Università degli Studi di Padova

Scuola di scienze umane, sociali e del patrimonio culturale

dBC

Fondamenti di informatica

(Prof. Nicola Orio)

Sicurezza

Corso di laurea in
Storia e tutela dei beni artistici e musicali

Informatica e sicurezza

Il computer è un indispensabile strumento di lavoro

- ✓ La privatezza è un problema importante
  - Conti bancari, brevetti, appalti
    - Strategie per proteggere l'accesso ai dati sensibili
- ✓ I malfunzionamenti hanno costi elevati
  - Sostituzione apparecchiature, perdita e/o reinserimento dei dati, inattività forzata
    - Strategie per ridurre il rischio di perdita dati
- ✓ Alcuni malfunzionamenti sono causati da malware
  - Strategie di protezione da attacchi informatici

Backup e versioning – 1

Obiettivo: non perdere dati

- ✓ Salvare gli stessi dati su supporti diversi
  - Hard disk (anche diversi), CD/DVD, USB-stick, cloud
- ✓ Molto improbabile che si rompano tutti
  - E' importante che i dati sui diversi supporti siano allineati
- ✓ Copie di backup
  - Frequenza giornaliera, settimanale, in base al rischio
    - Maggiore è la frequenza minore è il rischio di perdita
  - Operazione costosa
    - Maggiore occupazione di memoria, tempo delle copie

Backup e versioning – 2

Obiettivo: tenere traccia dei dati

- ✓ Tenere separate le diverse versioni
  - Evitare cancellazioni o sovrascritture, gestire l'accesso di più utenti, ripristinare uno stato precedente
- ✓ Versioning di un documento
  - Salvare i file successivi con nomi diversi
    - Nome principale identico, con aggiunta di data, numero incrementale, nome di chi ha modificato
  - Alcuni software consentono di gestire automaticamente il versioning dei documenti
    - Il versioning è utile anche con il backup

Crittografia – 1

L'informazione che viaggia può essere intercettata

- ✓ Problema comune da secoli
  - In Internet esistono programmi appositi per spiare
    - Chiamati "sniffer", perché "annusano" la rete
- ✓ Soluzione: usare la crittografia (o cifratura)
  - Il messaggio viene alterato sistematicamente
    - Solo chi conosce il procedimento può ricostruire il messaggio
    - Per gli altri risulta una sequenza di caratteri senza significato
  - Algoritmi basati su un codice, detto chiave
    - E' sufficiente sapere la chiave per decifrare il messaggio

Crittografia – 2

Gli algoritmi di cifratura sono pochi e noti

- ✓ Si va per tentativi per indovinare la chiave
- ✓ I calcolatori sono instancabili lavoratori
  - Facendo un milione di operazioni al secondo

Chiave	**Operazioni**	**Tempo necessario**
32 bit	$2^{32} \approx 4{,}3 \cdot 10^{9}$	1 ora e 15 minuti
64 bit	$2^{64} \approx 1{,}8 \cdot 10^{19}$	$5{,}8 \cdot 10^{5}$ anni
128 bit	$2^{128} \approx 3{,}4 \cdot 10^{38}$	10^{25} anni (>età dell'universo)

- ✓ Maggiore il numero di bit della chiave, maggiore il carico di lavoro dei sistemi che stanno comunicando

Crittografia simmetrica

Una sola chiave per cifrare e decifrare

- ✓ Per cifrare si trasforma il messaggio usando la chiave
- ✓ Per decifrare si fa l'operazione inversa
  - Usando la stessa chiave al contrario
    - Esempio: si somma/sottrae il valore della chiave al codice ASCII
- ✓ Funziona finché la chiave resta segreta
    - Si chiama infatti anche "a chiave segreta"
  - La chiave dev'essere comunicata al destinatario
    - Consegnata a mano, o attraverso canali sicuri
    - Impraticabile per il commercio elettronico

Crittografia asimmetrica – 1

Una coppia di chiavi diverse

- ✓ La prima serve per cifrare
  - Può essere nota a tutti (chiave pubblica)
- ✓ La seconda serve per decifrare
  - Deve restare segreta (chiave privata)

Caratteristiche

- ✓ Le due chiavi sono interscambiabili
  - Ciò che una chiave cifra è decifrato solo dall'altra
- ✓ Conoscere una chiave non consente di risalire all'altra, se non per tentativi

Crittografia asimmetrica – 2

Privatezza delle informazioni

- ✓ Alice usa la chiave pubblica di Bob per cifrare
- ✓ Bob è l'unico che può decifrare il messaggio
  - Bob è l'unico che conosce e può usare la propria chiave privata
  - Eva può anche intercettare il messaggio, ma non sa decifrarlo

Firma digitale

- ✓ Alice usa la propria chiave privata per cifrare
- ✓ Bob prova a decifrarlo con la chiave pubblica di Alice
  - Se ci riesce allora il mittente era veramente Alice
  - Se non ci riesce il messaggio proviene da altri (ad esempio Eva)

Obiettivi della crittografia

Segretezza o confidenzialità (secrecy)

- Impossibilità di comprendere un messaggio riservato

Controllo dell'integrità (integrity control)

- Impossibilità di modificare il contenuto di un messaggio se non da parte dell'autore

Autenticazione (authentication)

- Identificazione dell'identità di chi ha inviato un messaggio

Non disconoscimento (nonrepudiation)

- Impossibilità di disconoscere l'invio di un messaggio

Malware

Definizione di malware

- ✓ Software con effetto negativo per l'utente, che si installa, si esegue e si replica autonomamente
  - Spesso gli utenti collaborano inconsapevolmente alla sua installazione e diffusione
    - Il malware usa alcune strategie per diffondersi

Il malware (malicious-ware) precede Internet

- Internet facilita la comunicazione tra computer
- Il numero di utenti inesperti è molto elevato
- I computer sono sempre connessi

Tipologie di malware – 1

Trojan-horse

- ✓ Software innocuo, che invita a essere installato
  - Scritto però con una parte nociva all'interno
    - Metafora del cavallo di Troia
    - Si diffonde quando lui stesso è passato tra utenti o scaricato

Virus propriamente detto

- ✓ Software che si "attacca" ad altri programmi
  - Quando questi sono eseguiti lo è anche il virus
    - Il virus si replica attaccandosi ad altri programmi ancora
    - Per diffondersi basta che l'utente passi un programma qualsiasi

Tipologie di malware – 2

Worm

- ✓ Software che usa la rete per contagiare i computer
  - Come allegato a un messaggio di posta elettronica
    - L'utente apre l'allegato ed esegue il worm
    - Si diffonde spedendosi ad altri utenti
  - Come richiesta di un servizio esterno
    - Il sistema operativo installa il worm (senza avvisare l'utente)
    - Si diffonde contattando a sua volta altri computer

Il worm sfrutta errori di sistemi operativi o software applicativo per installarsi e diffondersi

Altre tipologie di malware

Spyware

- ✓ Raccoglie di nascosto informazioni sull'utente
  - Siti visitati, mail spedite, dati sensibili e le spediscono di nascosto

Wabbit

- Si limita a replicarsi all'infinito nel file system

Browser Hijackers

- Modifica la pagina iniziale del browser

Phishing

- Mail che indirizza alla copia di un sito reale (ad es. bancario)

Protezione dal malware – 1

Attenzione nell'installare nuovi programmi

- Trojan horse o affetti da virus

Cautela con i supporti rimovibili

- Funzione autorun di DVD o USB-stick con virus

Controllo degli allegati di posta elettronica

- Potrebbero essere worm

Attenzione alla navigazione

- Server che fanno installare trojan horse al browser

Protezione dal malware – 2

Mantenere sempre software aggiornato

- ✓ Ogni software ha degli errori
  - Il malware può sfruttare questi errori per installarsi
    - Gli aggiornamenti hanno delle patch (toppe) per questi errori
  - Particolare attenzione per il sistema operativo
    - Errori nel sistema operativo si riflettono su tutti i programmi

Usare software poco utilizzati

- ✓ I pirati informatici attaccano i software più diffusi

Scegliere software open source

Antivirus (o antimalware)

Il malware è un programma (sequenza di bit)

- ✓ L'antivirus riconosce la sequenze di bit caratteristica (signature) di un malware
  - E' necessario aggiornare continuamente gli antivirus
    - Gli aggiornamenti contengono le signature di nuovo malware
    - Un antivirus non aggiornato è inutile
  - E' ormai necessario utilizzare diversi antivirus
    - Ogni antivirus riconosce solo alcuni malware
    - Rischio di conflitto, usarli uno alla volta
  - In alcuni casi è necessario l'intervento di un esperto

Firewall

Un firewall (muro tagliafuoco) controlla il traffico tra due parti di rete

- Tipicamente LAN e Internet

- ✓ Filtra i pacchetti e blocca quelli non autorizzati
  - Può bloccare i pacchetti da computer non sicuri
    - La scelta di quali domini bloccare è di solito fatta dagli amministratori della rete
    - Può anche essere usato per bloccare la navigazione dei dipendenti
  - Può bloccare alcuni tipi di connessione
    - Ad esempio consente il protocollo HTTP ma non gli altri
    - Configurazione complessa, meglio utilizzare quelle standard