Sviluppo di Software Sicuro - S^3 Introduzione

Corso di Laurea Magistrale in
Sicurezza Informatica: Infrastrutture e Applicazioni
Università di Pisa – Polo di La Spezia
C. Montangero
Anno accademico 2009/10

Sommario

- Scopo del corso di S^3 (Sviluppo S^2)
- Contesto
- Contenuti del corso:
  - OCTAVE Allegro: analisi dei requisiti per S^2
  - KAOS: analisi dei requisiti + antimodelli per S^2
  - INFORMED: progetto dettagliato di S^2
  - SPARK: linguaggio e strumenti per la codifica di S^2
- Approccio
- Trivia
- Audit

S^3 2009/10 - Introduzione

SCOPO DEL CORSO

Software sicuro

- Classificazione di Jeannette Wing per
  - dimensioni crescenti del codice
  - garanzie decrescenti
- Quattro livelli
  - Crittografia
    - servizi di base: cifratura, firma, …
  - Protocolli
    - per comunicazione sicura, scambio chiavi, …
  - Sistema
    - servizi standard: SSH, remote file access, …
  - Applicazione
    - web-based banking operations, …

Scopo del Corso

- Presentare un approccio allo sviluppo di software *applicativo* che
  - considera gli aspetti legati alla sicurezza fin dall'inizio del processo di sviluppo
  - progetta e realizza i meccanismi di protezione durante la costruzione del sistema
  - non inietta soluzioni in un secondo tempo
- Costi minori
- Risultati (più) certi

S^3 2009/10 - Introduzione

CONTESTO

Contesto

- Ingegneria del software
  - processo di sviluppo
    - fasi e prodotti
  - modelli, metodi e strumenti
    - per gli aspetti di sicurezza
    - in ogni attività del processo
  - modello a cascata
    - per fissare le idee

Contesto

- La cascata
  - analisi -> requisiti
  - progetto -> architettura
  - progetto di dettaglio -> moduli
  - codifica -> sorgenti
  - testing -> risultati
  - dislocazione -> eseguibili

Contesto (limitato)

- La cascata
  - analisi -> requisiti
  - ~~progetto -> architettura~~
  - progetto di dettaglio -> moduli
  - codifica -> sorgenti
  - ~~testing -> risultati~~
  - ~~dislocazione -> eseguibili~~

S³ 2009/10 - Introduzione

CONTENUTI

Contenuti

- Analisi dei requisiti
  - OCTAVE Allegro
    - metodo *sistematico*
    - elicitazione dei requisiti di sicurezza
  - KAOS
    - metodo *formale*
    - elicitazione dei requisiti (in generale)
      - obiettivi (goal) delle parti in causa (stakeholder)
    - esteso alla definizione dei requisiti di sicurezza
      - obiettivi degli attaccanti (anti-modello)

Contenuti (2)

- Specifica del sistema
  - Modello formale
  - Z (leggi: zed)
    - linguaggio tipato basato su
      - teoria degli insiemi (Z per Zermelo-Frankel)
      - logica del prim'ordine
      - schemi, per strutturare la *specifica*

Contenuti (3)

- Progetto di dettaglio
  - aspetti statici: INFORMED
    - metodo per definire la struttura di un modulo SPARK
    - basato sulla suddivisione dello stato del modulo
    - secondo principi di coesione e disaccoppiamento
    - guidato dal modello formale
  - aspetti dinamici:
    - annotazioni SPARK dal modello formale Z

Contenuti (4)

- Programmazione in SPARK:
  - linguaggio basato su Ada
  - restrizione
    - per evitare le trappole che favoriscono vulnerabilità
      - array dinamici, puntatori, ...
  - estensione con commenti strutturati
    - asserzioni per verifiche statiche, *oltre* l'analisi dei tipi
      - data flow: inizializzazione variabili, ...
      - information flow: dipendenze di output da input
    - asserzioni da specifica Z
      - prove di correttezza
    - tre livelli di verifica (l'ultima semi-automatica)

S^3 2009/10 - Introduzione

APPROCCIO

Approccio

- Bottom-up
  - SPARK: codifica
  - INFORMED: progetto
  - Allegro: analisi sistematica
  - KAOS: analisi formale
- Un caso di studio reale: Tokeneer
  - stazione di verifiche biometriche
    - protezione ambiente con documenti/strumenti sensibili
  - ri-sviluppo Praxis per NSA
  - completamente disponibile
    - altri casi per aspetti particolari

Approccio (2)

- Supporto strumentale, dove appropriato
  - SPARK:
    - Examiner -> Verifiche statiche
    - con SPADE -> Prove di correttezza
  - SPADE
    - Prove di proprietà del modello formale
  - KAOS
    - Objectiver -> Modello dei requisiti
    - Profilo UML
- S^3: v0.1, chi vivrà vedrà

Trivia

- Testi
  - bibliografia su sito del corso
    - molto materiale in rete
    - altro sul sito
  - no lucidi
    - tranne argomenti particolari
- Strumenti
  - disponibili in laboratorio
  - in parte anche per download

Trivia (2)

- Esame in due parti
  - Progetto SPARK
    - variante Tokeneer
    - assegnato a metà semestre
    - consegna fine corso
    - in gruppi
  - (Progetto INFORMED/KAOS | orale)
    - consegna a un appello

Audit

- Glossario di termini di sicurezza
  - da un progetto SEI: CMU/SEI-2OO8-SR-O17
- Quali dei termini dal glossario
  - sono sconosciuti?
  - hanno un significato diverso?

S^3 2009/10 - Introduzione

PROSSIMO ARGOMENTO:
SPARK - INTRODUZIONE