Lezione 1
Introduzione al corso

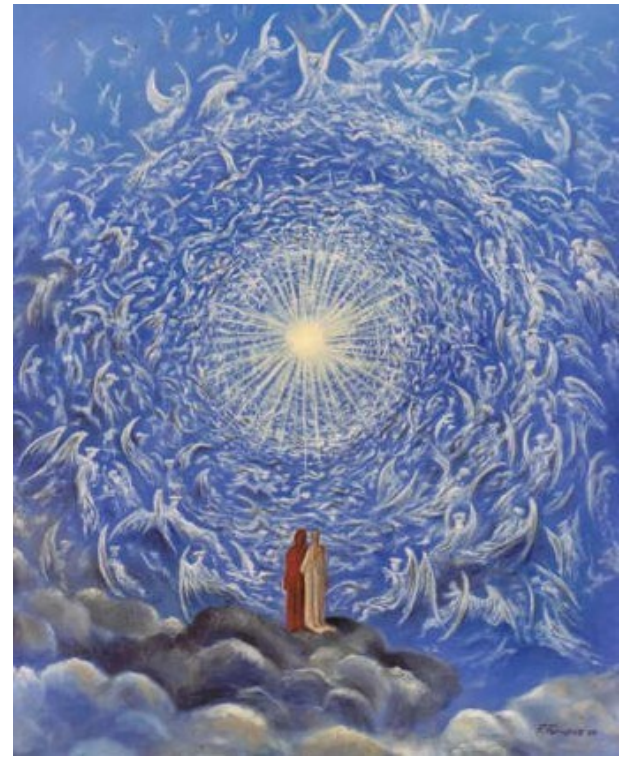
Sviluppo di software sicuro (9 CFU), LM Informatica, A. A. 2021/2022
Dipartimento di Scienze Fisiche, Informatiche e Matematiche
Università di Modena e Reggio Emilia
http://weblab.ing.unimore.it/people/andreolini/didattica/sviluppo-software-sicuro

Quote of the day

(Meditate, gente, meditate...)

“A l’alta fantasia qui mancò possa; ma già volgeva il mio disio e ‘l velle, sì come rota ch’igualmente è mossa, l’amor che move il sole e l’altre stelle.”

Dante Alighieri (1265-1321)
Divina Commedia, Paradiso,
Canto XXXIII, 142



Chi sono

(E come mi potete contattare)

Nome: Mauro Andreolini
Ruolo: RU, SSD INF/01
Ufficio: Matematica, 2° piano, MO-18-02-008
Contatti

https://weblab.ing.unimo.it/people/andreolini
mauro.andreolini@unimore.it
+39 059 2055192

Di che cosa mi occupo

(AKA "cosa faccio per campare")

- Ricerca
  - Sicurezza dei sistemi informatici
  - Sistemi distribuiti su larga scala (design, monitoring)
  - Sistemi operativi (networking, performance eval.)
  - Architetture ad alte prestazioni per il Web
  - Algoritmi per il monitoraggio di sistemi
- Didattica
  - Sistemi Operativi (LT 2° anno, 9 CFU)
  - Sviluppo di Software Sicuro (LM 1° anno, 9 CFU)

Obiettivi formativi del corso

(Che cosa saprete fare in più rispetto ad oggi)

Acuire la sensibilità ai rischi insiti in applicazioni non sicure.

Saper valutare il grado di sicurezza di una applicazione esistente.

Saper irrobustire una applicazione esistente.

Saper progettare ex-novo un software con caratteristiche di sicurezza (security, safety, privacy by design).

Contenuti

(Che cosa studierete esattamente)

Cenni storici.
Studio delle principali vulnerabilità (e relative conseguenze).
Strumenti per l'analisi di software esistente.
Ciclo di sviluppo del software sicuro (analisi requisiti, progetto, implementazione, collaudo, rilascio).

BIG FAT WARNING

(Sorry guys; I'm not gonna teach you things Elliot would do)

Il focus di questo corso **NON È** la violazione di applicazioni esistenti.

Il focus di questo corso **È** duplice:

irrobustire le applicazioni esistenti;

progettare le applicazioni ex-novo;

in modo tale da renderne più difficile la possibile violazione.

Struttura del corso

(Quando si studia cosa?)

Orari:

Lunedì	Aula M0.2, ore 14:00-16:00
Martedì	Aula M0.2, ore 9:00-11:30
Mercoledì	Aula M0.2, ore 11:00-13:00

Formato lezione:

- Didattica frontale (teoria, esercizi svolti dal docente)
- Esercizi di approfondimento da svolgere a casa

Il sistema considerato

(AKA "la vittima sacrificale")

Hardware: PC compatibile
ISA: x86/x86_64
SO: Debian GNU/Linux e derivati

→ È fortemente consigliato l'uso di un proprio portatile!
→ Usare una propria distribuzione GNU/Linux non è vietato, anzi…
→ Provare le tecniche apprese in altri ambienti (Windows, MacOS, Android) non è vietato, anzi...

Materiale didattico

(AKA “che cosa devo imparare a memoria per passare l'esame?”)

Dispense fornite dal docente

- Slide
- Siti Web di approfondimento

Punti bonus

(Stimoli per non far morire di noia i più bravi di voi)

Elargiti dal docente in occasioni speciali.

1. Lo studente fa una domanda inerente al programma a cui il docente non sa rispondere (shame on me!).
2. Lo studente individua errori non banali (no typo, sorry!) nelle slide del docente.

Domande a cui non so rispondere

(Sob...)

Lo studente pone un quesito relativo al programma didattico del corso.

- Non cercate di accaparrarvi punti con domande non inerenti al programma; non ci riuscireste.

Il docente non sa rispondere oppure fornisce una risposta poco convincente.

Il docente (dopo aver pianto lacrime amare) si segna il nome dello studente.

Ogni tre domande non risposte allo studente, il docente gli elargisce un terzo di punto bonus.

Errori non banali

(Sigh...)

Lo studente fa notare un errore non banale nelle slide con una sequenza di ragionamenti e con un "caso d'uso" che dimostra il problema.

- Non cercate di accaparrarvi punti setacciando le slide alla ricerca di errori ortografici; non ci riuscireste.

Il docente si convince dell'errore.

Il docente (dopo aver pianto lacrime amare) si segna il nome dello studente.

Ogni tre errori individuati dallo studente, il docente gli elargisce un punto bonus.

Modalità di esame

(Le dolenti note)

Colloquio orale. Niente scritti, niente parziali (se ne riparlerà quando sarete duecento).

Tre domande faccia a faccia con il docente.

Prima domanda: “domanda filtro”.

Seconda domanda: teoria e pratica.

Terza domanda: teoria e pratica.

Domanda filtro

(I'll kill you swiftly like a ninja)

Vi si chiede di risolvere uno degli esercizi visti a lezione, usando il portatile del docente.

Avete a disposizione un collegamento Internet.

Tempo limite: 10 minuti (senza deroghe). Se terminate l'esercizio, continuate l'esame. Altrimenti, siete subito respinti.

Domande successive

(Non è una passeggiata come può sembrare a prima vista)

Le domande 2 e 3 si svolgono nello stesso modo.

Il docente sceglie un argomento su cui interrogarvi e inizia a farvi parlare a piacere.

Seguono domande sempre più mirate per valutare la preparazione del candidato.

Viene verificata (a campione) la conoscenza dei comandi principali inerenti l'argomento.

Tempo limite: 10 minuti.

Il voto finale

(Viva l'aritmetica)

Voto finale = voto domanda filtro
+ voto domanda 2
+ voto domanda 3
+ punti bonus

Ogni imprecisione non banale commessa costa un punto.

E la lode?

(Già, la lode...)

Il docente decide se fare una ulteriore domanda per la lode. Lo studente decide se accettarla o no.

Se la accetta la subisce e, se non sa rispondere, il voto cala. **NON TENTATE LA SORTE!**

In alternativa, basta risolvere qualche arzigogolo e andare bene all'orale.

- “Bene”: terminare in <= 30 minuti senza dire fesserie colossali.

Norme comportamentali

(Repetita iuvant)

Lo studente deve mantenere un comportamento decoroso in aula.

> Non si mangia, non si beve, non si chiacchiera, non si dorme, non si ride, non si prova a battere il record al proprio videogame favorito, non si prova a sniffare il traffico di rete, non si prende in giro il docente, non si postano fesserie su Facebook et similia, etc.

Si esce dall'aula all'inizio, alla fine, o durante l'intervallo (a meno di clamorose incontinenze).