Modelli Formali per la Sicurezza

Corso per il Dottorato di Ricerca in Informatica

XXIX Ciclo

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
    - su appuntamento
  - URL http://www.di.uniba.it/~bianchi/

Il Problema (1)

- La sicurezza delle applicazioni informatiche, essenzialmente nel caso dei sistemi distribuiti
- Diversi aspetti
  - Gestione e definizione delle politiche di sicurezza delle risorse a livello generale e locale (a livello di singolo proprietario di risorse o di V.O.)
  - dati e risorse in Grid devono essere "controllate" (monitorate).
  - differenti servizi Grid e utenti (i processi) devono essere in grado di 'fidarsi' l'uno dell'altro (trusted).

Il Problema (2)

- La sicurezza è alla base di un sistema di computazione distribuita:
  - Mutua Autenticazione ⇒ processo per stabilire una mutua fiducia,
  - Autorizzazione ⇒ capacità di stabilire chi può fare cosa,
  - Certificati ⇒ provano l'identità di un soggetto.
- È necessario garantire formalmente la sicurezza, mediante l'uso di appropriati modelli

Modellazione (1)

- La realizzazione di sw richiede successive attività di modellazione per passare da una rappresentazione del problema da livelli di astrazione più alti a livelli più bassi
- Esistono diversi tipi di modellizzazioni
  - Informali
  - Semiformali
  - Formali

Modellazione (2)

- I modelli non devono e non possono rappresentare tutto il sistema
  - Separazione degli aspetti il più possibile ortogonali fra loro
  - Si deve essere consci del fatto che gli aspetti da cui il modello astrae possono avere effetti che NON possono essere considerati
- Per ogni aspetto di interesse si definisce un modello che:
  - lo rappresenti come concetto “chiave”
  - che astragga da altri aspetti meno importanti

Modellazione (3)

- Per risolvere un problema estremamente complesso
  - lo si divide in diversi livelli di astrazione, affrontati in sequenza, ad esempio: top-down, bottom-up, o combinati
- La scelta del modello è essenziale per poter affrontare problemi complessi e per la qualità della realizzazione
  - Eventuali failure possono avere effetti disastrosi
  - …

Modellazione (4)

- È spesso necessario adottare modellizzazioni che favoriscano la validazione dell’applicazione rispetto ai parametri di qualità desiderati

Formalizzazione

- Permette di creare una specifica più completa, uniforme e non ambigua rispetto a quanto ottenuto con altri metodi
- Della specifica formale può essere dimostrata la correttezza
- È spesso necessario adottare modellizzazioni che favoriscano la validazione dell'applicazione rispetto ai parametri di qualità desiderati

Svantaggio della formalizzazione

- Adottare metodi di sviluppo formali:
  - è difficile
  - è impegnativo
  - richiede molto tempo
  - richiede elevate competenze

Analisi di proprietà computazionalmente interessanti

- L'adozione di modelli formali facilita l'analisi di proprietà particolarmente interessanti dal punto di vista computazionale
  - Deadlock/Livelock
  - Starvation/Liveness
  - Reachability
  - Reversibility
  - ...

Il Metodo ASM

- È un metodo per lo sviluppo di sistemi sw complessi, basato sul formalismo delle Abstract State Machine
- Delega a chi svolge la modellazione la profondità del formalismo
- Permette verifica e validazione del sistema e di alcune sue proprietà, ma manca di un approccio sistematico

Obiettivi del Corso

- Fornire
  - conoscenze sui concetti fondativi dei formalismi presentati
  - capacità di applicarli per valutare alcuni sistemi per la sicurezza nei sistemi distribuiti
- Stimolare
  - analisi critica delle conoscenze acquisite

Prerequisiti e Caratteristiche Richieste

- Conoscenze di base fornite nei corsi di Informatica triennale e Magistrale
- Capacità di astrazione e formalizzazione
- Desiderio di applicare le conoscenze per indagare fenomeni che si presentano in pratica

Programma (1)

- Presentazione
- Un Esempio di Modellazione Formale di Protocolli di Sicurezza
- Introduzione alle Abstract State Machine (ASM)
  - Il problema
  - Scopo e caratteristiche
  - Applicabilità

Programma (2)

- Concetti di base
  - Richiami sulle FSM
  - Da FSM a ASM
  - Il formalismo delle ASM
- ASM Bohem-Jacopini
  - Costrutti di sequenza-selezione-iterazione
  - Parametrizzazione
- Il metodo ASM-based
  - Ground model
  - Raffinamenti verticali
  - Raffinamenti orizzontali

Programma (3)

- Introduzione a Distributed ASM (DASM)
  - sync_DASM
  - async_DASM
- Analisi delle Proprietà
- Esempi di applicazione
  - Routing Sicuro nelle Mobile Ad-hoc NETwork (MANET)
  - Kerberos

Valutazione

- Scopo della valutazione: verificare
  - l'apprendimento dei concetti
  - le capacità di applicarli per risolvere problemi specifici
- Seminario monografico, oppure svolgimento di un caso di studio

Bibliografia

- Testo
  - E. Börger, R. Stärk, *Abstract State Machine*, Springer 2003
- Lucidi del corso, disponibili a partire dal sito
  - http://www.di.uniba.it/~bianchi/didattica/2013_14/security/index.htm
- Ulteriori riferimenti
  - Articoli e lucidi citati / distribuiti durante le lezioni