Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Informatica per il Management

Sicurezza dell'identità digitale e Videogiocatori

Relatore:
Chiar.mo Prof.
Davide Sangiorgi

Presentata da:
Anthony Cazzola

Sessione straordinaria
Anno Accademico 2020-2021

A chiunque si senta schiacciato, in gabbia o oppresso e non capisce neanche da cosa:
Memento audere semper...

Introduzione

Vorrei iniziare questo lavoro contestualizzando, anche se in parte, quella che è la nostra società al giorno d'oggi. Oggi piu che mai siamo connessi ed interconnessi alla rete creando di fatto una sorta di società digitale parallela alla società stessa. Il termine società digitale si riferisce alla rappresentazione della società in rete la quale viene utilizzata per fornire prestazioni e servizi ricorrendo a strumenti informatici. Questo termine inizio ad imporsi solo dalla metà degli anni '80, quando nei media, nelle piccole e medie imprese e nel settore privato divennero fruibili nuove tecnologie e quindi nuove forme di interazione.

Come in molti altri tipi di società, anche in quella digitale é necessario che l'individuo si idendetifichi e acquisca una propria identità che lo renda univocamente riconosocibile e, con cui, potrà accedere a tutti quei servizi messi a disposizione dalla società (digitale). La tesi in questione si focalizzerà su come l'identità digitale venga gestita nel settore videoludico e dei rischi che la riguardano. Questo settore infatti, complice anche la recente pandemia e il conseguente lock-down, é cresciuto esponenzialmente e molte persone hanno intrapreso vere e proprie carriere nell'ambito videoludico. Recentemente, inoltre, i videogiochi online hanno ottenuto un'importanza tale da conquistare una loro categoria alle Olimpiadi: Olympic Virtual Series, cinque tornei di videogiochi annunciati dal CIO (Comitato Internazionale Olimpico). Verrà inoltre introdotto Aidentigo, un progetto al quale ho partecipato attivamente come tirocinante che ha lo scopo di notificare in tempo reale i videogiocatori qual ora ci fosse un attacco ai loro profili (quindi alle loro identità online).

La tesi avrà quindi, la seguente struttura:

- **Capitolo 1:** in questo primo capitolo si discuterà dell'identitÃ digitale, del perchè è necessaria, come ottenerla e quali sono i rischi legati ad essa. Verrà poi analizzata da un punto di vista giuridico
- **Capitolo 2:** nel secondo capitolo verrà brevemente esaminato il mercato e il settore videoludico introducendo la realta nella quale lavora Aidentigo .

- **Capitolo 3:** Infine, verrà esposto il contributo dato ad Aidentigo descrivendo le difficoltá incontrate e risultati ottenuti.

Indice

Capitolo 1

Identità Digitale

1.1 Cos'è e come ottenerla

Possiamo considerare l'identità digitale come quell'insieme di informazioni cedute dall'individuo per accedere ad un determinato servizio in rete. Informazioni che associano quindi, le azioni compiute in rete allâidentità reale del soggetto.

"Con il termine identitá digitaleÂ possiamo intendere la rappresentazione informatica di ciascun cittadino mediante i suoi dati identificativi"

Per la maggior parte dei servizi ai quali si vuole accedere mediante la rete sarà necessario cedere informazioni attraverso le quali creare un entità digitale. Il tipo e la complessità delle informazioni necessarie dipendono dal servizio al quale si vuole accedere. Un servizio di banking online, ad esempio, richiede informazioni piú dettagliate di quanto faccia un social-network. L'identitá digitale piú semplice è ottenuta mediante l'utilizzo di un id e una password in questo caso lâidentità' é rappresentata dal id e garantita dalla password scelta dall'utente. l'identitá cosí ottenuta mette in risalto un dei problemi legati a questa pratica: l'autenticazione; l'assicurarsi, cioè, che lâutilizzatore di un servizio in rete corrisponda effettivamente al titolare dell'identitá, ma anche che le informazioni date siano autentiche.
La fase di autenticazione puó basarsi su tre diverse caratteristiche:

- Conoscenza: "Una cosa che sai"per esempio una password o il PIN.
- Possesso: "Una cosa che hai", come uno smartphone o un token di sicurezza
- Inerenza: "Una cosa che sei", come lâimpronta digitale, il timbro vocale, il viso, l'iride, o qualunque altro dato biometrico.

Se l'autenticazione avviene con la sola password si parla di autenticazione ad un solo fattore. La sola password dovrebbe quindi garantire l'identitá dell'utente. Se, invece, l'autenticazione avviene attraverso due o piú differenti caratteristiche sopra citata, si parla di autenticazione a due fattori (2FA). Esiste anche un'autenticazione a tre fattori in cui vengono richieste, per l'autenticazione, tutte e tre le caratteristiche. In Italia per accedere ai servizi della pubblica amministrazione è necessario lo SPID (Sistema Pubblico Identità Digitale) basato appunto su un'autenticazione a tre fattori. Con l'autenticazione a piú fattori anche qual ora la password dovesse venire scoperta da un mal intenzionato la nostra identità in rete sarebbe protetta dal secondo o dal terzo fattore di autenticazione. Le caratteristiche biometriche possono definire il secondo fattore d'autenticazione, tutta via non é detto che tutti i dispositivi abbiano un lettore in grado leggerle. Come secondo fattore di autenticazione viene spesso utilizzato una one time password (OTP). L'otp puó essere emesso in diversi modi, fra i meno affidabili ci sono gli sms a causa della oramai nota truffa "SIM Swap Fraud". In pratica, un malintenzionato puó riuscire a trasferire da una SIM card a un'altra il nostro numero di telefono. Portare a termine un'operazione di SIM swapping illegittima significa ottenere il completo accesso al numero di telefono del legittimo (e ignaro) proprietario di tale numero e, soprattutto, permette di ricevere lâSMS con i codici di autenticazione a due fattori, Lo strumento piú affidabile sono i generatori di token: questi possono essere sia fisici, come quelli dati dalle banche ma anche digitali (soft-token). In questo caso l'otp viene generato da un'applicazione come google authenticator

1.2 Sicurezza delle password

Da ciò che è stato scritto nel paragrafo precedente si evince l'essenzialità delle password nel per garantire l'autenticazione di un utente in rete. Non esistono soluzioni tecnologiche di autenticazione che possono sostituire completamente la password; esse piuttosto possono servire come mezzo complementare per renderla più affidabile nel processo di autenticazione. Se esaminiamo ad esempio l'autenticazione biometrica possiamo constatare che oggi è utilizzata correntemente sugli smartphone ma abbiamo sempre una password che ci protegge rispetto ad un uso improprio del metodo di autenticazione.

Se non esistesse la password sarebbe impossibile fare il reset dei dati biometrici per sbloccare il dispositivo. Nonostante la loro importanza molti scelgono password non sicure o facilmente ottenibili. Nel 2021 le piú usate risultano essere: "123456","qwerty"," password". La sicurezza delle password passa attraverso diversi passaggi. Innanzi tutto é necessario scegliere una password complessa per evitare che gli attacchi di tipo brute-force riescano a risalire ad essa. Questi tipi di attacchi, come quelli a dizionario, infatti, combinano una moltitudine di caratteri fino ad ottenere un risultato considerabile. La complessità computazionale di tali algoritmi è molto elevata e il tempo necessario per ottenere un risultato valido dipende sia dalla potenza di calcolo del processore sia dalla complessità della password. Scegliere una password breve o semplice rende questi attacchi efficaci in tempi ragionevoli. Per irrobustire la sicurezza delle password, è opportuno crittografarle qualora si volessero salvare su un disco fisso; o meglio, renderla illeggibile a chiunque abbia accesso, remoto o fisico, al dispositivo sulla quale questa viene salvata. La crittografia é quella tecnica attraverso la quale si occulta il significato di un messaggio o di un testo e se ne permette l'accesso solo a chi é in possesso della chiave per la decodifica. La password non dovrebbe conoscerla nessuno ad esclusione

1.2.1 funzioni hash

Le funzioni hash sono particolari funzioni che permettono di ottenere un'unica stringa di caratteri a lunghezza fissa, dai dati che vengono forniti in input. Allo stesso tempo, praticamente impossibile eseguire il processo opposto per risalire ai dati o alla stringa iniziale. Fornire la password come input ad una funzione hash protegge da attacchi diretti nei quali l'hacker riesce ad avere accesso al dispositivo dell'utente o al database del fornitore del servizio al qual l'utente vuole accede. Questa tecnica tutta via non protegge dagli attacchi di tipo brute-force: se un malintenzionato venisse a conoscenza dal hash della password di un utente, la complessitá e il tempo impiegato ad ottenere la password in chiaro sarebbe proporzionale a quello di un attacco di tipo brute-force senza alcuna informazione. Di funzioni hash ne esistono diverse: la famiglia SHA e MD5 ne sono alcuni esempi; la loro qualitÃ , non che la loro utilitá, é data dalla resistenza che esse hanno alle collisioni: non essendo bigettive é possibile che a due input diversi corrisponda uno stesso output generando una collisione. La SHA-1 é stata il riferimento di questo tipo di funzioni fin che un gruppo di ricercatori non é riuscito a generare una collisione rendendo necessaria l'introduzione dello sha-2. Le funzioni hash sono utilizzate anche in crittografia per garantire l'integritá del messaggio: se insieme al messaggio si invia anche il suo digest (risultato dell'applicazione della funzione hash al messaggio), il destinatario una volta decifrato il messaggio potrebbe applicare la medesima funzione hash del mittente e verificare l'uguaglianza fra il digest ottenuto e quello ricevuto, verificando quindi l'integritá del messaggio. Il digest delle funzioni hash crittografiche infatti risulta totalmente diverso anche con un cambiamento minimo al messaggio originale, se i due digest dovessero differire anche solo di un carattere allora il messaggio sarebbe stato alterato. In oltre attraverso queste funzioni si può apporre quella che viene definita "firma digitale". La firma digitale, utilizzata per sottoscrivere un documento informatico, garantisce, in modo inequivocabile, l'integritá dei dati contenuti e l'autenticitá delle informazioni relative al sottoscrittore. Per ottenerla é necessario utilizzare algoritmi crittografici

asimetrici in cui esiste una chiave pubblica e una chiave privata; per firmare un documento si dovrà cifrare il digest del documento con la propria chiave privata così verrá generata l'impronta del documento. Il destinatario tramite la chiave pubblica, decifra la stringa della firma digitale che produrrá come risultato l'impronta del documento. Facendo poi passare la funzione hash sul documento originario e genererÃ l'impronta: a questo punto se le due impronte coincideranno il destinatario sarÃ sicuro dell'integritá e dell'autenticitá del documento ricevuto. In questo caso l'utilitá data dalle funzioni hash, oltre a verificare l'integritá del messaggio, é data dalla possibilitá che queste offrono di comprimere in stringhe fino a 512 bit testi e documenti di ordini di grandezza superiore (in sha-256 ad esempio Ã¨ richiesto che il messaggio in chiaro non sia più grande di $2^{64}bit$

1.2.2 SHA-2

SHA-2 rappresenta lo standard attuale per gli hash crittografici. Creato da NSA (National Security Agency) nel 1993, nell'ambito del suo progetto interno di autenticazione dei documenti elettronici. SHA e le sue derivate sono considerate le funzioni hash più sicure fino ad oggi. La sigla SHA-2 rappresenta una famiglia di quattro differenti algoritmi, tale sigla non é mai stata registrata ma si fa riferimento ad essa per indicare l'evoluzione rispetto SHA-1 rappresentato da una singola funzione. La caratteristica principale che differenzia i quattro algoritmi é la lunghezza del digest risultanti dopo una serie di ciclici (da 64 a 80) nei quali vengono svolte operazioni logiche e matematiche. Come é ragionevole pensare digest più corti espongo a un rischio di collisione più alto; d'altra parte i digest più lunghi richiedono maggiori risorse computazionali e maggior tempo di calcolo. Si ha quindi che SHA-224 fornirá un digest di 224 bit, SHA-256 di 256, SHA-384 e SHA-512 di, rispettivamente, 384 e 512 bit (SHA-1 forniva un digest di 160 bit). Un'altra differenza fondamentale é il rischio di collisioni che ogni algoritmo presenta: é ragionevole che più é basso il numero di bit del digest più le collisioni sono possibili. Questi algoritmi vengo usati in diversi protocolli di

sicurezza come in SSH(Secure Shell) o PGP(Pretty Good Privacy); il primo viene utilizzato maggiormente per l'accesso remoto ai server, mentre il secondo é un popolare protocollo per garantire la privacy durante lo scambio di mail. PGP consente solo al destinatario di leggere le mail inoltre evita che hacker o terzi di ottengano informazioni personali come l'ISP del mittente. In piú sha-256 è usato sia per la creazione(mining) di Bitcoin sia nelle blockchain per rappresentare le informazioni di un intero blocco della catena. Di seguito viene fornito un esempio di come funziona lo SHA-256: si otterá il digest di "hello world".

1.2.3 SHA-2: Esempio completo

Ad sesempio se volessimo ottenere l'hash della classica frase "hello world" dovremmo seguire i seguenti passaggi

Fase 1- Padding
Nella fase uno é necessario ottenere un messaggio composto da un multiplo di 512 bit. Dopo aver trasformato il messaggio in binario gli si aggiungerá un 1 alla fine e successivamente tutti gli 0 neccesari al raggiungimento di 448 bit, infine si utilizzeranno gli ultimi 64 bit per rappresentare la lunghezza del messaggio che, quindi, dovrá essere inferiore a 2^{64}. La conversione in binario di "hello world" risulta essere

01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111 01110010 01101100 01100100

Dopo le procedure di padding, otterremo:
01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111
01110010 01101100 01100100 10000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 01011000

Fase3 - Message schedule
Generalmente il messaggio viene diviso in N blocchi da 512 bit per ripetere la seguente procedura per ognuno di questi. Nel nostro caso essendo il messaggio corto é sufficiente un singolo blocco. Dal contenuto ottenuto nella fase 1 si ottiene quello che viene definito message schedule (W) Si può vedere il message schedule come un array di 64 entry ognuna delle quali conterrà

una parola di 32 bit. Le prime 16 entry sono uguali alle parole che risultano dividendo per 32 i blocchi di 512 bit ottenuti, mentre le restanti inizialmente sono riempite con parole contenenti solo zero poi sostituite come segue

for i from 16 to 63:
w[i] = w[i-16] + A0 + w[i-7] + A1

dove le funzioni A0 e A1
A0=(w[i-15] R^7) xor (w[i-15] R^{18}) xor (w[i-15] S^3)
A1 := (w[i- 2] R^{17}) xor (w[i- 2] R^{19}) xor (w[i- 2] S^{10})

Con R^n viene indicata una rotazione destra di n bit e S^n spostamento a destra di n bit.

Analizzando ciò che succede per "hello world" per l'entry w[16]

w[1] R^7 : 01101111001000000111011101101111 $\rightarrow$ 11011110110111100100000011101110
$w[1]R^18$: 01101111001000000111011101101111 $\rightarrow$ 00011101110110111101101111001000
$w[1]S^3$: 01101111001000000111011101101111 $\rightarrow$ 00001101111001000000111011101101
$s0 = 11011110110111100100000011101110 \oplus 00011101110110111101101111001000 \oplus$
$00001101111001000000111011101101 \Rightarrow s0 = 11001110111000011001010111001011$

$w[14]R^17$: 00000000000000000000000000000000 $\rightarrow$ 00000000000000000000000000000000
$w[14]R^19$: 00000000000000000000000000000000 $\rightarrow$ 00000000000000000000000000000000
$w[14]S^10$: 00000000000000000000000000000000 $\rightarrow$ 00000000000000000000000000000000
$s1 = 00000000000000000000000000000000$

$w[16] = w[0] + s0 + w[9] + s1 = 00110111010001110000001000110111$

Questo processo rilascia un message schedule di 64 parole ognuna rappresentata da 32 bit

Fase4- compressione

Per questa fase é opportuno definire diverse costanti e alcune funzioni. In particolare si definiscono otto costanti di hash facendo la radice quadrata dei primi otto numeri primi e considerando solo i primi 32 bit della loro parte decimale:

h0 := 0x6a09e667
h1 := 0xbb67ae85
h2 := 0x3c6ef372
h3 := 0xa54ff53a
h4 := 0x510e527f
h5 := 0x9b05688c
h6 := 0x1f83d9ab
h7 := 0x5be0cd19

Inoltre si avranno altre 64 costanti, k[0]-k[63] definite in questo caso facendo la radice cubica dei primi 64 numeri primi:

0x428a2f98 0x71374491 0xb5c0fbcf 0xe9b5dba5 0x3956c25b 0x59f111f1 0x923f82a4 0xab1c5ed5 0xd807aa98 0x12835b01 0x243185be 0x550c7dc3 0x72be5d74 0x80deb1fe 0x9bdc06a7 0xc19bf174 0xe49b69c1 0xefbe4786 0x0fc19dc6 0x240ca1cc 0x2de92c6f 0x4a7484aa 0x5cb0a9dc 0x76f988da 0x983e5152 0xa831c66d 0xb00327c8 0xbf597fc7 0xc6e00bf3 0xd5a79147 0x06ca6351 0x14292967 0x27b70a85 0x2e1b2138 0x4d2c6dfc 0x53380d13 0x650a7354 0x766a0abb 0x81c2c92e 0x92722c85 0xa2bfe8a1 0xa81a664b 0xc24b8b70 0xc76c51a3 0xd192e819 0xd6990624 0xf40e3585 0x106aa070 0x19a4c116 0x1e376c08 0x2748774c 0x34b0bcb5 0x391c0cb3 0x4ed8aa4a 0x5b9cca4f 0x682e6ff3 0x748f82ee 0x78a5636f 0x84c87814 0x8cc70208 0x90befffa 0xa4506ceb 0xbef9a3f7 0xc67178f2

Per procedere è opportuno definire anche alcune funzioni, nel dettaglio

$$(\mathrm{X},\ \mathrm{Y},\ \mathrm{Z}) = (\mathrm{X} \bigwedge Y) \bigoplus((\neg)X \bigwedge Z)$$
$$\mathrm{Maj}(\mathrm{X},\ \mathrm{Y},\ \mathrm{Z}) = (\mathrm{X} \bigwedge Y) \bigoplus(X \bigwedge Z)xor(Y \bigwedge Z)$$
$$\mathrm{S0}(\mathrm{X}) = (\ \mathrm{X}\ \mathrm{S}^{2}) \bigoplus(XS^{13}) \bigoplus(XS^{22})$$
$$\mathrm{S1}(\mathrm{X}) = (\mathrm{X}\ \mathrm{S}^{\ 6}) \bigoplus(XS^{11}) \bigoplus(XS^{25})$$

l'algoritmo di compressione prevede di inizializzare otto variabili(solitamente da "a" ad "h") con lo stesso valore delle otto costanti di hash e successivamente creare un loop di 64 iterazioni dove in ognuna di esse vengono combinate logicamente con le K costanti sopra elencate e il message schedule

for i from 0 to 63:
temp1 = h + S1(e) + Ch(e, f, g) + K[i] + W[i]
temp2 = S0(a) + Maj(a, b, c)
h = g
g = f
f = e
e = d + temp1
d = c
c = b
b = a
a = temp1 + temp2

Alla fine di questo ciclo, nel nostro caso avremmo che

$$\mathrm{h0} = \mathrm{6A09E667} = 01101010000010011110011001100111$$
$$\mathrm{h1} = \mathrm{BB67AE85} = 10111011011001111010111010000101$$
$$\mathrm{h2} = \mathrm{3C6EF372} = 00111100011011101111001101110010$$
$$\mathrm{h3} = \mathrm{A54FF53A} = 10100101010011111111010100111010$$

$$h4 = 510E527F = 01010001000011100101001001111111$$
$$h5 = 9B05688C = 10011011000001010110100010001100$$
$$h6 = 1F83D9AB = 00011111100000111101100110101011$$
$$h7 = 5BE0CD19 = 01011011111000001100110100011001$$

$$a = 4F434152 = 01001111010000110100000101010010$$
$$b = D7E58F83 = 11010111111001011000111110000011$$
$$c = 68BF5F65 = 01101000101111110101111101100101$$
$$d = 352DB6C0 = 00110101001011011011011011000000$$
$$e = 73769D64 = 01110011011101101001110101100100$$
$$f = DF4E1862 = 11011111010011100001100001100010$$
$$g = 71051E01 = 01110001000001010001111000000001$$
$$h = 870F00D0 = 10000111000011110000000011010000$$

Fase 5 - concatenazione

In fine basterá sommare alle costanti di hash le loro rispettive variabili e concatenarle per ottenere il digest del messaggio

$$h0 = h0 + a = 10111001010011010010011110111001$$
$$h1 = h1 + b = 10010011010011010011111000001000$$
$$h2 = h2 + c = 10100101001011100101001011010111$$
$$h3 = h3 + d = 11011010011111011010101111111010$$
$$h4 = h4 + e = 11000100100001001110111111100011$$
$$h5 = h5 + f = 01111010010100111000000011101110$$
$$h6 = h6 + g = 10010000100010001111011110101100$$
$$h7 = h7 + h = 11100010111011111100110111101001$$

Concatenando le otto variabili e, trasponendo il risultato in base esadecimale otterremo il seguente digest:

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

Da questo codice è matematicamente infattibile risalire alla stringa iniziale "hello world", a meno di un attacco a forza bruta che per definizione richiederebbe 2^L computazioni, dove L rappresenta la lunghezza del digest. In oltre se si esegusse la stessa operazione per "Hello world" cambiando solo minimamente la stringa iniziale, avremmo un digest completamente diverso, a rendere ancora più elevata l'affidabilità di tali algoritmi:

64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232534a8aeca37f3c

1.3 Tutela giuridica

Per spiegare come la legge tuteli l'identità digitale, è bene specificare ulteriormente il concetto di "identità" anche da una prospettiva socio-psicologica. Secondo la definizione fornita dalla psicologia e dalle scienze sociali, l'identità personale consisterebbe nella rappresentazione di un individuo in relazione al contesto sociale in cui si sviluppa la sua personalità. Definendo l'identità personale come bene-valore costituita dalla proiezione della personalità dell'individuo sulla società, essa rientra anche trai i beni giuridici tutelati dall'ordinamento. Obbiettivo dell'ordinamento, infatti, è quello di tutelare l'interesse del soggetto ad essere rappresentato nel contesto in cui vive e in cui esprime la sua personalità come determinazione del proprio io. Invero tra i diritti fondamentali della persona rientra anche il diritto del singolo a mantenere il controllo sulla sua rappresentazione rispetto la societ‘Ã . Anche la Corte Costituzionale si è espressa in tal senso definendo il diritto all'identità personale come

"Diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, lâindividuo"

In questo conteso si inserisce il concetto di "identità digitale" che altro non è che la rappresentazione attraverso una quantità sufficiente di dati (rilevanti) di un individuo reale.

La popolarità e l'utilizzo massiccio di Internet hanno comportato la creazione di milioni di identità digitali, al fine di svolgere in questo spazio virtuale le attività più disparate. Si possono pertanto individuare diverse tipologie di identità digitali, in relazione alle attività da compiere sul web, motivo per cui la nozione di identità digitale è comunemente intesa secondo due differenti accezioni, ovvero sia come rappresentazione nel mondo online di una persona fisica o giuridica, sia come insieme delle informazioni e delle risorse cedute dall'utilizzatore, che ne consentono l'identificazione nel mondo virtuale.

1.3.1 Decreti regolatori

Il Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, anche conosciuto come Decreto SPID, definisce allâart. 1, lett. o), l'Identità digitale come

"la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale".

Secondo questa definizione quindi, l'identità digitale sarebbe costituita dall'insieme di dati che abilitano il soggetto a compiere le proprie attività in rete, ossia le tecniche di autenticazione e identificazione dell'utente (ad es. le credenziali di accesso). Ne deriva, quindi, che il concetto di "identità digitale" comprenderebbe, da un lato, la proiezione dell'identità personale di un individuo sul web, dall'altro, l'insieme delle tecniche di identificazione del soggetto che gli consentono di agire nella realtà virtuale tramite strumenti informatici. Pertanto, la tutela giuridica dell'identitÃ digitale comprende due profili distinti: I due aspetti sono chiaramente collegati e molteplici sono gli effetti negativi che potrebbero derivare ad una tutela inadeguata.

- la tutela della privacy: tutelare l'identità digitale dell'utente, specie per i profili reputazionali

- la sicurezza informatica: proteggere l'identità dell'utente attravere sistemi di autenticazione/identificazione informatica

Per la tutela della privacy il GDPR è il riferimento europeo entrato definitivamente in vigore e sostituendo il codice privacy nel 2016. Il GDPR oltre definire il concetto di dato personale introduce anche dei controlli e principi volti a garantire la gestione dei dati da parte degli utenti, con particolare attenzione a quei dati che consentirebbero a terzi di ricostruire l'identità personale di un individuo. L'art. 5 e l'art. 6 descrivono sia come devono essere gestiti i dati sia come deve essere chiesto il consenso al trattamento. Considerando questi articoli (salvo rare eccezioni) l'individuo dovrá essere sempre informato, mediante un'informativa chiara ed efficace, circa le finlità, le modalità, la base giuridica nonché il tempo di conservazione dei dati richiesti. In più si avrà che il consenso al trattamento dei dati deve essere sempre espresso per essere considerato lecito soprattutto se i dati trattati consentono l'identificazione dell'individuo nella società.

Rispetto l'identità digitale, il rischio più grande al quale un utente viene esposto consiste nel furto di quest'ultima. Tale circostanza si realizza sia attraverso l'acquisizione illecita delle credenziali necessarie ad autenticarsi sul web, sia attraverso l'acquisizione (sempre illecita) di dati fondamentali per la creazione di un'identità fittizia. Acnhe se il furto d'identità costituisce reato, il codice penale vigente non ne prevede una specifica norma incriminatrice. Si può tutta via ricondurre ad altri due tipi di reato

- sostituzione di persona: art 494 C.P
- frode informatica: art 640ter, comma 3, C.P

Il reato di sostituzione di persona è disciplinato dallâarticolo 494 del codice penale, che stabilisce: *"Chiunque, al fine di procurare a sé o agli altri un vantaggio o di recare agli altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a séo agli altri un falso nome, o un falso stato, ovvero una qualità cui la legge attribuisce*

effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno."

Secondo questo articolo, quindi, il furto d'identità consiste nel sostituirsi ad un'altra persona e quindi ricavarne un vantaggio personale non necessariamente economico o procurare un danno alla persona sostituita. Mentre nell'articolo 640-ter C.P è stato introdotto il reato di furto d'identità' dell'utente come aggravante del reato di frode informatica. La frode informatica aggravata dal furto dâidentità digitale si realizza quando un soggetto, alterando in qualunque modo un sistema informatico, riesca a procurarsi un ingiusto profitto con conseguente danno per la vittima. Il fatto che il "furto o indebito utilizzo di identità digitale" appare concepito dal co. 3 art. 640-ter c.p. soltanto come un'aggravante della frode informatica, pertanto né il furto di dati, né l'indebito utilizzo di identità digitale possono da soli integrare il reato di frode informatica, dato che serve almeno un trasferimento illecito da un patrimonio all'altro. La tutela dal co. 3 art. 640- ter c.p. non può quindi operare per quei casi di furto o indebito utilizzo dell'identità digitale altrui che non sfocino in una diminuzione patrimoniale, ma che ad esempio comportino unâoffesa allâonore o alla reputazione della vittima.

Capitolo 2

Identità digitale videgiocatori: Aidentigo

2.1 Cenni storici

La storia dei videogiochi inizia intorno agli anni '50 quando questi venivano però considerati come strumenti di test più che videogiochi stessi. Nel 1958 venne ideato "tennis for two" il primo programma pensato esclusivamente per l'intrattenimento. Da li a poco questo nuovo settore finì per esplodere: gli anni '70 furono gli anni dei giochi arcade e si potevano trovare sale giochi un po ovunque. Sono gli anni in cui vine fondata L'Atari società destinata a dominare il settore per tutto il decennio successivo concludendo quello in corso con il lancio della prima console domestica (Atari 2600, 1977). Gli anni '80 sono caratterizzati da una crisi del settore che porta il fallimento dell'Atari ma anche da una ripresa che vede nuovi protagonisti spartirsi il mercato. Sono gli anni della Sony di Nintendo e di Commodore che col Commodore 64 che testimonia anche come i computer inizino ad essere usati anche in ambiti domestici.Grazie all'impiego delle tecnologie più moderne, i videogiochi percorrono nuove strade e lâazione di gioco e la grafica diventano sempre più innovative. L'evuluzione teconlogica caratteristica delgli anni '80 e '90 investe anche il mondo videoludico rendendo i giochi sempre più

giocabili e affascinanti. Una seconda rivoluzione oltre quella degli anni '80 avvenne neglia anni 2000 con l'utilizzo della rete come mezzo di supporto per video-giocare. Fino gli anni 2000 infatti i giochi erano prettamente offline, non poteva esserci interazione digitale fra i videogiocatori e, quindi, non era necessaria nenache un'identià digitale che rappresentasse i giocatori in rete. Gli anni 2000 decretano questo grande cambiamento: sarà ancora possibile giocare offline, tutta via il gioco online permette di introdurre una componente competitiva sulla qule si baseranno i tornei online: i videogiochi diventano veri sport (gli eSports) e i gamer migliori degli sportivi con ingaggi milionari. Dal 2000 fino ad oggi il mondo dei videogiochi si è evoluto in parallelo alla tecnologia, acquisendo man mano sempre più notorietà, secondo gli ultimi dati, oggi nel mondo ci sono 2,3 miliardi di giocatori. Un persona su tre gioca in digitale e non è un dato scontato.

2.2 Economia del settore

Già nel corso degli anni 2000 i pro-player sponsorizzati e stipendiati sono divenuti una realtà costante nel mondo dei videogiochi. Col lâaumento del numero di pro-player, lâimmagine degli eSports è cresciuta di conseguenza. Lâesplosione anche economica dei videogiochi competitivi ha portato il pro-player ad essere una professione remunerativa. Oggi infatti uno dei principali motivi che spinge i videogiocatori a tentare tale carriera è legato proprio allâaspetto economico. L'incremento dei guadagni dell' industria, nel 2020 sono quantificate in un 19,6% in piú rispetto allâanno precedente, per un incasso totale 175 miliardi di dollari. Per renderci conto del valore di questo dato, basti pensare che nel 2018 il fatturato globale delle industrie cinematografiche e musicali ammontava a 78 miliardi (42 cinema + 36 musica). Il settore videoludico sta detenendo il titolo di settore piú redditizio del mercato dell'intrattenimento digitale. Non solo si gioca sempre di più in tutto il mondo ma anche il "dove e come" si gioca registra valori incrementali su qualunque piattaforma presa in esame: mobile, PC e console. Da questo

si coglie la sempre maggiore importanza del gioco in mobilità, che genera quasi la metà dei ricavi totali dellâindustria. Si possono in definitiva trarre delle conclusioni considerevoli: se i tassi di crescita dovessero mantenersi costanti, nel 2023 lâindustria del gaming arriverebbe a generare ricavi per 217,9 miliardi di dollari. Si tratterebbe, nel quinquennio 2018-2023, di un aumento di valore del mercato globale del gaming del 9,4%. Un forte contributo a questo fenomeno l'ha sicuramente dato la pandemia, ma comunque non Ã¨ da ignorare il contributo che hanno dato le piattaforme di streamig. Attraverso queste piattaforme i videogiocatori possono intrattenere il pubblico senza essere necessariamente pro-player associati a qualche etichetta o organizzazione e ottenere allo stesso tempo guadagni considerevoli. Poco tempo fa sono trapelati in rete i guadagni di alcuni famosi streamer attivi su Twitch (piattaforma di straming più famosa, nata proprio per i videogiocatori), bench´Ã¨ non siano stati ne confermati ne smentiti da tutti gli interessati, le cifre arrivano fino a milioni di dollari all'anno.

2.2.1 Suddivisione del settore

Miliardi di persone, oggigiorno, trascorrono diverse ore della loro vita in una realtà virtuale alla quale possono accedervi mediante i videogiochi. Ciò che caretterizza i videogiochi rispetto ad altre forme di intrattenimento digitale è l'iterattività. I produttori di videogiochi, infatti la considerano un elemento fondamentale durante la produzione poiché più un gioco è interattivo più riuscirà a coinvolgere il giocatore facendolo sentire parte stessa del gioco. Se poi l'esperienza di gioco come ultimamente avviene, dovesse essere basata su una componente multigiocatore, allora l'interattività acquisirebbe anche un'altra accezione. In quest'ultimo caso i produttori dovranno ottimizzare non solo l'iterazione fra giocatore e gioco ma anche fra i diversi giocatori che utilizzano il gioco come mezzo di comunicazione o come punto d'incontro virtuale. Questo mercato nell'immaginario comune è sempre stato rappresentato dalle console, in questo momento sono tre le aziende che più di tutte rappresentano e si dividono parte del mercato: Sony, Microsof e Nintendo.

Figura 2.1: Andamento mercato videoludico

Tutta via se si analizzano i dati si riscontra che i giocatori che utilizzano le console sono solo una parte dell'utenza

Come si può notare dal grafico l'utenza di videogiocatori negli ultimi dieci anni è aumentata notevolmente e l'introito maggiore lo portano i giocatori da mobile, in questo segmento l'introito complessivo raggiunge i 68,5 miliardi di dollari di cui il 40% è frutto di acquisti in app mentre la pubblicità ne frutta "solo" il 30%. Questo dimostra come la concorrenza tra le aziende presenti in questo settore, che siano esse produttrici di hardware o software, sia continuo cambiamento e tale rivalità non risiede nel campo tecnologico, oramai considerato una base fondamentale per la sopravvivenza, ma nel soddisfare il bisogno del cliente. Si passa da un vantaggio competitivo basato sulla tecnologia ad un vantaggio centrato al cliente e su nuove idee di gioco. Infatti se analizzassimo il mercato delle console capiremmo come

il successo di Sony, Microsoft o Nintendo sia determinato, fra le altre cose, dalle esclusive riservate alle loro console più che dalla potenza della console stessa.

2.3 Note sulla sicurezza

Sebbene i gioocatori da mobile siano quelli spendono di piú per oggetti in gioco, non risultano il target preferito degli hacker. Infatti i giocatori da conosle e pc hanno un impatto sociale e mediatico molto più elevato e sono i più seguiti sia sulle principali piattaforme di straming ma anche sui social in generale. Impossesandosi dell'identità digitale di quest'ultimi un hacker potrebbe chiedere un riscatto proporzionale alla fama e al seguito del videogiocatore e non solo agli acquisti fatti da quest'ultimo. Inoltre i principali tornei eSportivi riguardano titoli presenti solo su console o pc, quindi, è ragionevole pensare che chi abbia fama in questo settore utilizzi questi device piuttosto che lo smartphone o il tablet. Poche major dei videogiochi chiedono un token (qualcosa che il gamer ha) o la verifica biometrica (qualcosa che il gamer è) per autenticare il videogiocatore. Spesso viene inviata una mail di verifica contente un codice univoco, implementando la verifica in due passaggi. Se la casella di posta fosse protetta solo dalla password allora non esisterebbe un secondo fattore di autenticazione e tutta la sicurezza si baserebbe su qualcosa che l'utente sa. Nel migliore dei casi viene utilizzato un sms di verifica che, come spiegato prima, è il metodo meno sicuro per garantire l'autenticazione.

2.4 Aidentigo

Aidentigo è una società con l'obbiettivo di proteggere i videogiocatori, o meglio, la loro identià online. Lo scopo di Aidentigo é quello di evitare che i videogiocatori siano vittime di furti di identit'a che costerebbe loro oltre a tutte lo ore spese sul gioco, gli oggetti comprati o trovati in gioco, le monete virtuali acquistate (con denaro reale) un danno economico e d'immagine non da poco se questi fossero streamer o videogiocatori di professione. Per compiere il proprio obiettivo Aidentigo intende sviluppare un'applicazione (ononima) attraverso la quale avvisare in tempo reale i videogiocatori nel momento in cui sorgano problemi di sorta con la loro identità, sia nel caso le loro informazioni sensibili dovessero trapelare in rete sia nel caso in cui qualcuno rechi alle loro identità un attacco diretto.
Il problema che Aidentigo evidenzia è rappresentato dal fatto che le mail dovrebbero virtualizzare il sistema di posta tradizionale, o al di più rappresentare un sistema di messaggistica che in quanto tale dovrebbe essere utilizzato per lo scambio di messaggi di posta. Tutta via in molti servizi online, fra cui anche quello del video gioco, la mail viene utilizzata come metodo di identificazione e autenticazione: alla mail viene associata un account quindi un'identità. Concretamente però non avverrà mai uno scambio di messaggi fra l'utente e la software-house ma piuttosto sarà una conversazione unidirezionale nella quale il fornitore del servizio manda messaggi di verifica o avvisi al giocatore. In questo modo ci si espone al rischio di mancata lettura da parte dell'utente di un avviso di sicurezza, a seguito di mal indirizzamento del messaggio nella posta indesiderata,o più semplicemente, a seguito di una disattenzione da parte dell'utente stesso. Se invece esistesse un'applicazione dedicata a notificare questi eventi, l'utente, attraverso la notifica, avrebbe un riscontro immediato rispetto al problema di sicurezza che coinvolge il suo account o i suoi dati e, potrebbe agire di conseguenza. Aidentigo, quindi, vuole offrire un dominio "utente@aidentigo.com" ad esempio, al quale l'udente possa associare la sua identità di videogiocatore e mediante il quale possa accedere anche all'app nella quale gestire le sue preferenze riguardo la

sua identità digitale. In particolare potrà scegliere quali aziende potranno inviargli mail, così da non ricevere posta da altri soggetti; in pratica la casella sarà oscurata a chiunque a meno delle aziende scelte dall'utente. Nei sistemi di mail tradizionale avviene il contrario: la casella è raggiungibile da chiunque conosca l'indirizzo, sarà poi il proprietario a bloccare mittenti inesiderati.

Capitolo 3

Esperienza tirocinio

3.1 Tesla consulting

Tesla Consulting è una azienda di Consulenza e Servizi informatici ad alto potenziale tecnologico completamente specializzata sulle tematiche della Cyber Security e della Digital Forensics (Informatica Forense) fondata da Stefano Fratepietro. Dal 2019 entra nel gruppo Be Think, Solve, Execute S.p.a, multinazionale italiana quotata nel segmento STAR della Borsa Italiana, leader nella consulenza e servizi informatici per il mondo finanziario ed assicurativo.

Grazie ad un importante lavoro di ricerca e sviluppo iniziato sin dai primi anni di attività, l'azienda si è fortemente specializzata nella realizzazione di consulenze tecniche nel settore dell'informatica forense, nella gestione degli incidenti informatici e nella creazione di servizi atti al monitoraggio pro-attivo con l'obiettivo di individurare, mitigare e gestire gli attacchi informatici ai dati, agli asset e alle persone.
Sono venuto a conoscenza di Tesala dato il mio interesse nel proseguire gli studi nel loro stesso campo. Fin dal primo colloquio Stefano si è dimostrato più che disponibile: proponendomi di lavorare insieme ad un team per Aidentigo.

3.2 Obiettivi

L'obbiettivo finale era la realizzazione di un app che potesse avvisare in tempo reale i videogiocatori qualora ci fosse un problema di sorta l'accesso e l'autenticazione del loro account di gioco. Il mio obiettivo primario quando sono entrato a far parte dell'organizzazione è stato la definizione e l'implementazione delle API necessarie per la comunicazione con un server (mail) sul quale avrei dovuto installare postfix e dovecot per la gestione della mail in ingresso e in uscita.
Nello specifico il mio compito, era quello di capire come utilizzare i protocolli IMAP e SMTP attraverso python per permettere agli utenti di: leggere le nuove mail, inviare, eliminare, cercare una mail e creare un nuovo utente quindi una nuova casella di posta.
Le prime attività svolte quindi, sono state quelle di programmazione delle api e inizializzazione del server. Come obbiettivo personale avevo quello di crescere professionalmente acquisendo delle nuove competenze anche in ambito di sicurezza informatica, ambito in cui lavora Tesla Consulting.

Attività svolte:

- Studio e comprensione dell'ambiente di sviluppo e del dominio di lavoro
- Sviluppo e implementazione API utilizzando python come linguaggio
- Configurazione mail server attraverso lâinstallazione e la configurazione dei demoni postfix e dovecot
- Irrobustimento del server

Al momento dell'assunzione esisteva già un progetto in essere che comprendeva: un applicazione front-end e delle API per la comunicazione con un database, alla definizione di questi artefatti non ho partecipato.

3.3 Analisi e valutazioni

Le mie competenze e conoscenze iniziali non erano sufficienti per il conseguimento del mio obbiettivo. Tutta via potendomi confrontare con esperti del settore e documentandomi autonomamente in rete ho potuto accrescere le mie conoscenze e consapevolezze rispetto la sicurezza informatica. In oltre ho rafforzato il mio utilizzo di python e appreso meglio come funzionano i sistemi di mailing e i soggetti che li compongo (MTA MDA MUA) La prima attività che ho svolto una volta che mi è stato presentato il progetto è stato lo studio e lâapprendimento dell'ambito e dell'ambiente di sviluppo.
Le mie conosceze rispetto al funzionamento di un mail server erano scarse, autonomamente, quindi mi sono documentato e ho appreso come funziona un sistema di mailg e come le mail vengono gestite dai server. Ho studiato quindi i soggetti che permettono il funzionamento della posta elettronica e i particolare ho appreso il funzionamento dei Mail transfer agent, dei Mail delivery agent e dei Mail user agent.

3.3.1 Mailing

I servizi di posta elettronica si basano sull'utilizzo di server che hanno funzioni particolari e usano protocolli specifici per lo smistamento delle mail in arrivo e in uscita.
La struttura di tali servizi infatti sfrutta dei server dedicati come:

- MUA (Mail User Agent): Definisce il client di posta che usiamo nelle nostre macchine per inviare e ricevere la posta
- MTA (Mail Transport Agent): Definisce i vari server che il messaggio attraversa per arrivare al mta del destinatario. Questi server comunicano tra di loro tramite il protocollo SMTP.
- MDA (Mail Delivery Agent): Definisce il software incaricato di prelevare la posta dal MTA del destinatario per immagazzinarla nella mailbox della persona a cui è destinata che provvederà a leggerla.

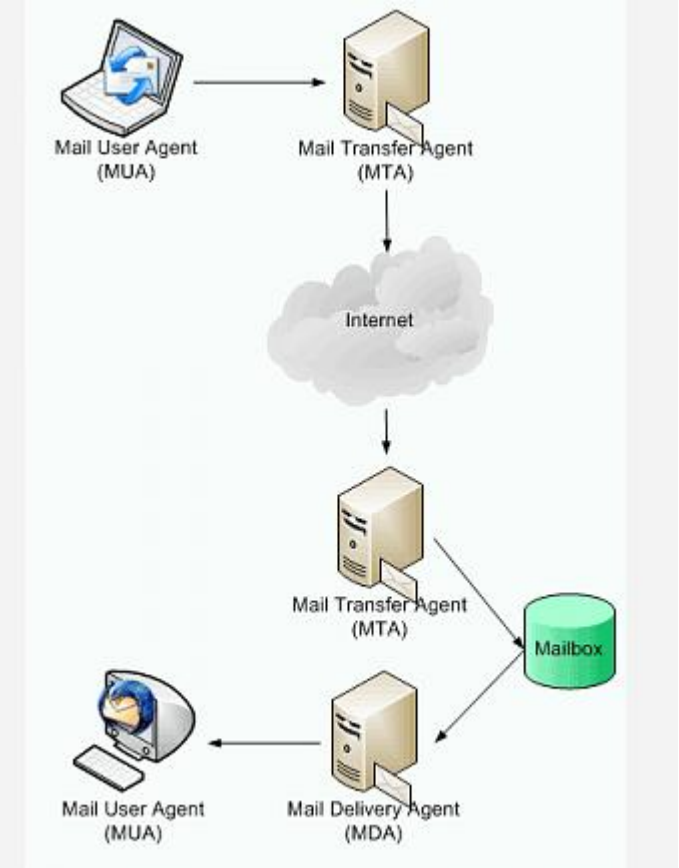

Figura 3.1: funzionamento mail

Al momento dell'invio di un'e-mail, il messaggio è inoltrato da server in server fino al server del destinatario. Più esattamente nel momento in cui viene richiesto lâinvio del messaggio il nostro client contatta il server SMTP (MTA), detto anche server di posta in uscita, che si occupa di inviare la mail ad altri server tramite il protocollo SMTP e interrogazioni DNS fino a ragigungere il server MTA di destinazione. Una volta raggiunto l'utimo MTA la posta viene prelevata e immagazinata nella mail box del destinatario dal MDA. Due protocolli principali permettono di rilevare la posta su un MDA:il protocollo POP3 (Post Office Protocol), il più vecchio, che permette di rilevare il proprio messaggio ed eventualmente di lasciarne una copia sul server;

il protocollo IMAP (Internet Message Access Protocol), che permette una sincronizzazione dello stato dei messaggi (letto, cancellato, spostato) tra più client di messaggeria. Con il protocollo IMAP una copia dei messaggi viene conservata sul server per poter assicurare la sincronizzazione. Il ritiro della posta avviene tramite un software detto MUA (Mail User Agent), Mozilla Thunderbird, Microsoft Outlook ne sono alcuni esempi. Un server di posta inoltre deve avere la disponibilità di un IP Statico e sia abilitato al reverse DNS: ossia partendo da un indirizzo IP verifica lâassociazione al nome dellâ host. Questa tecnica serve per verificare che chi spedisce la posta sia effettivamente colui che dice di essere e in caso contrario etichettare la mail come SPAM. Da questo deriva quindi una corretta autenticazione delle mail, e lâaccertarsi che il server non sia Open Relay cioè che verifichi la provenienza del messaggio prima di inololtrarlo evidanto che il proprio IP finisca in qualche black list. Per quanto riguarda l'autenticazione della mail a livello SMTP esiste un record nel quale vengono specificati i server autorizzati a spedire mail per conto di un certo dominio: il record SPF.

3.3.2 Postfix e dovecot

La parte più importante di un sistema di posta elettronica è probabilmente lâagente MTA (Mail Transfer Agent) che è responsabile della ricezione dei messaggi da Internet o dagli utenti interni e del loro arrivo a destinazione (agli altri server di posta elettronica oppure alle caselle degli utenti interni). Postfix è stato scelto quale agente di trasferimento della posta in quanto offre molteplici funzionalità, ha un eccellente sistema di registrazione degli eventi relativi alla sicurezza, è veloce, facile da configurare ed è attivamente sviluppato. La sua struttura è basata su diversi demoni che lavorano sinergicamente ma hanno aree di responsabilità distinte, possono operare in contesti di sicurezza distinti e possono impiegare regole differenti. Posfix accetta sia messaggi sia da sorgente locale, sia da rete esterna. In quest'ultimo caso il demone smtpd sarà in ascolto sulla porta 25 e in caso di arrivo di una mail sarà tale demone a gestirne la ricezione per poi avviare i processi necessari all'inoltro. La figura mostra come un messaggio attraversa un sitema Postfix

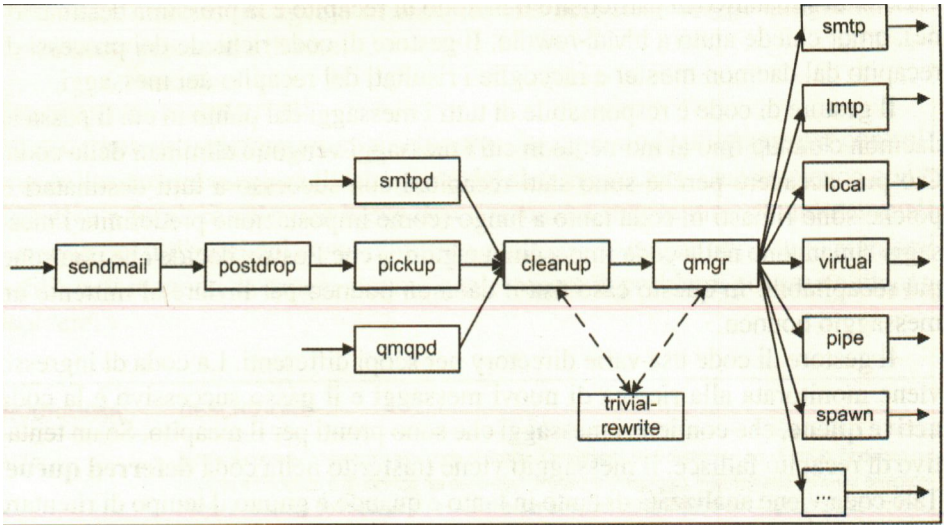

Figura 3.2: Funzionamento postfix

Dovecot invece rappresenta l'MDA utilizzato. Questo mail delivery agent

è stato progettato per garantire la sicurezza ed è attualmente utilizzato su più del 70 % dei mail server unix-like data la sua estrema configurabilità ed efficienza,' in pú è totalmente compatibile con postfix.

3.4 Definizione API

La prima attività che mi à stato chiesto di svolgere è stata la definizione delle api che avrebbero permesso all'applicazione, quindi all'utente, di contattare il server di posta per gestire la sua casella.

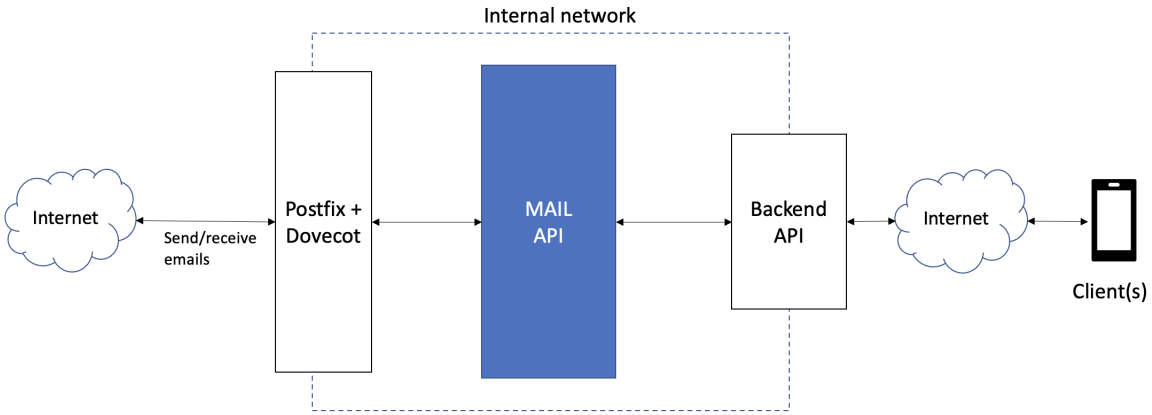

Figura 3.3: Obbiettivo tirocinio

L'API che avrei dovuto implementare sono quelle blu in figura, le MAIL API. Per omogeneità mi è stato chiesto di utilizzare python come linguaggio di programmazione poiché le api che permettevano la comunicazione con il database (Backend API), erano giÃ state scritte da un mio collaboratore in python. Nel dettaglio è stato chiesto di implementare le seguenti funzioni:

- Creazione nuovo utente (che lato API MAIL corrisponde alla creazione di una nuova mailbox)
- Controlla la presenza di nuove email (il client tramite meccanismo di polling del backend ad intervalli configurabili, verifica se ci sono nuove

email da mostrare all'utente. Il backend ritorna una lista contenente gli ID delle nuove email)

- Fetch delle email
- Invio nuova email
- Elimina email

La prima difficoltà nell'implementare queste api è stata quella di capire come potersi connettere col server utilizzando python. Durante lo svolgimento di questa attività ero completamente autonomo e non avendo esperienze pregresse mi sono documentato in rete individuando in paramiko la libreria adatta per lo scopo. Attraverso questa libreria è possibile collegarsi con un tunnel ssh ad uno specifico server e, mediante appositi comandi, far eseguire al server determinate istruzioni.

3.4.1 SSH

L'SSH consente a due computer di stabilire una connessione sicura e diretta all'interno di una rete potenzialmente non sicura.Ciò è necessario per garantire che terzi non possano accedere al flusso di dati e che i dati sensibili non finiscano nelle mani sbagliate. SSH cripta la connessione tra due computer consentendo a un computer di essere servito da un secondo computer. L'SSH non solo fornisce una connessione cifrata, ma garantisce anche che tra i computer designati vengano stabilite solo connessioni (in modo che non sia possibile alcun attacco man-in-the-middle) e che i dati corrispondenti non possano essere manipolati durante il tragitto verso il destinatario. L'accesso al computer remoto in origine avveniva sempre tramite la riga di comando così come i comandi da fare eseguire.
Poiché la porta utilizzata per le connessioni SSH è nota (la 22) e si sa che trasmette dati sensibili, essa è il bersaglio preferito dai criminali informatici. Alcuni utenti ritengono quindi utile riposizionare la porta SSH. Tuttavia si

tratterebbe solo di una protezione a breve termine, perché con uno scanner di porte è possibile trovare tutte le porte utilizzate da un calcolatore.

Nell'ottica di fare unit-testing, quindi testare ogni singola funzione che implementavo mi era necessario un server, temporaneo, su cui testare ciò che scrivevo. Sempre in autonomia quindi ho deciso di istanziare un istanziare server personale(ubuntu) AWS al quale connettermi in ssh sia attraverso il terminale sia attraverso paramiko. Sebbene fossi riuscito a implementare, attraverso paramiko: la creazione di un nuovo utente, l'invio di una nuova mail, e l'eliminazione di una mail discutendone con un responsabile abbiamo considerato questo approccio poco scalabile.Lanciare comandi da remoto infatti, era un procedimento troppo macchinoso e lavorava ad un livello (d'astrazione) troppo basso il che lo rendeva un procedimento poco scalabile. Ci siamo chiesti, quindi, se esistesserso librerie python che implementassero i protocolli IMAP e SMTP utilizzati per la ricezione e l'invio di mail.

3.4.2 SMTP E IMAP

Il protocollo SMTP (Simple Mail Transfer Protocol) è il protocollo standard che permette di trasferire la posta da un server ad un altro. Questo è un protocollo lavora al livello di TCP/IP.
Il protocollo SMTP funziona grazie a dei comandi testuali inviati al server SMTP (per default sulla porta 25). Ognuno dei comandi inviati dal client è seguito da una risposta del server SMTP composta da un numero e da un messaggio descrittivo.
All'apertura della sessione SMTP, il primo comando da inviare è HELO seguito da uno spazio e dal nome del dominio del vostro terminale. Dall'aprile del 2001, le specifiche del protocollo SMTP definite nella RFC 2821, impongono che il comando HELO sia sostituito dal comando EHLO. Il protocollo IMAP (Internet Message Access Protocol), consente al client di posta elettronica di accedere ad un server di posta gestendo la sincronizzazione tra i messaggi archiviati sul computer locale e il server di posta stesso. In pratica, lâIMAP

permette al client di scaricare la posta dal server e quindi di accedere, leggere e cancellare le email attraverso altre macchine, sincronizzando con il server le operazioni effettuate. Quando il client si connette al server di posta, IMAP controlla lo stato dei messaggi (se ci sono nuovi messaggi in arrivo, messaggi cancellati o email in bozza) senza scaricare le email, ovvero memorizzando i risultati in cache; se lâutente apre, cancella o archivia i messaggi, le modifiche vengono successivamente inviate al server. In questo modo, IMAP gestisce la sincronizzazione dei messaggi direttamente sul server.

Appurata l'esistenza di tali librerie (imaplib e smtplib) è stato necessario lo studio e la comprensione del funzionamento. Questa attività mi ha richiesto diverso tempo poiché le mie conoscenze sui protocolli e gli standard a cui facevano riferimento non era sufficiente per garantirne un corretto utilizzo. Le librerie infatti, esponevano diversi metodi e molti di questi si aspettavano in input un parametro quindi un oggetto e o una variabile definita secondo un certo standard e/o con una certa struttura.*parlo di imap e smtp* Una volta capito il loro meccanismo di funzionamento ho proseguito implementando le funzioni sopra elencate e testandole sul mio server; eccezion fatta per la prima: non ho trovato nelle librerie imaplib e smtplib comandi utili per la creazione di una nuova casella di posta(quindi un nuovo utente sul server) perciò ho deciso di mantenere per questa l'utilizzo di paramiko poich''e anche considerando gli svantaggi sopra descritti l'ho ritenuto il miglior modo.

Accertandomi che le api funzionassero correttamente ho esposto il codice al responsabile il quale mi ha incaricato di caricarlo su git-hub per integrarlo con quello già esistente.

Oltre ai risultati oggettivi e concreti ottenuti, quindi i files .py contenenti le api considero un risultato anche la conoscenza acquisita da qusta prima attività, infatti ho approfondito la conoscenza dei protocolli IMAP e SMTP ed inoltre ho approfondito il funzionamento, da un punto di vista sistemistico, di un mail server

3.5 Configurazione mail server

Una volta scritte e le Api mi è stato chiesto di configurare un server e predisporlo per l'invio e la ricezione di mail, anche in questo caso è stata un'attività prettamente individuale. La configurazione di un mail server l'avevo già affrontata autonomamente poichè la ritenevo necessaria per il testing delle API. Tutta via la prima volta ho configurato una macchina utilizzando ubuntu come sistema operativo e avendo totale accesso alla console AWS. Tesla consulting invece mi ha messo a disposizione una macchina con un differente sistema operativo, più leggero, centOS 8 e nessun accesso alla console di AWS. Anche se simili esistono alcune differenze tra i due sistemi operativi che rendono leggermente più complessa la configurazione su centOS. Non avendo a disposizione la chiavi per accedere con l'ssh ho dovuto, innanzitutto, generare la mia chiave pubblica che Matteo, mio diretto responsabile, si è occupato di caricare nella cartella .ssh di "centos", l'utente di default dell'istanza del server. Una volta stabilita, attraverso il terminale, la connessione con il server ho dovuto cambiare le repository per l'installazione softaware e migrare da quelle di centOS a quelle di un altra distro (CentOS Stream 8Â) poiché, le prime, non più supportate. Fatto ciò ho potuto procedere alla configurazione del mail server la quale si può suddividere in due fasi:

â¢ configurazione postfix â¢ configurazione dovecot

Un'operazione preliminare all'installazione dei due demoni (postfix e dovecot) che gestiscono la posta è quella di dover impostare l'hostname e di dire al server di preservarlo altrimenti amazon lo cancellerebbe ad ogni riavvio.

3.5.1 Configurazione postfix:

Una delle principali differenze che ho riscontrato tra ubuntu e centOS è l'apertura di un'interfaccia grafica che guida la condigurazione su ubuntu, assente su centOS. Infatti, dovendo lavorare con tale sisetema operativo, la configurazione del MTA (Postfix) avvienei file di configurazione (in /etc/posfix/main.cf e /etc/postfix/master.cf). Attraverso questi file è possi-

bile, fra l'altro, configurare i parametri TLS(transport security layer) e per rendere più sicura la comincazione tra il client e il server postfix. Una verifica della corretta configurazione e quindi di un'opportuna risposta del server si può avere attraverso il comando *telenet localhost 25*

3.5.2 Configurazione dovecot:

La configurazione di dovecot non è troppo dissimile da quella di postfix.Una volta installato infatti attraverso i file di configurazione ho scelto il il tipo di protocollo da utilizzare (IMAP o pop3) in ricezione, definito la cartella nella quale verranno salvate le mail in arrivo e abilitato la connessione TLS.

Dopo aver configurarto postfix e dovecot ho controllato che le porte standard per l'imap e smtp fossero in ascolto e ho voluto poi verificare che le API che avevo precedentemente implementato funzionassero, si è richiesta l'apertura delle porte per l'smtp e l'imap attraverso la shell di amazon. Verificato che le API funzionassero correttamente, aiutato dal mio responsabile, ho proceduto con l'irrobustimento della macchina nell'ottica di renderla il più possibile protetta da attacchi esterni.

3.6 Hardening del server

L'harening del server è stata, a mio avviso, l'attività più complessa fra quelle proposte.Prima di tutto ho capito cosa si intendeva per âhardeningâ: fondamentalmente ho dovuto irrobustire il server per renderlo meno vulerabile quindi più protetti i dati. Le prime cose che ho fatto quindi sono state: verificare che le configurazioni ssh permettessero il login solo mediate la chiave e non attraverso una password, rendere non modificabili file sensibili come /etc/passwd e /etc/shadow. Mi sono state sollevate almeno tre criticità da gestire durante questa fase:

- Il server essendo su internet è visibile anche da bot che provano attacchi di tipo brute-force si può attraverso i log verficare se qualche tentativo di accesso è andato a buon fine?

- L'api per mandare una mail non chiede nessun tipo di autenticazione, quindi chiunque può madare una mail attraverso il server?

- l'utente centos, quello di default, non ha una password assegnata come posso leggere la posta dell'utenza centos ? Un attaccante potrebbe sfruttarlo?

Verificando i log attraverso âgrep -i "accept" /var/log/logsecure-20220403â e grep -i "accept" /var/secure si è costatato che non cerano state intrusioni. Per quanto rigurarda l'invio della mail: effettivamente non cera nessun controllo di login, tuttavia la libreria smtplib fornisce un metodo per autenticarsi ho quindi modificato l'api in modo tale che prima di poter inviare una mail venga effettuato il log in. Per una miglior sicurezza Aidentigo poi, dovrebbe rendere disponibile l'autenticazione a due fattori, per garantire maggiormente l'identità dell'utente. L'utente di default delle istanza AWS non ha una password, infatti gli è consentito l'accesso lo mediante l'utilizzo della chiave privata, che viene fornita all'admin nel momento dell'inizializzazione del server. In questo modo il server risultava più protetto, ma esistevano ancora altri accorgimenti che si sarebbero potuti prendere ad esempio l'installazione di un software che blocchi un ip dopo un certo numero di tentativi di accesso o un firewall che protegga da tentativi di accesso non provenienti da internet. La parte cruciale di questa attività è stato comprendere che l'irrobustimento di una struttura non si basa solo nell'installazione di software che ne garantiscano la difesa ma anche nel pensare quale informazioni, sensibili o no, vengono esposte durante la configurazione e come queste informazioni, se utilizzate da mal intenzionati, possano minare la stabilità dell'azienda.

3.7 Conclusioni

Sono grato di aver potuto effettuare un'esperienza del genere che mi ha permesso di crescere sia a livello professionale acquisendo nuove skills.Attraverso questa esperienza ho capito che prima di specializzarsi in sicurezza informatica occorre capire il funzionamento sistemistico dei server, ad esempio, e avere profonda conoscenza della struttura di rete.

Conclusioni

Concludo questo elaborato sottolineando quanto sia importante la gestione della propria identità digitale al giorno d'oggi. In una società' sempre più orientata al metaverso e alla digitalizzazione in generale, mettere in sicurezza il proprio io digitale diventa una priorità. In questo scenario la password costituisce una difesa fondamentale e in quanto tale non andrebbe sottovalutata. Una password sicura dovrebbe essere abbastanza lunga (almeno otto caratteri) contenere sia maiuscole che minuscole oltre che numeri e caratteri speciali. In più non dovrebbe contenere parole di senso compiuto o informazioni che possano essere ricondotte al proprietario per scongiurare attacchi a dizionario o facilitare tecniche di ingegneria sociale. Attraverso queste tecniche è possibile che un hacker studi il suo bersaglio individuando interessi, abitudini e affetti al fine di restringere il dizionario sul quale basare l'attacco. Avendo queste informazioni l'attaccante potrebbe progettare il phishing delle informazioni: attraverso l'invio di messaggi di posta o la creazione di siti web, abilmente contraffatti (e in linea con il profilo psicologico della vittima) si riusciranno a ottenere le informazioni e i dati desiderati. In questo ultimo caso la robustezza della password sarebbe vanificata dall'ingenuità della vittima che non dovrebbe mai scrivere tali tipi di informazioni su siti e mail inaffidabili.
La robustezza della password e la sicurezza della propria identià dipende anche dall'unicità della password. Ad oggi si possono avere tante identià in rete quanti sono i servizi ai quali si vuole accedere, ocorrerebbe avere password diverse per ogni identià che si vuole mantenere. Una componente fonda-

mentale nel garantire la sicurezza è il metodo di autenticazione. Non tutti i servizi disponibili in rete ad oggi utilizzano l'autenticazione a due fattori per autenticare i propri utenti, esponendoli al rischio di furto d'identità. La gravità di tale crimine, oltre al crimine stesso che comporta la perdità della propria identità in rete, è data dalla non consapevolezza dell'utente a ciò che sta accadendo al proprio account che lo porta ad agire in ritardo. Aidentigo è un app con l'obbiettivo di rendere immediato all'utente un problema che riguarda la sicurezza del suo account. Il vantaggio di Aidentigo rispetto ai sistemi di identificazione moderni (i quali utilizzano una casella di posta) è la possibilità di avere un app dedicata alla notifica di eventi sospetti che consente all'utente di averne un riscontro immediato in tal modo non correrebbe il rischio di ignorare la mail o di agire in ritardo. In più l'applicazione è progettata da esperti di sicurezza informatica che curano ogni aspetto dell'app ponendo un forte accento sulla sicurezza appunto.

Bibliografia

Keith W. Ross *Reti di calcolatori e internet. Un approccio top-down.* 7/Ed.

Giusella Finocchiato *Diritto di intetnet* 2008

Sitografia

https://hls-dhs-dss.ch/

https://legaldesk.it/

https://semplicecome.it

https://www.pandasecurity.com/

https://www.zerounoweb.it/

https://academy.bit2me.com/

https://brilliant.org/

https://www.agendadigitale.eu/

https://www.bucap.it/

https://www.commissariatodips.it

https://www.extraordy.com

https://it.ccm.net

https://www.plesk.com

https://www.ilger.com

https://www.player.it

https://www.repubblica.it

https://help.infocert.it/