

Sviluppo di Software Sicuro - S³

Introduzione

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

Sommario

- Scopo del corso di S³ (Sviluppo S²)
- Contesto
- Contenuti del corso:
 - OCTAVE Allegro: analisi dei requisiti per S²
 - KAOS: analisi dei requisiti + antiodelli per S²
 - INFORMED: progetto dettagliato di S²
 - SPARK: linguaggio e strumenti per la codifica di S²
- Approccio
- Trivia
- Audit

S³ 2009/10 - Introduzione

SCOPO DEL CORSO

S3 - C.Montangero - Copyright 2010

3

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, ...

S3 - C.Montangero - Copyright 2010

4

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

S3 - C.Montangero - Copyright 2010

5

S³ 2009/10 - Introduzione

CONTESTO

S3 - C.Montangero - Copyright 2010

6

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

S3 - C.Montangero - Copyright 2010

7

Contesto

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

S3 - C.Montangero - Copyright 2010

8

Contesto (limitato)

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

S3 - C.Montangero - Copyright 2010

9

S³ 2009/10 - Introduzione

CONTENUTI

S3 - C.Montangero - Copyright 2010

10

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)

S3 - C.Montangero - Copyright 2010

11

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*

S3 - C.Montangero - Copyright 2010

12

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

S3 - C.Montangero - Copyright 2010

13

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)

S3 - C.Montangero - Copyright 2010

14

S³ 2009/10 - Introduzione

APPROCCIO

S3 - C.Montangero - Copyright 2010

15

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

S3 - C.Montangero - Copyright 2010

16

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
- S³: v0.1, chi vivrà vedrà

S3 - C.Montangero - Copyright 2010

17

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

S3 - C.Montangero - Copyright 2010

18

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

S3 - C.Montangero - Copyright 2010

19

Audit

- Glossario di termini di sicurezza
 - da un progetto SEI: CMU/SEI-2008-SR-O17
- Quali dei termini dal glossario
 - sono sconosciuti?
 - hanno un significato diverso?

S3 - C.Montangero - Copyright 2010

20

S³ 2009/10 - Introduzione

**PROSSIMO ARGOMENTO:
SPARK - INTRODUZIONE**

S3 - C.Montangero - Copyright 2010

21