

Sicurezza Informatica

Introduzione al Corso 2018-19

Docente

- Alessandro Bianchi
 - Dipartimento di Informatica – V piano
 - Tel. 080 544 2283
 - E-mail alessandro.bianchi@uniba.it
 - Orario di ricevimento:
 - mercoledì 15:30 - 17:30
 - URL <http://www.di.uniba.it/~bianchi/>

Il Corso

- Orario:
 - Giovedì 8:30-11.50 (4 ore da 50 min)
- Crediti
 - 4 (T1) + 1 (T2) + 1 (T3) = 6

Il Contesto (1)

- I problemi della sicurezza con la particolare accezione della riservatezza sono fondamentali in ogni dominio dell'informatica
- Dal punto di vista scientifico i temi della sicurezza ricadono all'interno della categoria delle proprietà di safety di un Sistema critico e complesso
 - In contrapposizione alle proprietà di **liveness**

Il Contesto (2)

- Sistema **critico** e **complesso**
 - Concetti astratti fondamentali
- La complessità è trattata rigorosamente sia dall'informatica che da altre discipline (es. la fisica o la biologia)
- Esistono diverse misure di complessità note a un informatico
 - Computazionale
 - Strutturale
 - di comunicazione
 - ...
- La criticità è stabilita informalmente dal dominio applicativo

Il Contesto (3)

- Proprietà di **liveness** e **safety** sono definite in genere informalmente dalla comunità di informatici
 - Formalmente solo in alcuni ambiti particolari,
- Secondo la definizione più usata(*):
 - **Safety** properties specify that “something bad never happens”
 - **Liveness** properties stipulate that “something good eventually happens”

(*). E. Kindler, Safety and Liveness Properties: A Survey, EATCS Bulletin, 53 (1994) 268–272

Per Aumentare la Confusione

- Il termine italiano “**sicurezza**” identifica due diversi aspetti, meglio resi in inglese
 - **Safety**, intesa come l'incolumità per persone, ambienti, altri sistemi, etc
 - **Security**, nel senso di prevenzione da malfunzionamenti, eventualmente causati da entità malevole
- Noi ci concentreremo sugli aspetti relativi alla security
 - Che comprendono anche la privacy, intesa come la garanzia della riservatezza delle informazioni

Approccio Sistemático

- Nel cyberspace non esiste distinzione tra organizzazioni pubbliche e organizzazioni private
 - Esistono risorse accessibili pubblicamente e risorse ad accesso controllato
- La ricerca è elemento essenziale per affrontare le minacce
- Tante modalità di approccio alla ricerca

Obiettivi

- **Fornire**
 - conoscenze su principi e tecniche per la sicurezza
 - capacità di applicare i concetti appresi nell'analisi di problemi reali
- **Stimolare**
 - analisi critica della tecnoscienza

Prerequisiti e Caratteristiche Richieste

- Conoscenze di base di informatica
 - Programmazione, Linguaggi, Algoritmi, Fondamenti
- Capacità di astrazione e formalizzazione
- Desiderio di applicare le conoscenze per indagare fenomeni che si presentano in pratica

Programma Preliminare (1)

- Parte 0: Introduzione
 - Presentazione: motivazioni e scopo del corso
 - Attacchi alla sicurezza, servizi e meccanismi di sicurezza, un modello per la sicurezza di rete
- Parte 1: Crittografia
 - Richiami di teoria dei numeri, strutture algebriche e complessità
 - Cifratura simmetrica e riservatezza dei messaggi.
 - Crittografia a chiave pubblica e autenticazione dei messaggi.

Programma Preliminare (2)

- Parte 2: Applicazioni di sicurezza di rete
 - Autenticazione
 - Sicurezza per email
 - Sicurezza IP
 - Sicurezza Web
 - Gestione
- Parte 3: Sicurezza di sistema
 - Intrusioni
 - Software dolosi
 - Firewall
 - Sicurezza per le basi di dati

Programma Preliminare (3)

- Parte 4: Approfondimenti
 - Sono sicuro che è sicuro? Modelli formali per la sicurezza
 - Mobile computing non è smartphone: Sicurezza nei sistemi mobili

Valutazione

- Scopo della valutazione: verificare
 - l'apprendimento dei concetti
 - le capacità di applicarli per risolvere problemi specifici
- Modalità: Tesina + **Prova Orale**
 - La tesina
 - Presentata in forma scritta deve approfondire un argomento trattato nel corso, oppure indagare altri temi, comunque attinenti la sicurezza
 - Il tema deve essere proposto dallo studente al docente, che lo deve accettare
 - Può essere svolta in gruppo (max 3 studenti)
 - La prova orale riguarda la tesina e l'intero programma

Bibliografia

- Testi
 - J. Pieprzyk, T. Hardjono, J. Seberry, *Fundamentals of Computer Security*, Springer, 2003
 - W. Stallings, *Sicurezza delle Reti – Applicazioni e Standard*, Pearson – Prentice Hall, 3rd Edition, 2007
 - W. Trappe, L.C. Washington, *Crittografia*, Pearson – Prentice Hall, 2nd Edition, 2009
- Lucidi del corso
 - disponibili a partire dal sito
http://www.di.uniba.it/~bianchi/didattica/2018_19/sic_inf/index.htm
- Ulteriori riferimenti
 - Articoli e lucidi citati / distribuiti durante le lezioni