

A.A. 2021/2022

FONDAMENTI DI SICUREZZA E PRIVACY

FEDERICA PACI

FABS :)

NOTA

Questi appunti/sbardinatura/versione “discorsiva” delle slides sono per mia utilità personale, quindi pur avendole revisionate potrebbero essere ancora presenti typos, commenti/aggiunte personali (che anzi, lascio di proposito) e nel caso peggiore qualche inesattezza!

Comunque spero siano utili!  

NOTA: queste sbobine, almeno all’anno accademico corrente, sono completamente inutili ai fini dell’esame dato che la professoressa fa solo domande inerenti al progetto. Sono comunque una lettura interessante, ma dato il punto appena espresso non ho speso troppissimo tempo a sistemarle.

**Questo file fa parte della mia collezione di sbobinature,
che è disponibile (e modificabile!) insieme ad altre in questa repo:
<https://github.com/fabfabretti/sboninamento-seriale-uniVR>**

Indice

1.1 - Introduzione alla cyber security	3
1.2 Attori cyber threat	3
2 - Covid attacks	4
3 - Classificazione degli attacchi	9
4 - Social engineering attacks	13
5 - Cyber war e attacchi alle infrastrutture	14
6 - Malware	18
7 - Autenticazione e attacchi password	23
8 -Gestione identità e accesso	26
9 - Access control.....	28
S10 - Seminario Sababa	38
11 - Introduzione alla privacy.....	39
12 - Metodologia LINDDUN.....	44
13 - Data anonymisation	47
S14 - Seminario DLP	54
15 - Risk management	57

1.1 - Introduzione alla cyber security

Definizione

La funzione principale della cyber security è proteggere i device che usiamo e i servizi a cui accediamo da accessi non autorizzati, danni o misuso. Consiste anche nell'impedire accessi non autorizzati alle nostre informazioni personali, memorizzate nei device e online.

Elementi

- Confidenzialità
- Integrità
- Disponibilità
- Autenticità
- Accountability
- Safety

Concetti chiave

Assets	Qualunque cosa che ha valore per l'organizzazione. Per esempio, organizzazioni, persone, computing devices, softwares...
Vulnerabilità	Bug o difetto che potrebbe portare al fallimento della confidenzialità, integrità o disponibilità.
Cyber threat	Qualunque circostanza o evento con il potenziale di impattare negativamente operazioni organizzative o assets
Attacco	Realizzazione di qualche threat specifica che impatta la confidenzialità, integrità, accountability o disponibilità di una risorsa.
Threat actor / attacker	Persona che sfrutta una vulnerabilità di sistema.
Rischio	Livello di impatto sulle operazioni organizzative, sugli assets, etc. in funzione della probabilità che accada.
Security controls / safeguards / countermeasures	La gestione di un sistema necessaria a prevenire attacchi.

1.2 Attori cyber threat

Chi sta dietro i cyber attacks?

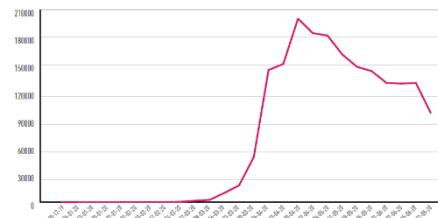
				
	Cybercriminali	Nation State	Hacktivists	Insider threat
Interesse	Profitto (illegale)	Intelligence Sabotaggio Sovversione (es. elezioni)	Portare avanti idee, orgoglio, divertimento	> Intenzionale: - Pubblicare info - Installare bombe logiche - Vendere info
Attacchi tipici	> Malware > Ransomware > Data breach > DDoS	> Malware > Data breach > DDoS	> web defacement > Data leak > DDoS	> Non intenzionale - Per sbaglio pubblica cose o cade in phishing
Vettori	> Malware > Emails > Internet	> Malware avanzati e offuscati con 0-day	> Exploit kit > Email > Botnet	

2 - Covid attacks

La situazione della pandemia ha portato ad un aumento degli attacchi.

Ci sono state 4 macrocategorie di attacchi:

- Phishing sfruttando cose sulla pandemia
- Ransomware
- Domini malevoli con la parola covid/coronavirus
- Fake news



Tutto questo fino alla prima parte della pandemia; da ottobre in poi, con i primi vaccini, hanno aggiunto un nuovo tipo di attacco, attaccando università e ospedali cinvoti nella ricerca sui vaccini, spesso provenienti da Corea Nord o Russia –

- es. gruppo russo Stronzi per ottenere accesso utilizzava attacchi di tipo bruteforce.
- Gruppi coreani usavano tecniche di phishing con motivi diversi; un gruppo faceva l'OMS e l'altro offerte di lavoro.

Phishing

La caratteristica comune è di **impersonare qualcuno di autorevole e dare urgenza su un'azione pericolosa** (dare info, aprire link/allegati)

Guardando più nel dettaglio le campagne di phishing con installazione di un malware, i più diffusi sono

- **Emotet:**
In giro da un bel po' di tempo, dal 2014, come malware per rubare credenziali di accesso alle banche. Poi si è evoluto ed è diventato un loader di altri malware.
Sfruttavano un allegro che conteneva le macro – le macro di default sono disabilitate; per essere eseguite bisogna indurre la vittima ad abilitarle. Una tecnica usata (per poi far installare emotet) si creava un messaggio che diceva che l'allegato era protetto e bisognava abilitare le macro per vedere il contenuto, oppure si faceva credere alle vittime che abilitare le macro non fosse dannoso.
Emotet è stato super diffuso quest'anno. Principalmente è stato utilizzato per installare altri malware, e a gennaio 2021 è stato oggetto di una **campagna coordinata di varie forze dell'ordine** internazionali per prendere controllo dell'infrastruttura botnet messa in piedi da attaccanti. Infatti Emotet nasce come malware che accedeva a conti online, ma poi ha preso un modello "malware as a service" – dava un'infrastruttura di server per deliberare malware su macchine infette da affittare. A gennaio, con l'azione coordinata, ha portato a prendere controllo di una buona parte dei server e ha reindirizzato tutte le macchine infettate verso server delle forze dell'ordine, dai quali sono stati inviati comandi per cancellare Emotet. Dato che da gennaio non va più, ora Trickbot cerca di prenderne il posto.
 - **Trickbot:** Uno dei malware più associato a emotet è trickbot, di natura modulare con funzioni precise; personalizzando i moduli si possono creare attacchi molto mirati. È stato utilizzato per installare ransomware e può fare lateral movement (propagarsi) o rubare informazioni sensibili.
- Tutta italiana: installazione di un ransomware (unicorn? Unico ransomware italiano!)
Veniva propagato tramite phishing, spacciandosi per Immuni. 🌟
- L'ultima tendenza di quest'anno è quella di installare **Cobalt Strike**, un software diventato famoso con l'attacco spiegato settimana scorsa. È un **tool a pagamento per fare penetration testing**; ha diverse funzionalità, come ad esempio bruteforcing, lateral movement sfruttando il protocollo samba di windows, scaricare altri malware o infine fare keylogging. È commerciale

ma si trovano facilmente versioni craccate in vendita sul mercato nero; ci aspettiamo che in questi anni questo tool sarà installato spesso.

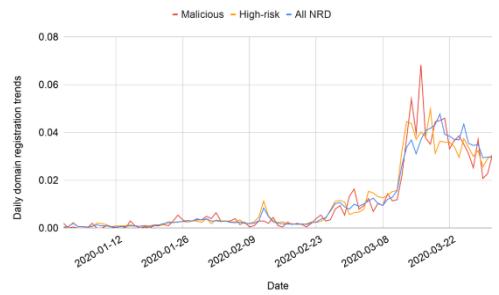
Esempi IRL

- Germania:
 - A livello internazionale c'è stata una massiva campagna di phishing per un'azienda che produceva dispositivi di protezione; è andata a mirare persone di alto profilo in questa azienda per rubarne le credenziali. Ottenute le credenziali potevano utilizzarle per avere info sulla distribuzione. (germania)
- Italia:
 - All'inizio si sfruttava la **crisi economica** delle aziende, esempio (siete stati licenziati bye! Nelle mail era presente un allegato che richiedeva le credenziali aziendali).
 - Non sono mancate nemmeno le campagne a basso profilo culturale, tipo le **frodi nigeriane**
 - Altre mail sfruttavano la **fonte autorevole**, OMS, e l'urgenza di un focolaio vicino per indurre le vittime ad aprire allegati.
 - Con la ripresa dell'economia sono circolate email impersonando il **ministero** dell'economia, oppure **finti aggiornamenti** di Immuni

Registrazione di domini malevoli

+700%, con tema covid! 40'000 dei domini registrati in marzo 2020 erano malevoli, con vari possibili fini:

- O perché utilizzati per siti phishing
- O per distribuire malware
- O per condurre frodi di varia natura



Esempi IRL

- Copia di **bank of America**
- Sito molto credibile sulla **vendita di mascherine**; con tanto di certificato del sito; però quando ordinavano le mascherine pagavano ma non ricevevano nulla :')

Fake news

Non è un attacco cos' dannoso (??? Profe ma che cazzo dice no offence). Hanno contribuito a piegare l'opinione pubblica e il senso di paura, aumentando il successo e la diffusione delle campagne di phishing e dell'installazione di malware.

Malware (ransomware)

La categoria più diffusa è stata quella dei ransomware, con +90%. Cercano file specifici, **cifrano** e **chiedono soldi in cambio della chiave di cifratura** – solitamente da pagare in criptovaluta. Con pure le evoluzioni:

- **Double extorsion**: siccome questo modello non era sufficiente, l'anno scorso un gruppo detto **Maze** ha introdotto **l'estorsione doppia** → copiare una parte dei dati delle vittime e salvarli su un server sotto il loro controllo. Se l'organizzazione non paga il riscatto si minaccia di rendere tutto pubblico (incluse IP e info dei clienti).
- **Triple extorsion** → si chiede il riscatto non solo all'azienda ma anche a dipendenti e clienti; il primo caso è stato un attacco ransomware contro una ditta finlandese che offriva servizi di consulenza psicologica. La ditta manteneva una copia di tutte le sedute fatte dai pazienti, e succede che quando la ditta è stata colpita alcuni dei pazienti hanno ricevuto email in cui si minacciava che se non avessero pagato 200\$ di riscatto avrebbero reso pubblici i transcript delle terapie.

Esempi IRL

- In quest'anno questa è stata usata anche contro grandi colossi tipo **apple**; ad aprile c'è stato un attacco organizzato da **REvil** che ha colpito quantacomputer, azienda tiwanese che produce dispositivi per hewlett packard, apple e altri. REvil ha chiesto un riscatto di qualche milione a Quanta; quando Quanta non ha pagato si è rivolta a apple (dato che c'erano anche documenti della apple). REvil ha pubblicato parte dei progetti su siti pubblici, ma poi sono stati rimossi (ergo si pensa che apple abbia deciso di pagare).
- **Colonial pipeline attack**: maggio di quest'anno, ha colpito uno dei maggiori distributori maggiori americani. L'attacco ha reso inagibili tutti i sistemi di distribuzione del carburante in europa, e ha bloccato per più di una settimana la distribuzione in america (con il prezzo che si è alzato!!), e c'è stato un messaggio da Colonial Pipeline che invitava a evitare di acquistare tutti il carburante per non alzare il prezzo → un attacco ransomware ha colpito una infrastruttura basilare, e ha avuto impatto pure sui privati.
- Altra caratteristica recente è quella di avere tecniche di evasione molto sofisticate. È stata usata nell'attacco contro Garmin, che è uno dei maggiori produttori di smart watch e geolocalizzazione. L'attacco è stato **altamente mirato**, perché il ransomware aveva addirittura un'estensione dedicata ".garminwasted". L'effetto è stato importante in quanto il servizio clienti non era più disponibile, tutte le applicazioni non funzionavano, addirittura la localizzazione degli aerei ha smesso di funzionare.
 - Oltre all'essere mirato a Garmin, è particolare la tecnica di evasione: una delle cose che monitorano i sistemi anti malware sono le windows API richiamate. I malware richiamano, solitamente, apertura lettura e cifratura. Monitorando queste API, l'antivirus può catturare le operazioni mentre si svolgono e identificare l'operazione. Questo ransomware usa una feature presente su tutte le macchine windows, il **windows cache manager**, usato per caricare le app più usate. Il ransomware, invece di cifrare il file su disco, prendeva i file voluti, li caricava nella cache e li cifrava lì; dopo aver cifrato un certo numero di file li riscaricava su disco → non veniva identificato dagli antimalware!!

Criptominers

Sono malware che infettano il device e usano le sue capacità computazionali per minare.

- **Kubernetes** è un nuovo modo di virtualizzare deployment di applicazioni, condividendo il SO in un container. Successivamente che sfruttando delle vulnerabilità di Kubernetes sono riusciti a deployare nei vari container un criptominer.
- **Botnet prometeus**: viene utilizzato per condurre attacchi distribuiti (trasforma i device infettati in zombie sotto il controllo dell'attaccante) e fu veicolo per installazione di XMRig, un software di base benevolo e open source spesso usato con altri malware per essere installato e fare mining.

Malware android

- **FluBot**: è un malware android che passava per SMS e ha colpito per lo più vittime europee e UKs. L'SMS che arrivava appariva venire da trasportatori tipo fedex/DHL e annunciava una consegna per la vittima; per accedere a queste info veniva installata una finta app DHL, e quando l'utente concedeva i permessi per accedere al telefono veniva installato FluBot con accesso a tutte le info – cercava in particolare carte di credito.

Attacchi IoT

Ormai i sistemi IoT sono sempre più comuni in ogni elettrodomestico, ma anche in sistemi critici come il controllo industriale o il monitoraggio del traffico.

Il problema è che sono anche **altamente vulnerabili**:

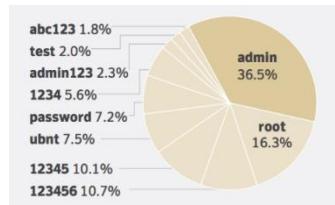
- **Comunicazione dei dati**
→ tipicamente un dispositivo IoT comunica i dati raccolti dall'ambiente a un'applicazione sullo smartphone – es. smartwatch o alexa – oppure nei casi industriali fra dispositivi e applicazioni web in cloud. Purtroppo il traffico spesso non è cifrato, ed eventualmente se i dati sono personali o legati alle abitudini o alla salute diventa un problema di integrità (no controllo) e privacy.
- **Usano meccanismi di autenticazione deboli, basati su password**
→ è molto facile indovinare la password perché spesso sono utilizzate password settate dai distributori, che non vengono mai cambiate dai consumatori. Spesso, per la stessa tipologia di dispositivo IoT, la password è sempre uguale! Quindi se un attaccante ha un dispositivo poi ha la password di tutti :O
- **Molti dei dispositivi, soprattutto su monitoraggio industriale, usano OS non più supportati**
→ tipo W7 o WXP! E anche il processo di aggiornamenti può essere complicato! Ad esempio, in ambito medico (monitoraggio paziente o diagnostica); non sono aggiornate perché bisognerebbe prelevarli dal loro ambiente e riportarli dal venditore... casino per sistemi che avrebbero impatto sulla produttività.....
- **Basse capacità computazionali e di memorizzazione; inoltre hanno una scarsa durata di batterie** → Quindi diventa difficile implementare meccanismi di controllo, autenticazione...

Esempi IRL:

- Solo quest'anno è stata scoperta **BadAlloc**, una vulnerabilità su milioni di dispositivi. I dispositivi con queste vulnerabilità eseguono software embedded implementando C. Il C è noto per avere numerose vulnerabilità sulla gestione della memoria → bufferoverflow!
Qui il problema è nelle librerie usate per allocare dinamicamente la memoria, nella heap. Quello che succede è che se si utilizza roba tipo la malloc, la malloc ha come parametro un numero intero che definisce la memoria da allocare e restituisce il puntatore. Se passo un numero che causa un integeroverflow (troppo grande o negativo), un attaccante può sovrascrivere l'area allocata e eseguire del codice malevolo. Non ci sono attacchi noti che si sa abbiano sfruttato questa vulnerabilità, però è stato consigliato di patchare ove possibile la vulnerabilità o non esporre i dispositivi su internet.
- **Ripple20**: scoperta l'anno scorso; è presente in una libreria prodotta da una piccola azienda americana negli anni 90 e che è usata nello stack TCP/IP; sono 19 vulnerabilità di cui 4 con score molto alto; alcune permettono di accedere a informazioni sensibili oppure di eseguire codice remoto. La complessità del capire se un dispositivo è soggetto è data dal fatto che questa libreria è spesso usata in __altri__ pacchetti, e gli stessi rivenditori non sanno che nel loro software è presente questa libreria!
- Ci sono poi **attacchi specifici per dispositivo**; per esempio sui **vocal assistant**, c'è stata una ricerca condotta da uni USA e Taiwan che hanno codificato dei comandi comuni usando gli ultrasuoni – non udibili al nostro orecchio, ma che vengono captati e l'OS assistant risponde. Si riesce quindi ad accedere a informazioni. Hanno fatto un test anche su google home, echo e alexa ma non ha successo
- **Baby monitor**: le vulnerabilità sono dovute al fatto che o non c'è autenticazione oppure è basato su password. Ci sono stati 2 casi noti in UK
 - Bambina in cui l'attaccante è riuscito a comunicare con la bambina e si è spacciato per babbo natale
 - Coppia di anziani con telecamere di sorveglianza; si è scoperto che 5'000 persone sono riuscite a spiarli e monitorarli. Ua. Ed è una puttanata, basa user Shodan (ricerca di

dispositivi connessi a internet); con shodan si sceglie che dispositivo attaccare e compare la lista con un sacco di info!

- **Mirai:** È diventato famoso perché, quando infettava dispositivi IoT come le telecamere, le trasformava in pot che inviava comandi per generare un elevato volume di traffic verso target specifici. Un esempio fu il DNS di Tim, che gestiva numerosi siti usati comunemente tipo Netflix. E' stato un first, poi usato. La vulnerabilità usata per installare Mirai era il fatto che fossero protetti da password. **TE LO MERITI SE SETTI PASSWORD COSÌ (cit la profe)**
- **Dispositivi in ambito medico:** è uno dei più vulnerabili. Per esempio, i sistemi più colpiti sono quelli di diagnostica per le immagini (ecografia, radiografia) e l'anno scorso c'è stata una serie di vulnerabilità:
 - Un modello di pompa per i pazienti diabetici è stato ritirato dal commercio perché consentiva di modificare i dati :O
 - Dispositivi usati per fare radioterapia; **CHE NON CRITTANO UN CAZZO AAAAA**
 - Monitoraggio dei pazienti: cose per la demenza senile; strumenti di promemoria utili per prendere medicine o percorso per casa. Nell'applicazione che gestiva il trattamento del paziente. Ma non essendoci alcun controllo...



Cloud attacks

Misconfiguration

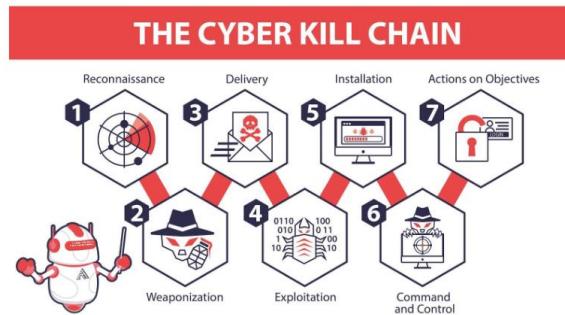
- **Amazon S3:** è uno dei servizi di amazon per memorizzare dati. Configurare correttamente l'accesso ai bucket è un bagno di sangue. **BAGNO DI SANGUEEEHEHE (cit la profe)**
 - È facile lasciare i dati nel cloud pubblici per sbaglio; un'azienda di ricerca ha scoperto che alla fine dell'anno scorso ha analizzato tanti bucket e scoperto che uno dei bucket era stato lasciato completamente pubblico e non cifrato. Dentro c'erano dati di un'azienda, come dipendenti, password di amministratore, SSN,
 - Azienda di prestiti per studenti; il bucket pubblico conteneva le registrazioni di tutte le telefonate degli studenti e copie dei documenti forniti per l'applicazione, come CDI o simile.
- **Powerapps:** permette di sviluppare facilmente applicazioni web (è di microsoft), supportando front e back end. Succedeva che essa fornisce API con cui accedere i dati; alcuni ricercatori si sono accorti che quando i clienti usavano questo portale, i dati diventavano pubblici ed era possibile modificare i privacy settings dei dati solo manualmente (che ovviamente, non sapevano nessuno, erano lasciati pubblici). Ci sono stati anche clienti noti per il tracciamento dei contagi, tipo la Ford, Microsoft stessa (**LOL**), applicazioni di lavoro.

Problemi di infrastruttura o di software per gestirla

- **Server:** l'anno scorso telecom francese ha subito un ransomware perché i server avevano una versione vulnerabile del software. Finito tutto bene perché Bretagne Telecom aveva dei backup :')
- **Software:** microsoft azure ha scoperto 2 vulnerabilità
 - Azure stack, che è un software per industriale per gestire l'infrastruttura. Nel data service... non prevedevano autenticazione; bastava fare un'HTTP request e accedere ai dati di organizzazioni così, liberamente.
 - Azure ??? aveva una vulnerabilità buffer overflow per eseguire cose.

3 - Classificazione degli attacchi

Cyber Kill Chain



È una sequenza di fasi in cui può essere separato un attacco informatico. Ha 7 fasi:

Reconnaissance	<p>Consiste nello scegliere un obiettivo per raccogliervi più info possibili. Può essere proprio l'obiettivo primario o anche un secondario (es. attacco un fornitore per attaccare apple).</p> <ul style="list-style-type: none"> Passiva: raccolta di informazioni in modo passivo, senza interazione, come whois (es: leggo il proprietario su whois e faccio attacco di phishing chiedendo di rinnovare il dominio vicino alla scadenza), Shodan, Google, social media, mantego... Attiva: interazione con gli host per avere info. Tool utile: <ul style="list-style-type: none"> nmap, che permette di mappare tutta la rete dell'obiettivo, dando anche info sui singoli host (tipo il SO, analizzando il traffico di rete restituito).. Port scanning, vulnerability scanning.
Weaponization	<p>Creo il codice malevolo fatto per sfruttare la debolezza individuata.</p> <p>Tools:</p> <ul style="list-style-type: none"> Social Engineering Toolkit: copiare sito legittimo, email di phishing con pdf malevolo, chiavette infette... Metasploit: ha un vasto database di codice già fatto per sfruttare diverse vulnerabilità (es. per adobe/office/OS..) Cobalt Strike Cain e abele Aircrack ...
Delivery	Come deliverare attacchi ? Social engineering, chiavette infette lasciate in giro, phishing email...
Exploitation	Sfruttiamo effettivamente la vulnerabilità : user exploitation, javascript hijacking, malware, SQL injection, buffer overflow...
Installazione	L'attaccante vuole mantenere l'accesso ottenuto sulla macchina. <ul style="list-style-type: none"> Chiavi di registro: Uno dei modi più comuni è quello di modificare i registri; ad esempio, aggiungendo il proprio programma a quelli da autoavviare. Macro da eseguire che esegue dei comandi su powershell. DLL hijacking: c'è un percorso da cui vari programmi prendono delle librerie; se un attaccante riesce ad incollare il suo dll malevolo può fare eseguire quello.
Canale command and	Tipicamente è un server sotto i controllo degli attaccanti . Questo può essere fatto per:

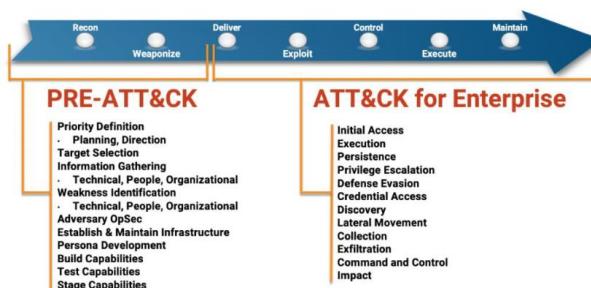
control server (C2)	<ul style="list-style-type: none"> Eseguire un comportamento diverso in base all'attaccante Ransomware: prima vogliamo copiare e salvare parte dei dati Mantenere controllo di uno dei dispositivi <p>Si può fare sia via http che cloud servers. Esistono anche tecniche di evasione per non far sgamare il traffico anomalo.</p>
Action and objectives	<p>Azioni vere e proprie.</p> <ul style="list-style-type: none"> Prendere credenziali Aumentare i propri privilegi Lateral movement Far parte dell'armata per fare DDOS

MITRE PRE-ATT&CK e ATT&CK

La roba vista sopra:

- Non descrive bene cose più complesse, tipo attacchi multi stage
- È ad alto livello

Dunque arriva **MITRE**, un'associazione no profit americana che ha creato una sepcie di wikipedia degli attacchi recenti. (ma non sa gestire una query sul testo dal loro sito. Vaaaabeh).



- Pre-attack:** weaponization, creazione del codice malevolo
- Attack for enterprise:** da delivery a action

Descrivono matrici di attacco di ciascuna piattaforma.

Ci sono differenze fra PRE e Enterprise → PRE non sono contro un obiettivo specifico, dunque non dice per quale piattaforma è adottata. Enterprise sì.

Matrice enterprise: sono 17 gruppi di tecniche (totaledi 226 tipo). **Qualche esempio:**

- Initial access:
 - Phishing:** <https://attack.mitre.org/techniques/T1566/>
3 modi di implementarlo: link nell'email, clonare servizio legittimo, allegato infetto.
 - Chiavette usb:** <https://attack.mitre.org/techniques/T1091/>
 - Supply chain:** Compromettere prima un software fornito da terze parti per colpire il primo obiettivo: <https://attack.mitre.org/techniques/T1195/>
 - Ottenimento di account validi: <https://attack.mitre.org/techniques/T1078/>
- Esecuzione:
 - Scripts presenti su Windows: <https://attack.mitre.org/techniques/T1059/>
powershell, macro in visual basic che eseguono powershell.
 - Vulnerabilità client tipo buffer overflow
 - <https://attack.mitre.org/techniques/T1053>
- Mantenere il controllo sulla macchina:

- Autostart (solo windows) <https://attack.mitre.org/techniques/T1547>
- Privilege escalation: arrivare ad avere i poteri dell'admin. Tecniche simili a quelle per la persistenza.
 - Creazione di chiavi di registro, creare servizi di windows,
 - Process shadowing: crea un processo legittimo, lo sospende e poi copia codice malevolo nello spazio di quel processo; poi riprende l'esecuzione.
- Evasione
 - Codifica delle stringhe e dei comandi ricevuti da C2 utilizzando codice in base64 o cifrato, tipo la cifratura XOR.
 - Nascondere cartelle e file (es. per non far trovare le copie di se stessi).
- Accesso alle credenziali
 - Vulnerabilità in password managers, tipo keypass :')
 - Keyloggers
 - ...
- Infezione di altri host
 - Network sniffing con wireshark!
- Lateral movement
 - Raccolta info su altre persone nell'organizzazione; prima becco un pesce piccolo e poi posso passare ai capi.
 - Thread hijacking: ottenute le credenziali del dipendente guardano l'ultima email ricevuta o inviata; se la copiano sul C2, generano una reply finta e la rimandano alla vittima – che magari esegue l'azione.
- Collection
 - ...
- Command and control
 - Protocolli web tipo http e https
 - Protocolli tipo FTP
 - Domain generation algorithm
 - Crittografia
 - ...
- Exfiltration: come rubare i dati
 - Di solito tramite C2
 - Servizi standard tipo cloud, chiavette usb, github.

Esempio: Trickbot

È vecio. Tipicamente arriva via documento che ha dentro una macro che scarica trickbot.

Trickbot ha una struttura modulare; ciascuna istanza aveva una configurazione diversa dei moduli in base all'obiettivo da raggiungere; ad esempio

- Lateral movement via problemi col protocollo Samba
- Rubare credenziali
- Installare altri malware tipo Emotet o ransomware.

KillChain



MITRE ATT&CK

Secondo il MITRE, le tecniche usate sono tutte queste:



4 - Social engineering attacks

Sono attacchi mega diffusi da più di 40 anni 😊

La pubblicità è ingegneria sociale. **I FIGLI SONO INGEGNERIA SOCIALEEEE TI MANIPOLANO PER AVERE QUELLO CHE VOGLIONO CIT LA PROFE**

L'ingegneria sociale è una manipolazione psicologica delle vittime che le porta a svolgere azioni che normalmente non compierebbero (e sono tendenzialmente fuori dal loro interesse). Infatti, nella cybersecurity, l'umano è considerato la parte più debole.

Kevin Mitnick dice: "A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent in technology is essentially wasted".

Solitamente, ad attaccare in questo modo sono:

Hackers	Ladri di identità	Scam artists
Tecniche adottate per installare malware, ransomware, credenziali finanziarie... <ul style="list-style-type: none">○ Wannacry : tre anni fa ci fu un'enorme guaio per la banca bangladesina, che sfruttarono email di fishing per accedere al sistema swift usato per trasferire denaro all'estero. Qualsiasi banca che fa trasferimenti all'estero deve avere un conto corrente presso la NY Federal Bank; si salvarono parte dei soldi grazie a un tipo nel nome del destinatario	Mirano ad accedere alle info personali delle vittime e usano queste per impersonarle oppure da mettere in vendita. <ul style="list-style-type: none">○ Via ingegneria sociale accedono al suo account gmail e hanno spammato la gente con email su perché non votarlo	Sfruttano dei pretesti per truffe tipo lotterie, romance, etc al fine di far pagare. <ul style="list-style-type: none">○ Arrivava l'assegno (scoperto) via posta, ma per riceverlo ci vuole il contrassegno da 40 dollari.

Hanno 4 fasi:

- **Information gathering:** è come la reconnaissance edlla cyebr kill chain.
 - *Shoulder surfing*: l'attaccante è in prossimità della vittima e sbircia sul suo pc.
 - *Dumpster diving*: frugare nella spazzatura.
- **Stabilire fiducia con la vittima:** impersonare il capo, sfruttare le reti sociali...
- **Exploitation:** si sfruttasi alavero raccolto info specifiche sulla vittima che la fiducia per portare la vittima a compiere l'azione richiesta.
- **Esecuzione:** l'attaccante raggiunge l'obiettivo (es. installare l'hardware)

Attacchi di phishing

Ce ne sono tanti tipi:

- **Phishing** : Spear phishing → miriamo a un oggetto preciso
Esempio: mail da parte dell'"agenzia delle entrate"; di solito su punta sull'impersonarsi o sul fatto di dover agire in poco tempo.
- **Whaling** : mirano a persone con elevate responsabilità, tipo ceos
- **Viral hoax** : mirano a divulgare informazioni false
Condotto soprattutto tramite reti sociali. Sfrutta la curiosità dellaggente.
- **Vishing** : attacchi di phishing condotti tramite telefono
Esempio: una serie di utenti in USA ha ricevuto un audio che si spacciava per apple e chiedeva di ricontattarli.
- **Impersonation** : Si sfrutta il fatto che la mail arriva da qualcuno di cui mi fito o che ha autorità
Una dipendente riceve ua telefonata dal manager per pagare fornitori.

- **Tailgating** : di persona

Sfruttail fatto che abbiamo l'indole di aiutare il prossimo. Ci si finge di non avere card e ci si accoda a un dipendente vero, che per gentilezza lascia fare.

- **SMSiShing**

Un attacco di phishing è un tentativo di acquisire informazioni sensibili attraverso il fingersi un'entità di fiducia in un a comunicazione digitale.

Efficacia

88% of organizations around the world experienced spear phishing attempts in 2019

95% of all attacks on enterprise networks are the result of successful spear phishing

30% of the emails are opened by the target victims

12% clicked on the link in the email or open the attachment

15% of victims are target at least one more time within the same year

97% of users cannot identify a sophisticated phishing email

Solo l'anno scorso, Google ha bloccato 100 MLN di emails.

Caratteristiche tipiche

- Manca la veste
- **Titolo a cazzo di cane**
- **Manco c'è il tuo nome**
- Si visualizza solo il nome del sender e non il titolo, senza far notare l'effettivo indirizzo da cui arriva.
- Typos e inglese **alla cazzo di cane**
- Link con il testo != dal hyperlink.

Tattiche di influenza

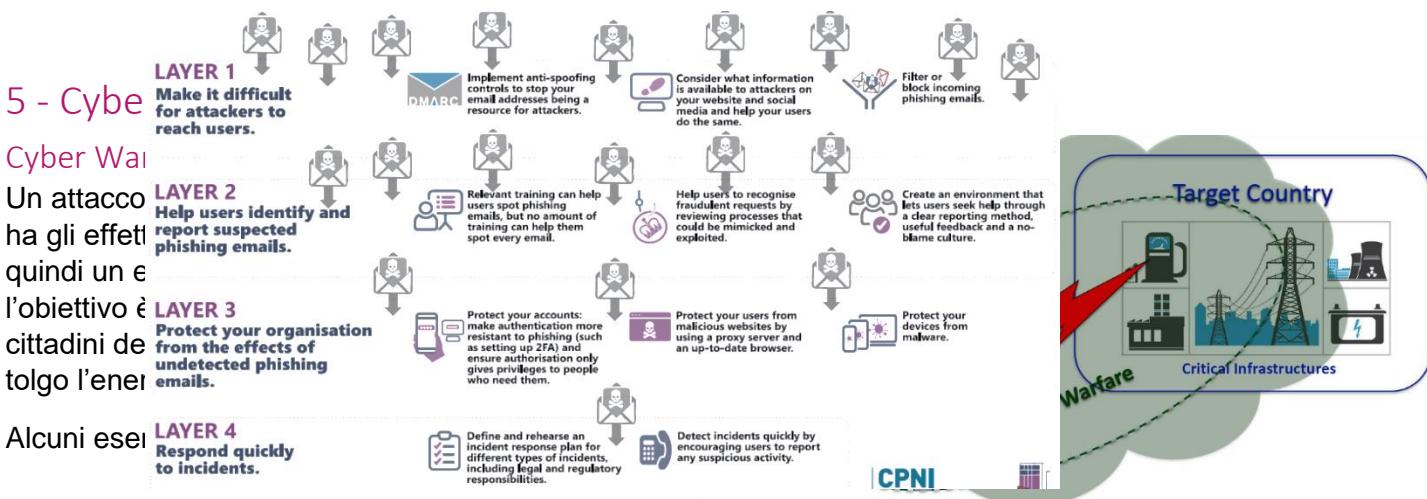
- Sfruttamento della relazione di autorità o fiducia
- Scarsità di tempo, per portare le vittime a non poter riflettere
- Social proof: è tentato di fare la cosa se sa che anche altri che conosce la hanno fatta

Tecniche più efficaci: authority e scarcity. E fra questi? Studio della Paci e di un suo studente. Uaaa. Vince la scarcity.

Phishing websites

Lingua sbagliata, dominio canato, no HTTPS... → PhishTank: verifica dei siti phishing.

Prevenzione



- Chimica

- Difesa

- Ospedali

- Trasporti

- Nucleare
- Comunicazioni
- Energia
- Finanza
- Telecomunicazioni
- Spazio
- Acqua

I principali rischi per queste infrastrutture che forniscono servizi vitali, vogliamo garantire alcune proprietà:

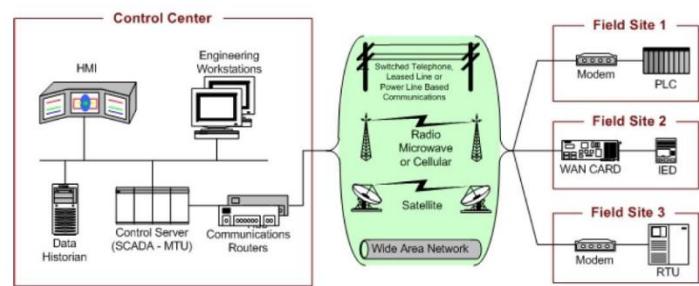
- **Availability:** devono sempre funzionare
- **Integrità:** le informazioni processate da queste infrastrutture non devono essere modificate dagli attaccanti
- **Safety:** sicurezza dell'infrastruttura. Se ho un attacco che modifica il funzionamento di una turbina per farla esplodere ho un impatto sulla safety 😊 🚨 🚨 🚨 🚨

Sono attacchi molto recenti; il primo è stato nel 2010. Quindi, questi sistemi hanno dei sistemi di controllo industriale.

Industrial control systems

SCADA

È il più diffuso **me thinks**. Consiste in un server che comunica con le stazioni locali e raccoglie dati sul funzionamento dei vari dispositivi. Li salva nel server data historian, da cui operatori e ingegneri possono visualizzare lo stato e inviare comandi ai controllori delle stazioni locali. Ci sono due tipi di controllori: PLCs e remote terminal unit.

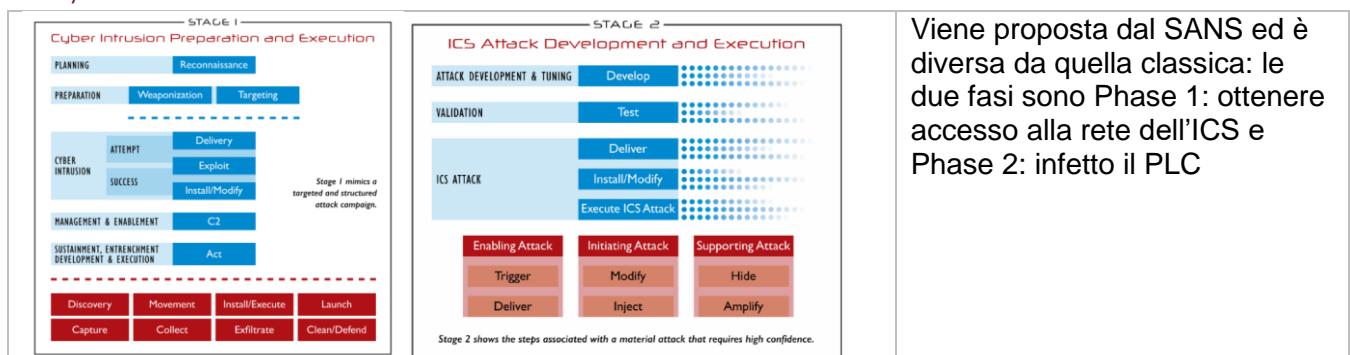


PLCs

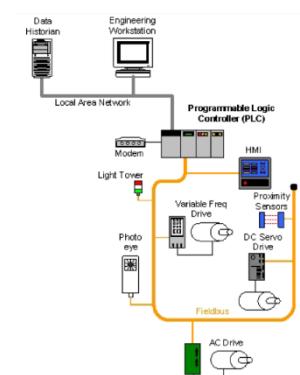
Questi sistemi presentano diverse vulnerabilità.

- Questi sistemi inizialmente erano sistemi chiusi, non connessi alla rete. Ora invece lo sono! Questo li espone ad attacchi a cui non erano soggetti
- Per garantire l'availability, il ciclo di un computer/macchinario è lunghissimo (10-20 anni). Quindi molti ICS eseguono software o **sistemi operativi obsoleti**.
- Autenticazione fatta con **sistemi basati su password**, che è spesso molto debole o la stessa per tutti i dispositivi di un modello.
- **Access control:** solitamente non abbiamo controlli sull'accesso
- **Analisi degli attacchi inesistente:** spesso non si mantiene nessun log delle attività, quindi in caso di attacco è difficile ricostruire

ICS cyber kill chain

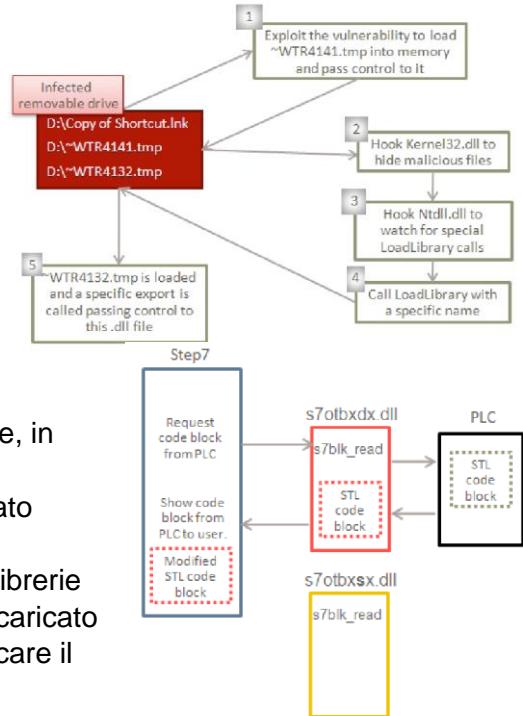


Viene proposta dal SANS ed è diversa da quella classica: le due fasi sono Phase 1: ottenere accesso alla rete dell'ICS e Phase 2: infetto il PLC



Esempio: Stuxnet

- Infetta la macchina, se non è la macchina obiettivo (drive della siemens) si disattiva
- Usa due **zero days** (stampante, chiavette) per sostituirsi al programma del PLCs. Installa un rootkit per prendere info sulle turbine, e faceva casino e poi mandava le info registrate prima – regolari – ai controlli
- **Reconnaissance** dai video di propaganda
- **Propagazione:** due zero day vulnerabilities. Propagazione tramite chiavetta usb: si creano 3 files sulla chiavetta.
Quando si plugga la chiavetta si esegue il .lnk e si carica uno dei .tmp, che carica WTR4132, il quale contiene stuxnet. Inoltre, in autorun.inf c'era una copia di stuxnet
- **Command and control:** aggiornava stuxnet, ma non è mai stato utilizzato.
Modifica del PLC: Creano una versione malevola di una delle librerie (s7otbcdx.dll). Quella legittima è stata rinominata e poi hanno caricato la loro versione malevola. Questa libreria permetteva di modificare il codice presente sul PLC e inviare comandi.
Potevano sia far partire i rotori, sia cambiare la pressione del gas inserito



Esempio: Sandworm

Conducono cose brutte (spesso con spearphishing) in politica

2015 – attacco elettrico ucraina

Causa il blackout in una regione di kiev per un massimo di 6 ore. Il disagio non è stato così grosso, il casino è che è stato il primo critico... Compromettono gli interruttori che consentivano la trasmissione... apprendoli. Coi plc. **Bravi bravi** Ci riescono perché:

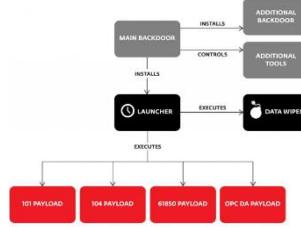
- Nell'estate precedente hanno condotto una campagna di spearphishing contro i dipendenti, rubando le credenziali per accedere alla vpn.
- Ottenuto l'accesso alle VPN rendono non utilizzabile le loro workstations
- Per impedire che venisse notificato fanno anche un DDOS all'assistenza.

Black energy: viene installato quando gli operatori aprono il phishing email. Aveva una struttura modulare, con 2 funzionalità per mappare la VPN e due moduli per rubare le credenziali. Aveva anche la capacità di collegarsi con CC per scaricare cleandisk, il secondo malware

2016 – secondo attacco

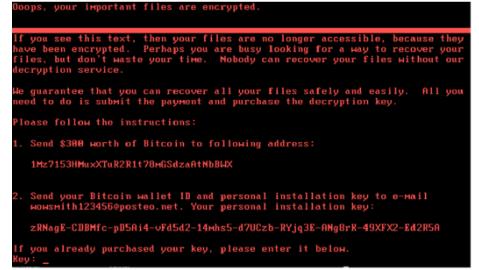
Lo stesso gruppo di hacker fa un attacco per la trasmissione dell'energia. I due attacchi hanno degli elementi in comune: anche qui si passa da **spearphishing**. Il malware usato questa volta era **Industroyer**, un malware tipo stuxnet: l'obiettivo era rendere inutilizzabili i remote terminal unit che controllavano gli interruttori. La caratteristica che lo rende specifico è che aveva dei moduli che **implementavano i 4 possibili protocolli** usati dalla workstation.

- Installa backdoor + una di riserva
- Scarica tool per rubare le credenziali e per il ddos contro protection della siemens
- Il cuore era il **launcher**, che implementava ed eseguiva **4 payload** – uno per protocollo di comunicazione.
- Dopo qualche ora viene eseguito il **data wiper**; in questo caso guardavano i servizi attivi e modificavano i path nei registri per rendere la macchina non bootabile.



2017 –Nopetya

All'inizio era un **ransomware** che ha colpito tutto il mondo partendo dall'ucraina. Veniva diffuso in maniera simile ai supply chain attack: mira un fornitore delle vittime. Tipo, tutte le aziende ucraine usano un software per mandare dati al governo. Sandworm riesce a **intercettare il traffico** che dalle macchine andava a richiedere aggiornamenti di **M.E.Doc** e lo ridirigono su un loro server installando così notpetya.



La stranezza è che chiedeva il riscatto, ma usavano lo stesso indirizzo per i bitcoin in tutte le infezioni – consentendo la tracciabilità – e chiedevano la conferma via mail del pagamento avvenuto. Inoltre, la chiave mostrata era solo quella del main drive; la chiave usata sulla macchina non era recuperabile. Si pensa dunque che l'obiettivo fosse **solo mettere piede sulle macchine infette**, non fare soldi.

6 - Malware

La parola malware viene da software malevolo. Si tratta di software o firmware che ha lo scopo di eseguire un processo non autorizzato che avrà un impatto negativo sulal confidenzialità, integrità o disponibilità di un sistema informatico.

L'infezione avviene attraverso:

- **Accesso diretto al sistema:** dischi infetti, chiavette usb
- **Social engineering:** spear phishing, whale phishing
- **Siti malevoli**

Ne esistono numerosi tipi:

Virus	<p>Sono facilmente identificabili dal software antivirus, perché solitamente hanno una specifica signature. Le caratteristiche sono:</p> <ul style="list-style-type: none">• Modificano e compromettono software• Possono riprodursi e infettare altre macchine; hanno isogno di un'azione umana per eseguire <p>Si dividono in:</p> <ul style="list-style-type: none">• Macro: macro contenuta in un contenuto malevolo. Non è un vero eseguibile ma una serie di comandi scritti in scripting• Polimorfici: cambiano comportamento in base al sistema operativo o alla macchina• Companion: sono i più insidiosi, perché si mascherano da software legittimo o da programmi comunemente presenti
Worms	<p>Hanno l'obiettivo di dare all'attaccante il controllo della macchna, solitamente installando backdoor. Poi tipicamente rubano dati. Si replicano, ma senza bisogno di azione umana sfruttando vulnerabilità</p>
Trojans	<p>Nascono come software malevolo che accede a info sensitive sulla macchina della vittima</p>
Rootkits	<p>Di solito sono installati nel kernel del sistema operativo, fra il software e l'hardware. Stando lì hanno la capacità di monitorare tutte le chiamate a funzione della libreria eseguita dal software. In questo modo nascondono la presenza di altro malware, intercettando le chiamate alle API di windows.</p> <ul style="list-style-type: none">• Danno capacità di accesso amministratore alle macchine infettate. <p>Ci sono tre tipi:</p> <ul style="list-style-type: none">• Livello applicativo: sono embedded in applicazioni apparentemente legittime. Sono semplici files eseguibili che possono essere identificati e rimossi• Livello kernel:• Livello masterboot record: se viene compromesso non si carica nemmeno l'OS <p>Per le ultime due l'unica è reinstallare il sistema operativo, e a volte anche questo non è sufficiente; bisogna buttare tutto :')</p>
Droppers/downloaders	<p>Sono malware che contengono il payload. Tipicamente sono macro infuse in allegati. Quando il documento è aperto il malware viene estratto dal dropper e copiatot sulla macchina.I downloaders, anziché avere il malware nel dropper, lo scaricano da un sito</p>
Keyloggers	<p>Sono tipologie di malware che di solito sono installate da altri malware, tipo trojans o ransomware. Catturano tutti i caratteri digitati e le salvano in un file locale nascosto, poi inviato all'attaccante</p>

Bots	trasformano le macchine infette in zombie al servizio dell'attaccante. Spesso usati in dDOS
Criptominers	usano le risorse delle macchine infettate per fare mining di crittovalute . Un esempio è (lemonduck), che usa un software opensource per infettare dispositivi e minare
Ransomware	infettano i pc epoi chiedono il riscatto

Gestione

- Prevenzione**

Tipicamente questi oggetti arrivano via ingegneria sociale; la soluzione migliore quindi è un software che analizza e blocca direttamente il contenuto delle email.

- Riduzione della diffusione**

Se l'infezione è avvenuta, dobbiamo impedire la diffusione. Una cosa usata spesso è la presenza di vulnerabilità nelle macchine infette → assicurarsi che il SO sia aggiornato.

- Proteggere le credenziali admin e non usare solo password, ma associare un terzo elemento di autenticazione – come ad esempio una OTP generata da un'applicazione sul telefono della vittima.
- Attenzione alle mail di phishing
- Educare i dipendenti sui malware che possono colpirli
- Backup regolari

- Riduzione dei danni**

- Cambiare tutte le password
- Disconnettere tutti i dispositivi dalla rete
- Installare antivirus e fare scansione/pulizia

Ransomware attacks

Esempio: <https://github.com/goliate/hidden-tear/blob/master/hidden-tear/hidden-tear/Form1.cs>

Se prima erano solo per windows, ora ce ne sono tanti anche per android, linux e macos. Tipicamente, vengono diffusi tramite mail di phishing + allegato malevolo o con lo sfruttamento di vulnerabilità dell'OS. Ne esistono di 4 categorie:

			
Ransomware	Lockers	Master Boot	Wipers

Ransomware
Crittano i contenuti e solitamente richiedono un riscatto per la decrittazione.

Lockers
Bloccano l'accesso al sistema operativo mostrano una schermata in cui richiedono il riscatto per lo sblocco (senza crittare)

Master Boot
Boot record ransomware: cifra il masterboot record o lo modifica in modo che il SO non sia più caricabile.

Wipers
Cancella tutto fraaa 

Un ransomware è composto da quattro componenti:

			
Trojan behavior serve a farlo arrivare sulla macchina	File encryption and decryption routines Cifratura dei file	Key extraction mechanism Routine che si occupa di estrarre la chiave estratta per la cifratura (di solito è generata sulla macchina infetta e poi passata all'attaccante)	User interaction module Interfaccia con l'utente in cui si presentano le istruzioni del pagamento del riscatto

Cifratura

Ne esistono due tipi:

Chiave simmetrica	Chiave pubblica/privata
--------------------------	--------------------------------

Si usa una chiave per cifrare e decifrare; di solito un ransomware deve cifrare tanti files e questa è più veloce 😊	la privata è nota all'attaccante, mentre la pubblica è quella usata per cifrare la chiave simmetrica e una volta cfrata la chiave pubblica dell'attaccante è mandata all'attaccante. (?)
---	--

I primi ransomware usavano metodi di cifratura un po' naive, tipo codifica della chiave nel codice ransomware o algoritmi bucabili come XOR e RC4. Il processo è il seguente:

- Sulla macchina della vittima si crea la chiave di cifratura (o eventualmetne dal C2). Nelle prime versioni la chiave era codificata nel ransomware xD
- Cifratura: magari solo alcune estensioni
- Cifratura della chiave simmetrica con quella dell'attaccante e spedita
- La chiave simmetrica è cancellata dal pc della vittima

Kill switches

Sono condizioni inserite nel codice che sostanzialmente **stoppano l'esecuzione del malware**. Di solito sono inserite per **evitare di infettare le proprie macchine**. Il più famoso è quello di WannaCry, scoperto da un tipo (**poi arrestato**) che scoprì che il comportamento era legato a un dominio: guardava se un certo dominio era attivo; se veniva restituito quel dominio, faceva una richiesta e se riceveva risposta **faceva harakiri**. Così il tipo riesce a bloccare la diffusione di wannacry.

Bad rabbit (🐰🐰🐰🐰)

Distrugge il masterboot record. Cercava di scrivere infpub.bat sotto la cartella di windows. Se non ci riusciva si fermava, ma faceva lateral movement sfruttando la stessa vulnerabilità di wannacry.

CyberKillChain

Weaponization Costruzione del ransomware.	<p>Ne esistono tre tipi:</p> <ul style="list-style-type: none"> • Fileless ransomware: sono ransomware non associati a un file eseguibile; arrivano mediante phishing da un allegato malevolo, che carica direttamente il ransomware in memoria e lo esegue. Un software antivirus non è in grado di identificarlo • Diversificazione del payload: ormai i client di posta bloccano gli .exe, quindi solitamente si include il ransomware all'interno di documenti o immagini o DLL da far caricare in memoria al posto dei dll legit. • Diversificare il porcesso di accesso ai files: i ransomware vanno tipicamente a modificare l'estensione dei file prima di essere cifrati, oppure vanno a modificare le informazioni associate ai files nella Master File Table (disponibile in NTFS) per rendere inaccessibili i files <p><i>Evasion</i></p> <p>Esistono inoltre varie tecniche di evasione. Introduzione di un intervallo di tempo fra una cifratura e l'altra. Questo perché i ransomware usano tante cifrature di fila, e questo tipo di operazione è monitorata dai software antivirus e antimalware. Introducendo del ritardo si riesce a ritardare l'identificazione da parte dell'antivirus</p> <ul style="list-style-type: none"> • Cifratura solo a un certo evento. Un esempio tipico è quando inizia il processo di backup, per impedire all'utente di recuperare i files • Data evasion: <ul style="list-style-type: none"> - spesso i ransomware creano dei files sulla macchina delle vittime; quindi eliminano questo file prima o dopo della cifratura per eliminare le tracce. - Anti-dump: molto spesso per analizzare il codice si aspetta che il codice venga eseguito e poi si scarica il codice dalla memoria. Per impedire l'analisi esistono delle tecniche che bloccano il dump. • Code evasion
---	--

	<ul style="list-style-type: none"> - Reverse engineering permette di analizzare un ransomware dando input il ransomware, che genera il codice (dal quale posso capire il comportamento). Per impedire l'analisi statica ci sono delle tecniche di anti-disassembly, che cifrano il ransomware stesso oppure aggiungono offuscamento o lo paccano. Inoltre ci sono tecniche che prevengono l'analisi nei debugger. Banalmente, basta anche solo controllare un certo flag (che viene attivato dai debugger) e impostare un blocco quando questo è attivo. - Inoltre è possibile anche disattivare il ransomware quando esso si rende conto di essere in una macchina virtuale, basato sul mac-address • Analisi del traffico di rete: il ransomware comunica con un C2 per comunicare la chiave di cifratura e ricevere istruzioni. <ul style="list-style-type: none"> - Il traffico può essere cifrato - Posso usare reti tipo TOR che garantiscono l'anonimato, perché il traffico gira fra diversi nodi e quindi non si capisce sorgente e destinazione. - Domain shadowing: cambio l'indirizzo IP associato al C2 						
Delivery	<ul style="list-style-type: none"> • Phishing, spearphishing • Malvertisement: consiste in siti legittimi che vengono compromessi con della pubblicità che, quando la vittima ci clicca, reindirizzano a siti dove è ospitato il ransomware e viene scaricato sulla macchina della vittima • Ridirezione del traffico generato da siti legittimi: la vittima visita un sito legittimo per aggiornare un software e l'attaccante intercetta il traffico e lo redirige verso un sito compromesso dal ransomware 						
Exploitation L'obiettivo è avviare il processo.	<ul style="list-style-type: none"> • Exploit kits: dal darkweb si possono comprare exploit kit per sfruttare le vulnerabilità, tipo Neutrino (Adobe reader) e Blackhole(adobe flash). Ovviamente questo ha senso se la macchina infetta ha adobe nella versione giusta e nel programma giusto • Exploits mirate: zero-day vulnerability o altre vulnerabilità trovare in reconnaissance 						
Installazione L'obiettivo è rendere i files non accessibili e diffondersi sulla rete.	<ul style="list-style-type: none"> • Crittare tutto, probabilmente anche i backup • Cifrare anche il master boot record • Diffusione: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Exploits</td><td style="padding: 5px;">Usava una vulnerabilità del protocollo samba di Windows. In questa vulnerabilità consentiva all'attaccante di eseguire codice in remoto sulla macchina. Usano l'EternalBlue exploit kit realizzato dalla NSA e tenuto nascosto per 5 anni (perché voleva usare questa vulnerabilità per attaccare altri paesi xDxDxD) È snowden a rivelare l'esistenza di questo toolkit, e così Windows ha dovuto fixare. Lul.</td></tr> <tr> <td style="padding: 5px;">Chiavette</td><td style="padding: 5px;">Si sfrutta la funzionalità di autorun: modifico autorun.inf per eseguire il ransomware.</td></tr> <tr> <td style="padding: 5px;">Condivisione di rete</td><td style="padding: 5px;">I file share si usano per fare backup. Di solito i files sono condivisi via un server a cui si connettono tutte le macchine dell'organizzazione. Il computer infetto carica una copia del ransomware, e quando le altre macchine vi si connettono lo scaricano+eseguono :O Una variante potrebbe anche essere NON scaricare il file stesso ma creare dei link al file. Il file lnk + pulito, aka non viene sgamato dall'antivirus</td></tr> </table> 	Exploits	Usava una vulnerabilità del protocollo samba di Windows. In questa vulnerabilità consentiva all'attaccante di eseguire codice in remoto sulla macchina. Usano l'EternalBlue exploit kit realizzato dalla NSA e tenuto nascosto per 5 anni (perché voleva usare questa vulnerabilità per attaccare altri paesi xDxDxD) È snowden a rivelare l'esistenza di questo toolkit, e così Windows ha dovuto fixare. Lul.	Chiavette	Si sfrutta la funzionalità di autorun: modifico autorun.inf per eseguire il ransomware.	Condivisione di rete	I file share si usano per fare backup. Di solito i files sono condivisi via un server a cui si connettono tutte le macchine dell'organizzazione. Il computer infetto carica una copia del ransomware, e quando le altre macchine vi si connettono lo scaricano+eseguono :O Una variante potrebbe anche essere NON scaricare il file stesso ma creare dei link al file. Il file lnk + pulito, aka non viene sgamato dall'antivirus
Exploits	Usava una vulnerabilità del protocollo samba di Windows. In questa vulnerabilità consentiva all'attaccante di eseguire codice in remoto sulla macchina. Usano l'EternalBlue exploit kit realizzato dalla NSA e tenuto nascosto per 5 anni (perché voleva usare questa vulnerabilità per attaccare altri paesi xDxDxD) È snowden a rivelare l'esistenza di questo toolkit, e così Windows ha dovuto fixare. Lul.						
Chiavette	Si sfrutta la funzionalità di autorun: modifico autorun.inf per eseguire il ransomware.						
Condivisione di rete	I file share si usano per fare backup. Di solito i files sono condivisi via un server a cui si connettono tutte le macchine dell'organizzazione. Il computer infetto carica una copia del ransomware, e quando le altre macchine vi si connettono lo scaricano+eseguono :O Una variante potrebbe anche essere NON scaricare il file stesso ma creare dei link al file. Il file lnk + pulito, aka non viene sgamato dall'antivirus						
Command & control	Command&control: Se la chiave è generata sul C2, può avvenire prima del processo. Altrimenti, l'altra fase avviene a fine processo di cifratura: si comunica la chiave di cifratura e le info per pagare il riscatto. Una cosa very important è sapere come contattare il C2.						

	<ul style="list-style-type: none"> • In ransomware naive, gli IP erano una lista nel codice. Ma così li blocco facili • Domain generation algorithm: C2 decide un algoritmo per generare il nome del dominio associato. Dato che è generato dinamicamente ogni volta che devo contattare il C2, questo rende impossibile creare una blacklist! • Botnets
Action and objectives	<p>In base alla tipologia del ransomware posso avere uno scopo diverso. In genere voglio pagare un riscatto.</p> <ul style="list-style-type: none"> • Nei primi ransomware si usava l'IBAN o paypal :') • Bitcoin

Prevenzione

- Non cliccare su cose, non aprire allegati...
- Fare backup
- Non dare password in giro
- Aggiornare le cose...

Correre ai ripari

- Sconnettersi dalla rete per evitare la dispersione
- Antivirus
- Cercare un ransomware decryption tool, se esiste per il ransomware beccato
- Recupero dei backup time 😊

<https://www.nomoreransom.org/>

7 - Autenticazione e attacchi password

Si definisce autenticazione utente la determinazione dell'identità, solitamente basata su una combinazione di:

- Qualcosa che la persona **sa** (password)
- Qualcosa che la persona **ha** (smart card, token)
- Qualcosa che la persona **è** (fingerprint).

Autenticatori (token based authentication)

L'utente deve presentare un token per essere autenticato. Ne esistono numerosi tipi.

OTP	<ul style="list-style-type: none">• Single factor: genera un numeretto ogni 30 o 60 secondi. C'è un valore segreto con una funzione di hash che calcola il valore.• Multi factor: c'è un secondo fattore di autenticazione; contengono una chiave simmetrica e si usa la crittazione per ottenere l'OTP.
Smart Cards	Sono l'equivalente di una carta con un piccolo processore, e vi sono memorizzati i certificati di chiave pubblica e privata di quelal carta. Per supportare l'autenticazione abbiamo bisogno di un lettore apposito; poi il processo di autenticazione segue un processo di challenge and response: <ol style="list-style-type: none">1. User scrive un pin2. Il lettore manda una challenge3. La smartcard genera un valore randomico e segna A B con la chiave4. Il lettore epiò verificare la validità della firma con la chiave pubblica. <p><i>Vulnerabilità</i>: Rubare o perdere l'oggetto</p>

Biometria

Anche qui mi serve un lettore della caratteristica fisica. Sono molto diffusi. La caratteristica fisica deve essere:

- **Universale**: tutti devono averla
- **Distintiva**: deve essere univoca per ciascuno
- **Invariante**: non deve cambiare nel tempo
- **Facilmente leggibile**

La registrazione consiste nel catturare l'impronta e salvarla in un lettore; al momento della scansione verrà confrontato il vettore salvato con quello registrato al momento. C'è un margine di errore.

Caratteristiche comunemente usate:

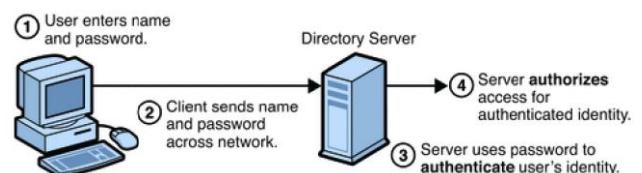
<ul style="list-style-type: none">• Impronte• Iride• Monitor dell'ECG!	<ul style="list-style-type: none">• DNA• Facial recognition	<ul style="list-style-type: none">• Voce• Modo in cui si cammina (gait)
--	--	--

Limitazioni:

- **Accuracy**: possono soffrire di falsi positivi e falsi negativi
- **Facile rubare le impronte**
- **Gli utenti sopportano poco** (es. retina è scomoda da scannerizzare)

Autenticazione basata su password

Molto diffusi perché **semplici ed economici**. Ma anche molto **debolì** (vedi Mirai botnet). In media, un utente gestisce 22 password! Quindi spesso o si usano pattern semplici, o si usa la stessa password – magari sia per account di lavoro che privati.



Problemi:

- **Password overload e reuse:** in media abbiamo 22 password diverse. E quindi sono ripetute su più siti.
- **Password predibili:** avendo tante password spesso si scelgono pattern molto semplici

Attacchi:

Ci sono tanti modi di attacco:

- **Offline attacks**
- **Active online attacks:** l'attaccante deve interagire per beccare la password
- **Passive online attack:** le password sono storate in locale! Posso ottenere una copia del file dai registri di windows (local machine → SAM) o anche dal file system. Di solito l'accesso è protetto ma ecco.
- **Non technical attacks**

Password offline

È possibile rubare le password dalle macchine delle vittime, dato che i vari sistemi operativi le salvano in varie posizioni.

Windows	Linux	Apple
<ul style="list-style-type: none">• Local machines: SAM database• C:\Windows\System32\config• Mounted as a HKLM/SAM	<ul style="list-style-type: none">• Local machines: etc/shadow	<ul style="list-style-type: none">• var/db/dslocal/nods/default/users• <user>.plist

Queste password sono normalmente storate sotto forma di hash. L'hash può essere di tipo LM o NTLM
Windows usa LM.

Attacchi bruteforce

Calcoliamo tutte le possibili combinazioni di caratteri fino alla lunghezza massima, fa l'hash e lo confronta fino a trovare hash che matchano. Il problema è che ci vuole moltissimo. Tool comune: John The Ripper

- **Attacco di dizionario**
L'attaccante prova password da un dizionario di password comunemente usate, e le compara con la password crittata o hashata. In questo modo ci vuole molto meno!
- **Hybrid attacks**
Uso di un dizionario + variazioni delle parole, per esempio con caratteri speciali e numeri.
- **Rainbow tables**
Tabelle che per tutte le parole di uso comune computano l'hash. Sono molto più rapide di bruteforce puro, dizionari e hybrid attacks. Lo svantaggio è che sono moooooooooooooolto pesanti

Strength di una password

Esistono diversi modi per misurare la sicurezza della password, e in generale non si vuole considerare solamente la formula sopra "grezza" ma anche quanto quella password è comune/probabilmente disponibile in dizionari.

- **Bruteforce:** La forza di una password può essere misurata in base a quanto è resistente a un attacco bruteforce, stimando quanti tentativi ci vorranno per l'attaccante prima di indovinare la password corretta. Normalmente si calcola come $|A|^n$, con A numero di simboli che possono comparire e n lunghezza della password.
- **Zxcvbn:** è una misura di forza della password che assume che la password sia una serie di uno o più pattern concatenati. Questi pattern possono essere:

Contromisure

- **Salting:** aggiungiamo dei numeri random (sale) alle password, cosicché l'attaccante deve riscostruire l'hash e anche questo valore.
- **Controllo dell'accesso:** restringo l'accesso solo agli user privilegiati e mantengo le password hashate separate dagli user ID.
- **Procedura di reset veloce**

Dictionary attack online

Intelligent search: si provano parole associate all'utente. Obv non hai certezza di beccarla.

Contromisure:

<ul style="list-style-type: none">• Politica che obbliga gli utenti a scegliere password sicure• Cambiare frequentemente le password• Aiutare gli utenti generando le password in modo automatico	<p>→</p> <p>in realtà però non sono più sicure, perché imporre alle vittime troppe regole e troppi cambiamenti non fa altro che forzare le vittime a usare i pattern e rende le password facilmente craccabili.</p> <p>Quindi misure più efficaci sono:</p> <p>→</p>	<ul style="list-style-type: none">• Implementazione di lockout: se il sistema registra un certo n di login canali, blocchiamo l'accesso dell'utente. Non è sempre semplice perché <i>si rischia di bloccare l'account di un tentativo legittimo!</i>• Throttling (tempo fra un tentativo e l'altro)• Protecting monitoring: se ci sono login mando una notifica• Password blacklist: impedisco di usare password troppo comuni.• Autenticazione a più fattori
--	--	--

Intercettazione

L'attaccante sniffa il traffico di rete, e se è fortunato è in grado di vedere la password in chiaro. Soprattutto se non si usa HTTPS.

Contromisure:

Crittare la comunicazione con protocolli sicuri

Keylogging

Ingegneria sociale

- Phishing
- Shoulder surfing
- Dumpster diving...

Contromisure:

Training e user awareness.

Social engineering

Literally cose già viste, tipo phishing, shoulder surfing, dum

Contromisure:

training e user awareness.

8 -Gestione identità e accesso

Problema dell'avere tanti account: spesso all'utente è richiesto di ricordare tante password, e allo stesso tempo tanti siti devono memorizzare i dati dell'utente, con il rischio di data breach. Possiamo risolvere questi problemi con sistemi **dell'identità digitale**, dato che il processo di autenticazione è delegato a un sistema di identità digitale (anziché ai singoli servizi). **Quindi si solleva il service provider dall'implementare l'autenticazione e dal dover proteggere i dati**, mentre permette ai dati di non dover memorizzare tante credenziali diverse.

Identità digitale

Un'identità digitale è una rappresentazione di cosa conosciamo di un individuo. Può essere banalmente solo user e password, o includere anche altre info identificanti come nome, cognome, nazionalità, indirizzo...

Lo scopo è:

- **Mantenere l'identità** dell'utente e **associarvi attributi**
- Verificare l'identità dell'utente e **certificare che l'utente è autenticato** al servizio.

Gli attori sono:

Soggetto	Identity provider	Service provider
colui di cui vogliamo verificare l'identità	soggetto legale che verifica l'identità ed è in grado di rilasciare una prova che l'utente è identificato con successo	fornisce servizi online, e verifica le dichiarazioni rilasciate dall'identity provider (fidandosi) per concedere i servizi

Ci permettono di implementare il SSO.

Single Sign On (SSO)

Un utente può riutilizzare lo stesso set di credenziali per accedere a più servizi online. Tipicamente l'utente che vuole accedere a un servizio è rediretto sulla pagina dell'identity provider; questo verifica l'identità, e se questa è verificata l'identity provider manda un'asserzione di validità (**token**) al service provider.

Esistono due scenari principali:

1. **Un utente vuole usare la propria identità per accedere a più servizi offerti dallo stesso fornitore**
Esempio: Utente usa le proprie credenziali Google sul server di autenticazione di Google sia per Gmail che per Youtube; dopo essersi autenticato per Gmail, se il token è ancora valido accede direttamente a Youtube, dato che Google Account valida il token e reindirizza su Youtube. Altrimenti si riautentica e ottiene un nuovo token.
2. **Usare un'identità digitale per accedere a servizi usati da provider diversi (Cross Domain SSO)**
Esempio: Mi autentico su EasyJet e poi uso quel token per accedere a Booking.com e Hertz.

Federated identity

Per implementare questo scenario dove i fornitori non appartengono allo stesso dominio bisogna introdurre il concetto di **Identity Federation**, ovvero dove diversi fornitori di servizi decidono di "fidarsi" di un altro autenticatore che fa parte della federation. Deve esserci trust e un accordo.

Un esempio è SPID, con il quale possiamo accedere sia a servizi di PA che ad altri servizi privati che vi aderiscono. Esiste:

- lo SPID registry per verificare chi può fornire lo SPID

- gestori di attributi qualificati che rilasciano documenti colelgati
- Fornitori di servizi pubblici e privati

Gli attori sono simili:

- Agenzia per l'Italia Digitale AgID: agenzia che si occupa di accreditare i fornitori di servizi che possono rilasciare lo SPID
- **Identity provider**: entità certificate da AgID che rilasciano gli SPID
- **Service provider**: forniscono servizi
- **Attribute Provider**: rilasciano attributi sulla base dei quali si rilascia l'ID digitale

Lo SPID prevede 3 livelli di identità, che corrispondono a tre livelli di autenticazione sicura;

Level1		Level2		Level3
username e password	→	level1 + OTP via app o SMS	→	level2 + dispositivo fisico (tipo smartcard e lettore) dato dall'identity provider

SAML

Per implementare lo SPID e in generale le identità federate abbiamo bisogno di un meccanismo per trasmettere info sul processo di autenticazione. Il protocollo usato è **SAML** (security assertion markup language) ed è un **protocollo** XML che consente di scambiarsi attributi e token. È usato tipicamente nella cross domain SSO. SAML ci permette di rilasciare dichiarazioni su autenticazione, attributi, permessi garantiti all'utente sulle risorse

Tipicamente in un'asserzione bisogna specificare:

<ul style="list-style-type: none"> • Issuer • Issuance Condizione di validità: può essere un periodo di tempo oppure determinate condizioni (es. solo su alcuni servizi) 	<ul style="list-style-type: none"> • Identificativo univoco dell'asserzione • Info sul soggetto, tipo il nome e il dominio a cui appartiene • Timestamp
--	--

Shibboleth

È un altro protocollo per implementare le identità federate. Si **basa su SAML** ed è utilizzato per autenticare utenti che vogliono accedere a informazioni fornite da istituti di ricerca. Un esempio è la **UK access management federation**, con la quale uno studente di oxford può accedere anche alle risorse delle altre università.

Abiamo sempre tre entità: utente, identity provider (università mia), service provider (università altra)

1. Quando lo studente tenta di accedere è rediretto a WAYF, che permette di selezionare quale servizio della federazione gli ha fornito le credenziali.
2. Viene poi rediretto alla propria università per fare l'accesso.
3. Se l'autenticazione ha avuto successo, la sua università genera un handle che identifica questa sessione.
4. L'università obiettivo potrebbe richiedere attributi aggiuntivi per garantire l'accesso.

9 - Access control

I sistemi di autenticazioni sono la prima linea di difesa contro gli attacchi informatici: associano ad un utente i permessi e le azioni che egli può compiere in un organismo. Li usiamo per settare i permessi in google drive/doc, applicazioni...

Vogliamo garantire tre funzionalità:

- **Authentication**
- **Authorization**: concedere un permesso a un'entità di sistema.
- **Accountability/auditing**: permette di verificare chi ha acceduto a quali risorse, e capire se ci sono stati attacchi.

Componenti

- **Access Policy**: esprimono le condizioni per cui un utente può accedere al sistema.
- **Access Model**: Sono formalizzate a un determinato modello di controllo dell'accesso
- **Access Control Mechanism** : serve per capire se l'accesso deve essere garantito o meno , ed è un'architettura con vari meccanismi che usa le politiche per garantire o negare l'accesso.

Elementi

- **Soggetto**: può accedere agli oggetti
- **Oggetti**: risorsa ad accesso controllato
- **Permesso**: come un utente può accedere a quella risorsa.

Modelli principali

- **Discretionary access control (DAC)**: associamo i permessi direttamente all'identità verificata di un utente
- **Mandatory access control (MAC)**: tipicamente usati in contesti dove bisogna accedere a informazioni classificate, tipo militare; si basano sull'assegnazione di etichette di sicurezza sia agli utenti che alle risorse a cui si vuole accedere. Non ne parliamo bc già visti 😊
- **Role based access control (RBAC)**
I permessi non sono associati all'utente, ma a un ruolo – e poi l'utente può ricoprire il ruolo
- **Attribute-based access control (ABAC)**
Le politiche di controllo sull'accesso sono espresse come condizioni su attributi dell'utente – ad esempio, posso consentire a un utente di accedere solo in un determinato periodo di tempo o solo da un dispositivo.

DAC – discretionary access control

L'amministratore della risorsa può decidere a chi grantare o revocare i permessi. Viene rappresentato attraverso la matrice di controllo degli accessi, che ha righe per soggetti e colonne per oggetti.

Il problema è che ci vuole un sacco di spazio! Posso provare a spalmare la matrice sugli oggetti o sui soggetti.

	objects		
	news.doc	photo.png	fun.com
alice	read	view	view
bob	read write	view edit	view modify
charlie			
dave		view	

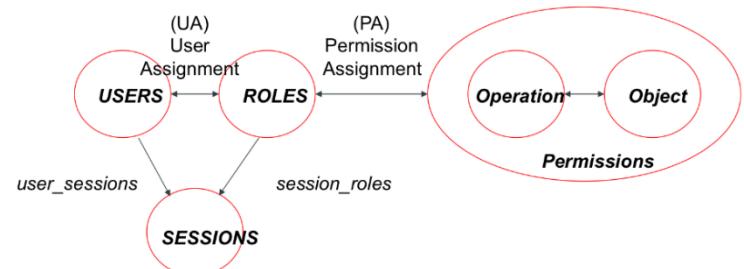
<p><i>Access control list</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">news.doc</td><td style="width: 33%; padding: 5px;">photo.png</td><td style="width: 33%; padding: 5px;">fun.com</td></tr> <tr> <td style="padding: 5px;">bob read write read</td><td style="padding: 5px;">alice view, edit bob view, edit dave view</td><td style="padding: 5px;">alice view bob view modify</td></tr> </table>	news.doc	photo.png	fun.com	bob read write read	alice view, edit bob view, edit dave view	alice view bob view modify	<p>Potrei separarla su ciascun oggetto</p> <ul style="list-style-type: none"> • Ma poi se voglio modificare/cancellare un utente mi tocca scorrere tutti i files. Inoltre, se volessi listare i permessi attuali dovrei guardare tutte le liste. • Per ogni elemento avrò 253 righe :') E setto a view quelle richieste. 						
news.doc	photo.png	fun.com											
bob read write read	alice view, edit bob view, edit dave view	alice view bob view modify											
<p><i>Capability list</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; padding: 5px;">news.doc</td><td style="width: 33%; padding: 5px;">photo.png</td><td style="width: 33%; padding: 5px;">fun.com</td></tr> <tr> <td style="padding: 5px;">Alice's capability read</td><td style="padding: 5px;">Bob's capability read write</td><td style="padding: 5px;">Charlie's capability fun.com</td></tr> <tr> <td style="padding: 5px;">news.doc</td><td style="padding: 5px;">photo.png</td><td style="padding: 5px;">fun.com</td></tr> <tr> <td style="padding: 5px;">Dave's capability view</td><td></td><td></td></tr> </table>	news.doc	photo.png	fun.com	Alice's capability read	Bob's capability read write	Charlie's capability fun.com	news.doc	photo.png	fun.com	Dave's capability view			<p>Per ogni utente memorizzo quali sono i permessi che ha sulle risorse del sistema.</p> <ul style="list-style-type: none"> • Il vantaggio è che per ogni utente posso facilmente determinare le risorse a cui ha accesso, ed è facile revocare o modificare i permessi di ciascun utente. <p>Nei setting reali, le capability list funzionano meglio rispetto alle access control list. Comunque è poco adatto.</p>
news.doc	photo.png	fun.com											
Alice's capability read	Bob's capability read write	Charlie's capability fun.com											
news.doc	photo.png	fun.com											
Dave's capability view													

RBAC – Role based access control

I permessi sono associati a un **ruolo**, che rappresenta solitamente una qualifica nell'organizzazione dell'azienda, e poi si assegnano gli utenti al ruolo. In questo modo possiamo assegnare permessi in maniera più efficiente. RBAC fu introdotto da un megaricercatore nel 96, e standardizzato nel 2004. Ne esistono tre famiglie che differiscono nei concetti supportati:

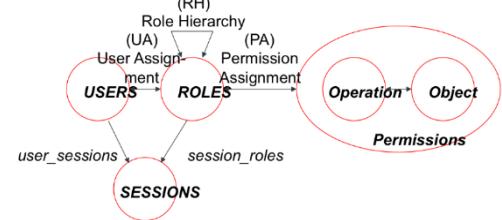
RBAC0: Core RBAC

- **Utenti**: sono assegnati ai ruoli tramite la user assignment relationship
- **Ruoli**: posizioni nell'organizzazione.
- **Permessi** : assegnamo i permessi a ciascun ruolo con la permission assignment relationship.
- **Sessione**: è usata per specificare il ruolo ricoperto da un utente in un determinato momento. Servono a verificare cose tipo il fatto che non posso essere docente e allievo di un corso insieme.



RBAC1: Core RBAC + gerarchia fra i ruoli

La gerarchia dei ruoli **semplifica l'assegnamento dei permessi**: quando un ruolo è supernodo di un altro, nella definizione dei permessi non serve specificare tutti i permessi sottostanti perché "li **eredita**"



RBAC2: RBAC1 + Separation of duty constraints (vincoli di separazione del dovere)

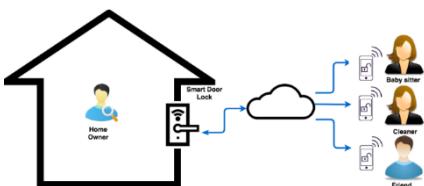
Implementano il **principio di least privilege**, ovvero che per completare un'azione su una risorsa abbiamo bisogni di almeno due utenti diversi. L'esempio classico è l'approvazione di un mutuo, che richiede l'approvazione da un impiegato e anche del direttore della banca; nell'ambito di RBAC, questo principio si implementa con i vincoli di separation of duty. Ne esistono due tipo:

- **Vincoli statici**: assume che un utente non può essere **assegnato contemporaneamente a più di tot ruoli**. (esempio, un utente segnato come studente e professore non può completare l'azione)

- **Vincoli dinamici:** consideriamo il concetto di sessione, ovvero un utente non può attivare nella stessa sessione due o più ruoli presenti in un insieme di ruoli predefinito. Ad esempio se in una sessione sono professore non posso attivare anche studente nella stessa sessione.

Vantaggi	Svantaggi
+ Non devo assegnare manualmente gli users ai permessi , quindi è più efficiente	- Soffrono di problematiche di scalabilità : pensando a una banca, ci sono in media 50'000 impiegati con 1400 filiali... Magari ci sono 1300 ruoli
+ Riduce il downtime degli impegnati.	- Utenti assegnati a privilegi più alti di quelli dovuti , perché spesso per evitare che un utente non riesce a portare un lavoro a termine si definisce un ruolo ad hoc (torno a DAC) o gli do un livello superiore a quello dovuto.
+ È usato ad esempio da Amazon o in ambito finanziario.	- Gli utenti privilegiati ne abusano: <ul style="list-style-type: none"> ○ Le spie della NSA che snoopano le morose ;) ○ Calciatore che si era recato in un ospedale e i dipendenti dell'ospedale vanno a snoopargli la cartella medica, rivelando ai giornali le sue informazioni come scoop.

ABAC – Attribute-based access control

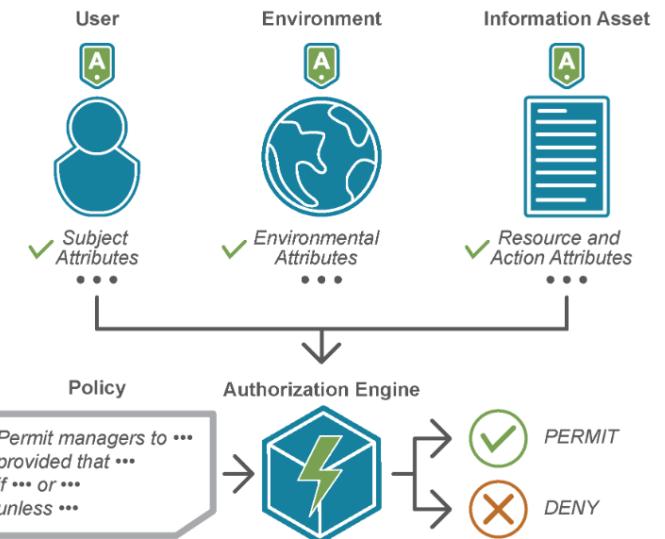


Vorremmo fare cose magiche tipo permettere alla babysitter di accedere solo se è in prossimità, e intorno ai suoi orari di lavoro.

Vogliamo dunque definire la situazione in base ad **attributi** (=essere babysitter), **all'ambiente** (posizione, orario) e **risorse** (solo al lucchetto intelligente).

L'accesso è garantito o negato in funzione di attributi dell'accesso. Prendiamo in esempio il caso della cartella di un paziente ricoverato per problemi di cuore.

- **Attributi del soggetto:** dove vive, dove lavora
Es: medico e cardiologo
- **Attributi legati al contesto:** da ove fa l'accesso
Es: deve collegarsi dall'ospedale e che utilizzi un pc dell'ospedale
- **Attributi della risorsa** richiesta: owner, progetto a cui appartiene il file, condizioni sul contenuto
Es: può accedere solo a cartelle cliniche con patologie al cuore



Per questo, ABAC diventa il modello di riferimento standard in tutte quelle organizzazioni dove servono autorizzazioni flessibili e dinamiche.

XACML

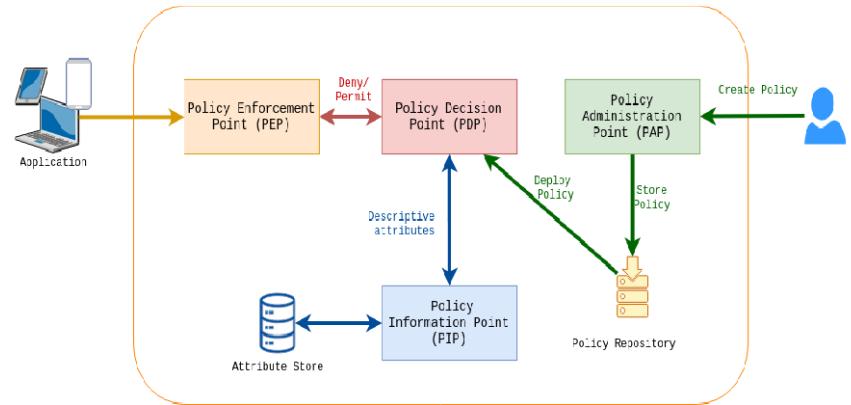
Lo standard è il linguaggio XACML. Fornisce:

- Linguaggio per **specificare le politiche** come condizioni sugli attributi del soggetto richiedente

- Linguaggio per **specificare richiesta di accesso e relativa risposta**
- Architettura che identifica le **componenti software da implementare** per decidere se una richiesta va accettata o meno.
- **Algoritmi per valutare se una richiesta di accesso deve essere negata o garantita.**

Architettura

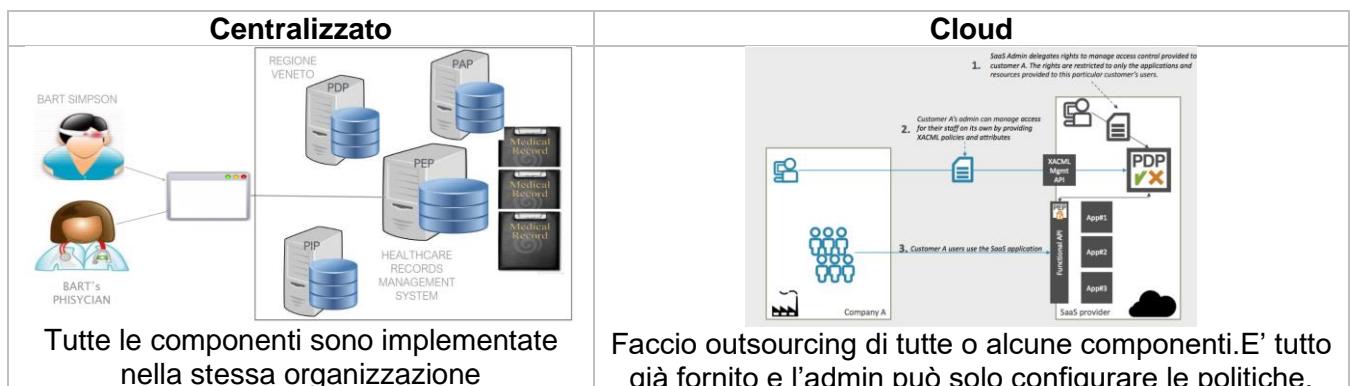
- **PEP: Policy Enforcement Point**
Intercepta tutte le richieste di accesso e le redirige al policy decision point
- **PDP Policy Decision Point**
Decide se garantire l'accesso in base alle policy
- **PAP: Policy Administration Point**
Serve a dare un'interfaccia all'amministratore per configurare le politiche
- **PIP: Policy Information Point**
Fornisce gli attributi al PDP



Esempio di esecuzione:

1. L'amministratore deve definire le politiche via PAP.
2. Il soggetto richiedente richiede l'accesso. La richiesta è intercettata dal PDP, che la redirige verso il context handler; non è sempre presente ma serve quando le richieste di accesso non sono generate direttamente in XACML. Il context handler quindi prende la richiesta e la trasforma nel formato standard, per poi mandarla al PDP.
3. Il PDP può richiedere al context handler di fornire gli attributi.
4. Il context handler contatta il PIP, che recupera gli attributi dal sistema di identità digitale e si occupa anche di recuperare gli attributi del contesto e della risorsa.
5. Il PDP decide se garantire l'accesso o meno in base al valore degli attributi e restituisce la risposta al PEP.
6. Nella risposta è possibile includere le obbligazioni, ovvero azioni da eseguire per il PEP in concomitanza al garantire l'accesso. (Per esempio, potrebbe dover mandare una email all'owner della risorsa acceduta, o di creare un log).

Ci sono vari scenari di implementazione:



Formalizzazione

La formalizzazione delle politiche avviene attraverso due componenti: **politiche e regole**. Una politica è costituita da una o più regole. Ciascuna regola va valutata come parte di una policy; quindi non avrà mai una decisione indipendente da una regola.

Le regole e le politiche hanno il <target>, che associa la risorsa e la richiesta di accesso della risorsa. Il target può contenere le condizioni, specifici:

- <Match>: sono le condizioni
- <AnyOf> e <AllOf> combinano le condizioni in maniera intuitiva.

Esempio:

```
<Target>
<AnyOf>
<Match MatchId = "urn:oasis:names:tc:xaml...:string-equal">
<AttributeValue DataType = ...> Pamoda <.../>
<AttributeDesignator AttributeId = .../>
= l'attributo subjectID deve essere Pamoda
```

...

La richiesta deve essere di tipo Pamoda.

Una regola ha tre componenti:

- Target: se no n c'è applico a tutto
- Condizione <Condition> ha dentro un <Apply> con la condizione.

...

Ci sono 4 tipi di algoritmi:

- Deny: se nella politica ho una regola le cui condizioni sono soddisfatte, allora l'effetto di valutare quella politica sarà di negare l'accesso.
- Permit: Se ho anche solo una regola valutata a permit, allora l'intera politica è permit.
- First applicable: valuta le regole della politica nell'ordine della politica. L'effetto è uguale all'effetto di valutare la prima regola che incontriamo.

... non ho capito tbh. Potrei cambiare l'algoritmo...?

<https://medium.com/identity-beyond-borders/a-beginners-guide-to-xacml-6dc75b547d55>

User managed access (OAUTH)

E' l'utente a garantire o meno accesso alle sue risorse. È utile per contesti tipo i social o la smarthome.

Abbiamo bisogno di un protocollo che assicuri che solo alcune applicazioni possano accedere a queste cose.

È un protocollo usato per esempio quando facciamo il SSO con google o facebook.

Esiste un'entità (authorization server) che rilascia un access token quando l'utente garantisce l'accesso alle proprie risorse usando quella specifica applicazione. (Es. vuoi permettere a XXX di accedere al tuo nome/cognome?)

- **Resource Owner:** entity capable of granting access to a protected resource
- **Resource Server:** the server that stores that resource owner resources
- **Authorization Server:** the server issuing access token to the client after authenticating the resource owner and obtaining its authorization
- **Client:** a third-party application that requests access to protected resources on-behalf of resource owner and with its approval

Esempio: accesso a spotify via facebook



Resource Owner



Client Application



Authorization Server/
Resource Server



Protected Resources

Quindi:

- Protected resources: credenziali
- Application: spotify
- Authorization server: facebook

Spotify vuole un access token da facebook per accedere alle credenziali.

Oauth supporta tre scenari in base allo scenario

- L'applicazione è rilasciata da un service provider diverso da chi fornisce l'authorization server
- La client application è dello stesso fornitore dell'authorization server
- L'applicazione accede ai dati per conto di sé stessa, anziché per conto di un utente.

ESEMPIO:

- Resource owner



- Protected resources



- Client application (fornita da SHIELD)



- Authorization server/ resource server: Gerbis



1. Mysuite redirige tony all'interfaccia dell'authorization service. Nella registrazione specificiamo il nome dell'applicazione e un URI per dire dove redirigere l'utente quando egli ha garantito all'applicazione l'accesso a ironman. + il tipo di autorizzazione
2. Gervis manda due informazioni: ID dell'app e una password condivisa fra app e auth server
3. Tony crede a Jarvis di accedere a ironman. Specifica cosa serve (access token), client id (ottenuto prima) e il redirect URI.
scope specifica la risorsa a cui ottenere accesso
State è un numero casuale generato per evitare attacchi
4. Tony si autentica con l'authorization service e viene generato l'authorization code. Questo codice è la prova che tony è tony; continuo a includere il numero casuale.
5. Tony può richiedere l'access token e specifica
6. Mandiamo token e refresh token per ottenere nuovi access token senza rieseguire il tutto

Ciò si applica se i due fornitori sono diversi

SECONDO FLUSSO: stesso fornitore

(no.)

TERZO SCENARIO: client credential grant flow

(no fra ho sonno)

Exercise 1 – HomeBanking Application

- Alice has a bank account at MyBank
- MyBank provides Alice with a mobile app MyBankApp through which she can access her account balance and credit card/debit card transaction history
- MyBank issues Alice with a login and password to access the MyBankApp
- Think about:
 - Who are the actors?
 - What are the protected resources?
 - What grant flow would you use?

Esempio:

- Resource owner: alice
- Resource server: mybank
- Auth server: mybank
- Client:mybankapp
- Scenario2 (stesso servizio)

Exercise 2 – Smart Home

- Alice lives in a smart home with a smart lighting system
- Alice can control her smart light system with MyBulb mobile app
- The smart light systems exposes APIs to switch/on and off the smart bulbs that are part of the system
- Think about:
 - Who are the actors?
 - What are the protected resources?
 - What grant flow would you use?
- Time: 5 min

Same ma è il primo flow.

S10 - Seminario Sababa

Shadow brokers → whistle blowers

Gli attori sono una amrea e ci sono un sacco di casi

- Wannacry → attacco alla banca del bangladesh, gruppo coreano

I moderni attori non sono altro che un evoluzione storica di quanto visto nelle slide precedenti:

- **Utilizzando strumenti informatici per carpire informazioni**
- 1. **Furto/manipolazione di dati**
- 2. **Investimento in società digitali e di cybersecurity**
- 3. **Apparato normativo (Patriot Act in US, equivalenti in EU, Russia, Cina e altri)**
 - Utilizzando strumenti informatici per azioni di Sabotaggio (No-Petya, Stuxnet,..)
 - Utilizzando strumenti informatici per influenzare l'opinione pubblica (fake news), o l'opinione di persone/gruppi di persone specifiche (targeted fake news)
 - Utilizzando cyber attacchi per finanziare la nazione (WannaCry)
 - Conquistandosi insiders e whistleblower (Snowden vive in Russia)

→ stuxnet è il primo a non eseguire nessuna delle azioni tipiche, ma a manomettere fisicamente le turbine!

Gli piace tanto l'acciaio 😊😊😊 In

Zero day → 1M sul mercato nero, oppure una responsible disclosure per farla patchare, oppure bug bounty.

Blue team → “difensori” del sistema

Red team → penetration testers

“l'università dei magici hackers”

11 - Introduzione alla privacy

Effettivamente, negli scorsi anni siamo passati online per quasi tutto:

Conversazioni faccia a faccia	→	Instant messaging
Lettere	→	Email
Cash	→	Credit cards
Inseguimento	→	Tracking della posizione
Ricerche su libri	→	Ricerca su google
Conoscere gli amici di qualcuno	→	Social network graph

La privacy è preda di diversi predatori:

- **Surveillance capitalism:** concetto sviluppato da Shoshana Zuboff. Il capitalismo reclama qualcosa da fuori del mercato per venderlo e comprarlo; nel caso del surveillance capitalism, ciò che viene reclamato è la **private human experience**, e viene venduta e comprata come "behaviourial data".
- **Sorveglianza dei governi:** programmi di sorveglianza collettiva come PRISM (denunciato da Snowden ❤️).
- **Data leak:** enti privati, quali google e facebook, sono tenuti a tenere i dati al sicuro ma sono spesso soggetti a data breach.

Dall'altro lato, ci sono anche delle iniziative che cercano di aiutare a garantire la privacy:

- **GDPR:** definisce i principi secondo i quali chi raccoglie i dati personali deve seguire per garantire il minimo rischio
- **Tor:** è un browser che permette di navigare in maniera completamente anonima.
- **Privacy badger:** previene l'online tracking. Quando visitiamo un sito web il contenuto è caricato da diversi fornitori, e alcuni provengono dagli advertiser; a volte carichano del contenuto che permette di tracciare quali siti web sono stati visitati. Questa iniziativa è finalizzata a bloccare il tracking delle attività online, identificare e bloccare l'esecuzione dei tracker.
- **Dp³t:** protocollo sviluppato da centri di ricerca europei con lo scopo di consentire il tracciamento dei contatti senza rivelare identità degli utenti coinvolti.



Dati personali

Il GDPR dice che i dati personali sono **qualsiasi informazione che rende un individuo identificato o identificabile**. Può essere identificazione **diretta** (nome, cognome, CF) o un'info **indiretta**, che anche se non associa nome cognome permette di distinguere l'individuo dagli altri. Un esempio è l'indirizzo IP, perché permette di monitorare quello che facciamo attraverso quel computer.

Attori

Le entità fondamentali sono:

- **Data subject (DS)** : l'individuo a cui si riferiscono i dati
- **Data controller (DC)** : entità che raccolgono i dati, decide lo scopo della raccolta e come saranno processati.

Definire il concetto di privacy

Non è semplice definire la privacy in quanto è un concetto che può avere un significato diverso per ciascuno di noi. Questo problema è stato catturato da Andrew Solev:

Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from “an embarrassment of meanings”.

Di conseguenza, nel corso della storia sono state date diverse definizioni.

1890: the right to be let alone (Warren and Brandeis)

Arriva in risposta a due innovazioni: giornali scandalistici e macchina fotografica. La vedono come volontà di non rendere pubbliche foto personali. È la stessa definizione di confidenzialità attuale.

1970: diritto dell'individuo di decidere quale quando el proprie informazioni devono essere pubbliche (Wenstinst)

È alla base di molte leggi attuali: vogliono che sia l'individuo a poter decidere

1970: tassonomia della compromissione della privacy (Solove)

Non definisce la privacy in quanto troppo personale; definisce le attività che però la ledono.

2001: the freedom from unreasonable constraints on the constructions of one's identity (psicologi Agre & Rotenberg)

Si applica a quei governi dove c'è la surveillance. Se un individuo sa che le proprie conversazioni sono monitorate, sarà condizionato su quali informazioni condividere. Oppure, in ambito social network, c'è il caso del cyberbullismo che settano degli standard per come un adolescente vuole apparire online e portano l'adolescente a non essere libero di esprimersi per evitare ripercussioni.

2004: Privacy as Contextual Integrity

Lega la privacy al contesto. In un contesto potrebbe essere appropriato condividere informazioni che, in altro contesto, non verrebbero condivise. L'appropriatezza è data da delle norme che definiscono come essi sono protetti. Per esempio in ambito medico è appropriato condividere info sulla salute. In altro contesto, tipo forum pubblico dove si parla di patologie, magari non c'è norma che garantisca la privacy e potrebbe essere rischioso condividere altrettante info.

2018: Transparency, purpose, proportionality, accountability (GDPR)

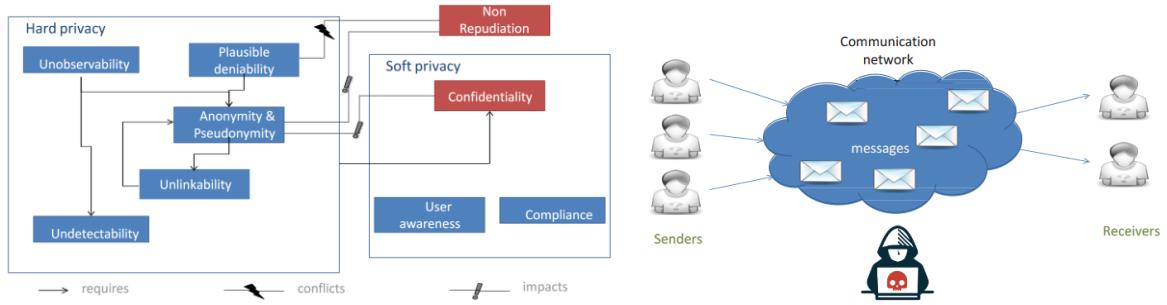
- **Trasparenza:** quando un data controller raccoglie i dati, deve specificare per quale motivo li raccoglie e come li tratterà o condividerà.
- **Purpose:** deve specificare il motivo per cui li raccoglie
- **Proportionality:** devono essere proporzionali e finalizzati al purpose; non devo raccogliere più dati del necessario
- **Accountability:** il data controller deve mantenere traccia di chi ha accesso ai dati.

Classificazione della privacy

Sono suddivise in base a due macrosuddivisioni:

Hard Privacy	Soft Privacy
<p>Parte dall'idea che il data controller non è un'entità affidabile, quindi il data subject deve condividere meno dati possibili.</p> <p>Significa anche che è il data subject a doversi proteggere, per esempio cifrando i propri dati prima di trasmetterli.</p>	<p>Il DS si fida del data DC, e quindi lascia che sia lui ad adottare le misure di protezione.</p>

Questi due scenari sono caratterizzati da una serie di proprietà, definite rifacendosi ad un preciso modello di attaccante – ovvero un attore sulla rete che ha l'obiettivo di individuare degli item of interests (IOI).



Proprietà

Anonymity	C'è se nel nostro sistema non possiamo associare l'identità di un utente a un certo IOI (che può essere un'azione o informazione personale). Va considerata rispetto a un insieme →→ → Ad esempio, un attaccante non riesce a determinare quale attore ha spedito o ricevuto un messaggio	A diagram showing a central cloud labeled 'Communication network' containing 'messages'. It is connected to four user icons. Two icons are grouped together and labeled 'Sender anonymity set', while the other two are labeled 'Receiver anonymity set'.
Pseudonymity	Anziché usare il vero nome per identificare un soggetto uso un ID casuale. Questo però comporta che se abbiamo un utente che usa sempre lo stesso pseudonimo siamo comunque in grado di tracciarlo.	
Unlinkability	Si nasconde la presenza di un link tra due IOI. Supponiamo di avere un attaccante che osserva la rete. Se la proprietà è soddisfatta, l'attaccante non vede se due messaggi sono mandati dallo stesso utente o se sono nella stessa sessione di comunicazione. Può essere usata anche per definire l'anonymity: come unlinkability fra un utente e le sue azioni.	
Undetectability	Garantisce che se un attaccante guarda la rete non riesce a capire se un IOI esiste o meno <ul style="list-style-type: none"> ○ Ad esempio, non sa se un messaggio è stato mandato o se è solo rumore. L'attaccante e gli utenti non coinvolti non si accorgono neanche dell'esistenza della comunicazione, mentre sender e receiver sì. 	An icon showing a document with a question mark next to it, and a stack of three coins.
Unobservability	assume che l'undetectability sia vera per tutti i soggetti non coinvolti nella trasmissione, ma aggiunge l'anonymità di soggetto ricevente e mittente. Mittente non sa chi è il ricevente e ricevente non sa il mittente.	An icon showing a stack of three coins with a question mark next to it, and a user icon with a question mark.
Plausible deniability	Garantisce che un utente può negare di aver compiuto un'azione (essere presente in un luogo, aver visitato una pagina...) È desiderabile in un ambiente di online voting, ma in sistemi in cui effettuo pagamenti online preferisco avere la non-replication (ovvero che io mantengo traccia).	
Confidentiality (DC)	È responsabilità del data controller porteggiere i dati da un accesso non autorizzato. Si traduce nel garantire che i dati sono cifrati o l'accesso è controllato.	
Compliance (DC)	Rispettare i principi dettati dalle leggi	
Awareness (DS)	L'utente deve essere a conoscenza delle conseguenze delle proprie azioni.	

Minacce alla privacy

Solove definisce una tassonomia precisa delle minacce alla privacy.

Informaiton collection

- **Surveillance:** monitoring delle attività dell'individuo
 - Smart contatori :') permettono di pagare di meno perché danno info molto precise su quanto consumiamo, per esempio un singolo dispositivo. Problem: paghiamo meno ma è possibile per i fornitori analizzare i consumi e infierire informazioni su di noi, tipo quanto ci laviamo o quando siamo a casa.
 - Smart tv
 - Angry birds era usata dalla NSA inglese per catturare info!
- **Interrogation:** le informazioni sono estorte dall'individuo, forzandolo a dare info che normalmente non fornirebbe.
 - Probing: phishing che richiede agli utenti di resettare il login

Information processing

- **Aggregation:** il DC raggruppa le informazioni su un individuo da diverse sorgenti, e impara nuove informazioni che l'individuo non pensava sarebbero state inferite.
 - Target americano ha predetto che una tipa era in cinta e mandava i coupon della roba.
- **Identification:** il DC raggruppa le informazioni e riesce a trovare l'identità del soggetto
 - Raccoglie i dati dei click di un individuo e determinava nome e cognome.
- **Insecurity:** il DC non adotta le misure di sicurezza necessarie per prevenire un accesso
- **Secondary use:** il DC raccoglie i dati per uno scopo e poi li riutilizza per qualcos'altro.
 - Cambridge analytica: genera profili psicologici poi usati per influenzare la campagna elettorale in america
- **Esclusione:** l'utente non ha visione di quali sono i dati raccolti dal DC.

Information dissemination

- **Breach of confidentiality:** c'è un accesso non autorizzato
 - Equifax: società di recupero crediti che analizzava il credit store.
- **Disclosure:** info di una persona sono divulgate.
- **Exposure:** resa pubblica di foto o altro intime
 - Icloud nel 2014 che dissemina i nudini di attrici americane.
- **Increased accesibility:** si aumenta l'audience
- **Blackmail:** minaccia di rendere pubblica e si chiede il riscatto
 - Ransomware per non pubblicare le info
- **Appropriation:** usiamo i dati personali per impersonare qualcuno
 - Reti sociali go brrr
- **Distortion:** diffusione di info false per cambiare opinione agli altri
 - Troll che si divertono a sparare troiate

Invasion

- **Intrusion:** Sono situazioni dove altri individui o governi interferiscono con la vita privata.
 - Reti sociali e stalking: femminicidi nonostante ordini restrittivi dove l'assassino fa stalking attraverso i social.
 - Cyberbullismo: ripercussioni notevoli fino al suicidio
- **Decisional interference:** involves the government's incursion into the data subject's decisions regarding her private
- **Affairs**

PETS: privacy enhancing technologies

Permettono di proteggere la privacy. Possono essere applicate sia dal DC che dal DS. Possono essere applicate a livello di rete, browser, database...

Data protection technology

Lo scopo è garantire la compliance con i principi del GDPR. Sono tipicamente adottati dal DC.

- **Cifratura:** i dati personali devono essere protetti e cifrati sia dal DC che quando il DC li trasmette.
- **Autenticazione** e autorizzazione degli utenti
- **Mantenimento dei log** (magari con Log4J per aggiungere un po' di)
- **Interfaccia agli utente per cancellare i propri dati** (right to be forgotten)
- **Purpose-based control:** un dato può essere acceduto solo se lo scopo per cui accedo è lo stesso scopo per cui ho raccolto il dato.

L'assunzione è che il DC sia un ente affidabile, e non ci fidiamo degli attaccanti esterni che potrebbero voler accedere ai dati personali. Obv non ho garanzia che il DC non usi i dati per scopi diversi!

User awareness technologies

- **Privacy friendly defaults:** bisognerebbe usare di default settings che proteggono i dati (es. in automatico i post dovrebbero essere condivisi con poche persone)
- **Tool per capire con chi stiamo condividendo** (tipo facebook mirror per vedere il profilo da altri punti di vista).
- **Interfacce che semplificano la privacy** (es. interfaccia per i privacy settings).
- **Privacy policy comprensibili.**
- **Privacy nudges:** vedere quante volte un'info è stata condivisa e con chi.

Anonymity technologies

- **Assicurare l'anonymity**
 - K-anonymity in un database per non capire il record legato a un individuo
 - Anonymous communication per navigare indistrubati – Tor
 - Anonimità in autenticazione: idemix (un utente prova che possiede un segreto senza rivelarlo).

Altre tecnologie

- **Memorizzazione sicura sul cloud**
 - Esempio: privateStorage fornisce una cifratura lato client – i dati sono cifrati prima di uploadare e la chiave simmetrica è solo offline per il client.
- **Searchable encryption:** cercare se un documento cifrato ha delle parole chiave e recuperare i documenti positivi.
- **Computazioni su dati cifrati**
 - Homomorphic encryption: calcolo di funzioni su dati cifrati. Al momento non esiste :')
 - Secure multiparty computation: un insieme di utenti che vogliono calcolare una determinata funzione sulla base di input di ciascun utente, ma vogliono anche mantenere privati gli input.

12 - Metodologia LINDDUN

- Cosa significa privacy by design?
- Come identificare i problemi di privacy?
- Come mitigarli?

- LINDDUN è una metodologia di modellazione che aiuta i SW engineers con poca esperienza in ambito privacy a mitigare i problemi
- Contiene della conoscenza: tassonomia delle minacce alla privacy, cataloghi delle threats sotto forma di alberi, e mitigazioni per ciascuna minaccia.

LINDDUN: metodologia che permette di identificare possibili attacchi e mitigazioni. È una metodologia:

- **Model based:** l'analisi parte dal creare un modello grafico del sistema
- **Knowledge based:** per fare in modo che anche ingegneri che non hanno una solida conoscenza del concetto di privacy possono identificare i principali attacchi e le soluzioni. Si realizza tramite una tassonomia (LINDDUN) degli attacchi, e per ciascuna categoria una lista di mitigazioni.

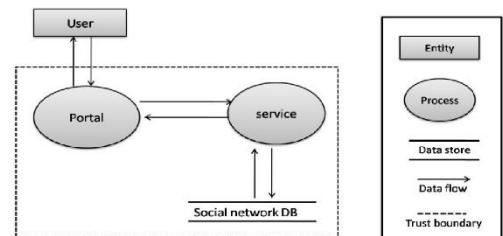
Tre fasi principali:

1. Modellazione del sistema via data flow diagrams
2. Identifichiamo per ciascun elemento i possibili attacchi
3. Valutazione del rischio associato agli attacchi (e individuazione delle mitigazioni)

1. Creare il modello del sistema

Noi usiamo un esempio di rete sociale. Ingredienti :

- **Entità:** utenti di sistema o della rete sociale, o ancora servizi che possono interagire.
- **Processi**
- **Data store:** dove salvo i dati
- **Data flow:** come le informazioni sono date in input e processate
 - Nell'esempio: interazione utente-portale, portale-servizio, servizio-DB
- **Trust boundary:** identifica le componenti del sistema di cui possiamo fidarci (aka che non saranno soggette ad attacchi).



a. Identifichiamo gli attacchi che si applicano.

Threat	Privacy property	LINDDUN considera attacchi per ciascuna delle threat viste la volta scorsa, strettamente collegati ai principi di privacy già visti.
Linkability	Unlinkability	
Identifiability	Anonymity, Pseudonymity	
Non repudiation	Plausible Deniability	
Detectability	Undetectability	
Disclosure of information	Confidentiality	
Unawareness	Awareness	
Non compliance	Compliance	

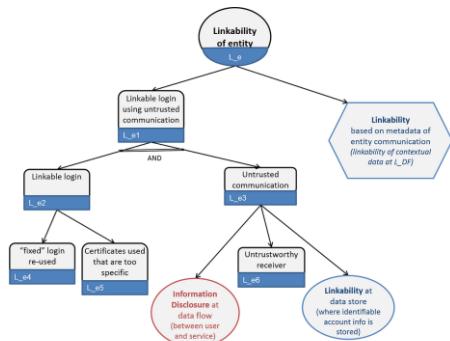
	L	I	N	D	D	U	N
External Entity	X	X				X	
Process		X	X	X	X		X
Data Store		X	X	X	X		X
Data Flow	X	X	X	X	X		X

	L	I	N	D	D	U	N
Social Network DB	X	X			X		X*
User -Portal	X	X			X		X*
Portal - Service							X*
Service – Social Network DB							X*
Portal							X*
Service							X*
User	X	X			X	X*	

Ciascuna delle entità viste può essere vulnerabile ai seguenti attacchi:

Con questa tabella alla mano, per ciascuno degli elementi della prima tabella genero un riassunto di a quali rischi è effettivamente esposto ciascun componente nella nostra rete. Consideriamo fidati gli elementi interni alla trust boundary, service e portal, eccetto il DB.

Infine per ciascuna delle X bisogna identificare esempi concreti. La metodologia ci aiuta con un catalogo di attacchi available at <https://www.linddun.org/>, separati in 150 mila alberelli.



DFD Element	Threat Type	Threat tree leaf nodes
User	Linkability	<ul style="list-style-type: none"> - Fixed login re-used (L_e4) - No message confidentiality (ID_df4) - No channel confidentiality (ID_df7)
	Identifiability	<ul style="list-style-type: none"> - Username and password used as login (L_e12) - Weak password (L_e17) - Weak username (L_e18) - No message confidentiality (ID_df4) - No channel confidentiality (ID_df7)
	Unawareness	<ul style="list-style-type: none"> - No user-friendly privacy support (U_4))

2. Documentare gli attacchi

Si può usare un template fornito sempre dagli amici del LINDUNN. Altrimenti posso avere i misuse case, dove ho la prospettiva dell'attaccante del sistema.

Template	Misuse case
<p>MUC01: Linking data Summary: Data entries can be linked to the same person Assets, stakeholders, and threats*: By combining the entries, the misactor has access to more information Primary misactor: skilled insider/skilled outsider Basic Flow: Bf1. The misactor gains access to the database Bf2. Because too much data are stored, information can be inferred Leaf node(s)*: Lds_1, Lds_6 Root node(s)*: L_d DFD Elements*: Social network data store (4)</p>	

3. Quantificazione del rischio

LINDUNN non dà un modo preciso, ma ci rimanda ad altri metodi di risk assessment, come la Owasp: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

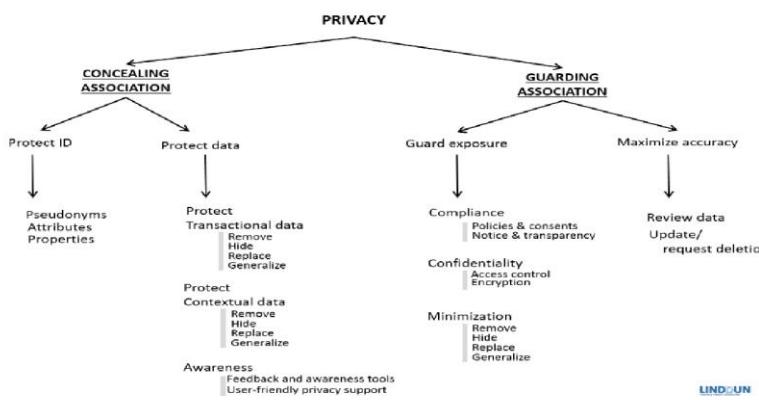
Identifichiamo, per ciascuna delle categorie, un valore da 0 a 9:

	Threat agent factors	<ul style="list-style-type: none"> • Skill level: quanto skillati sono gli agenti? • Motive • Opportunity • Size
Stima del rischio	Vulnerability factors	<ul style="list-style-type: none"> • Ease of discovery: quanto è facile per gli agenti sgambarare la vulnerabilità • Ease of exploit • Awareness: quanto bene si conosce questa vulnerabilità • Intrusion detection: quanto è facile sgambarare? Abbiamo log o detection attiva?
Stima dell' impatto	Lato tecnico	<ul style="list-style-type: none"> • Loss of confidentiality • Loss of integrity • Loss of availability • Loss of accountability
Stima dell' impatto	Lato buisness	<ul style="list-style-type: none"> • Danno economico • Danno alla reputazione • Violazione di regolamentazioni e leggi • Violazione della privacy

Assegnato un punteggio, bisogna combinarli per avere un punteggio unico; calcolo valore medio di ciascuna delle due categorie, e poi medio questi due risultati. Infine per calcolare il rischio uso questa tabella

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

4. Mitigare il rischio



Tutto questo è ispirato da Microsoft Stride, che è l'equivalente lato sicurezza. Per entrambi esistono giochi di carte.

13 - Data anonymisation

Problema

Spesso le organizzazioni **condividono i dataset con altre organizzazioni** al fine di **analizzare i dati**. Vogliamo però garantire che l'analisi non compormetta la privacy di nessuno degli individui. Se non si adottano misure appropriate, è possibile che un attaccante inferisca:



- **Reidentification:** chi è ciascun paziente
- **Inferenza di altre info:** per esempio quale sia la sua patologia

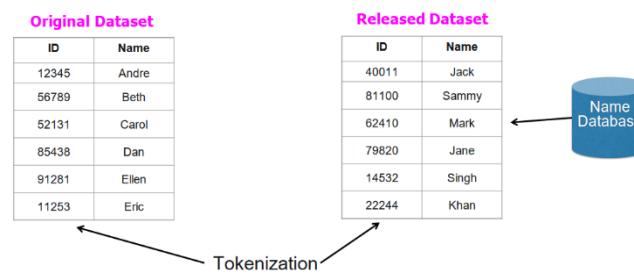
Di solito su un dataset abbiamo:

- **Identificativi esplicativi:** nome, codice fiscale, passaporto numero, CDI numero
- **Quasi-identifier:** sono attributi che possono essere presenti all'interno di dataset pubblici come data di nascita, età, indirizzo...
Se combino queste info con quelle di dataset pubblici posso reidentificare un individuo
- **Attributi sensitivi** (🍪): malattia, stipendio...

Key Attributes		Quasi-identifiers		Sensitive attributes	
ID	Name	DOB	Gender	Zipcode	Disease
12345	Andre	1/21/76	Male	53715	Heart Disease
56789	Beth	4/13/86	Female	53715	Hepatitis
52131	Carol	2/28/76	Male	53703	Bronchitis
85438	Dan	1/21/76	Male	53703	Broken Arm
91281	Ellen	4/13/86	Female	53706	Flu
11253	Eric	2/28/76	Female!!!	DOB è quasi identifier !!!	

Per proteggere questi dati ho diverse tecniche:

- **Sostituzione:** Sostituisco alcuni attributi identificativi con degli altri valori; es sostituisco tutti i nomi con nomi comuni
- **Tokenizzazione:** sostituisco il valore numerico con un numero totalmente casuale.



Tutto questo non basta: AOL, google di una volta, per scopi di ricerca rendeva pubblico i dataset con le ricerche dei vari utenti. Per rendere il dataset anonimo aveva sostituito gli usernames con un numero casuale. Due giornalisti del NYT, in poche ore, guardando le ricerche e legando più ricerche fatte dallo stesso utente, riescono a reidentificare le persone; ad esempio una signora georgiana vedova con tre cani. :')

Un altro esempio è natanya swene (?), ricercatrice che poi propone la k anonymity. Avendo a disposizione un dataset con tutti i dati dei cittadini che avevano votato, e a un altro in cui erano stati tolti il SSN e il nome di un'agenzia di assicurazioni per tenere traccia dei rimborsi, incrociò i dati e sgama il governatore del massachusetts 😞

K-anonymity

Un database dovrebbe essere diviso in classi di equivalenza dove i quasi-identifiers hanno tutti lo stesso valore, e devono esserci almeno K records con lo stesso valore.

Se ho un dataset con un insieme di valori tutti con lo stesso quasi identifier, è più difficile reidentificare; la probabilità sarà $1/k$, quindi se ho pochi record con lo stesso valore nei quasi identifiers avrò una probabilità elevata di reidentificare un individuo.

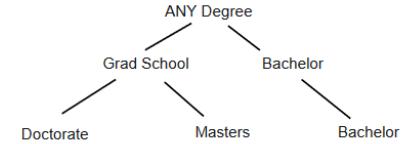
Esempio

Original Database				Released Database		
Name	Zipcode	Age	Disease	Zipcode	Age	Disease
Hilary	47677	29	Heart Disease	476**	2*	Heart Disease
Jenny	47602	22	Heart Disease	476**	2*	Heart Disease
Bob	47678	27	Heart Disease	476**	2*	Heart Disease
Izzy	47905	43	Flu	4790*	≥40	Flu
John	47909	52	Heart Disease	4790*	≥40	Heart Disease
Fred	47906	47	Cancer	4790*	≥40	Cancer
Sam	47605	30	Heart Disease	476**	3*	Heart Disease
Carl	47673	36	Cancer	476**	3*	Cancer
Sarah	47607	32	Cancer	476**	3*	Cancer

Sostituisco tutto il valore di zipcode età con un valore più generale, per soddisfare la condizione di avere k records con lo stesso valore. Per esempio, qui ho tre valori!

Ci sono due tecniche utilizzate:

- **Generalizzazione:** prendo un valore e lo sostituisco con un valore che è più generale; quindi se ho un valore numerico come l'età lo sostituisco con un intervallo, o se ho una stringa definisco una gerarchia di valori e prendo qualcosa di più generale
- **Soppressione:** elimino direttamente il record (perché generalizzando è comunque troppo specifico)



Bisogna bilanciare la privacy con l'utilità dei dati, perché per esempio tolgo FLU in quanto unico poi non mi risulta nelle analisi!

Esempio

Per trovare K devo vedere quante righe hanno i quasi identifier uguali; per k-anonimizzarlo posso sopprimere il nome e la religione (in quanto non rilevante), e generalizzare l'età

Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yad	24	Female	Kerala	Hin	Viral infection
Sallie	28	Female	Tamil Nadu	Muslin	TB
Sumi	27	Male	Karnataka	Par	No illness
Joan	24	Female	Kerala	Chri	Heart-related
Bahusana	23	Male	Karnataka	Budhist	TB
Ramya	19	Male	Kerala	Hind	Cancer
Kish	29	Male	Karnataka	Hin	Heart-related
Johnson	17	Male	Kerala	Christia	Heart-related
John	19	Male	Kerala	Christian	Viral infection

Attacchi contro la K anonymity

La k anonymity non è comunque una soluzione perfetta:

- **Homogeneity:** Se non ho eterogeneità nel sensitive data, lo sgamo uguale!
Il valore dell'attributo sensitivo è uguale per tutti i k record 😞
- **Background knowledge:** i giapponesi hanno meno probabilità di sviluppare problemi di cuore; quindi può escludere heart disease e concludere che ha il cancro.
L'attaccante ha delle informazioni aggiuntive e riesce a escludere alcuni valori facendo inferenza

Homogeneity attack

Bob	
Zipcode	Age
47678	27

Background knowledge attack

Umeko	
Zipcode	Age
47673	36

A 3-anonymous patient table

Zipcode	Age	Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
4790*	≥40	Flu
4790*	≥40	Heart Disease
4790*	≥40	Cancer
476**	3*	Heart Disease
476**	3*	Cancer
476**	3*	Cancer

Insomma, K anonymity fornisce un certo tipo di protezione dalla reidentificazione, ma non protegge da attacchi in cui si fa inferenza sui valori dell'attributo sensitivo a causa del fatto che il valore è lo stesso.

L-diversity

Tale Machanavajjhala lo propone nel 2006: il valore dell'attributo deve essere distinto in ciascun record di classe di equivalenza.

Distinct L-diversity

Ad esempio, in questa classe di equivalenza, abbiamo L=3 ma comunque è facile inferire cose: ho altissima probabilità che la risposta sia HIV...

...	Disease
	HIV
	Bronchitis
	Pneumonia

8 records have HIV
2 records have other values

Entropy L-diversity

I valori dell'attributo sensitivo non solo devono essere diversi, ma anche la distribuzione dei valori dell'attributo sensitivo deve essere la stessa. Lo si traduce con l'entropia: per ogni classe di equivalenza definiamo entropia la somma di tutti i valori che l'attributo può assumere

Entropy ℓ -diversity. The entropy of an equivalence class E is defined to be

$$\text{Entropy}(E) = - \sum_{s \in S} p(E, s) \log p(E, s)$$

in which S is the domain of the sensitive attribute, and $p(E, s)$ is the fraction of records in E that have sensitive value s .

L'entropia è soddisfatta se l'entropia è \geq del logaritmo di L .

Esempio

Similarity attack

Bob	
Zip	Age
47678	27

A 3-diverse patient table

Zipcode	Age	Salary	Disease
476**	2*	3K	Gastric Ulcer
476**	2*	5K	Gastritis
476**	2*	9K	Stomach Cancer
4790*	≥40	6K	Gastritis
4790*	≥40	100K	Flu
4790*	≥40	70K	Bronchitis
476**	3*	60K	Bronchitis
476**	3*	80K	Pneumonia
476**	3*	90K	Stomach Cancer

Conclusion

1. Bob's salary is in [3k,9k], which is relatively low
2. Bob has some stomach-related disease

l-diversity does not consider semantics of sensitive values!

→ La L diversity non realizza/considera che sono tutte cose semanticamente simili

Esempio2

- 1 e 1 vuol dire che ho 50% di azzeccarci che sia + o -!
- Queste due classi rispettano la definizione, ma la seconda mi dice per certo che è positivo!!!

- Example: sensitive attribute is HIV+ (1%) or HIV- (99%)
- Consider an equivalence class that contains an equal number of HIV+ and HIV- records
 - Diverse, but potentially violates privacy!
- l-diversity does not differentiate:
 - Equivalence class 1: 49 HIV+ and 1 HIV-
 - Equivalence class 2: 1 HIV+ and 49 HIV-

l-diversity does not consider overall distribution of sensitive values!

→ La L diversity non tiene conto della distribuzione all'interno dell'intero dataset.

t-closeness

La distribuzione di attributi sensibili dentro ciascun quasi-identifier deve essere vicina alla distribuzione di questo attributo nell'intero database.

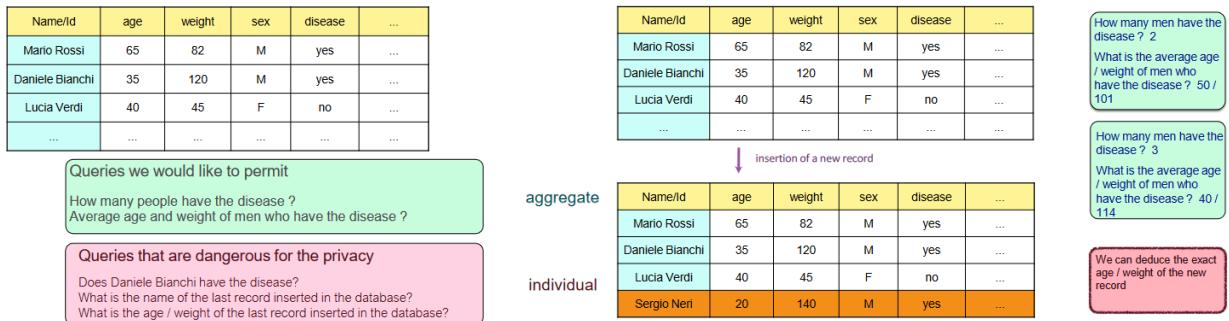
Query predefinite

Conclusione: anonimizzare i dati non è sicuro, perché non ci protegge da vari attacchi (attribute disclosure), e in più è difficile da implementare.

Quindi, una soluzione alternativa è consentire solo delle query sui dati. Tipicamente le query restituiscono dati aggregati, tipo “quanti soggetti hanno patologia X?”, o l’età media dell’utente con una certa malattia. O infine algoritmi di machine learning.



Anche questo approccio ha dei problemi.

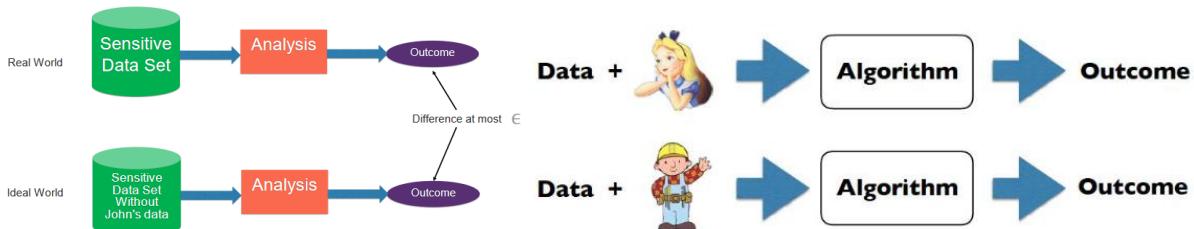


→ non funziona.

Privacy differenziale

Al contrario delle altre non è una tecnica ma una proprietà che deve soddisfare l’algoritmo di analisi.

Se io prendo il dataset e faccio l’analisi, e poi tolgo quel record, il risultato deve essere molto simile; in questo modo preservo la privacy e ho anche un’analisi utile.



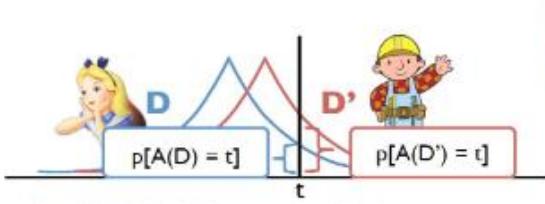
Esempio

So che Alice fuma. E ha partecipato a uno studio dove correlano profilo genetico con l’avere il cancro, pubblicando dataset

Il secondo no viola la privacy:

- I dati di alice non ci sono
- Quello che bob inferisce è basato su info di pubblico dominio e che non mi danno una certezza, oltre ad essere generico su molte persone (tutte quelle che fumano). La privacy differenziale infatti assume che il rischio di privacy non sia 0, ma sempre molto basso (tanto che qui posso infierire dati pur non utilizzando proprio i dati di alice nel secondo studio).

Formalmente:



For all D, D' that differ in one person's value,
If $A = \epsilon$ -differentially private randomized algorithm, then:
Max-divergence of $p(A(D))$ and $p(A(D'))$

$$\sup_t \left| \log \frac{p(A(D) = t)}{p(A(D') = t)} \right| \leq \epsilon$$

Un algoritmo è differentiamente privato se il rapporto tra la probabilità che l'algoritmo calcolato su $D = t$ e la probabilità che lo stesso algoritmo calcolato su D' mi dia T (tutto in valore assoluto) deve essere \leq di ϵ .

Proprietà

Post processing variance		Se faccio un'analisi differentiamente privata e sul risultato applico un altro algoritmo, anche il risultato del secondo rimane differentiamente privato (se non processo più i dati dal database)
Robustness under composition		Se prendo il dataset ed eseguo diverse analisi, il rischio sarà al più il rischio di ciascuna analisi singola <i>Esempio</i> Gertrude partecipa a studio con $\epsilon = 0.01$ Poi gli studiosi fanno un altro studio con $\epsilon = 0.02$. Il rischio totale è al più 0.03.

Implementazione

Uno dei metodi più usati è la global sensitivity, che usa la distribuzione di Laplace.

Given: A function f , sensitive dataset D
Define: $\text{dist}(D, D') = \#\text{records that } D, D' \text{ differ by}$

Global Sensitivity of f :

$$S(f) = \max_{\text{dist}(D, D') = 1} |f(D) - f(D')|$$

Prendo il valore della funzione e lo perturbo con del random noise, prendendolo da una variabile con una distribuzione di Laplace.

La global sensitivity è la differenza fra il valore della funzione fra il dataset e un altro dataset in cui cambia un record.

Per avere una f che soddisfa la privacy differenziale, prendo il valore $f(D) + Z$ (rumore) che ha una

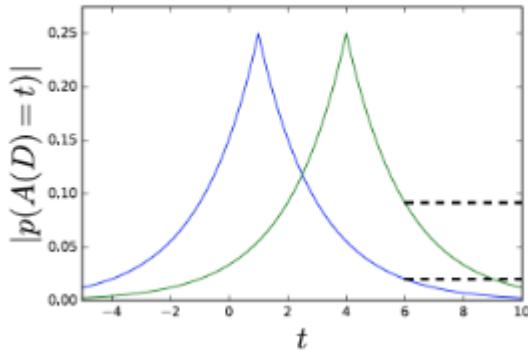
$$Z \sim \frac{S(f)}{\epsilon} \text{Lap}(0, 1)$$

distribuzione pari a con

Laplace distribution:

$$p(z|\mu, b) = \frac{1}{2b} \exp\left(-\frac{|z - \mu|}{b}\right)$$

(con b che sarebbe la larghezza della distr)



Il senso è che più epsilon è piccolo, più sarà elevata la dev standard del noise aggiunto.

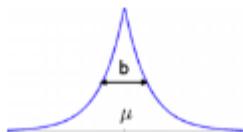
Esempio

$f(D) = \text{Mean}(D)$, where each record is a scalar in $[0, 1]$

Global Sensitivity of $f = 1/n$

Laplace Mechanism:

Output $f(D) + Z$, where $Z \sim \frac{1}{n\epsilon} \text{Lap}(0, 1)$



N n record

Epsilon deve essere piccolo

→ se n grande e epsilon piccolo, standard deviation sarà piccola; e l'accuratezza sarà grande

Morale: se vogliamo raggiungere tutti i poli del triangolo privacy, record tanti e accuratezzad evo avere tanti record, epsilon piccolo e accuratezza dati.

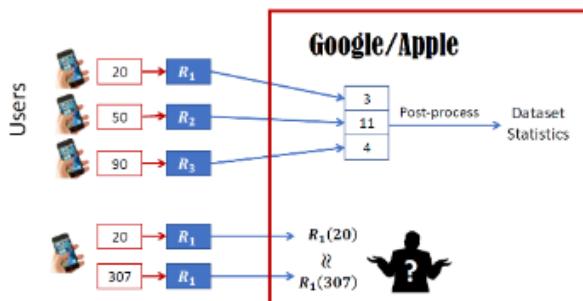
Applicazioni

Sempre di più è usata per fare:

- Training di algoritmi di machine learning (classificazione e clustering)
- query aggregate
- generare dataset sintetici con distribuzioni uguali a dataset veri ma senza bisogno di dare dataset veri in giro (magari ci faccio ML)

Esempi

- **US census bureau 2020:** In America c'è un censimento periodico, e si possono fare query su questi dati. L'analisi soddisfa la privacy
- **Google:** Ha un'implementazione open source che chiama RAPPOR, ed è usata per fare analisi sulle ricerche degli utenti
- **Apple:** Non ha reso pubblico l'algoritmo :) Alcuni ricercatori vi hanno avuto l'accesso e hanno fatto RE del codice, e non è così privata perché usa un epsilon intorno a 11.



Sia google che apple usano la privacy differenziale locale per avere info su dati telemetrici; anziché catturare il dato reale, aggiungono al dato singolo un rumore, e questo dato perturbato può comunque essere analizzato.

Apple lo usa per mantenere traccia di quali sono le emoji più usate.

Ci sono due implementazioni della privacy differenziale:

- **Tensor flow** (google): algoritmi di machine learning che soddisfano la privacy
- **Opacus** (facebook): same



Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12

Jim Tang
University of Southern California
juntang@usc.edu

Aleksandra Korolova
University of Southern California
korolova@usc.edu

Xiaodong Bai
Tsinghua University
bxd12@tsinghua.edu.cn

Xuegang Wang
Indiana University
wangxg@indiana.edu

Xiaofeng Wang
Indiana University
wxf@indiana.edu

ABSTRACT

In June 2016, Apple made a bold announcement that it will deploy local differential privacy for some of their user data collection in order to ensure privacy of user data, even from Apple [27, 28]. The details of Apple's approach remained sparse, although researchers [7, 29] have since approached hunting at the algorithmic那末 we need to achieve differential privacy. They did not include a precise explanation of the approach taken to privacy guarantees. This work is the first to provide the first detailed analysis of the mechanism used by Apple to implement differential privacy and investigate how it can be used for understanding the privacy guarantees provided by the deployment of differential privacy.

In this work, through a combination of experimental study and dynamic code analysis of macOS Sierra Version 10.12 implementation, we shed light on the choices Apple made for privacy budget management. We discover and describe Apple's set up for differentially private data processing, including the overall data pipeline, the parameters used for differentially private perturbation of each user of data, and the frequency with which such data is sent to Apple's servers.

We find that although Apple's implement ensures that the differential privacy loss per each dataset intended to be returned is at least 2, the overall privacy loss paid per the whole data is significantly higher than what is claimed.

1 INTRODUCTION

Differential privacy [2] has been widely recognized as the leading standard data privacy definition by the academic community [6, 11]. Thus, as one of the first large-scale commercial deployment of differential privacy (preceded only by Google's Earth Engine [7]), Apple's deployment is of significant interest to privacy theoreticians and practitioners alike. Furthermore, since Apple one of the first company to privacy with other consumer companies, understanding the actual privacy protections afforded by the use of differential privacy on its devices and mobile OSes may be of interest to consumers and consumer advocacy groups [10].

However, Apple is publicly doing communications about its deployment of differential privacy have been extremely limited; neither its developer documents [1, 2, 21, 22, 24] nor internal reports prompting the users to opt-in to differentially private data collection [25] gives a and provide details of the technology, except say what data types it may be applied to. Two aspects of the deployment are crucial to understanding its privacy merit: the algorithms or processes used to ensure differential privacy of the data being sent and the privacy parameters being used by those algorithms. Although one can speculate about the algorithms deployed once

S14 - Seminario DLP

Definizione

Il DLP è un po' in divenire vecchio; rimane comunque una tecnologia importante per proteggere il dato

DLP: Data leak prevention insieme di tecnologie che servono a localizzare e catalogare info sensibili.
Oppure, Data Loss Protection: classificare risorse per proteggerle accuratamente.

→ non abbiamo una forte definizione, è flessibile.

Scenari

Le soluzioni DLP nascono da questo scenario:

- Datacenter
- Sedi remote connesse via mpls
- 3rd parties connesse via vpm
- Internet

Con l'evoluzione attuale della rete, un coverage completo è un po' troppo ambizioso.

Obiettivi

- **Discover**: localizzare dati critici da proteggere. Le aziende a volte manco sanno dove sono i dati!
- **Monitor**: capire come sono usati i dati; non è detto che l'azienda sia consapevole di dove i dati vengono spostati e salvati.
- **Protect**: protezione del dato
- **Bonus che vedremo dopo**

Devono riconoscere qualsiasi tipo di dato:

- Definiti da normative (HIPAA; GDPR...)
- Dati definiti dal business stesso: i loro dati

Con qualunque struttura:

- Valori con una struttura definita (tipo codice fiscale)
- Non definibili a priori: design, dati personali...

In modo indipendente dal formato: dati strutturati e non strutturati.

Deve anche poter operare su tutti i canali di comunicazioni ove il dato viaggia: endpoint, network, storage, cloud.

2 - Scenari dlp

Data at rest: dato memorizzato in qualche maniera, in uno storage o in una casella di posta, in share di rete...

→ discovery

Data in motion: DLP controlla il dato finché sisposta. Lavora a livello L7(e inon in basso) per ragioni di praticità e fattibilità.

→ protect

Data in use: si lavora a livello di endpoint indirizzando dispositivi esterni, cut and paste, sovrapposto ai casi precedenti. Può interagire con l'utente.

Policy DLP

Detection	Response
<ul style="list-style-type: none">• Contenuto / evento trigger: Identificare il dato target della policy• Contesto: chi sta usando il dato e cosa ci sta facendo	<ul style="list-style-type: none">• Azione: impedire l'azione o attuare una remediation, o chiedere giustificazione all'utente. E notificare l'evento.

La risposta dipende dal canale.

Una stessa policy può gestire più dati.

Posso anche prevedere delle eccezioni legate al contesto.

Tecniche di detection:

- **Attributi del file:** tipo, nome dimensione
- **Contenuto:** keywords o tags, formati standard tipo CF o CC, regular expressions..
- **Individuazione di dati strutturati e non strutturati:** serve per dati più complessi.
 - Individuazione: selezioni le colonne importanti e calcolo l'hash per costruire l'indice.
 - Detect: in ogni file controlla se c'è del match.

03 – Prerequisiti

Perché funziona, il progetto di un DLP deve avere dei requisiti.

1. Mandato aziendale forte
2. Necessario il coinvolgimento delle figure di business, che devono capire il valore.
3. Fondamentale coinvolgere HR & legal (dato che è una sorveglianza)
4. Fondamentale comprendere cultura e rapporti aziendali, spesso dipendenti da cultura locale.

Struttura aziendale

- CEO
 - CFO: direttore finanziario
 - COO, CPO...
- CIO: chief information officer. È il capo della IT. Dovrebbe essere sotto il CEO ma spesso non lo è. Vuole solo fornire servizi agli utenti.
 - CTO
 - CSO. Sicurezza
 - CISO chief information security officer: è controversa perché non si capisce bene come è messo. Dovrebbe essere indipendente dal CIO, dato che vuole proteggere info e mettere vangoli.

Policy aziendali

Non è pensato per l'hacker esterno; è pensato per figure interne all'azienda e perdite involontarie del dato!

E le policy devono essere chiare per poter essere implementate

Classificazione del dato

Poche aziende lo fanno, ma i dati dovrebbero essere classificati per sapere come trattare i dati.

Analisi del rischio

04-strategie implementative

1. Definisco una strategia globale: devo coprire il perimetro intero per più passaggi
2. Preparare il business individuando i key user, i referenti e così e istruendoli un minimo
3. Individuare un business case da cui partire, aka un pezzettino da cui iniziare a proteggere in modo facile per dimostrare che il DLP è worth it.

Scegliere tecnologia adeguata

È una delle ultime cose fatte, perché così non sono vincolato dalla tecnologia.

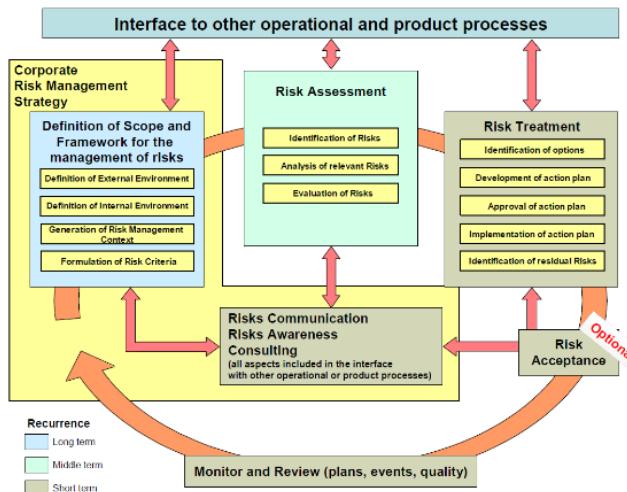
Implementazione

- Prima versione:
 - È bene non iniziare col blocco: metto le regole in modo read only cos' che traccia tutto e mi fa la parte di monitoring e discovering.
- Versione definitiva
 - Incident management: persona viola la regola aziendale. Servono dei flussi di notifica che gestiscano casi eccezionali o delicati (es. top manager)
 - Tuning e manutenzione della regola

15 - Risk management

Alle aziende serve un processo per **identificare il rischio**. Il risk management fornisce informazioni a un'organizzazione per capire dove agire per gestire questo rischio.

Per alcune organizzazioni questo fatto è un **obbligo legislativo dato da certificazioni** e ambiti: ISO 27001 certificazione, GDPR, PCI DSS è uno standard da tenere per procesare informazioni delle carte



Tutto si ripete a cadenza periodica, e può essere rifatta anche nel caso in cui si introducano nuove features o cambiamenti nel sistema (es. l'azienda decide di salvare i dati sul cloud anziché su dischi).
→ ciclico!

Standard

Fornisce una serie di standard che supporta le fasi viste nel paragrafo precedente. Il vantaggio del NIST è che è tutto open source! Noi oggi vediamo solo lo standard sul risk-assessment.

Esistono anche altri standard:

- ISO/IEC IS 27005: processo di risk management in generale
- ISO 31000 standard generale
- IT-Grundschutz metodologia sviluppata in germania
- EBIOS: metodologia del governo francese

Infine ci sono anche metodologie solo sul risk assessment:

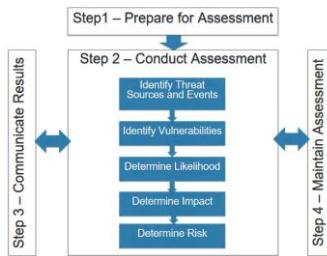
- OCTAVE
- CORAS – è completamente basata sull'uso di simboli grafici.

Elementi di rischio

Parlando di rischio, definiamo i fattori utilizzati per quantificare il rischio:



Standard NIST 800-30



1. Preparazione del risk assessment

Potrei volerlo fare perché è cambiato lo scenario e sono emersi nuovi attacchi possibili (es. si è scoperta una nuova vulnerabilità), oppure perché abbiamo introdotto nuove funzionalità.

Obiettivo: stabilire il contesto per il risk assessment.

Vogliamo identificare:

- Scopo dell'assessment
- Scope dell'assessment
- Assunzioni e constraints
- Modello di rischio
- Assessment approach
- Analysis approach

Ci sono tre approcci possibili:

- **Approccio qualitativo:** Definisco la likelihood utilizzando delle etichette come la probabilità è alta, media o bassa oppure l'impatto è alto, medio, basso (NIST)
- **Approccio quantitativo:** likelihood e impatto sono quantificate con un numero
- **Irido:** utilizzo i numeri per quantificare il valore di likelihood e impatto, ma poi per presentare i risultati a CEO e management senior si usano delle etichette.

Approccio di analisi:

- **Partire dal concetto di asset** e calcolare tutti i rischi
- **NIST:** Focus sui **possibili attaccanti** e legare le categorie di attaccanti agli assets di sistema.

2. Condurre il risk assessment

2.1 Identificazione delle categorie di attaccanti

Obiettivo: produrre una lista di cyber security threats

Qual è l' effetto?	Skill? Risorse? Motivazione?	Adversarial	Soggetti che vogliono sfruttare la dipendenza dell'organizzazione sulle cyber risorse. <ul style="list-style-type: none">• Outsider, Insider, Competitor, Supplier, Nation state
		Accidental	Comprende gli utenti che compiono un'azione con un effetto negativo ma senza volerlo, tipo un amministratore che sbaglia i settaggi. <ul style="list-style-type: none">• User, privileged user
		Strutturale	Situazioni in cui l'infrastruttura che supporta il deployment ha una failure non è più disponibile <ul style="list-style-type: none">• IT equipment, environmental controls, software
		Environmental	Attacchi dati dai disastri naturali, tipo incendi, inondazioni, terremoti <ul style="list-style-type: none">• Disastri naturali o umani, infrastructural failure.

Esempio

- Adversarial per Poste italiane: hackers
- Non-adversarial: tizi impegati di 50 anni che non sanno usare il pc

2.2 Identificazione degli eventi minaccia

Obiettivo: Identificare la minaccia maggiore

- Come potrebbe succedere? Cosa danneggia?
- Che tipo di eventi possono essere iniziati dagli individui individuati in 2.1?

2.3 Identificazione delle vulnerabilità

Obiettivo: definire le vulnerabilità che un threat event potrebbe sfruttare, e la loro gravità.

Cosa rende possibile le threat?

2.4 Determinare la likelihood del threat event

Obiettivo: determinare la likelihood del threat event

Per stimare la likelihood dell'evento considero capacità, intento e targeting e quanto è difficile sfruttare la vulnerabilità.

- **P diversa per adversarial e non adversarial:**

Qualitative Values	Semi-Quantitative Values	Description	
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the threat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

Qualitative Values	Semi-Quantitative Values	Description	
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur, or occurs more than 100 times a year .
High	80-95	8	Error, accident, or act of nature is highly likely to occur, or occurs between 10-100 times a year .
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur, or occurs between 1-10 times a year .
Low	5-20	2	Error, accident, or act of nature is unlikely to occur, or occurs less than once a year, but more than once every 10 years .
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur, or occurs less than once every 10 years .

- **P che la threat abbia successo:**

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values	Description	
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

- **P totale:** Infine, uso i risultati delle cose precedenti per trovare la likelihood generale nella seguente tabella:

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

2.5 Determinare l'impatto e il rischio

Type of Impact	Impact	Impact	Description
Harm to Operations	<ul style="list-style-type: none"> • Inability to perform current business functions • Non compliance • Direct Financial Costs • Damage to image of reputation 	Very High	Threat event could have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations or the Nation
Harm to Assets	<ul style="list-style-type: none"> • Damage to or loss of physical facilities • Damage to or loss of information systems or networks • Damage to or loss of equipment • Damage to or loss of information assets • Loss of intellectual properties 	High	Threat event could have severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations or the Nation
Harm to Individuals	<ul style="list-style-type: none"> • Loss of life • Identity Theft • Loss of PII • Damage to the reputation 	Moderate	Threat event could have serious effects on organizational operations, assets, individuals, other organizations or the Nation
Harm to Other Organizations	<ul style="list-style-type: none"> • Non compliance • Direct Financial Costs • Damage to image of reputation 	Low	Threat event could have limited effects on organizational operations, assets, individuals, other organizations or the Nation
Harm to the Nation	<ul style="list-style-type: none"> • Damage to a critical infrastructure 	Very Low	Threat event could have negligible on organizational operations, assets, individuals, other organizations or the Nation

Adverse Impact	Likelihood of Threat Event				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

3. Comunicazione dei risultati

Obiettivo: comunicare i risultati dell'assessment e le informazioni connesse.

Fatto tutto ciò dobbiamo fare un report per condividere i risultati dell'analisi. Questo si concretizza comunicando i rischi high e very high al **management dell'azienda**.

Infine bisogna condividere i rischi anche con gli altri **stakeholder**, tipo i clienti di posteitaliane e il rischio di phishing oppure i sistemisti per log4j.

4. Mantenere aggiornato il risk assessment

Obiettivo: mantenere la conoscenza del rischio

Se entra in vigore un nuovo requisito causa nuova legge sulla protezione dei dati. Allora devo valutare quali sono i rischi per la mia organizzazione nell'adottare le nuove protezioni, e quale sia la nuova misura di rischio associata.

Se ci sono nuove tecniche di attacco o categorie di attacanti, analogamente dovrò riaggiornare l'analisi

Se introduco nuovi servizi, same