Reti di Calcolatori e Sicurezza

Panoramica estesa

Capp.0,1,2 Schneier

Thanks to Giampaolo Bella for slides
draft!!

Sicurezza non è

- Crittografia
- Firewall
- Antivirus
- Linux
- Password
- Smartcard
- Superare l'esame
- …

Thanks to Giampaolo Bella for slides draft!!

Sicurezza non è crittografia

- Crittografia scienza esatta come branca della matematica
  - *Impossibile violare RSA in tempo polinomiale*
- Sicurezza scienza inesatta perché basata su persone e macchine
  - *Acquisto on-line insicuro*

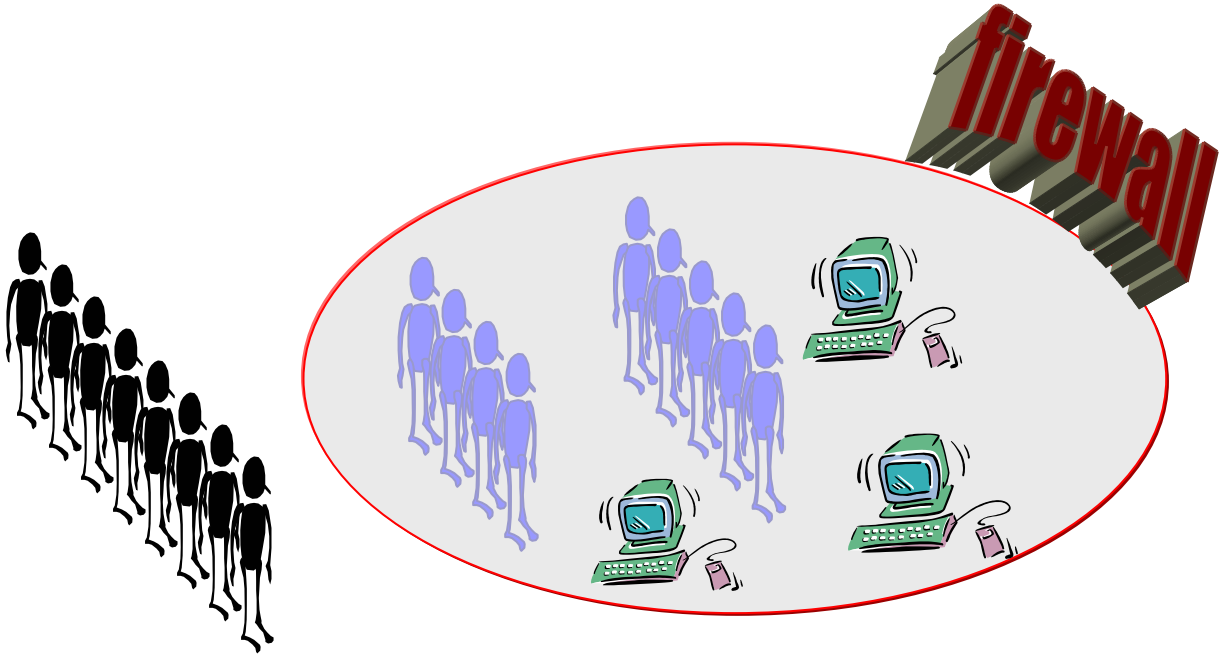
Thanks to Giampaolo Bella for slides draft!!

Sicurezza non è password

- La password più diffusa è *amore*
- Attacchi dizionario
- Come scegliere una buona password
- Come ricordare una buona password
- Usare una password per sempre?

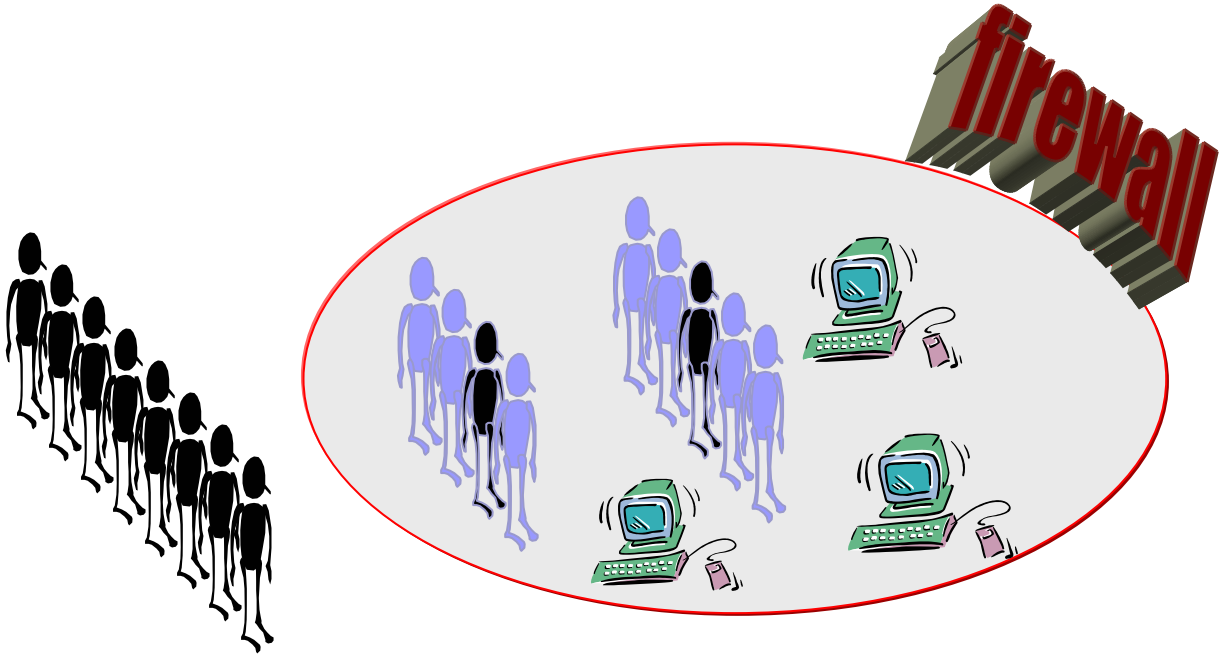
Thanks to Giampaolo Bella for slides draft!!

Sicurezza non è firewall



Thanks to Giampaolo Bella for slides draft!!

Sicurezza non è firewall



Thanks to Giampaolo Bella for slides draft!!

Sicurezza

1. Non prodotto ma processo
2. Anello più debole di una catena
3. Proprietà multilivello
4. Concetto mai assoluto – contesto?
5. Sicurezza da che cosa?
6. Livelli di sicurezza

Thanks to Giampaolo Bella for slides draft!!

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…

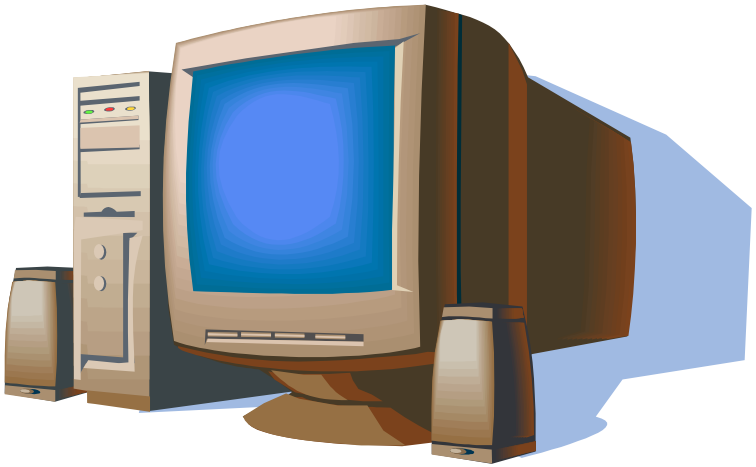
Thanks to Giampaolo Bella for slides draft!!

Sistema

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

Thanks to Giampaolo Bella for slides draft!!

Sistema – esempi



Thanks to Giampaolo Bella for slides draft!!

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

Thanks to Giampaolo Bella for slides draft!!

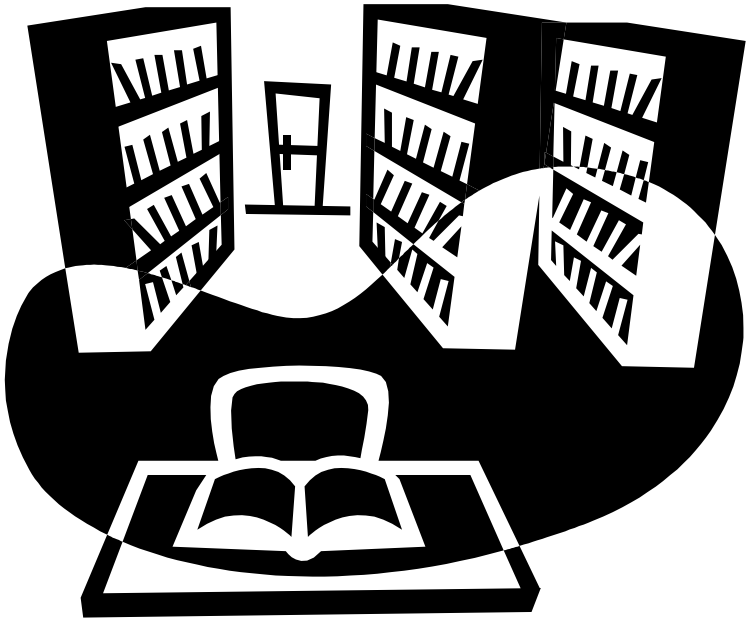
Problemi di sicurezza causati da

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*

Thanks to Giampaolo Bella for slides draft!!

Il dilemma della Sicurezza

Teoria versus Pratica



Thanks to Giampaolo Bella for slides draft!!

Il dilemma della Sicurezza

Teoria versus Pratica

Teoria

- Condizioni ideali – prevedibili
- Ipotesi ben precise
- Risultati ben precisi

Pratica

- Condizioni reali – imprevedibili
- Ipotesi meno precise
- Risultati meno precisi

Esempi: protocolli di sicurezza, crittografia perfetta, …

Thanks to Giampaolo Bella for slides draft!!

Come proteggersi?

Thanks to Giampaolo Bella for slides draft!!

Come proteggersi?

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

Thanks to Giampaolo Bella for slides draft!!

Come proteggersi?

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

Thanks to Giampaolo Bella for slides draft!!

Planning security!

3. Prevenzione
   - *Crittografia*
   - *Politiche*
   - *Antivirus*
   - …

4. Rilevamento
   - *Logging*
   - *Intrusion detection*
   - …

5. Reazione
   - *Intrusion management*
   - *System recovery*
   - *Tribunale*
   - …

Thanks to Giampaolo Bella for slides draft!!

Planning security!

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

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.)

Thanks to Giampaolo Bella for slides draft!!

I conti con la realtà

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. Non è un semplice predicato booleano [!!!!!!!!!!!!!!!!!!!!!!!!!!!!]
  4. E' costosa nel senso di risorse computazionali, gestione, mentalità, utilizzo
  5. Rimane un campo aperto anche per i colossi dell'Informatica

Thanks to Giampaolo Bella for slides draft!!

Minacce note

- Esistono leggi
- Non tutti le osservano
- Esistono capitali
- Alcuni violano le regole specialmente per impossessarsi di capitali illecitamente
- Ogni tipo di frode ha i propri “ferri”

Thanks to Giampaolo Bella for slides draft!!

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*

Thanks to Giampaolo Bella for slides draft!!

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*

Thanks to Giampaolo Bella for slides draft!!

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…*

Thanks to Giampaolo Bella for slides draft!!