Sistemi e Reti
Simulazione seconda prova d'esame
Area di progetto, proposta di correzione

EMANUELE SCAPIN
ITT G. Chilesotti - Thiene (VI)
11 maggio 2018

Sommario

Il presente documento intende fornire una possibile e plausibile correzione alla prova d'esame di Sistemi e Reti che gli studenti delle classi quinte hanno analizzato e implementato durante l'area di progetto tenutasi nei giorni 19-20 e 23 Marzo 2018. La prova somministrata era quella prevista dal ministero come sessione suppletiva 2016 della seconda prova scritta.

Si intende fornire una traccia di correzione soprattutto della parte riguardante la progettazione della rete, quindi della prima parte, anche utilizzando le parti più significative fornite dagli studenti, mentre per la seconda parte si fornisce un estratto delle migliori risposte fornite dagli studenti stessi.

Keywords: sistemi , reti , esame , simulazione , progettazione, LAN

Introduzione

La richiesta è quella di progettare una rete per una compagnia di taxi che vuole implementare un sistema automatizzato di prenotazioni da parte dei clienti, il testo richiede che il servizio sia raggiungibile con tutti i mezzi di comunicazione sia fissi che mobili (telefono, Web, App, SMS, ecc.), si può quindi ipotizzare che l'azienda abbia la necessità di avere una rete locale LAN con un centralino telefonico, almeno un server web, un server con database, oltre agli usuali elementi presenti un una rete locale.

Non è chiaro dal testo le dimensioni dell'azienda, il numero di dipendenti, la suddivisione in reparti, la struttura dell'edificio in cui dovrebbero

essere collocati gli operatori e quindi di come dovrebbe essere cablata la rete, si faranno quindi delle ipotesi.

1 Prima parte

L'azienda di gestione del servizio taxi non è presentata nel dettaglio per quanto riguarda la dimensione per numero di persone impiegate e non è definito lo stabile o gli stabili in cui sono presenti i vari uffici della stessa. Per semplicità si può ipotizzare che tutte le attività siano presenti in un unico edificio, diviso per uffici, anche su più piani.

1.1 Cablaggio

Il cablaggio strutturato è una metodologia di progetto e realizzazione degli impianti di telecomunicazione interni agli edifici che si è resa necessaria a causa della crescente complessità degli impianti telefonici e delle reti dati. Il cablaggio può essere di tre tipi: orizzontale, verticale e di campus.
Il cablaggio orizzontale, o HCC (Horizontal Cross-Connect), riguarda il cablaggio del singolo piano. Comprende il permutatore di piano e i cavi ethernet che raggiungono i connettori a muro. Il cablaggio verticale, invece, riguarda il collegamento tra i vari piani di un edificio ed è anche chiamato VCC(Vertical Cross-Connect). Gli armadi di piani sono collegati tra loro dalla dorsale di edificio (Intrabuilding Backbone) e si collegano al permutatore di edificio (Intermediate Crossconnect).
Infine, il cablaggio di campus collega edifici diversi di uno stesso comprensorio attraverso un collegamento diretto e veloce, la dorsale di comprensorio (Interbuilding Backbone). In questa azienda, visto che il numero di dipendenti non è molto elevato, si suppone che la progettazione del cablaggio riguardi esclusivamente i piani dell'edificio, mentre sarà a carico dell'ISP i relativi collegamenti verticali e dorsali.
I cavi utilizzati devono essere di cat 7 (velocità fino a 10 Gbps) per non rallentare il traffico interno tra le eventuali VLAN e i server. Si consiglia inoltre una connessione internet con almeno 20Mbps in upload per garantire la funzionalità del server web senza interruzioni o rallentamenti.

1.2 Topologia della rete

Si possono fare alcune ipotesi:

1. per garantire la storicizzazione dei dati è necessario un server con database, meglio un DBMS gratuito come MySQL o PostgreSql per evitare costi sulle licenze,

2. per erogare i servizio web si può prevedere almeno un server web per il deploy delle portale che erogherà sia in Internet che in Intranet, quindi con IP pubblico e in DMZ;
3. per la gestione della telefonia si può ipotizzare un altro server che funga da centralino telefonico,quindi con IP pubblico e in DMZ;
4. la connettività tra il dispositivi sui veicoli taxi potrebbe essere effettuata tramite connessione GSM/GPRS (questa soluzione deve prevedere un sistema di ricezione con sim telefonica) oppure con connettività dati 3G/4G/Lte su chiamate a web service o API erogate tramite un application server[1] (questo potrebbe essere lo stesso server web del punto 2).

L'analisi della realtà ci porta a fare le seguenti scelte.
Considerando l'organizzazione standard delle aziende, la compagnia di taxi viene divisa in quattro sezioni:

1. sezione amministrativa, che comprende sia il controllo delle direttive manageriali sia la gestione hardware e software di tutta la strumentazione della compagnia (computer, server, telefoni, switch...);
2. sezione logistica/sala operativa, che gestisce e controlla i mezzi e le persone impiegate;
3. sezione call center, formata dagli operatori che rispondono alle richieste telefoniche;
4. sezione manageriale/altra, i cui compiti riguardano la gestione del patrimonio aziendale, del personale e della strategia commerciale;
5. sezione tecnica con i server e quella per i server i DMZ.

La prima soluzione adottata è di tipo tradizionale e prevede la divisione della LAN aziendale in sottoreti, in modo da separare le varie realtà dell'azienda e le macchine server, in particolare le macchine da mettere in DMZ. L'approccio sarà inoltre tradizionale per quando riguarda la gestione delle macchine server, definendo quindi delle singole macchine e non proponendo la gestione di host con macchine virtuali, magari ridondate, né proponendo una gestione di tutti o di alcuni server in cloud [2].

[1] Non necessita di server o sim telefoniche dedicate ma utilizza la stessa tecnologia per l'erogazione degli altri servizi web.

[2] L'utilizzo di un server in Cloud è un'opzione, soprattutto analizzando le caratteristiche e i costi che propone Amazon. Si può optare per la scelta del server in cloud principalmente per una valutazione dei costi offerti da Amazon, che comprendono diversi servizi quali macchine server, database e backup. Verrebbe utilizzata una macchina virtuale che faccia da firewall, con ad esempio PFSense, applicazione open-sourse (completamente gratuito) che si installa in un qualsiasi PC come se fosse un semplice sistema operativo. Attraverso questo

Se l'azienda non è di grandi dimensioni e non ha un numero elevato di postazioni, operatori e impiegati, si può proporre una soluzione con reti di classe C.

Proposta con sottoreti di classe C	
Rete	Indirizzo di rete
Call center	192.168.1.0/24
Centrale operativa	192.168.2.0/24
Amministrazione	192.168.3.0/24
Altra	192.168.4.0/24
Server	192.168.10.0/24
DMZ	192.168.50.0/24

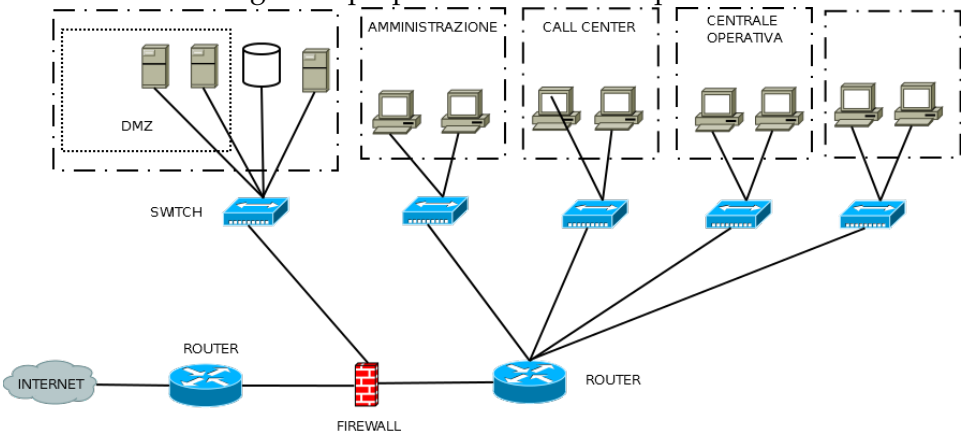
Se invece l'azienda è di grandi dimensioni e ha un numero elevato di postazioni, operatori e impiegati, si può proporre una soluzione con reti di classe A.

Proposta con sottoreti di classe A	
Rete	Indirizzo di rete
Call center	10.1.0.0/16
Centrale operativa	10.2.0.0/16
Amministrazione	10.3.0.0/16
Altra	10.4.0.0/16
Server	10.10.0.0/16
DMZ	10.50.0.0/16

La soluzione potrebbe essere quindi schematizzata con la figura seguente, dove abbiamo un router per la connessione per l'esterno e uno per la connessione con l'interno, tra di essi collochiamo il firewall per mezzo del quale si crea la connessione ai server della rete dedicata e in base al quale definiamo le regole per la DMZ definita su una rete distinta. Il router interno potrebbe anche essere sostituito da uno switch/router, le prestazioni sarebbe analoghe.

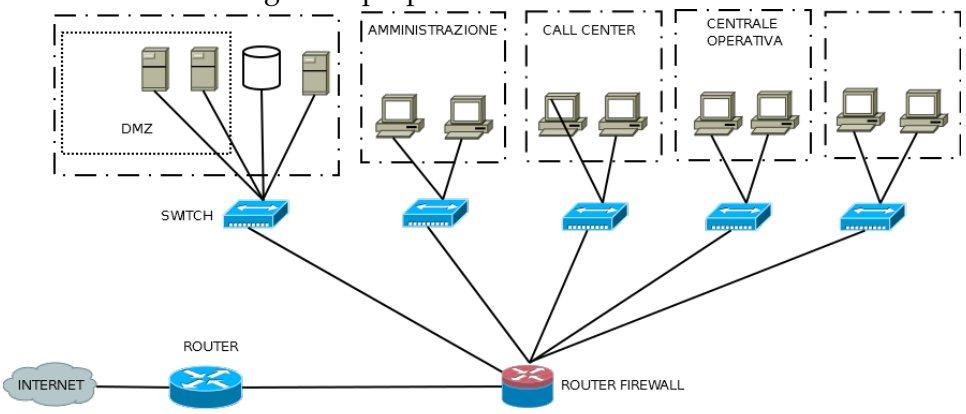
programma, il server in cloud verrà configurato per permettere l'accesso solo e soltanto da determinate macchine, anche se Amazon garantisce una certa sicurezza in ambito software. La potenza dei server può essere scalata a seconda delle esigenze, così da poterla aumentare e diminuire a seconda dei periodi più carichi di lavoro e di richieste da parte dell'utenza. L'utilizzo di una possibile DMZ potrebbe non essere quindi contemplato dato che i Server utilizzati non sarebbero in sede e il rischio di attacco malevolo all'interno dei Database sarebbe davvero basso.

Figura 1: proposta con firewall separato



Se si vuole risparmiare su qualche componente allora la soluzione presentata nella figura seguente prevede un router interno/firewall a cui connettere tutte le reti della LAN, questo componente farà pure da firewall e implementerà la DMZ.

Figura 2: proposta con firewall-router



La sottorete che connette i router e il firewall tra loro potrebbe essere definita diversamente, anche con subnet /29, in quanto deve garantire un numero limitato di indirizzi IP.
In ogni caso il firewall definirà anche la NAT oltre che le ACL per i permessi di transito e quindi le regole che definiscono la DMZ.
Deve inoltre essere previsto il Domain Controller (DC), al posto di prevederne uno per ogni sottorete, soluzione ridondante e onerosa, meglio prevederne uno solo per tutta la LAN, verrà collocato assieme agli altri server e verrà raggiunto da tutte le reti grazie ad una opportuna configurazione

dei router. Il DC lavorerà anche come DHCP Relay per tutta la rete.

1.3 Server

Per quanto riguarda la gestione dei telefoni e quindi delle comunicazioni via SMS, così come richiesto dal testo del tema proposto, si può ipotizzare di individuare un server dedicato che funga da centralino telefonico, questo naturalmente dovrà avere un ip pubblico per permettere la connettività dall'esterno e verso l'esterno della rete, con porte 5060-5070 aperte per il VOIP. Si può pensare a una soluzione ragionevole rispetto ai costi con un server Linux con installata una delle tante alternative presenti sul mercato per quanto riguarda i centralini telefonici. Per quanto riguarda la gestione degli SMS ci sono due alternative, la prima è integrare il centralino telefonico con un modulo per SMS [3], l'altro è di far gestire gli SMS da servizi forniti da terzi [4] che necessitano di una connessione al sistema tramite API per l'acquisizione dei messaggi. Il dato che arriva via SMS verrà trattato come una prenotazione così come le richieste via telefono, via web oppure via app.
Le informazioni andranno memorizzate su un database presente su un server dedicato, si può ipotizzare quindi una macchina Linux con un DBMS MySql (porta di default 3306) o PostgreSql (porta di default 5432). Questa macchina deve essere configurata opportunamente sia in base alla mole di dati da memorizzare (disco) sia in base al numero di transazioni da eseguire (CPU e RAM).
Le informazioni andranno erogate tramite una applicazione web il cui deploy verrà fatto tramite un server web dedicato, probabilmente con l'ultima versione di Apache, si deve tener presente che l'applicazione web deve essere utilizzata in Internet dai clienti ma anche in Intranet dagli operatori e dagli impiegati dell'azienda.
Vista la natura delle informazioni erogate, la localizzazione del veicolo permette di localizzare anche il conducente in modo continuativo, in conformità alla normativa vigente si deve erogare le informazioni sul web in HTTPS, sulla porta 443, quindi è indispensabile pensare all'acquisto di un certificato SSL da una Certification Authority e installarlo opportunamente su Apache. Anche questa macchina deve essere configurata opportunamente soprattutto in base al numero di richieste simultanee via HTTP/HTTPS (CPU e RAM).
Per rendere fruibile il web sia all'esterno che all'interno sarà necessario

[3] Necessita dell'acquisto di una SIM.

[4] Ad esempio Twillio (https://www.twilio.com) fornisce la gestione di SMS, necessita dell'acquisto di un numero telefonico e di una connessione tramite API .

implementare una NAT Loopback o hairpinning se la connettività verso la WAN è garantita da un solo indirizzo IP pubblico, quindi subnet /32, mentre se l'azienda ha la possibilità di usufruire di più indirizzi IP pubblici [5] il router sarà in grado di instradare correttamente le richieste.
Se per l'erogazione di pagine web è presente un server web dedicato si può pensare alla presenza di un application server per erogare web service e API, invocati dalle app per smartphone e tablet, magari tramite Tomcat, oppure per risparmiare si può installare Tomcat nello stesso server web dove è presente Apache, configurando una connessione tra Apache e Tomcat, e quindi permettendo di erogare il servizio tramite le porte 80 e 443 di HTTP e HTTPS, senza dover dedicare altre due porte a questo tipo di comunicazione.
Come già detto ci sarà un server per il Domani Controller che faccia anche da DHCP Relay di rete.
Si può anche ipotizzare la presenza di un server di posta elettronica (con porte 25, 110 e 143 aperte per l'invio e la ricezione), anche se oramai si tende a utilizzare tecnologie cloud.
Può essere utile pensare ad un server che faccia da file system condiviso, naturalmente se necessario, e sicuramente andrebbe preso in esame un server dedicato ai backup, il backup del database probabilmente avrà cadenza giornaliera, mentre il backup delle altre macchine - che hanno informazioni che vengono modificate saltuariamente - potrebbero avere cadenza settimanale [6].

I server che devono essere visibili al mondo esterno, come il server web, il server del centralino VOIP, e l'eventuale application server devono essere collocati in una DMZ per isolarli dal reso della rete e garantire la sicurezza. A titolo esemplificativo si possono riportare di seguito alcuni esempi di regole ACL del firewall per la definizione della DMZ, dove si ipotizza che il server web abbia ip 192.168.50.10 e il server database abbia ip 192.168.10.2 con database PostgreSql con porta 5432 aperta. Il server web può connettersi al server database sulla porta in cui questo è in ascolto mentre è isolato da tutto il resto della rete.

[5] Si pensi per esempio ad un indirizzo ip pubblico per la navigazione in internet, uno per il server web, uno per il centralino telefonico, magari un altro per un application server (web service e API).

[6] Si deve ricordare che il D.Lgs 196/2003, per quanto riguarda i requisiti minimi di sicurezza, stabiliva la necessità del salvataggio periodico dei dati (backup) e della possibilità del loro ripristino (recovery), il regolamento europeo GDPR - che andrà in vigore il prossimo 25 maggio 2018 - obbliga il responsabile del trattamento dei dati (l'azienda) a implementare le opportune forme di sicurezza in quanto aggrava gli oneri in caso di perdita dei dati.

Regole ACL in entrata e DMZ					
Protocollo	Origine	Porte Entr.	Destinazione	Porte Dest.	Stato
TCP	Any	Any	192.168.50.10	80	Permit
TCP	Any	Any	192.168.50.10	443	Permit
TCP	192.168.50.10	Any	192.168.10.2	5432	Permit
Any	Any	Any	Any	Any	Deny

Si deve prevedere un numero di gruppi di continuità per garantire la continuità del servizio in caso di problemi di erogazione dell'energia elettrica.

1.4 VLAN

In alternativa si può prevedere l'utilizzo di VLAN, secondo lo standard 802.1Q, per la divisione delle infrastrutture in sottoreti distinte. Le VLAN vengono distinte in base alla suddivisione della società e possono avere gl'indirizzi già previsti nella proposta precedente. Naturalmente in questo caso i dispositivi switch devono prevedere la possibilità di connessioni *trunk* così come i router, configurati secondo il protocollo di Inter VLAN/ Routing "Router-on-a-stick".
Per quanto riguarda la topologia della rete e la configurazione dei router e del firewall non ci sono differenze sostanziali con la proposta precedente.

Proposta VLAN con sottoreti di classe C		
Rete	Indirizzo di rete	VLAN ID
Call center	192.168.1.0/24	1
Centrale operativa	192.168.2.0/24	2
Amministrazione	192.168.3.0/24	3
Altra	192.168.4.0/24	4
Server	192.168.10.0/24	10
DMZ	192.168.50.0/24	50

1.5 Wireless

Se si volesse estendere la rete proposta affinché sia utilizzabile con tecnologia wireless bisogna prevedere dei dispositivi Access Point, magari connessi con una sottorete distinta, collocati in modo da offrire la massima copertura degli spazi utilizzabili all'interno dell'edificio e degli uffici. L'accesso per semplicità potrebbe essere effettuato tramite chiave e, per maggior controllo, sul MAC Address dei dispositivi. Se si volesse implementare un controllo

sugli accessi degli utenti autorizzati sarebbe invece necessario implementare un server dedicato Radius o similare.

2 Seconda parte

2.1 Punto 1

I clienti possono eseguire le richieste del servizio attraverso : una chiamata telefonica, un servizio WEB o APP, SMS. Nel caso di una chiamata per richiedere un taxi, il cliente viene reindirizzato al centralino aziendale che si occuperà, attraverso il portale web amministrativo, di prenotare un taxi con nominativo, la data di prelievo del cliente con relativa ora, il luogo e il numero di persone. Sia nel caso del servizio via WEB che APP, l'utente dovrà iscriversi al sito e compilare tutti i campi necessari per richiedere un taxi; l'unico campo non obbligatorio è il nominativo dato che viene ricavato dalla sua iscrizione. L'app consiste in un portale WEB riportato sotto forma di app scaricabile dagli appositi AppStore a seconda del dispositivo. A livello di sicurezza, verrà implementato un servizio a chiave pubblica e privata con HTTPS, così da garantire la riservatezza dei dati. Il servizio SMS viene garantito grazie a Twilio, un'azienda che si occupa di stabilire numeri telefonici a pagamento che possono essere utilizzati per ricevere messaggi a scopo lavorativo. Successivamente alla ricezione del messaggio, se rispetta i parametri pre impostati, viene restituita una stringa che verrà elaborata dai server aziendali in cloud ed inserita tra le richieste; se i parametri non vengono rispettati, viene inviato un messaggio FORM dove vengono indicati i parametri da rispettare per prenotare un taxi.

Nel progetto la sicurezza può essere garantita tramite due firewall uno posto prima e uno dopo della dmz (precedentemente spiegata), per far si che non si connettano utenti esterni con quelli interni. Ogni computer è provvisto di un anti-virus che viene aggiornato periodicamente. Le password nel data base sono codificate in formato md5. Principali vantaggi e svantaggi del cloud.

Vantaggi:

1. Non ci sono investimenti iniziali da fare sull'hardware e sul software, viene gestito tutto dalla azienda incaricata, backup, recovery e la sicurezza.
2. Elevata flessibilità e scalabilità: è semplice adeguare il servizio secondo le varie esigenze che si presentano.
3. La connessione al cloud può avvenire da qualsiasi luogo e momento, il software é online e l'unico prerequisito è avere un device e una connessione ad internet.

Svantaggi:

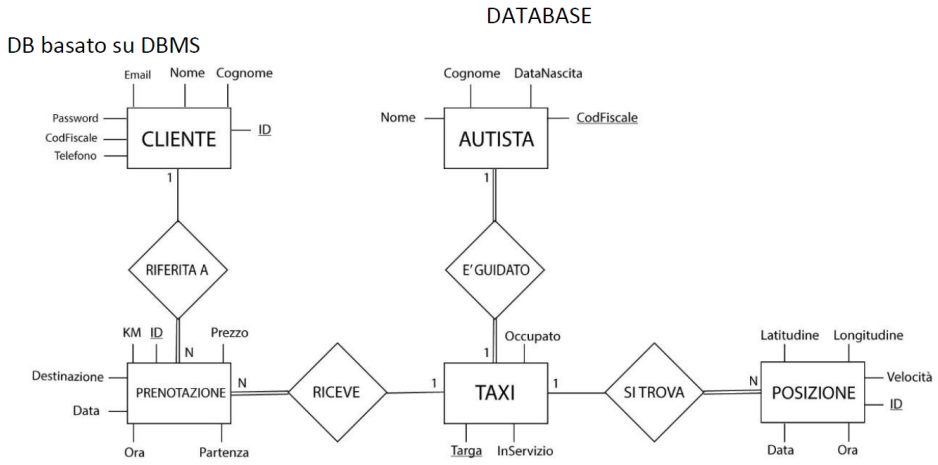
1. Il servizio di cloud funziona correttamente solo se in azienda è presente una connessione stabile.

2.2 Punto 2

L'idea di fondo dello schema del database dovrebbe procedere in questo modo: un cliente può effettuare delle prenotazioni, a una prenotazioni vene associato un taxi, selezionato tra quelli liberi più vicini al cliente richiedente, per cui è necessario avere la posizione dei taxi per effettuare la geolocalizzazione degli stessi, naturalmente ogni taxi ha un autista in servizio associato.

Lo schema proposto parte dal presupposto che ad ogni taxi è associato un autista fisso, se non fosse così bisognerebbe modificare lo schema.

Figura 3: Schema concettuale E/R proposto



Lo schema logico risulterà quindi come segue.

CLIENTE(ID, Nome, Cognome, Email, Password, CodFiscale, Telefono)
PK=ID

PRENOTAZIONE(ID, Partenza, Destinazione, Ora, Data, Km, Prezzo, ID-Cliente)
PK=ID
FK=IDCliente riferito a CLIENTE(ID)

TAXI(Targa, InServizio, Occupato, IDPrenotazione, CodAutista, IDPosizione)
PK=Targa
FK=IDPrenotazione riferito a PRENOTAZIONE(ID)
FK=IDPosizione riferito a POSIZIONE(ID)

AUTISTA(CodFiscale, Nome, Cognome, DataNascita)
PK=CodFiscale

GUIDA (CodFiscale, Targa)
PK=CodFiscale,Targa
FK=CodFiscale riferito a AUTISTA(CodFiscale)
FK=Targa riferito a TAXI(Targa)

POSIZIONE(ID, Latitudine, Longitudine, Velocità, Data, Ora)
PK=ID

Lo schema proposto ha comunque dei limiti:

1. l'associazione tra autista e taxi - è guidato - potrebbe essere una relazione N:M in modo tale da permettere a un autista di guidare taxi diversi in tempi diversi (registrando le informazioni di data inizio e data fine utilizzo, con data fine utilizzo NULL nel caso sia ancora in uso all'autista;
2. l'entità prenotazione potrebbe essere riformulata come associazione N:M tra cliente e taxi con gli stessi attributi presentati nell'entità.

Un breve estratto di codifica per la richiesta del servizio taxi in linguaggio PHP, basato sullo schema del database proposto, potrebbe essere il seguente.

```
<html>
  <head>
  </head>
  <body>
        <?php
        if(isset($_POST["invia"]))
        $conn=mysqli_connect("localhost","root","","taxiDB");
        $partenza=$_POST["partenza"];
        $dest=$_POST["dest"];
        $mail=$_POST["mail"];
        $idCliente= mysqli_query($conn,"SELECT ID FROM CLIENTE
                                    WHERE email='".$mail."'");
        mysqli_query($conn, "INSERT INTO Prenotazione
```

```
            (Partenza, Destinazione, IDCliente, Data, Ora)
            VALUES ('".$partenza."','".$dest."','".$idCliente."',"
            .date("d/m/y").",".date("H:i:s").")");
        ?>
        <form method="POST" action="#">
                <a>Inserisci partenza</a><br>
                <input type="text" name="partenza">
                <a>Inserisci destinazione</a><br>
                <input type="text" name="dest">
                <a>Inserisci email</a><br>
                <input type="email" name="mail">
                <input type="submit" name="invio">
        </form>
  </body>
</html>
```

2.3 Punto 3

Con l'espansione di internet negli ultimi decenni, molte aziende hanno deciso di offrire servizi web o semplicemente hanno deciso di pubblicare una pagina web per farsi conoscere. Chiaramente questo ha portato molti vantaggi a livello pubblicitario e sempre più persone hanno scoperto brand o start-up di altri Paesi.

Tuttavia esporsi così evidentemente su Internet può anche diventare rischioso: soprattutto se ci sono malintenzionati che vogliono accedere a dati riservati aziendali. I tipi di attacchi che un'azienda può subire dall'esterno sono 2 infatti: attacchi attivi o attacchi passivi.

Gli attacchi passivi sono a loro volta di 2 tipi: ci possono essere attacchi mirati al contenuto dei pacchetti(SNIFFING) o attacchi mirati all'analizzare il sistema o il traffico della rete.

Gli attacchi attivi invece sono di molteplici tipi:

1. Intercettazione, dove si vogliono acquisire password per rubare o modificare dati sensibili. Molte volte vengono installati software preventivamente all'interno della rete per creare finti server o finti servizi per rubare password o altri dati ai vari utenti;
2. Sostituzione di un host, dove si falsifica l'indirizzo di rete del mittente per accedere senza autorizzazione in un sistema informatico;
3. Produzione, in cui vengono generati componenti (script,programmi,...) che danneggiano il sistema. Ad esempio generando virus che cancellano file,corrompono file o danneggiano i server;

4. Phishing, dove si attirano gli utenti in server pirata per rubare loro le credenziali o per installare nei loro pc virus o trojan;
5. Intrusione,cioè la vera e propria intrusione nel sistema, attuata probabilmente con i precedenti metodi. A questo punto l'intruso può fare ciò che gli pare e cancellare o modificare tutto ciò che trova.

2.4 Punto 4

I certificati sono emessi da un'autorità di certificazione (CA), che potrebbe essere una qualsiasi amministrazione centrale fidata, che garantisce per l'identità di coloro per cui emette i certificati e a cui associa una data chiave. La CA, infatti, è una terza parte fidata la cui firma sul certificato garantisce l'autenticità della chiave pubblica legata all'utente. Nel certificato, la stringa che identifica l'utente deve essere un unico nome nel sistema (nome distinto) che la CA tipicamente associa con l'entità real-world (identità reale dell'utente). Per esempio una compagnia potrebbe emettere certificati ai suoi dipendenti, o un'università ai suoi studenti, o una città ai suoi cittadini. Per prevenire la perdita di certificati, la chiave pubblica della CA deve essere attendibile, visto che essa permette ad ogni utente nel sistema, attraverso l'acquisizione e la verifica dei certificati, di trasferire la fiducia nella autenticità della chiave pubblica in ogni certificato firmato dalla CA. Quindi una CA deve pubblicizzare la sua chiave pubblica ed esibire un certificato di un'altra CA a più alto livello che attesti la validità della propria chiave pubblica, servendosi, quindi del trasferimento di fiducia. Esempi di informazioni addizionali che la parte dati del certificato potrebbe contenere sono:

1. periodo di validità della chiave pubblica;
2. numero seriale o un identificatore di chiave che identifica il certificato o la chiave;
3. informazioni addizionali sull'entità soggetto;
4. informazioni addizionali sulla chiave;
5. stime di qualità relative all'identificazione dell'entità soggetto, alla coppia di chiavi e alla politica di emissione;
6. informazioni che facilitano la verifica della firma (per esempio l'algoritmo di firma, nome della CA);
7. lo stato della chiave pubblica (revoca dei certificati).

Una PKI, infrastruttura a chiave pubblica, è un'architettura che definisce i meccanismi e le politiche che sono necessarie, al fine di garantire l'autenticazione delle chiavi pubbliche. Una PKI può essere pubblica o privata: in

questo caso i servizi offerti sia di autenticazione che di certificazione globale, possono essere non gratuiti, ma regolati da contratti e accordi commerciali. Un'architettura PKI definisce:

1. come devono essere formattati i certificati;
2. come vengono gestite le relazioni che esistono tra le CA e gli utenti, oppure tra diverse CA;
3. le politiche che permettono la revoca dei certificati;
4. i servizi che possono essere offerti da un certificato.

È buona noma, prima di considerare valido un certificato, controllare che il suo numero di serie non compaia nell'ultima versione disponibile della CRL emessa dalla CA che ha emesso il certificato.

Come richiedere un certificato digitale:

1. generazione della coppia di chiavi asimmetriche da utilizzare per cifrare le comunicazioni: le comunicazioni tra CA e richiedente devono essere protette e quindi viene generata una coppia di chiavi dal CA direttamente seguendo la procedura indicata sul suo sito;
2. il richiedente comunica informazioni circa la propria identità alla Certification Authority: ricevute le chiavi è ora possibile comunicare le informazioni riguardanti il richiedente quali il nome di dominio, l'indirizzo email, il nome e cognome del richiedente ecc.;
3. la Registration Authority inizia la verifica dei dati ricevuti: le operazioni di controllo dei dati pervenuti alla CA possono variare a seconda del soggetto e del tipo di certificato richiesto e in questa fase possono essere richiesti anche ulteriori dati, come ad esempio l'iscrizione alla Camera di Commercio o la partita IVA;
4. se i controlli vanno a buon fine, la Certification Authority genera il certificato e lo firma digitalmente con la propria chiave privata: viene cifrato per garantire che i dati in esso contenuti non vengano modificati;
5. il certificato firmato viene inviato al richiedente che provvederà a installarlo o a farlo installare sul proprio server.

Conclusioni

La presente proposta di correzione non può certo dirsi esaustiva, in quanto essendo il tema proposto molto generico, non fissando precise caratteristiche

della rete da progettare né la dimensione e la struttura dell'azienda, può dare la possibilità a varie ipotesi di partenza e quindi una molteplicità di scelte implementative.
Per una trattazione più completa ed esaustiva degli argomenti teorici della seconda parte - specificatamente i punti 1, 3 e 4 - si rimanda al libro di testo o ad altro libro che tratta le reti di computer.
Ringrazio dell'aiuto nell'analisi della rete e delle proposte di progettazione l'amico Walter Sartori della NEW s.a.s. di Cornedo Vicentino, e il suo ex collega Cristiano, la loro esperienza sul campo è stata preziosa.
Ringrazio inoltre la collega Alessandra Chilese per il prezioso supporto e l'aiuto nella stesura di questo documento.
Last but not least ringrazio gli studenti per i lavori prodotti, tra le proposte più interessanti sono stati estratti alcuni pezzi per questo documento.