SICUREZZA

La sicurezza dei dati è un aspetto rilevante ; sicurezza fisica (safety) delle persone
(security)
da danno digitale è un file (prodotti di calcoli ...) che è associato ad una persona

SICUREZZA INFORMATICA

problema di costi → inferiore cmq al danno che avrei

non è un concetto assoluto.

Complicare la sicurezza diminuisce l'accettabilità dei servizi.

Dimensionare la sicurezza in base alle minacce → difesa adeguata
e al danno
Valutare i rischi

All'interno delle strutture esiste un comitato per la sicurezza → politiche, regole, ...

Modelli:

- per occultamento : nascondere le info, non renderle pubbliche
- difesa perimetrale : solo attacchi dall'esterno → firewall
- difesa in profondità : su ogni terminale → login e password
  → protegge anche dagli attacchi interni

FIREWALL

disaccoppia internet da intranet.

Limite: non protegge dai virus, non protegge contro le connessioni che non lo attraversano
(es. collegare un pc dentro una rete ad una terza), non protegge da attacchi interni o fisici

⇒ non può essere l'unico elemento di difesa

IDS (sistema di rilevazione degli intrusi)

sistemi software/hardware in punti strategici che rilevano il traffico e chi lo produce
→ guardano se c'è qualcosa di anomalo

Posso integrare questo sistema anche a livello di singolo pc

→ problema: falsi positivi e negativi : può sbagliare

CRITTOGRAFIA

protegge i dati → confidenzialità, integrità, autenticazione, non ripudiabilità

fa un lavoro di cifratura → decifratura in ricezione per tornare ai dati veri

devo avere una chiave di cifratura → algoritmo per modificare i dati

- chiave simmetrica segreta
- chiave pubblica asimmetrica

  ↳ serie di coppie di chiavi : una personale e una pubblica (→ su internet, in un db)

  per criptare uso la mia chiave privata e quella del ricevente pubblica

  ↳ ricevo, decripto con la mia privata e quella pubblica del mandante

  le chiavi vengono generate da un organizzazione ad albero

↳ è faticoso per il processing, e modotto per tanti dati, ma molto sicuro

FIRMA DIGITALE

si basa sulle chiavi asimmetriche: quella privata per "firmare" e quella pubblica per verificarla (nota a tutti).

Qualcosa che inserisco ad un documento, file che attacco.

Ha le stesse funzioni della firma manuale

- autenticità
- integrità
- non ripudiabilità

Per firmare: applico un algoritmo per estrarre una parte del documento, elaborarla → digest. A questo punto si fa la cifratura asimmetrica → firma digitale attacco la firma in fondo al documento

(a questo punto potrei criptare il documento, ...)

In ricezione: verifico che il digest calcolato con l'algoritmo dal documento, e quello decriptato (con la chiave pubblica) dalla firma siano uguali.

↳ non è riproducibile, non può essere usato per un testo diverso dall'originale

Certification Authority → CAR e quello italiano

Applicazioni:

- firmare le prescrizioni, i referti (x medici)
  ↳ es. per una "second opinion": teleconsulto
- firmare richieste (di prestazioni ai vari consulenti interni)
- prenotare ricoveri, prestazioni ambulatoriali, accedere ai dati.

VIRTUAL PRIVATE NETWORK

Reti private virtuali → è un metodo di sicurezza per trasmettere info.

es. tra due ospedali legati tra loro, tra ospedale e casa del paziente

→ creo una rete protetta sulla rete pubblica. ↳ vantaggio di sicurezza dei dati e anco sicuramente presente

INTERNET

Comunicazione tra client e server → protocollo http

si va al server tramite dell'URL. Il server risponde con protocollo html

servizi web 2.0 → social networks, blog, ...

↳ anche per la sanità

Chi cerca info sanitarie su internet → un italiano: 12-15 milioni

PORTALE = siti che danno la possibilità di interagire con gli utenti 24-10-2017

↳ oggi tutti gli ospedali ne hanno uno, ma non si trovano informazioni di dettaglio perché servono dai medici che li fanno dentro

↳ ci sono portali che si fanno entrare da medici, da esterni ⇒ soprattutto strutture private

[HALO - CLINIC: fa servizio di visita alle persone via rete ↔ specialisti] dia 33

↳ la realizzazione di portali deve essere usabile: trovare le info con al max 3 click

L'ospedale deve essere in rete:

- dare informazioni
- ....

CUP = centro unificato prenotazione

↳ però la prenotazione è ancora telefonica

↳ deve essere inserito però in un contesto più ampio, legando

news letter → per divulgazione medico-scientifica e formazione degli operatori.

PROBLEMA: credibilità della fonte

e-health (electronic health)

→ però servono persone per dedicarsi al portale

RETI di Sensori (WSN)

↳ NODI della rete

oggetti di dimensioni piccole (monete), autonomi, per comunicazione a breve raggio (15m)

realizzare un'attività di monitoraggio in un'area limitata (es. casa)

ricevono segnali e li ritrasmettono agli altri → funzionamento in maniera della rete telefonica a celle

quando si trova il gateway i dati vengono mandati su una rete geografica.

→ si sparpagliano questi oggetti per la casa

→ sono nati per consentire la ricezione da sensori (es. pressione, temperatura, battito cardiaco, ...

→ es. a quello ospedaliero: x creare una rete con urgenza

→ nato per scopi militari, x creare reti

→ progetto per misurare (attenzione) accendere/spegnere il riscaldamento in funzione della presenza di persone (nelle scuole)

è una mini-rete wireless che funziona come la rete geografica, con le celle

body sensor network = creare una rete sul corpo = es. sensore pressione, accelerometro ...

convergono tutti ad un'unità: cellulare, wireless)

se sul corpo umano arriva un campo ad alta frequenza, si generano correnti superficiali → non riesce a penetrare
il problema è di potenza emessa → alte potenze fanno male
(in Italia al max ½ W → altri paesi 2W)

→ WSN: possono anche avere un piccolo microprocessore per fare elaborazioni

PEC = posta elettronica certificata
↳ è una email legiferata: per garantire che sia stata inviata e che sia arrivata
ci sono dei gestori (del mittente e del destinatario) che si fanno garanti
↳ ricevuta di accettazione dal gestore del mittente
↳ ricevuta di consegna dal gestore del destinatario
⇒ è regolato da leggi: le ricevute hanno validità giuridica

IOT

Internet delle cose → dare internet anche agli oggetti
es. fare servizi di sanità elettronica per grandi numeri di pazienti
questi servizi sono già disponibili [illegible] normale internet
usato nel telemonitoraggio per grandi numeri di persone
software installato sui cellulari dei pazienti → gestisce le info dei pazienti e decide se mandarle → le manda, espone in bacheca.

instant messaging
si usa una porta
↳ NEAR REAL TIME
usa un canale portato
XMPP
(per essere veloce, realtime)
es. TELEMONITORAGGIO

PUBLISH SUBSCRIBE = l'utente pubblica, il gestore passa a raccogliere
↳ è one way, non si sprecano messaggi per dire che i dati sono pronti, evita l'intasamento
↳ utile per un discorso di prevenzione (molte persone), per gli anziani
↳ dal punto di vista costi non aggiungo altro oltre al software

[internet dei servizi: creare da solo il servizio con i vari blocchi già fatti;
internet dei contenuti:
↳ evoluzioni future]