that A is the true origin of the document, and that the document has not been altered
  Generiamo una coppia di chiavi crittografiche RSA (la pubblica e la privata) e firmiamo un documento. Il documento sarà poi inviato a un ente ricevente il quale potrà usare la firma per verificare che il documento non è stato modificato.
  1) A ha documento che deve essere trasferito a B. Sia esso mydoc.txt
  2) A crea la sua chiave privata RSA2048
  > openssl genrsa -F4 -out gabrieleprivate.key 2048
  3) A crea la sua chiave pubblica
  > openssl req -batch -new -x509 -key gabrieleprivate.key -out gabrielepublic.crt
  Questa chiave (gabrielepublic.crt) deve essere inviata a B
  4) Usando la chiave privata, A cread la firma digitale
  > openssl dgst -sha256 -sign gabrieleprivate.key -out mydoc.txt.sha256 mydoc.txt
  A trasmette a B sia il documento originale (mydoc.txt) che la firma digitale (mydoc.txt.sha256)
  5) Usando la chiave pubblica di A, B usa la firma digitale ricevuta per verificare l'integrità del documento ricevuto
  > openssl dgst -sha256 -verify <(openssl x509 -in gabrielepublic.crt -pubkey -noout) -signature mydoc.txt.sha256 mydoc.txt
  Verified OK
  Questa operazione garantisce anche l'autenticità del mittente, in quanto unico possessore della chiave private.
- Cifrare il documento
  1) Encrypt a file using triple DES in CBC mode using a prompted password
  > openssl des3 -salt -in mydoc.txt -out mydoc.des3
  2) Decrypt:
  > openssl des3 -d -salt -in mydoc.des3 -out mydoc.dec -k mypassword
  Oppure
  1) Encrypt a file then base64 encode it (so it can be sent via mail for example) using Blowfish in CBC mode:
  > openssl bf -a -salt -in mydoc.txt -out mydoc.bf
  2) Decrypt:
  > openssl bf -d -salt -a -in mydoc.bf -out mydoc.dec
- To install OpenSSL on Windows: https://tecadmin.net/install-openssl-on-windows/

Internet Protocols

- IRC (Internet Relay Chat): protocollo TCP/IP client-server di chat famoso negli anni 80

Google search operators

- <website> site:<item> search the item only inside that website
- filetype:<filetype>
- inurl:<item> search in the page's url
- intitle:<item> search in the page's title
- inanchor:<item>
- intext:<item> search in the body text
- ext:<item> match filetype
- cache:<item>
- @<item> search in blogs
- #<item> search hashtags
- monitor:<item>
- -<item> to exclude item
- *<item> to match any word
- "<item>" to search exact-match

- OR, AND logical operators
- (<item1>) <item2> to prioritise criteria
- #1..#2 to match any integer between #1 and #2
- $<#>. to match exact price
- <item1> AROUND(n) <item2> search for terms within n words of each other

Cryptocurrency

- Cryptowallet: è il portafoglio elettronico, una app sw o hw per eseguire transazioni con cripto-valute. Un wallet contiene una chiave privata. Se vogliamo essere pagati dobbiamo fornire la nostra chiave pubblica.
- Un Bitcoin è un hash generato da SHA-256 a partire da blocchi di 512 bit. L'hash, da 256 bit, deve avere almeno 18 bit a zero, il che ha una prob di 1/10^20. Il valore di un Bitcoin è passato da $20000 a $6000, e oggi richiede un costo di estrazione pari a $10000.

Darknet

- Darknet: rete sovrapposta (overlay network) a Internet ma non indicizzabile dai motori di ricerca (Clearnet) e quindi inaccessibile a Google. Pensata per salvaguardare la privacy. Esempi sono Tor, I2P, Freenet
- Deep Web: insieme delle Darknet attive. Vi si può accedere usando speciali sw e configurazioni anonimizzanti
- Tor: browser basato su Firefox che può essere usato per navigate come proxy sulla clearnet in modo anonimo e sicuro.
- Hidden Service: indirizzo di rete TOR con nome di dominio con suffisso .onion, in quanto basato su un routing "a cipolla"
- I2P (Invisible Internet Project): rete anonima P2P a prova di censura. Ogni utente connesso partecipa alle comunicazioni dell'intero network. Eepsite: indirizzo di rete I2P con nome di dominio con suffisso .i2p, basato su un routing "a aglio". Esempio: http://i2pwiki.i2p

Others

- GAN (Generative Antagonistic Network): tecnica in cui si usano due AI, una che genera un output falso e l'altra che deve discriminare tra input veri e falsi
- Face morphing: effetto che trasforma progressivamente una immagine in un'altra
- Deep Fake: video che subiscono modifiche sostanziali tramite algoritmi di Deep Learning
- Blue-boxing: devices allowing its user to receive long-distance calls free of charge to the caller. Blue-box worked to the subscriber line. Red-box worked with the public telephone
- TrustedBSD
- Evilmaid attacks. Rubber Ducky di Hak5
- http://goo.gl/Xb3hna
- In Italia vengono spesi 250 milioni di euro in intercettazioni
- Anonet: a secure F2F (Friend To Friend) social network. You can join Anonet only upon invitation of a member
- Jailbreak significa evasione, nel senso che il device evade dalla gabbia delle restrizioni imposte dal gestore dell'ecosistema
- Homebrew significa fatto in casa
- Wannacry è basato su EternalBlue, un exploit basato su un bug del protocollo SMB 1. EternalBlue era sfruttato da NSA ma nel 2016 la posse The Shadow Brokers lo ha trafugato e diffuso su Dark Web. Altri malware sono basati sullo stesso exploit, come il ransomware NotPetya e il trojan bancario Retefe
- Beneficial Hacking: the positive impact hackers have on technology
- PMK (Pairwise Master Key): chiave maestra in grado di generare chiavi provvisorie temporanee
- *Security by Antiquity*: where the cybersecurity is based on the antiquity of the system. For example the ICBM missile control system is 30 years old. Modern botnets could not run on such old computers.

- TOR (The Onion Router): the second generation of onion routing internet protocol, to allow anonymous communications over the internet.
- PII (Personally Identifiable Information): such as work and home phone numbers, work and home addresses, criminal history, Social Security numbers, and credit reports
- theHarvester: simple python script to gather emails, subdomains, hostsnames, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database (https://github.com/laramies/theHarvester)
  Example: to find email addresses belonging to example.com using Google
  host $ python theHarvester.py -d example.com -b google -l 1000
- Physical ATM skimming: the act of modifying a real ATM and placing a device such as a keypad or a card-reading slot on top of the ATM to capture and steal information from ATM cards.

Cybersecurity in IoT

- Secure Boot
- Trusted Firmware Updates
- Root of Trust

FDA recommendations to mitigate cybersecurity risks of Medical Devices

- Manufacturers should monitor, identify and address vulnerabilities and exploits during product life cycle
- FDA requires to be notified of device changes only under specific circumstances
- The this context the use of the word should means that something is suggested or recommended, but not required.
- Active voluntary participation in an ISAO is encouraged
- The guideline apply to MD, software that is a MD, including mobile applications
- Software as a MD (SaMD): a software which is not part of a hardware MD, whose intended use is a medical purpose
- Compensating Control: a safeguard or countermeasure external to the MD design. For example instructing users to remove the ability of unauthorized access to the device from the hospital network
- Controlled Risk: a risk of patient harm that is acceptable
- Uncontrolled Risk: a risk of patient harm that is not acceptable
- Cybersecurity Routine Updates and Patches: changes to a device intended to reduce one or more controlled risks. They are not considered a repair. Examples are software or firmware updates, hardware updates, changes to IFU, labelling, etc. These changes are not required to be notified to FDA
- Cybersecurity Signal: any information about a potential for, or confirmation of, a vulnerability or exploit that affects or could affects a MD
- Vulnerability: a weakness in a information system, including human behavior, that could be exploited by a threat
- Exploit: the concrete use of a vulnerability (accidental or voluntary) that could impact the safety or essential performance of a MD, or the use of a MD as a vector to compromise a connected device or system
- Threat: any circumstance or event with the potential to adversely impact a device, assets, individuals. For a MD the emphasis is on safety and essential performance
- Threat Modeling: the process of optimizing Network/Application/Internet security by identifying objectives, assessing vulnerabilities and to define countermeasurements to prevent, protect from, respond to and recover from threats, or mitigate their effects. According to NIST SP 800-30, for each vulnerability a risk must be rated as a combination of the likelihood of occurrence of a threat (low, medium, high) and the potential impact (low, medium, high)
- Harm: a physical injury or damage to the health of people, or damage to property or the environment
- Patient Harm: a physical injury or damage to the health of patience, including death. Loss of confidential or Protected Health Informations are not included

- Remediation: any action taken to reduce an uncontrolled a cybersecurity risk to an acceptable level
- Cybersecurity risk management programs address vulnerability that may permit the unauthorized access, use, modification, misuse or denial of use of information that is stored, accessed or transferred from a MD to elsewhere. Can be premarket or postmarket. It includes mechanisms to monitor third party software components for new vulnerabilities, as well as a threat modeling. For each vulnerability you can evaluate whether the risk is controlled/uncontrolled filling a matrix with combination of “exploitability” (High, Medium, Low) and “severity of patient harm” (Negligible, Minor, Serious, Critical, Catastrophic).

References

– Framework for improving critical infrastructure cybersecurity
– Cybersecurity for networked medical devices containing Off-the-Shelf (OTS) software