Sicurezza e privatezza I

Introduzione al corso

Materiale didattico

- Stallings: Sicurezza delle reti. Mc Graw Hill
- Note del docente su linguaggi logici
- Articoli di supporto per la prima parte del corso
  - Terminologia e concetti di base
  - Modelli di politiche
  - Meccanismi
- Slides
  - Tutto reperibile sul sito del corso a parte il libro
  - secpriv
  - pgpp3p

Logistica

- Docente:
  - Piero Bonatti
  - Studio 3.25 nella palazzina 3 di Via Claudio
    bonatti@na.infn.it
- Pagina del corso
  - Home di Piero Bonatti => Teaching
  - http://people.na.infn.it/~bonatti/didattica/
- Ricevimento:
  - Per appuntamento (e-mail)

Contenuti

- Panoramica su sicurezza e privatezza
  - Problematiche
  - Cenni alle soluzioni
  - Con approfondimenti su alcuni argomenti
- Insegnamento molto interdisciplinare e “trasversale”
  - Teoria, metodologie, tecnologie, applicazioni

Sicurezza è

- Protezione delle informazioni digitali mediante crittografia
  - Tecniche algebriche; complessità computazionale
- Protezione dallo sfruttamento di bachi
  - Nei S.O. e nei protocolli di rete
  - Nelle applicazioni
  - *Best practice* e standards per gestione emergenze (tecniche di software engineering)
- Configurazione politiche nel rispetto di vincoli di comportamento
  - Modelli logici e statistici
  - Tecniche di ottimizzazione combinatoria e A.I.

Sicurezza è anche

- Applicazione delle tecniche crittografiche per ottenere primitive di più alto livello
  - Posta elettronica sicura, votazioni, ...
  - Tecniche algoritmiche
- Affidabilità, software sicuro
  - Tecniche di analisi e verifica formali del software
  - Trattati dai Proff. Benerecetti e Peron nei corsi di specifica e verifica formale del software

Esami

- Scritto + orale
  - Esempi sul sito del corso
  - Esercitazioni verso la fine del corso
- In caso di scritti disastrosi non è possibile ritentare l'esame nella stessa sessione
  - Se non si consegna è come non avere partecipato
- È... matematico che vengano chieste le dimostrazioni dei (pochi) teoremi presentati nel corso

Fine introduzione

Domande?

Piano di lavoro

- Primo semestre (6 CFU)
  - Concetti di base
  - Modelli di politiche
  - Linguaggi per la specifica di politiche
  - Meccanismi
  - Network security
  - Crittografia
  - Aspetti avanzati
  - Privacy