Sicurezza Informatica

Ing. Ivan Bruno
Department of Information Engineering
University of Florence
ivan.bruno@unifi.it

DISIT Lab
http://www.disit.dinfo.unifi.it/

Sicurezza Informatica

- Il termine “sicurezza”, non si riferisce solo a quella fisica (security o safety).
- Tale concetto va integrato in una visione più moderna, attenta ai temi della sicurezza informatica, dei dati e delle informazioni.

Sicurezza Informatica

1. *Tutti i programmi contengono degli errori*

2. *I grandi programmi contengono più errori di quelli piccoli*

3. *Un programma importante per la sicurezza ha degli errori nella sicurezza*

4. *Se non si esegue un programma non c'è modo di sapere se contiene errori*

Sicurezza Informatica

L'impiego diffuso di Internet e delle nuove tecnologie, ha fatto scomparire i sistemi isolati e modesti situati all'interno di reti informatiche prevalentemente chiuse.

Oggi l'interconnessione è sempre più accentuata e le connessioni travalicano i confini nazionali.

A seguito della crescente interconnettività, i sistemi informativi e le reti sono esposti attualmente a minacce e rischi sempre più numerosi e di più varia tipologia.

Tutto ciò solleva nuove problematiche di sicurezza.

I RISCHI...

Sistemi informativi e reti informatiche sono sempre accompagnati da nuovi e crescenti rischi.

I dati e le informazioni conservati e trasmessi attraverso i sistemi informativi e le reti, sono continuamente esposti a rischi legati a varie modalità di accesso e utilizzazione indebiti, alla loro sottrazione o alterazione, alla trasmissione impropria di codici, ad attacchi o alla loro distruzione, e necessitano di opportune garanzie.

Alcuni problemi di sicurezza reali

Il siciliano Giuseppe Russo arrestato per essersi impossessato via Internet di mille numeri di carta di credito di cittadini USA ed averli adoperati	Grossa fetta di potenziali acquirenti si rifiuta di fare acquisti online a causa di problemi di sicurezza recentemente occorsi
Un canadese di 22 anni condannato a un anno di reclusione per aver violato molti computer dei governi USA e Canada	Stanotte, qualcuno di voi potrebbe…

Situazione attuale

Spesso si crede che sia sufficiente installare un **antivirus** e generare una password per salvaguardare l'integrità dei dati e risolvere quindi tutti i problemi sulla sicurezza.

E' necessario invece che ci sia una consapevolezza maggiore dei problemi inerenti la Sicurezza Informatica, ovvero delle soluzioni di sicurezza idonee che rappresentino una **garanzia adeguata di privacy secondo la normativa vigente**.

Sicurezza è....

1. Non prodotto ma processo
2. Anello più debole di una catena
3. Proprietà multilivello
4. Non un concetto assoluto ma dipende dal contesto
5. Individuare cosa mettere in sicurezza e proteggersi da chi
6. Più livelli di sicurezza

Sicurezza come sistema

- Il mondo è un sistema contenente sottosist.
- Internet è fra i sistemi più complessi
- Un sistema gode di certe proprietà
  - Attese
  - Inattese
- Es: I **bug** sono proprietà inattese e spiacevoli

Sistema - proprietà

- Complessità delle proprietà direttamente proporzionale alla complessità del sistema
- Sicurezza di Internet!!
- **Sicurezza di un sistema** vs. sicurezza dei suoi componenti
- Sicurezza a questo punto appare come proprietà di un sistema

Problemi di sicurezza causati da

1. Complessità
   - *Che sistema operativo!*
2. Interattività
   - *2 sistemi diventano 1 grande*
3. Proprietà emergenti
   - *L'avvento di X comporta Y*
4. Predisposizione ai bug
   - *Programma un sito di e-commerce*

Sicurezza Informatica

CLASSI DI ATTACCO

Sicurezza informatica: classi di attacco

Furto di password

- al momento del collegamento remoto
- rubando il file delle password e poi decrittandolo con appositi programmi
- rimedi
  - non inviare password in chiaro
  - Usare metodi di autenticazione
  - nascondere file password
  - non usare password banali
  - dare scadenza alle password

Sicurezza informatica: classi di attacco

Con inganno (phishing, social engineering)

- si invia messaggio (via telefono, e-mail, fax...) che chiede di effettuare una azione potenzialmente pericolosa
  - inviare/modificare password
  - eseguire programma sconosciuto che chiede password
- rimedi
  - autenticare accuratamente le richieste
  - curare la formazione!!

Sicurezza informatica: classi di attacco

Bachi e clandestini

- approfittare di un errore nel sw per inserirsi e compiere azioni indesiderate sul sistema
- allegare ai messaggi di posta elettronica programmi che aprono le porte o spediscono informazioni riservate
- rimedio
  - segnare il software con le procedure di autenticazione
  - non lanciare programmi sconosciuti con i privilegi di amministratore

Sicurezza informatica: classi di attacco

Fallimento della autenticazione

- esempio
  - server che valida le richieste in base all'indirizzo da cui provengono. Se si utilizza quell'indirizzo si viola il sistema
  - Sql injection: stringa magica="' or 'a'='a"
- rimedio
  - usare sistemi di autenticazione sofisticati
- I sistemi che devono garantire un livello più elevato di sicurezza (vedi bancomat) richiedono almeno due fattori, tipicamente:
  - Qualcosa che si conosce (codice)
  - Qualcosa che si possiede (carta)

Sicurezza informatica: classi di attacco

Fallimento del protocollo

- si sfrutta la conoscenza del protocollo a basso livello
- difficile da realizzare
- rimedio:
  - usare la crittografia

Sicurezza informatica: classi di attacco

Diffusione di informazioni

- alcuni protocolli tendono a distribuire informazioni sulla struttura interna della rete
  - finger, DNS, e-mail
- rimedi
  - usare un firewall per impedire l'uscita di pacchetti indesiderati
  - configurare bene i server

Sicurezza informatica: classi di attacco

Negazione del servizio (DoS – Denial of Service)

- si tenta di impedire l'uso di un particolare servizio.
- esempi
  - riempire disco di posta per bloccare sistema
  - rallentare o impedire la connessione inviando falsi ICMP Destination Unreachable o falsi broadcast
  - Richieste simultanee di accesso ai servizi
- rimedio
  - filtrare le richieste (difficile capire se si è in questo caso o in presenza di guasto del sistema)

Sicurezza informatica: problemi TCP/IP

- TCP
  - le porte < 1024 *dovrebbero* essere affidabili
- UDP
  - la sostituzione degli indirizzi è più semplice di TCP non essendoci gestione della connessione quindi l'indirizzo del mittente non è affidabile
- SMTP (basato su TCP)
  - mittente non affidabile
  - pericolo di negazione del servizio
  - diffusione delle informazioni in caso di destinatario sconosciuto

Sicurezza informatica: TCP/IP (SMTP)

- Estensioni MIME possono portare
  - esecuzione programmi pericolosi direttamente o indirettamente
  - a condurre azioni sconsiderate

    Content-Type: Message/External-body

    name=“.rhosts”;

    site=“ftp.unni.org”;

    access-type=“anon-ftp”;

    directory=“.”

    Content-Type: text/plain

    Sostituisce al file .rhosts della direttrice corrente quello prelevato dal sito (in modo trasparente)

Sicurezza informatica: problemi TCP/IP

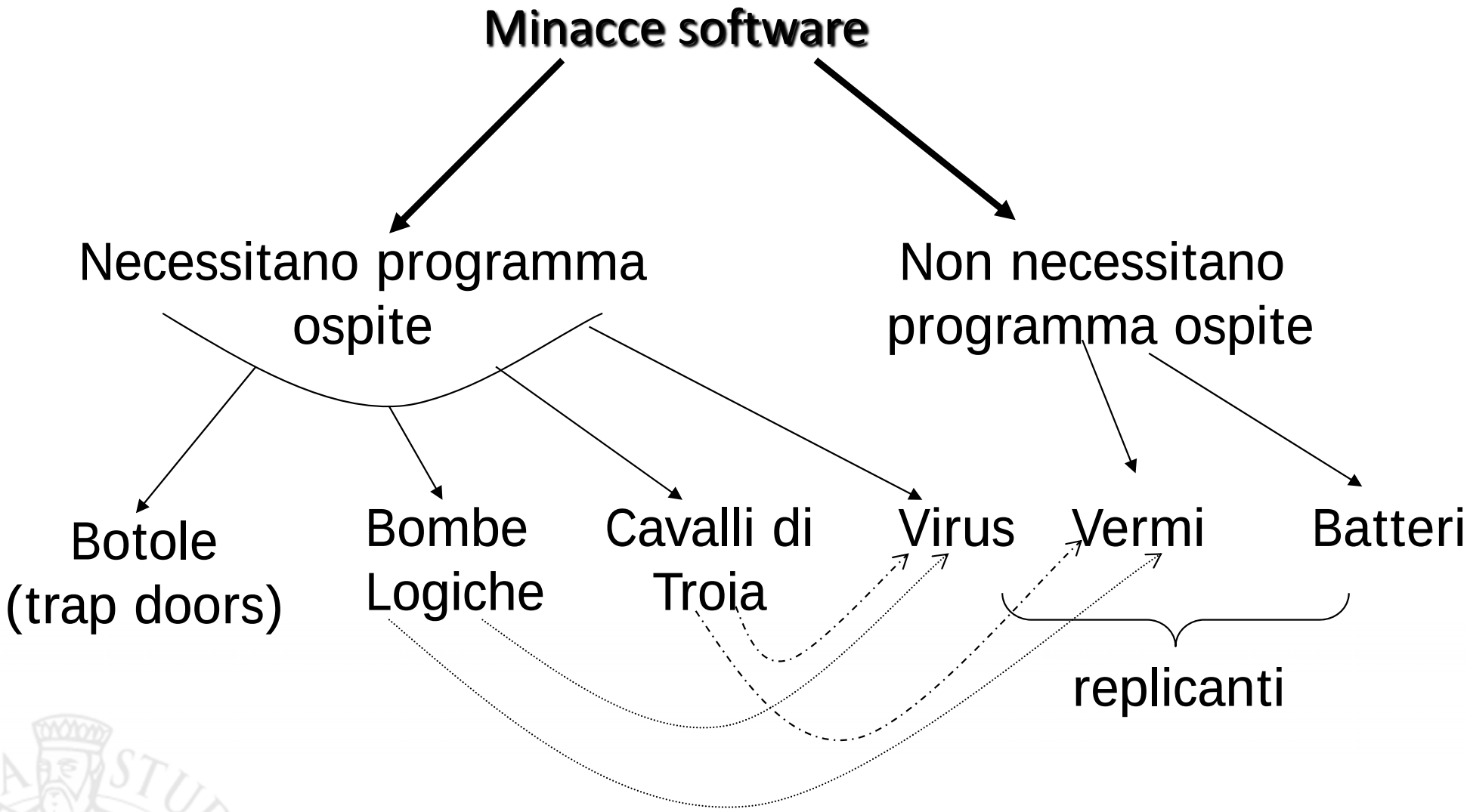
- Telnet (basato su TCP)
  - non sempre è possibile lavorare su macchine affidabili
    - usare telnet sicuro (RFC 1416)
  - scambio password è inaffidabile
    - usare meccanismi di crittografia

Sicurezza informatica: problemi TCP/IP

WWW/FTP

- lato client
  - i documenti ricevuti possono contenere ordini di attivazione di programmi (visualizzatori, Java, activex...) che possono creare problemi
  - il formato MIME può nascondere insidie
- lato server
  - Autenticazione, pagine dinamiche e richieste di file possono creare problemi se il software middle-tier è bacato
  - condivisione albero con FTP-anonimo
    - si depongono file nella zona FTP e poi si chiede al server di eseguirli
    - rimedio: directory di FTP-anonimo scrivibili sono del gruppo ftp e non sono eseguibili da altri gruppi
  - server web deve girare in un ambiente ristretto per evitare problemi specialmente se si usano linguaggi interpretati come asp, php e script

Virus e minacce software



Virus e minacce software: fasi

- fase silente: virus inattivo, attivato da qualche evento
- fase di propagazione: si duplica in altri programmi che vanno in esecuzione; si mette in aree particolari del disco
- fase di attivazione: si attiva per compiere le azioni programmate. Può essere attivato da un evento esterno
- fase di esecuzione: compie le funzioni di danneggiamento e/o disturbo

Sono spesso progettati per un particolare s.o. o piattaforma hw

Virus e minacce software: tipi

- parassita: si attacca ad un eseguibile e si replica;
- residente in memoria: si carica in memoria come parte di un programma residente;
- settore di boot: infetta boot record o MBR;
- furtivo (stealth): nato per nascondersi dagli antivirus (tecnica più che un tipo)
- polimorfico (mutante): cambia ad ogni infezione anche attraverso tecniche criptografiche
- macro virus: sono la tipologia in più rapido sviluppo (due terzi dei virus), indipendenti dalla piattaforma, infettano documenti non eseguibili, si diffondono facilmente, si basano sulle macro di Word (Excel, ...);

I VIRUS !

Modalità di diffusione

- Ciò che distingue i virus propriamente detti dai worm è la modalità di replicazione e di diffusione: un virus è un frammento di codice che non può essere eseguito separatamente da un programma ospite, mentre un worm è un applicativo a sé stante. Inoltre, alcuni worm sfruttano per diffondersi delle vulnerabilità di sicurezza, e non dipendono quindi dal fatto di ingannare l'utente per farsi eseguire.
- Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di diffusione dei virus da una macchina ad un'altra era lo scambio di floppy disk contenenti file infetti o un virus di boot. Il veicolo preferenziale di infezione è invece oggi rappresentato dalle comunicazioni e-mail e dalle reti di peer to peer.
- Nei sistemi informatici Windows è di consuetudine usare il registro di sistema per inserire in chiavi opportune dei nuovi programmi creati ad hoc dal programmatore di virus che partono automaticamente all'avvio. Uno dei punti deboli del sistema Windows è proprio il suo registro di configurazione. Esistono vari programmi per tenere d'occhio le chiavi pericolose del registro di Windows, uno di questi è Absolute Startup, che ad intervalli di tempo regolari esegue una scansione delle zone a rischio del registro per vedere se un nuovo virus o programma anomalo è stato aggiunto in quelle chiavi.

Firewall

- E' un componente situato fra due reti che gode delle seguenti proprietà:
  - tutto il traffico dall'esterno verso l'interno e viceversa deve passare attraverso il firewall
  - solo al traffico autorizzato, definito dalle politiche di sicurezza locali, è consentito il transito
  - il firewall stesso è immune dalle penetrazioni

Firewall

- Zona demilitarizzata (DMZ): sottorete di macchine che forniscono servizi per compensare gli effetti dei filtri.

Firewall

controllo del servizio: determina tipi di servizio Internet accessibili dall'interno e dall'esterno filtrando il traffico sulla base degli indirizzi e delle porte

controllo direzione: dei flussi di dati

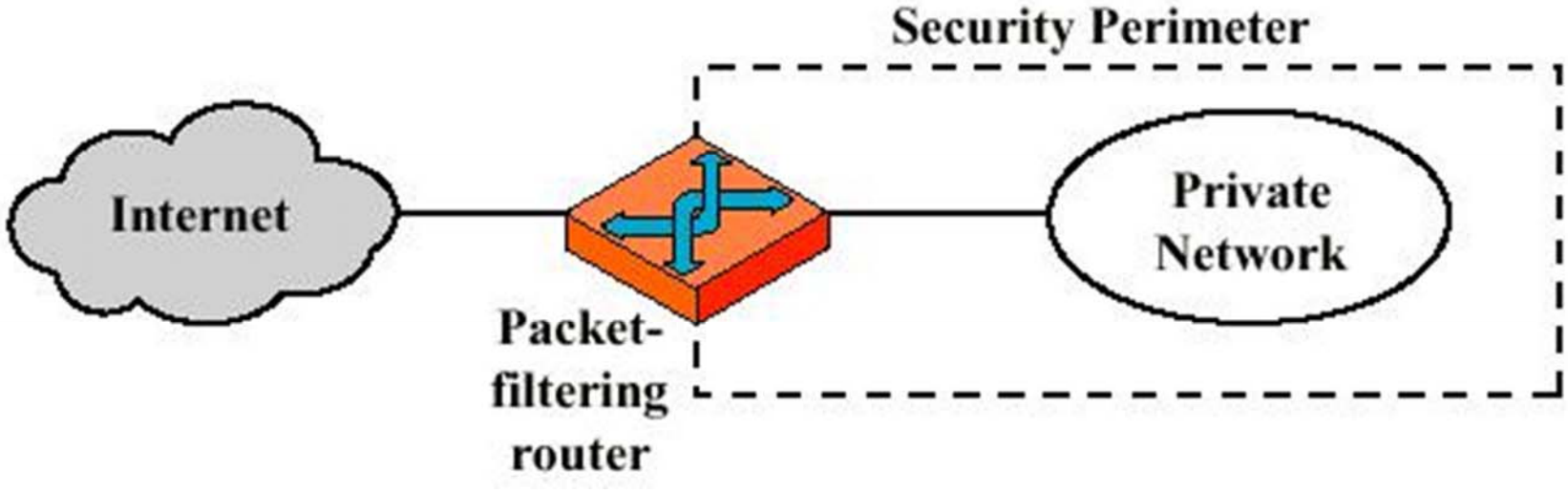
controllo utente: accesso al servizio da parte di utenti interni ed esterni

controllo comportamento: come sono usati i servizi

limiti:

- non può impedire l'aggiramento ad esempio attraverso un modem
- non può impedire attacchi dall'interno
- non può proteggere dal trasferimento di programmi o file infetti da virus

Firewall: filtri di pacchetto



- Selezione basata su datagram IP
- Semplici e poco costosi
- Non sempre molto efficaci
- Primo livello di sicurezza
- Facilmente realizzabile con i router

Sicurezza Informatica

COME PROTEGGERSI

Come proteggersi?

- Physical security
  - Accesso fisico di utenti alle macchine (datacenter, CED)
- Operational/Procedural security
  - Policy di sicurezza
- Personnel Security
  - …
- System Security
  - Acl, log, …
- Network Security
  - Firewall, IDS, buon routing e filtri

Planning security!

1. Limitazione rischi
   - *Davvero serve una connessione permantente alla rete?*
2. Uso di deterrenti
   - *Pubblicizzare strumenti di difesa e punizione*

Planning security!

3. Prevenzione
   - *Crittografia*
   - *Politiche*
   - *Antivirus*
   - *…*
4. Rilevamento
   - *Logging*
   - *Intrusion detection*
   - *…*
5. Reazione
   - *Intrusion management*
   - *System recovery*
   - *Tribunale*
   - *…*

Soluzioni contro gli attacchi informatici

- Buona pianificazione della rete con hardware adeguato (router, switch ecc.) insieme alla divisione della rete in aree a livello di sicurezza variabile.
- Controllo dell'integrità delle applicazioni (bugs free) e verifica della correttezza delle configurazioni.
- Utilizzo di software che controllino e limitino il traffico di rete dall'esterno verso l'interno e viceversa (es. firewall, router screening ecc.)
- Utilizzo di applicazioni che integrino algoritmi di crittografia in grado di codificare i dati prima della loro trasmissione in rete (es. PGP, SSH, SSL ecc.)

Stato dell'arte in Sicurezza

- La sicurezza
  1. Richiederebbe spesso il ridisegno, il che non è sempre possibile!
  2. E' una proprietà di vari livelli architetturali [OS, rete, ...]
  3. E' costosa nel senso di risorse computazionali, gestione, mentalità, utilizzo
  4. Rimane un campo aperto anche per i colossi dell'Informatica

Minacce nuove – automazione

- Microfurti diventano una fortuna
  - *Limare 1/1000€ da ogni transazione VISA*
- Violazioni quasi senza tracce
  - *Il mio PC ha fatto improvvisamente reboot*
- Privatezza a rischio
  - *Hanno telefonato: sanno che sono iperteso*

Minacce nuove – distanza

- Non esiste distanza
  - Internet non ha confini naturali
- Ci preoccupano tutti i criminali del mondo
  - *Adolescente inglese viola sistema italiano*
- Leggi versus confini nazionali
  - *Denunce contro… Internet*
  - *Mecca: trovarsi in uno stato americano con scarsa cyberlaw e mancanza di estradizione*

Minacce nuove – tecniche diffuse

- Rapidità di propagazione delle tecnologie
  - *Hacker pubblica lo script del proprio attacco*
  - *Scaricato crack slovacco per texteditor*
- Diventare hacker spesso non richiede abilità
  - *Scaricato script per attacco di negazione del servizio (DoS)*
  - *Trovato su Internet parte del codice rubato di Win2K e verificato che…*

Come mi proteggo io ?

- Personal firewall (del SO o altro)
- Antivirus (Norton o avg)
- Antispyware (ADAware, SpyBot)
- Service pack e patch sempre aggiornati
- Blocco dei servizi e dei device non necessari.

Come si protegge una azienda ?

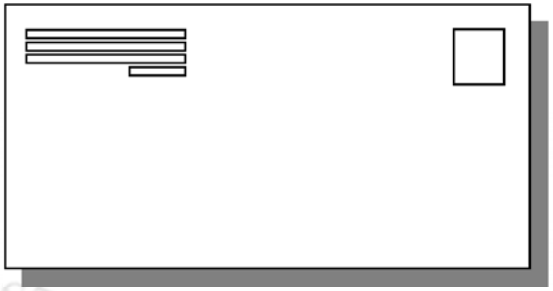
- Controllare le informazioni pubblicamente disponibili
- Identificare una naming convention non troppo esplicativa per i sistemi/reti/servizi esposti all'esterno
- Controllare periodicamente le informazioni che escono dall'azienda e finiscono sui motori di ricerca
- Verificare la presenza di informazioni sensibili in newsgroup o forum
- Mantenersi in contatto con le comunità di hacker e con i siti dedicati alla sicurezza. www.securiteam.com, www.zone-h.org, www.securityfocus.com, www.packetstormsecurity.org, www.k-otik.com

VPN

Le Virtual Private Network, specialmente se basate su protocollo SSL si stanno imponendo come soluzioni per la creazione di extranet. Hanno buone prestazioni di sicurezza. Non richiedono l'installazione di software lato client (di solito impiegano una applet java o un controllo ActiveX). Possono essere usate in quasi tutte le situazioni (dietro fw, nat, proxy). Supportano un ristretto numero di protocolli basati su TCP e UDP.

$1cur&zz@ dei D@t1

- Rendiamo sicure le nostre comunicazioni ed i nostri dati:
  - Crittografia e password.
  - Conservazione dei documenti



Password

- I pirati informatici usano strumenti sofisticati che consentono di determinare rapidamente migliaia di *probabili* password con l'uso di *semplici indizi* ricavabili dalle caratteristiche dell'account e del suo titolare.
- È solo questione di tempo …

Password

- La password deve essere facile da ricordare ma …
  - difficile da intuire
- Pensare una frase da utilizzare per la costruzione della password
- Usare **passphrase** (frase di accesso)
- Sostituire alcuni caratteri con simboli
  - Assurdo → @ff%$0
- Usa il controllo delle password.

Password

- La Password vuota
  - È più sicura di una sequenza 12345
    - Non permette il collegamento a computer diversi.
    - Il computer non è accessibile da persone diverse.
    - Non usarla per computer diversi
- La segretezza
  - Non comunicarla
  - Non scriverla in luoghi accessibili da altri
  - Non spedila per posta elettronica

Password

- Sicurezza
  - Modificare frequentemente
  - Non inserirla in computer sui quali non si ha il controllo
- Furto
  - Controllare frequentemente le informazioni protette
  - I Report degli acquisti on line
  - Rivolgersi alle autorità competenti.
- Attenzione al furto della propria personalità

Password e accesso al sistema

- Se qualcuno riesce ad accedere al vostro computer …
  - Avrà a disposizione tutte le password che il computer contiene
  - Atenzione quindi a proteggere il computer da accessi indesiderati
    - Virus
    - Trojan
    - Ecc.

Password: SI-NO

SI

- Lunga: almeno 7 caratteri e/o simboli.
- Includere maiuscole, minuscole, numeri e simboli.
- Variata: non ripetere gli stessi caratteri
- Numeri e lettere scelti casualmente.

NO

- Utilizzare in tutto in parte l'account
- Parole reali in qualsiasi lingua
- Nomi e date di nascita
- Numeri e lettere in sequenza … alfabeto
- Lettere o simboli con sequenza ricavata dalla tastiera.

Password: la gestione

SI

- Password diverse per siti diversi.
- **MODIFICARE LA PASSWORD FREQUENTEMENTE**

  … almeno ogni sei mesi

NO

- Annotare la password sullo schermo.
- Utilizzare la funzionalità *memorizza la password.*
- Annotare la password sulla rubrica

Password: Sicurezza ?!?

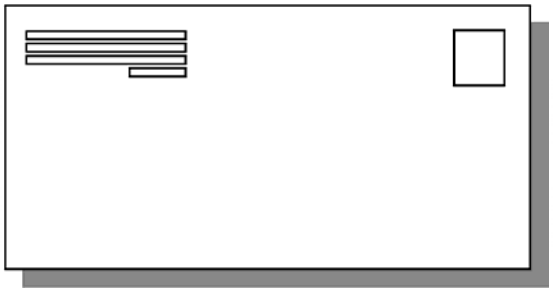
MAI !

Controllate frequentemente i documenti che ricevete

Estratti conto, fatture, comunicazioni importanti … ecc.

- Se avete ragionevoli dubbi non esitate a contattare chi dovrebbe avervi inviato il documento.
- … forse il vecchio telefono o la posta

  servono ancora.



Password: gli attacchi

Tentativi di intrusione (se li conosci → li eviti)

- Casuali tentando di indovinare nomi probabili: figli, città di nascita, squadre sportive, ecc.
- Dizionario in linea ottenuto con file di testo delle parole usate.
- Dizionario non in linea ottenuto da file di account e password dell'utente sia crittografate che non ….
  - Attenzione ai dizionarui delle password personali
- Brute force: l'attacco è operato cercando di identificare le password nei file utilizzati per gli attacchi.

Password

Efficacia della password:

- Password complesse
  - Lettere minuscole, maiuscole, numeri
  - Simboli @ $ % * § …….
  - Simboli particolari: Alt+123 { - Alt+125 } – Alt + 135ç
  - Caratteri unicode € , #, ¬ »

1. Utilizzare almeno 3 degli elementi espressi. Meglio 5.
2. Usare almeno 8 caratteri e simboli

Password

Efficacia della password:

Ricordare

Usare lettere e simboli appositamente creati di una frase:

Voglio comprare 14 dischi

Voglio compr@re 14 $ischi → Vc@14$chY

Password

- Il sistema operativo Windows
  - Allungare la password con caratteri NULL fino a 14 caratteri Alt+0144 - ed altri
  - Crittografare la password
  - Tutti i caratteri Unicode, usando ALT+nnnn
  - Massimizzare l'entropia: entropia significa disordine

Password

- Esempi di uso di ALT+ nnnn
- è → alt+0200
- ã → alt+0195
- ã → Alt+0227
- Ø → Alt+0216
- © → Alt+0169

Password

- Non utilizzare dati personali
- Non utilizzare password costruite con parole note: maggio → 0maggio.
- Aggiornamento
  - Non creare nuove password simili alle vecchie.

La crittografia

- Metodo per rendere non comprensibile un documento a chi non ha le necessarie autorizzazioni.
- La crittografia ha origini antiche …
- Nella seconda guerra mondiale fu usata da tutte le potenze belligeranti.

La crittografia

- Stabilisce delle regole per sostituire insiemi di lettere con insiemi diversi contenti lettere e numeri in modo da rendere inintelligibile il messaggio inviato a chi non conosce la chiave di lettura.

La crittografia

- Alla costruzione di queste regole hanno contribuito matematici di chiara fama.
- Ricordiamo tra gli altri
  - Turing, che sintetizzò il principio di funzionamento di un computer.
  - Shannon, noto per i suoi studi sulla comunicazione.
  - Ecc.

La crittografia

- …
- Se esistono le regole esse possono essere trovate.
- Gli stessi matematici citati lavoravano su due fronti:
  - Crittografia
  - Decrittografia.

La chiave crittografica

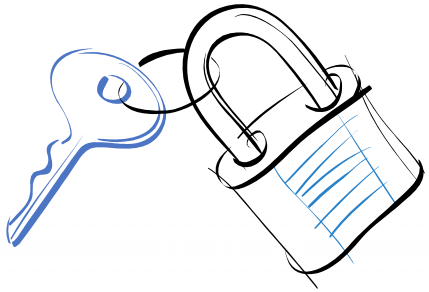
- Per evitare decrittazioni si deve modificare frequentemente la chiave crittografica …
- Problema

- *Come inviare la chiave senza che sia conosciuta?*

La chiave crittografica

- 1^ soluzione: **non inviarla**

1. *Il mittente invia il messaggio crittografato.*
2. *Il ricevente introduce nel messaggio la sua crittografia e restituisce il messaggio.*



La chiave crittografica

- *Il primo mittente toglie la crittografia iniziale e re-invia il messaggio.*
- *Il ricevente legge il messaggio con la sua crittografia*

Chiave crittografica

- Oggi si preferisce il metodo delle due **chiavi asimmetriche**
  - Pubblica
  - Privata

- La pubblica è distribuita a tutti i corrispondenti dal ricevente.
- La privata permette di leggere i messaggi solo a chi le possiede entrambe

Chiave crittografica

- Chi invia la posta deve possedere la chiave pubblica inviatagli dal destinatario.
- Per decifrare la posta occorre la chiave privata e la pubblica.
- Il destinatario ha entrambe le chiavi.

SICUREZZA

- Assoluta …

SICUREZZA

- Da un lato i crittografi lavorano per rendere le chiavi crittografiche difficili da individuare.
- … ma gli stessi crittografi lavorano per decrittare i documenti crittografati.

Chiave crittografica

- Tuttavia …
- Se costruite a “regola d’arte” …
- Un computer della potenza attuale … per trovare le chiavi

Può richiedere più di 1000 anni di tentativi

Chiave crittografica

- La presenza di due chiavi
  - Pubblica
  - Privata
- È preferibile perché evita l'invio della chiave privata.

- Esiste ancora tuttavia ….

La CHIAVE SIMMETRICA

È COMUNE A MITTENTE E DESTINATARIO.

Più facile da gestire e
più facile da trovare.

Ovviamente la chiave deve essere segreta, onde evitare l'uso a persone non autorizzate.

Crittografia e firma digitale

- Metodi matematici complessi presiedono alla formulazione di regole che non siano facilmente decifrabili.
- Tali metodi vengono utilizzati per la

Firma digitale

Problemi della firma digitale

- La firma è originale?
- Il documento è originale o è stato manipolato?

La *Firma digitale*

- La pratica della firma digitale si sta sviluppando rapidamente.
- Essa è riconosciuta valida in atti pubblici e privati, secondo normative fissate dalla legge.

La *Firma digitale*

- L'originalità della firma deve esser garantita da un ente certificatore riconosciuto che fornisce sia la chiave pubblica che quella privata.
- Tale ente deve rispondere a regole fissate dal legislatore.

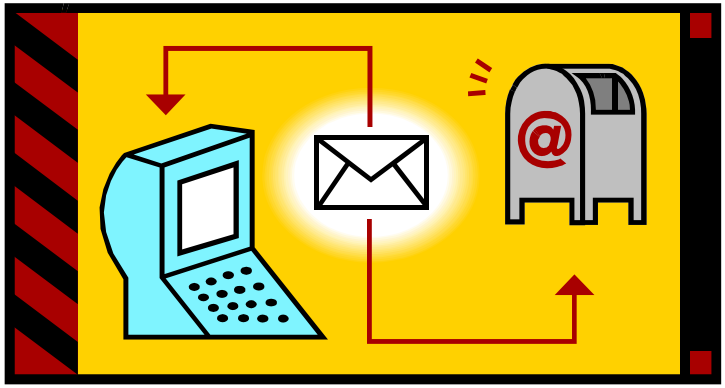
Firma digitale e documento

- Garantita la validità della firma digitale, dobbiamo ricordarci che il documento su cui è posta viaggia nella rete

- QUINDI …

Firma digitale e documento

- Può essere modificato da un intervento esterno.



Firma digitale e documento

- È possibile controllare se il documento ricevuto è uguale a quello spedito.
- Una funzione matematica particolare può fornire un' **impronta digitale** del testo.
- L'uso di tale impronta rende possibile il controllo dell'originalità del testo ricevuto.

Il documento

- L'integrità del documento è garantita da procedure particolari che permettono al destinatario la verifica dell'integrità.
- L'impronta è la tecnica usata: la probabilità che la stessa impronta appartenga a documenti diversi è 1 su $16*10^{18}$
- 1 su 16.000.000.000.000.000.000-