esercizi su leggi, pianificazione e progetto

soluzioni

timestamp authority

- progetta un servizio basato su firma digitale ed una “time authority” che permetta di provare a terzi che un certo documento esisteva in un certo istante e che non è stato cambiato da allora
- primitive
  - metti timestamp al documento
  - verifica timestamp

entità in gioco:

utente

autorità

metti timestamp(m: documento)

utente: h=hash(m)

utente: invia h all’autorità

autorità: t è un timestamp, $tf=[h|t]_{autorità}$

utente: memorizza tf assieme ad m

verifica timestamp(m,tf): t

utente: decripta tf con chiave publica dell’autorità e ottiene h|t

utente: verifica che h=hash(m)

utente: return t

timestamp authority e firma

- progetta un servizio che permetta di provare a terzi che la firma digitale è stata apposta su un documento in un certo istante
  - con una tolleranza comparabile ai tempi di latenza della rete
- primitive
  - metti firma con timestamp
  - verifica firma con timestamp

entità in gioco:

utente

autorità

Il sistema prova che il documento era firmato in un certo istante.

metti_firma_con_timestamp(m: documento, chiave privata di utente)

utente: h=hash(m)

utente: hf=$[h]_{utente}$

utente: mf= m|hf

utente: mettitimestamp(mf)

verifica_timestamp(mf,tf): t

utente: decripta tf con chiave pubblica dell'autorità e ottiene hf|t

utente: decripta hf con la chiave pubblica dell'utente ottenendo h

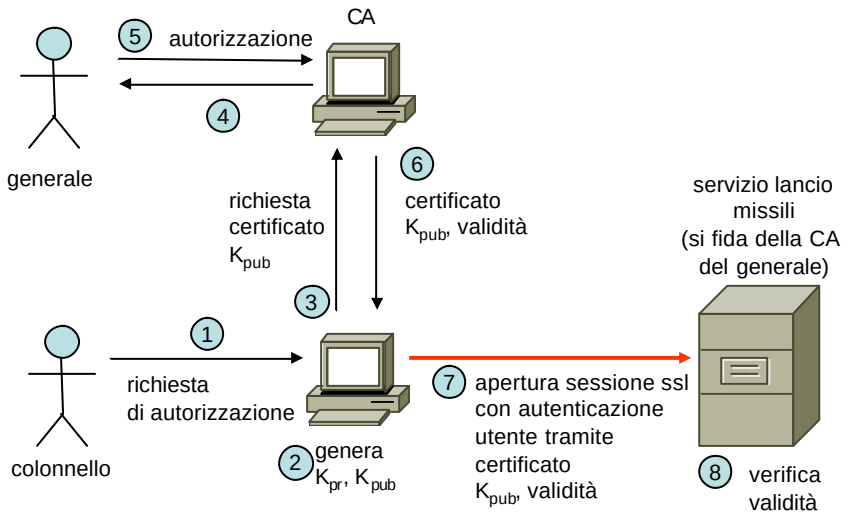
utente: verifica che h=hash(m)

utente: return t

lancio missili

- il servizio “lancio missili” può essere utilizzato da un colonnello solo per un tempo limitato (ore o minuti) e solo se autorizzato da un generale.
- supponi che il servizio lancio missili abbia una interfaccia accessibile tramite https
- progetta un sistema informatico che automatizzi la procedura di controllo mediante l’uso di una PKI

lancio missili: una soluzione



- che vulnerabilità ha questa architettura? che precauzioni prenderesti?

lancio missili: alcune vulnerabilità/precauzioni

- sicurezza fisica del server!
- integrità della CA del generale
- dipende dal clock del servizio e della CA
  - la sincronizzazione tra i due va assicurata in qualche modo “sicuro”
- il generale potrebbe dover scegliere il tempo di validità del certificato
  - limite sulla possibilità di autorizzare per un tempo molto lungo (es max. 1 ora)
- se la rete non è fidata si devono prendere ulteriori precauzioni
  - denial of service
  - autenticazione del server
    - cioè il colonnello deve essere sicuro che che il server sia quello vero

ateneo

- un ateneo tratta tra gli altri i seguenti dati
  - generalità dei dipendenti
  - generalità degli studenti
  - esami sostenuti
  - informazioni sui progetti di ricerca
  - finanziamenti ottenuti dai dipartimenti
- nel DPS dell'ateneo quali dati figureranno tra i "trattamenti"

trattamenti

generalità dei dipendenti

generalità degli studenti

esami sostenuti

ospedale

- un ospedale italiano deve **memorizzare le cartelle cliniche** dei pazienti in un dbms
- che precauzioni deve prendere per rispettare la normativa?
- proponi una architettura

dbms con memorizzazione su fs cryptato

oppure

dbms con supporto alla criptazione

oppure criptare i campi a livello applicativo prima di inserirli nel db (difficile fare query che coinvolgono tali campi)

azienda

- una azienda italiana ti chiede un sistema via web (su intranet) per rendere noto ai pazienti le ferie e i loro giorni di malattia
- che precauzioni deve prendere per rispettare la normativa?
- proponi una architettura.

i dati devono viaggiare cifrati

https (ssl/tls)

il database da cui vengono estratti i dati deve essere cifrato

azienda e protocolli

- struttura aziendale
  - sede centrale Bologna
    - server
    - amministrazione
    - accesso a internet
  - 2 sedi sede Roma e Milano
    - amministrazione
    - sala ospiti wifi
    - accesso a internet
  - agenti di commercio
- sviluppa una politica aziendale per il piano di sicurezza che...
  - protegga i dati dell'azienda
  - sia conforme alla legge 196/2003
- progetta una rete che implementi la politica

esempio

i segreti industriali devono essere protetti da tutti coloro che non fanno parte del personale dell'azienda

i dati sensibili devono essere cifrati

il server C tratta dati personali **sensibili**

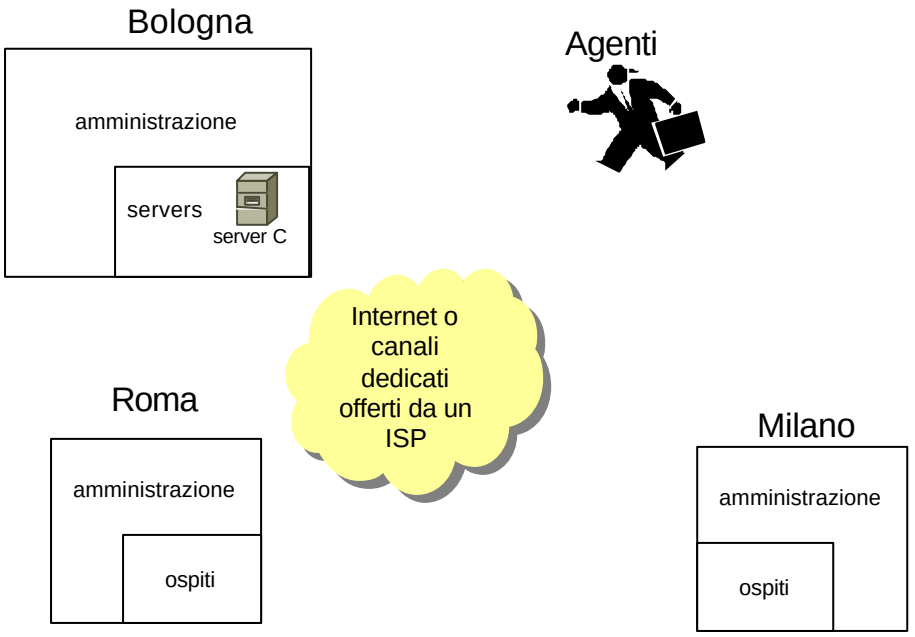
le comunicazioni delle sale ospiti devono essere separate da quelle della azienda

ecc.

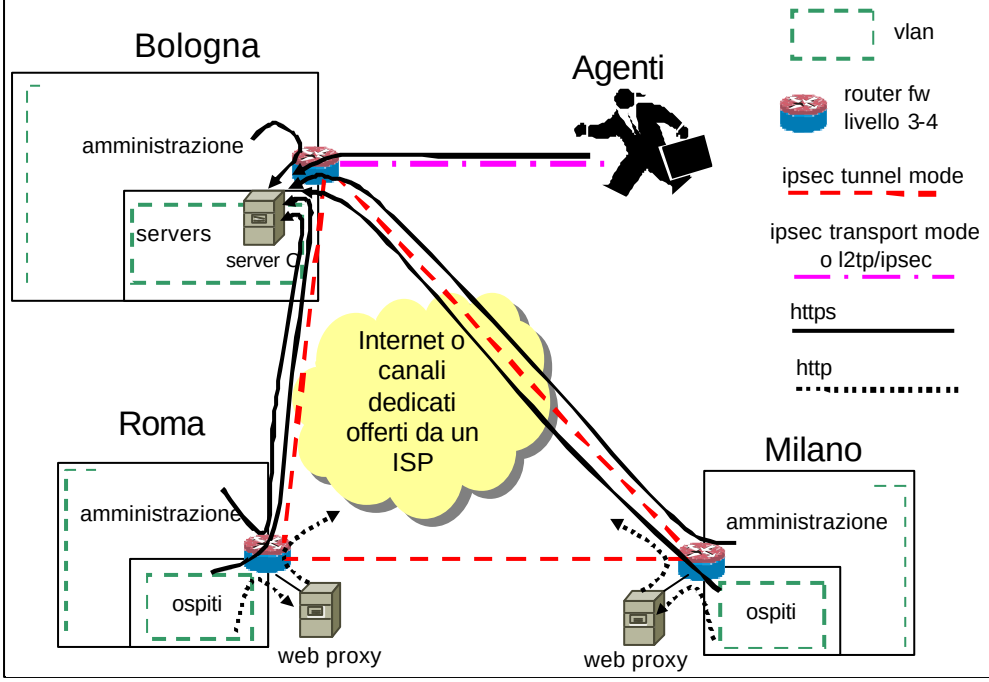
azienda e protocolli

- policy
  - i servizi offerti dai server di Bologna sono usufruiti dalle amministrazioni di tutte le sedi, dagli agenti di commercio via Internet e contengono segreti industriali
  - gli agenti si collegano da Internet e devono accedere a tutti i server e ai calcolatori delle amministrazioni
  - il server C (customer) offre servizi agli utenti e alle amministrazioni
  - il server C tratta dati personali **sensibili**
  - dalle sale ospiti si deve poter navigare su internet e accedere al server C

lavora su questo schema



un possibile progetto



...e inoltre

- database centralizzato degli incaricati per i trattamenti
- backup settimanale dei dati
- aggiornamento antivirus e software per i trattamenti ogni 6 mesi
- DPS ogni anno
- formazione degli incaricati