Ingegneria del Software e sicurezza

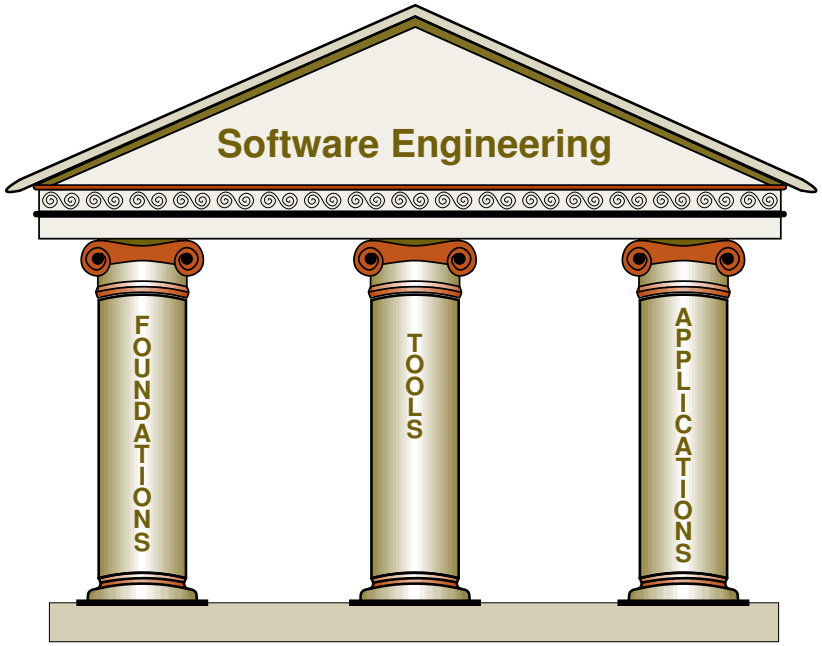
Formazione, Ricerca, Opportunità di Impiego

Luca Viganò
Dipartimento di Informatica, Università di Verona

Aula Gino Tessari, Mercoledì 25 Gennaio 2012, 16:30-19:10

Ingegneria del Software e Sicurezza

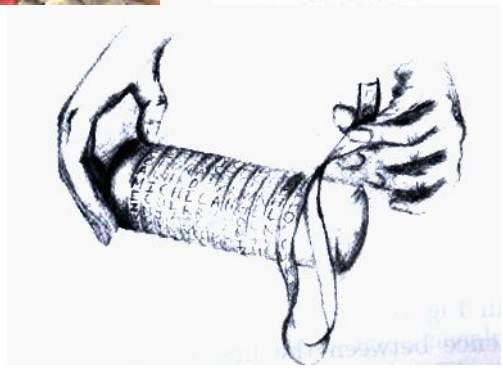
Software engineering is the practical application of scientific methods to the specification, design, and implementation of programs and systems

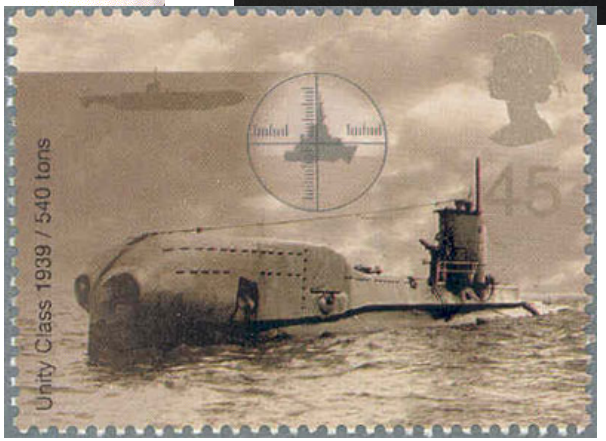


Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

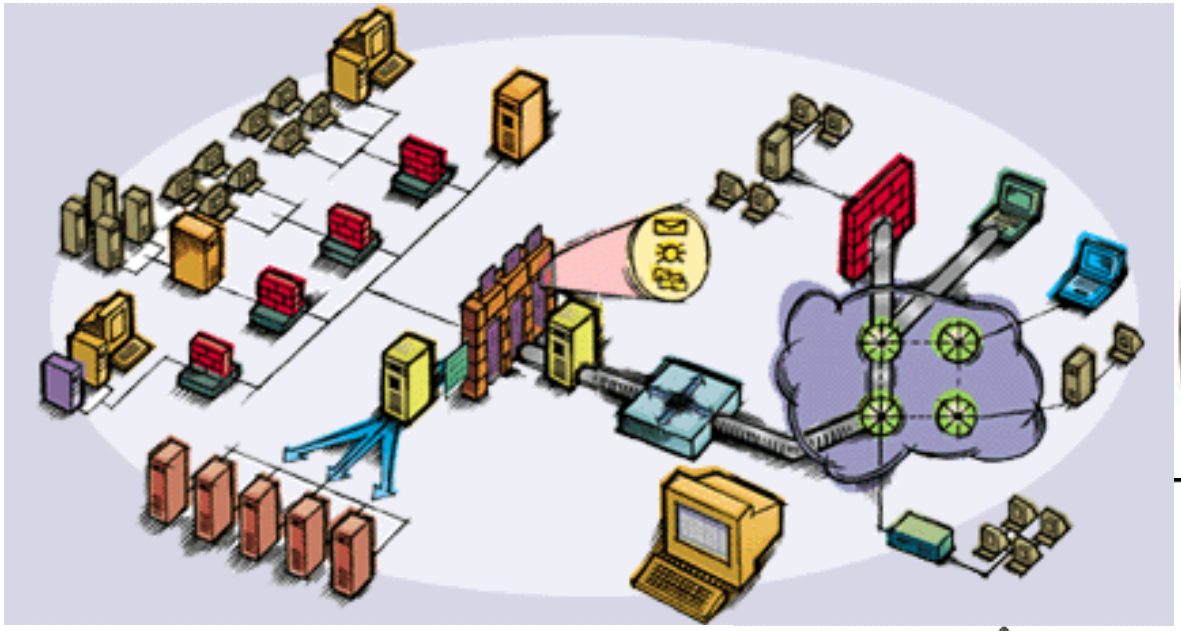
La sicurezza informatica: il passato

La sicurezza delle informazioni: un problema prettamente militare

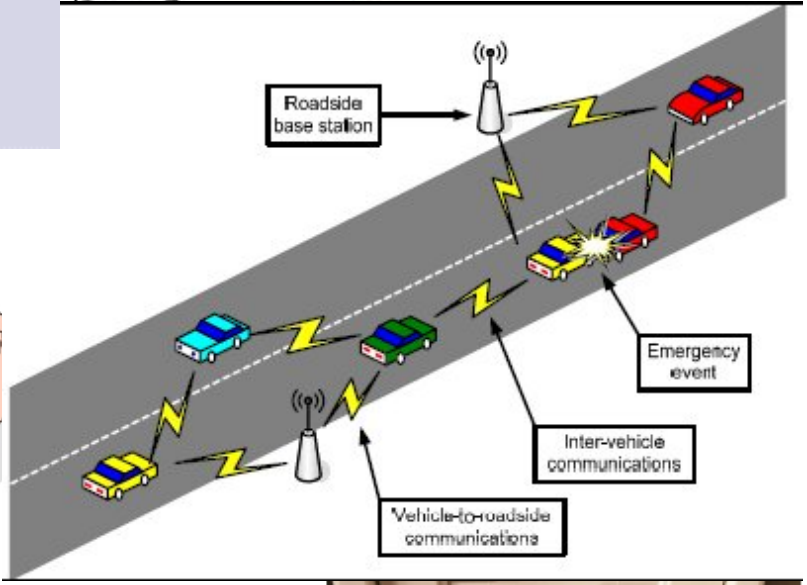


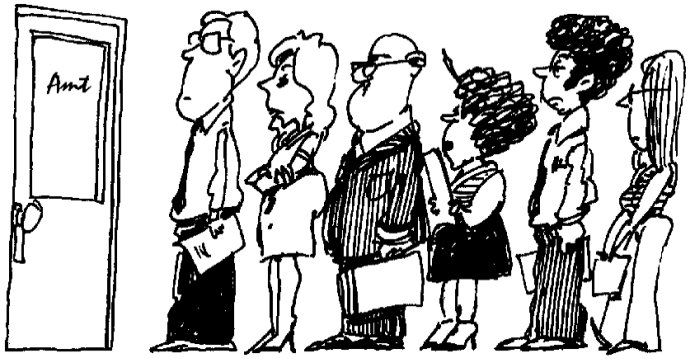


Presente e futuro: Internet dei Servizi

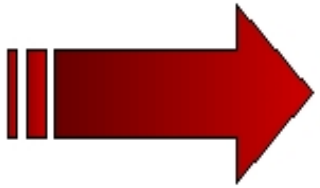



VOTE


Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications


Amt


SOCIAL NETWORK



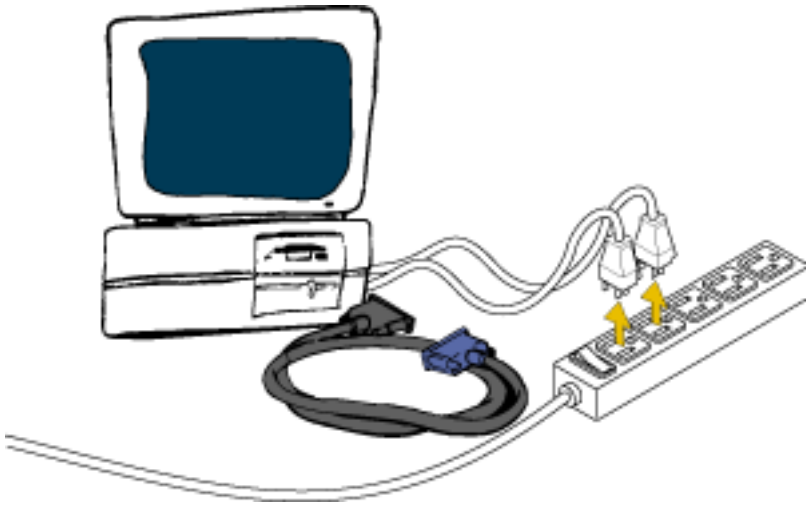
La sicurezza informatica

"On the Internet, nobody knows you're a dog."

"On Facebook, 273 people know I'm a dog.
The rest can only see my limited profile."

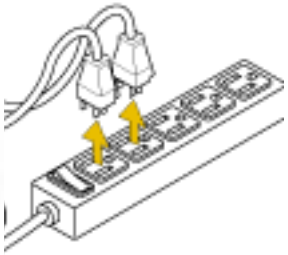
L’unico computer davvero sicuro…

Scollegato dalla rete e spento



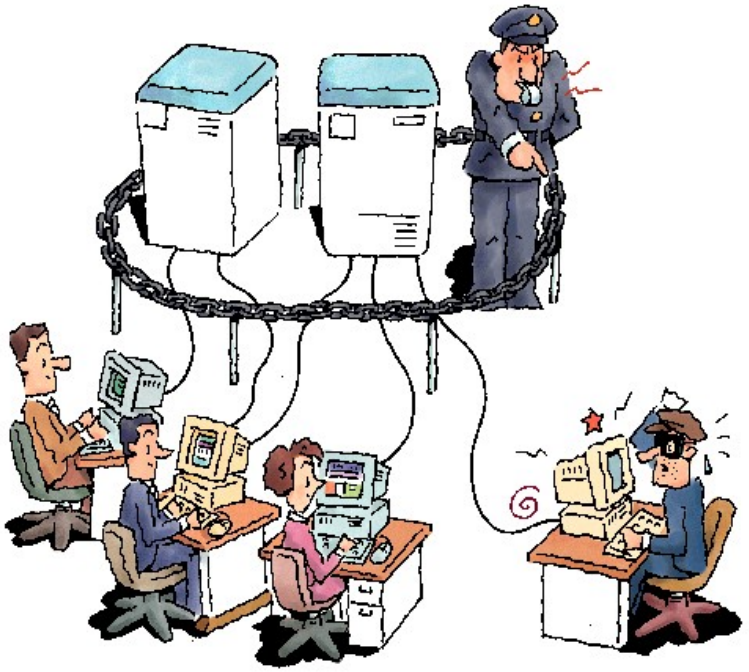
L’unico computer davvero sicuro…

Scollegato dalla rete e spento



Security engineering

- One must take a **holistic approach** to **security engineering**.



- Designing adequate mechanisms is challenging and careful "screening" is not enough.

- History if full of examples of "security breaches" due to poor "security screening".

Security engineering

Software/security errors in design are costly

- **Money**: updates are costing hundreds of millions Euros
- **Time**: software is delayed by years
- **Acceptance**: eroding confidence in Internet Security and new applications

Human validation impossible. We need:

- Techniques and tools that support formal analysis of software
- by either finding flaws or establishing their correctness

Optimally, these tools should be completely automated, robust, expressive, easily usable, so that they can be integrated into the software development and standardization processes.

PROGRAMMA

16:30 – Introduzione

16:40 – Il Curriculum Magistrale

- Il curriculum
- Sicurezza dei sistemi
- Sicurezza delle reti
- Verifica automatica di programmi
- Analisi statica e protezione
- Crittografia

Relatori: I docenti del curriculum

17:10 – Alcune applicazioni

- W32.Relock: un virus per Windows 7
  Relatore: M. Passuello
- Come difendere i security protocols
  Relatore: M. Peroli
- Slicing e verifica del software
  Relatore: D. Nikolic

17:40 – La ricerca avanzata

- I gruppi / laboratori di ricerca
- Il dottorato di ricerca
- Le opportunità dei progetti europei

Relatore: Luca Viganò

18:10 – Il mondo delle imprese

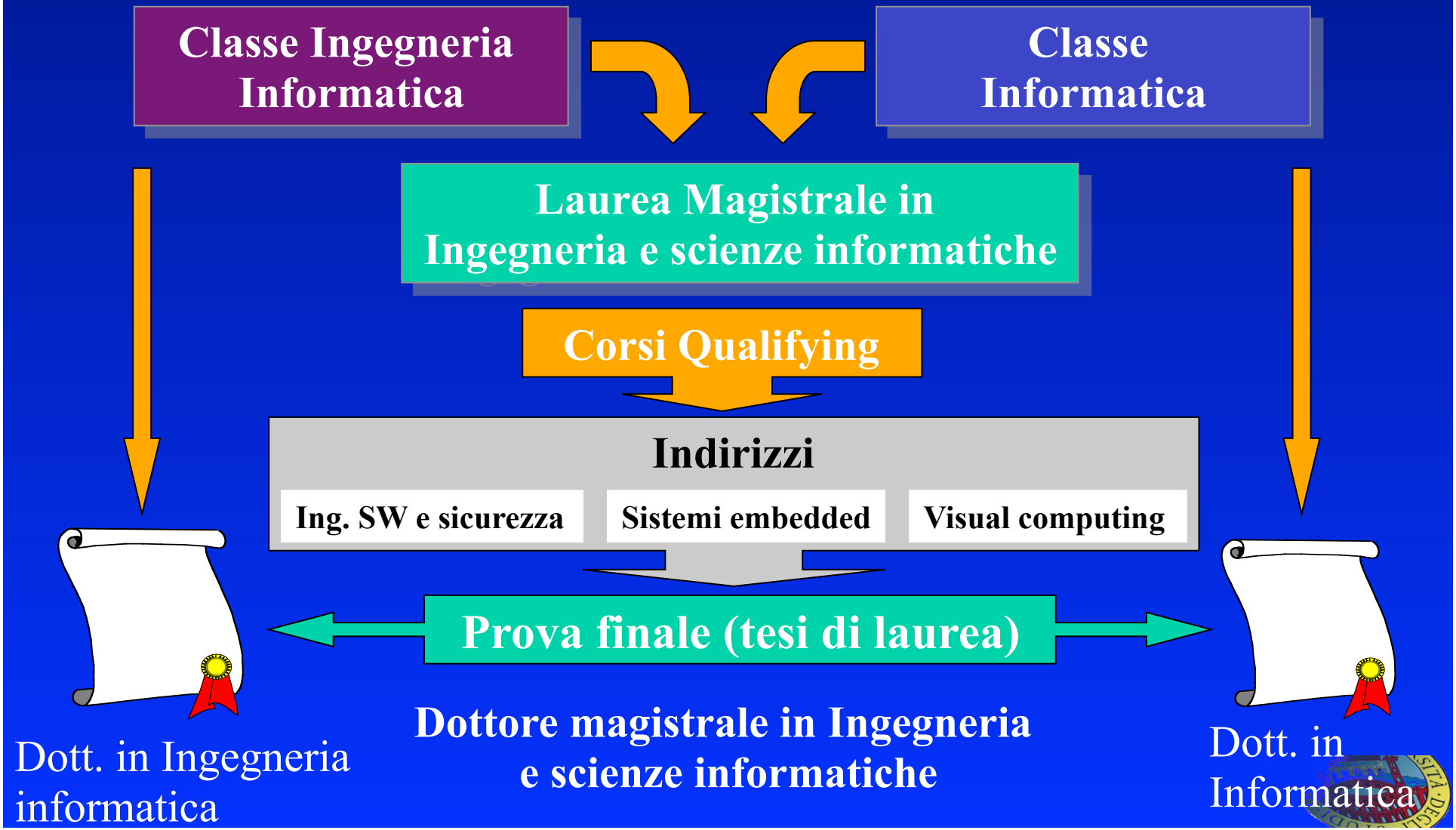
- ALBA S.T.
  Relatore: Alessio L.R. Pennasilico
- IBM Italia
  Relatori: Carla Milani e Davide Veronese
- JULIA S.r.l.
  Relatore: Paolo Fiorini

19:10 – Chiusura dei lavori

Laurea Magistrale in Ingegneria e scienze informatiche

- La riforma D.M. 270 consente di istituire corsi di laurea interclasse.
- Ciò ha consentito alla Facoltà di Scienze MM FF e NN, sfruttando le competenze dei propri docenti, di istituire un corso di laurea magistrale che integra la classe di **Ingegneria Informatica** con la classe di **Informatica** (primo caso in Italia).
- Lo studente che si iscrive al corso di laurea magistrale in Ingegneria e scienze informatiche può scegliere la classe in cui ottenere il titolo e se sceglie **Ingegneria Informatica** diventa, a conclusione del suo percorso, a tutti gli effetti un dottore in **Ingegneria informatica**.

Laurea Magistrale in Ingegneria e scienze informatiche



Laurea Magistrale in Ingegneria e scienze informatiche

- Tre insegnamenti qualifying da 12 crediti (da superare entro il primo anno):
  - Algoritmi (algoritmi, complessità)
  - Fondamenti (logica, linguaggi)
  - Sistemi (sistemi e segnali, sistemi a eventi discreti)
- Tre indirizzi (5 insegnamenti = 30 crediti):
  - Ingegneria del software e sicurezza
  - Visual computing
  - Sistemi embedded.
- Tre insegnamenti a scelta da 6 crediti nelle aree di Sistemi informativi, Robotica, BioInformatica, Informatica quantisitica, Web semantico.

Indirizzi Laurea Magistrale

Sicurezza	▪ Crittografia ▪ Sicurezza delle reti ▪ Verifica automatica di programmi ▪ Sicurezza dei sistemi ▪ Analisi statica e protezione
Visual	▪ Interazione uomo macchina ▪ Comunicazione multimediale ▪ Teoria e tecniche del riconoscimento ▪ Interazione non visuale ▪ Visione computazionale
Embedded	▪ **Architetture avanzate** ▪ **Sistemi operativi avanzati** ▪ **Progettazioen di sistemi embedded** ▪ **Sistemi embedded di rete** ▪ **Software per sistemi embedded**

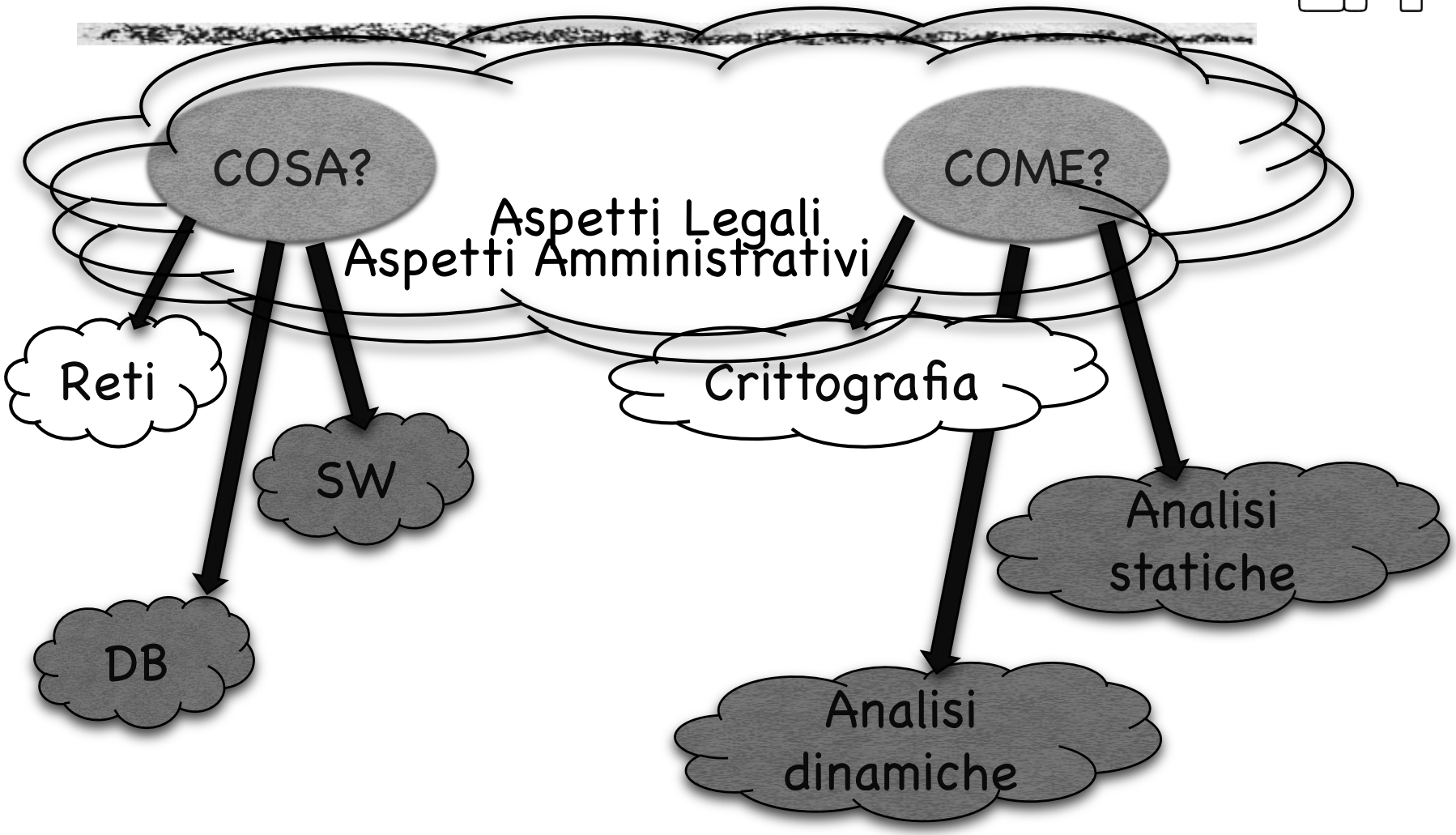
Sicurezza dei Sistemi

Presentazione del corso

2011/2012

Dott.ssa Isabella Mastroeni

Sicurezza = Proteggere



Sistemi Informatici

(in senso generale)

- Problema di sicurezza
  - Triade di sicurezza

COSA?

- Modelli classici
- Meccanismi standard
  - Controllo accessi
  - Autenticazione
  - Monitor

Analisi statiche

Analisi dinamiche

COME?

Database

- Problema di sicurezza
  - Protezione dati sensibili
  - Privacy
  - Affidabilità

COSA?

- Modelli
- Tecniche di protezione
  - Controllo accessi
  - Perturbazione
  - …

Analisi statiche

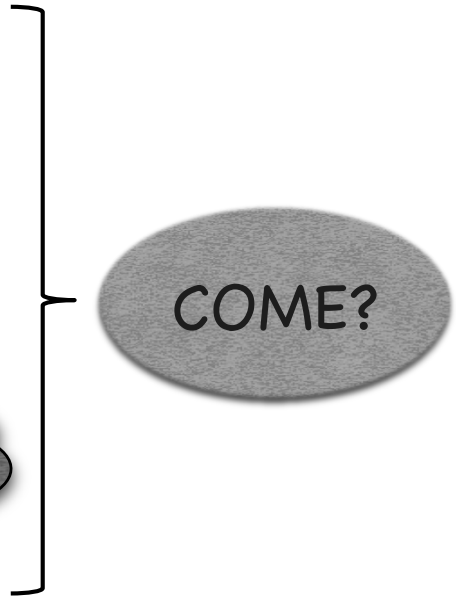
Analisi dinamiche

COME?

Software

- Problema di sicurezza
  - Vulnerabilità del SW

- Modelli
- Meccanismi
  - Antivirus
  - IDS



Aspetti comuni

- Aspetti legali
  - ✓ Concetto di crimine informatico
  - ✓ Legge sulla privacy
  - ✓ Proprietà intellettuale

- Aspetti amministrativi
  - ✓ Politiche e pratiche di sicurezza
  - ✓ Pianificazione di sicurezza
  - ✓ Analisi dei rischi

Ingegneria del Software e sicurezza

Sicurezza delle reti

Luca Viganò

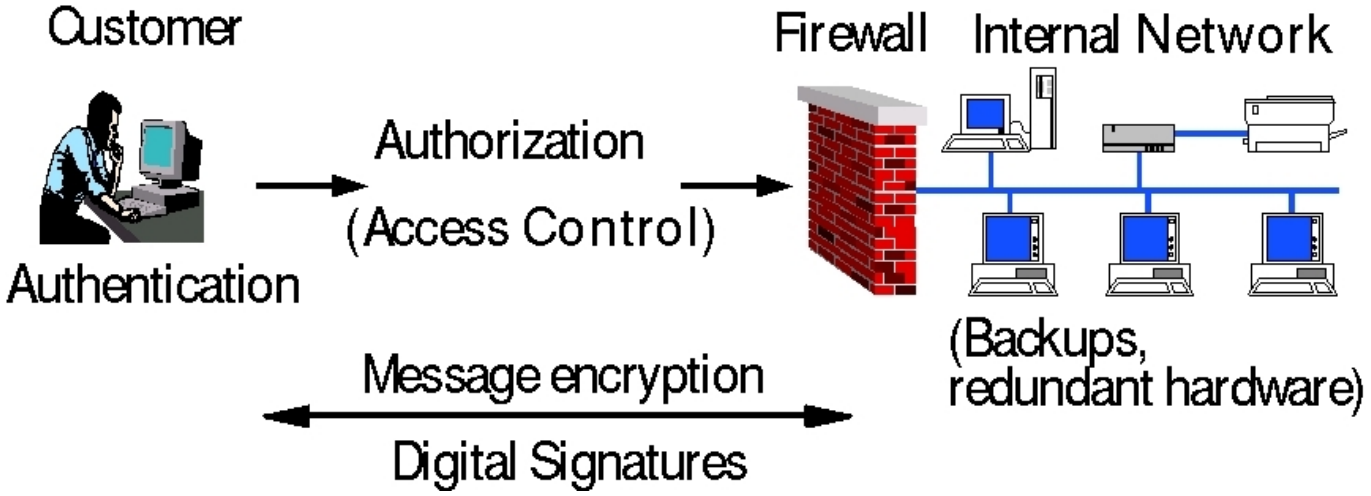
Dipartimento di Informatica, Università di Verona

Aula Gino Tessari, Mercoledì 25 Gennaio 2012, 16:30-19:10

REGIS
research group in information security

Sicurezza delle reti

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction



Network security consists of

- the provisions made in an underlying ***computer network*** infrastructure,
- ***policies*** adopted by the ***network administrator*** to protect the network and the network-accessible resources from ***unauthorized*** access and use, and
- the effectiveness/lack of these measures combined together

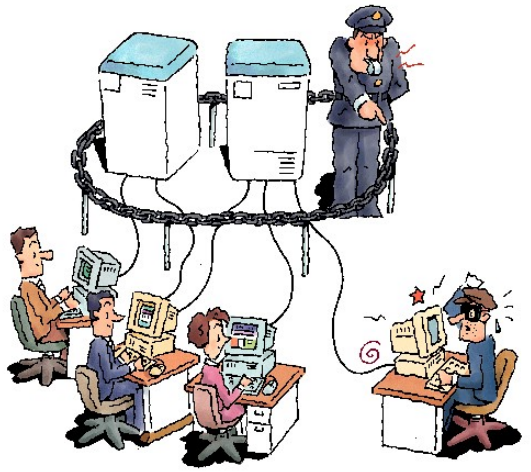
REGIS
research group in information security

Obiettivi del corso

Introduce the principal methodologies and technologies for the security of distributed networks

Basic **theoretical** and **applied** notions for the practical development and the formal analysis of networks and systems for information security

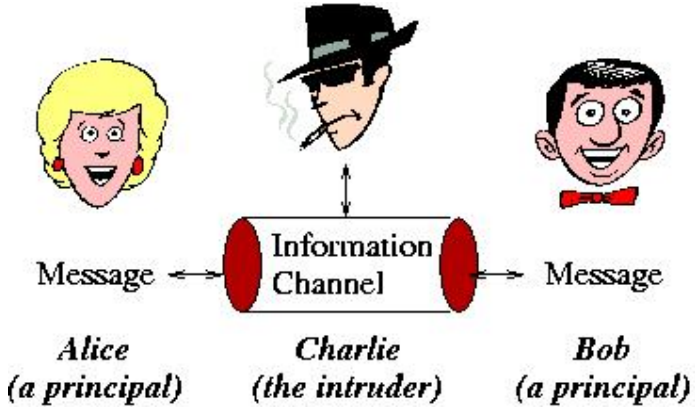
- **Teoria**: 32 h
- **Laboratorio**: 28 h
  (Applied Information Security Lab)

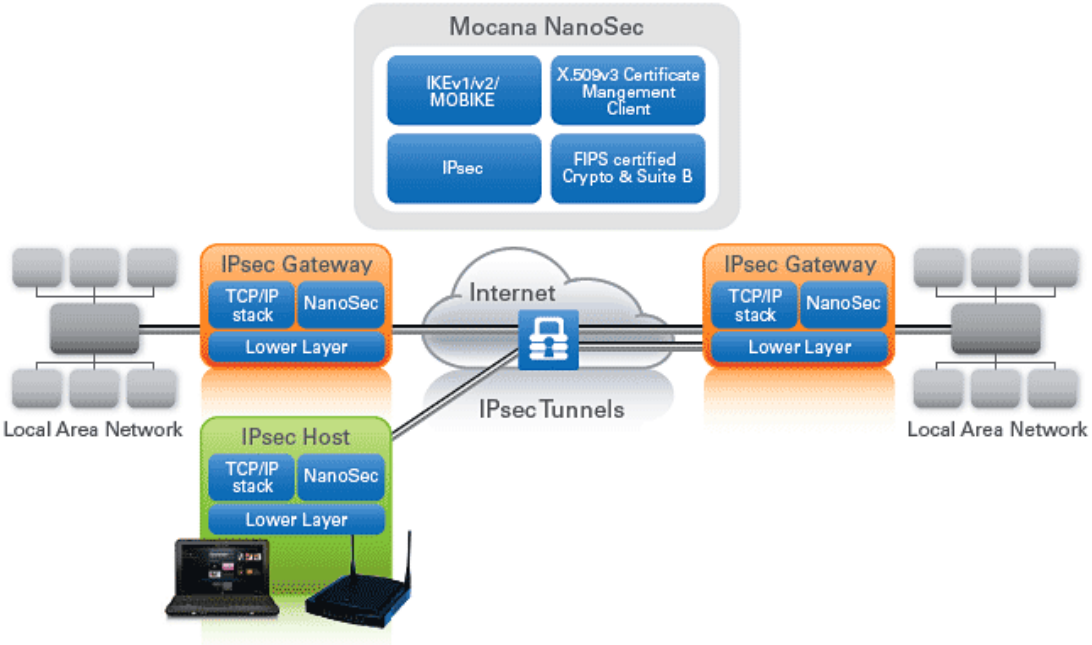


REGIS
research group in information security

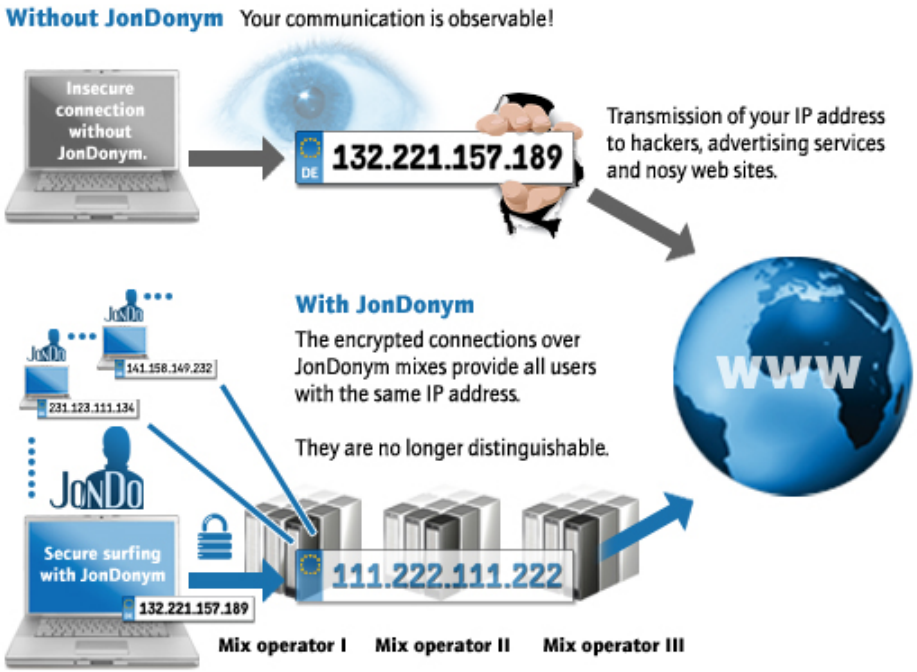
Syllabus

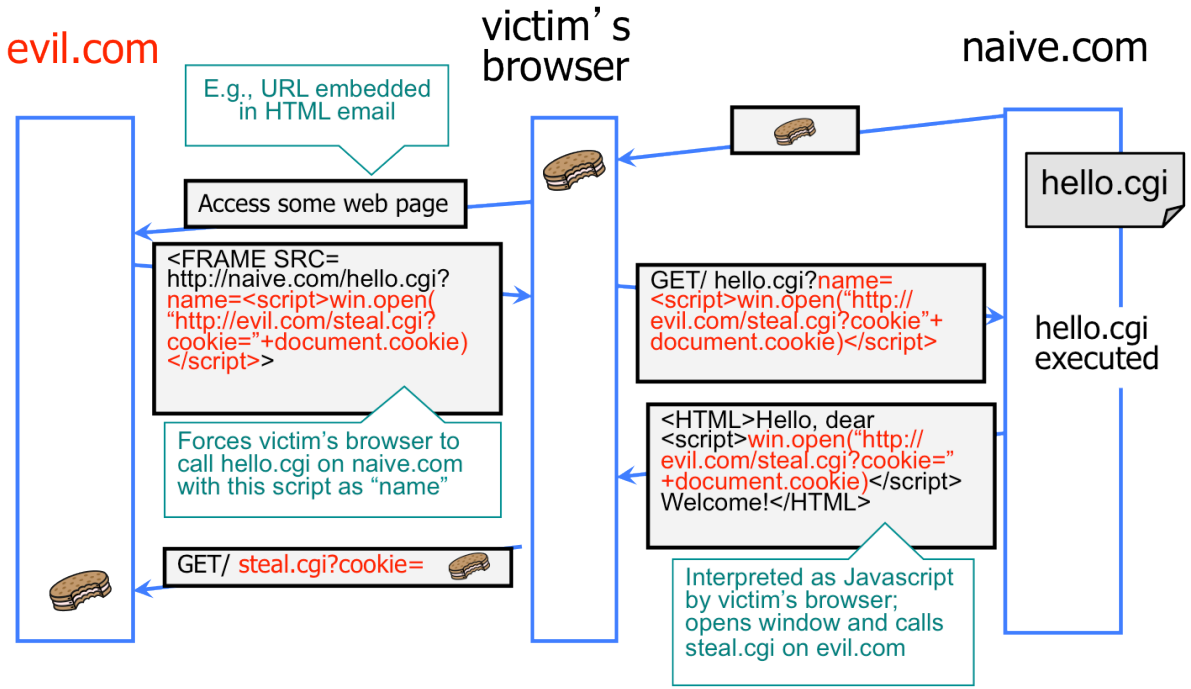
- **Introduction and basic notions of network security**
  - Public key infrastructures for network security
  - Security properties of communication channels
- **Protocols for network security**
  - Development and use of Internet security protocols
  - Case studies: Needham-Schroeder Shared-Key, Kerberos, Diffie-Hellman Key-Exchange, IKE, IPSec (IP Security)
  - Protocol threat models and attacks





- **Privacy and anonymity**
  - Policies, mechanisms, problems
  - Mix Networks and Crowds
- **Web Services and service-oriented architectures**
  - XSS, XSRF, injections, …





REGIS
research group in information security

Laboratorio

- Security principles
- The Virtual Environment
- Network services
- Authentication and Access Control
- Logging and Log Analysis
- Web Application Security
- Certificates and Public Key Cryptography
- Risk Management

REGIS
research group in information security

Ingegneria del Software e sicurezza

Verifica automatica di programmi

Luca Viganò (per Maria Paola Bonacina)
Dipartimento di Informatica, Università di Verona

Aula Gino Tessari, Mercoledì 25 Gennaio 2012, 16:30-19:10

Obiettivi del corso

L'insegnamento presenta problemi e metodi per l'analisi e la verifica di programmi, mediante tecniche di ragionamento automatico quali dimostrazione automatica di teoremi o model checking.

Obiettivo del corso è che lo studente, oltre a padroneggiare tecniche specifiche, comprenda i problemi inerenti da un lato a esprimere il comportamento dei programmi in formule logiche e dall'altro a progettare ragionatori automatici capaci di gestire tali formule in modo efficiente.

Il corso prevede lo svolgimento di un progetto.

Syllabus

- Dimostrazione automatica di teoremi in logica proposizionale: la procedura di Davis-Putnam-Logemann-Loveland.
- Dimostrazione automatica di teoremi in logica del primo ordine: risoluzione e sovrapposizione.
- Teorie al primo ordine.
- Logica di Hoare, annotazioni, correttezza parziale e totale, stati, cammini, invarianti.
- Generazione di invarianti.
- Procedure di decisione per la soddisfacibilità modulo teorie: uguaglianza, strutture di dati, combinazione di teorie per condivisione di uguaglianze, procedure di decisione basate su risoluzione e sovrapposizione.

Università degli Studi di Verona

Analisi Statica e Protezione

Analisi Statica e Protezione: "ASP"
Prof. Roberto Giacobazzi – 2° anno

due temi principali

ANALISI STATICA

- DATAFLOW ANALYSIS
- INTERPRETAZIONE ASTRATTA

PROTEZIONE DEL CODICE

- OFFUSCAMENTO
- TAMPERPROOFING
- WATERMARKING

Ma non solo! Verranno trattati anche aspetti di privacy, copyrights, tecniche di reverse engineering, disassemblaggio, …

OBIETTIVI DEL CORSO

Vedere strumenti, metodologie e tecniche per ragionare sulle proprietà dei programmi.

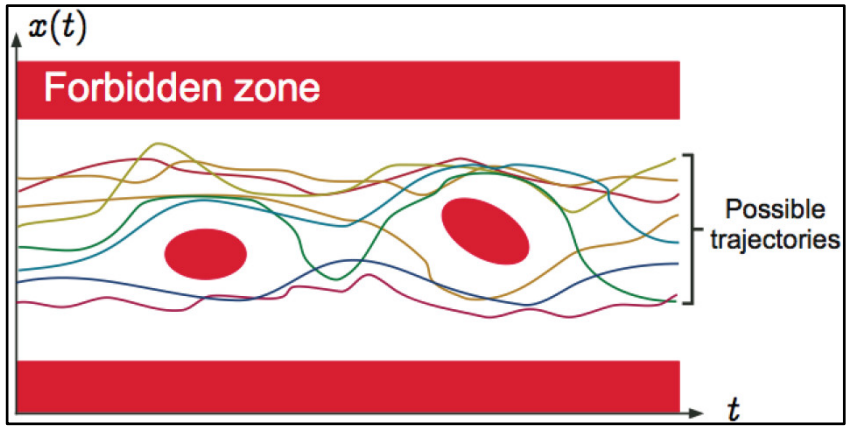
Conoscere l'analisi statica come strumento per valutare sicurezza e affidabilità di sistemi SW.

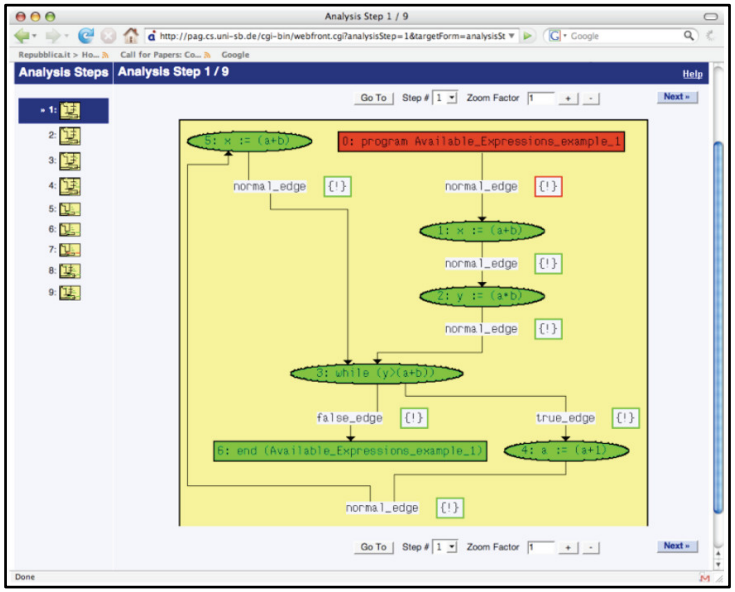
Padroneggiare le basi fondamentali per realizzare sistemi SW sicuri ed affidabili.

Metodi e tecniche per l'analisi e la trasformazione del codice.

Capire potenzialità e vantaggi di alcune tra le principali tecniche di difesa del codice.

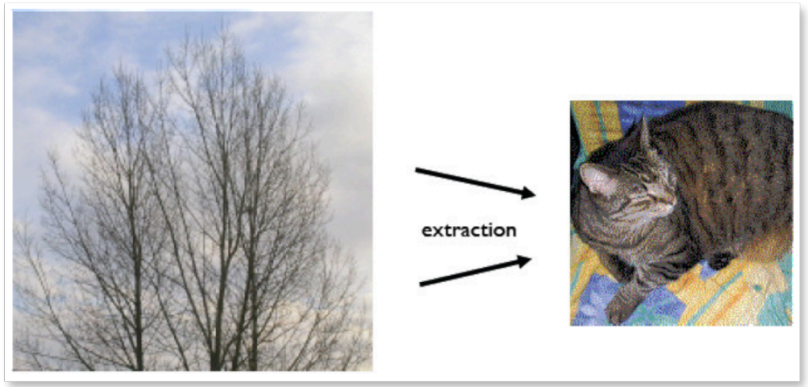
ANALISI STATICA

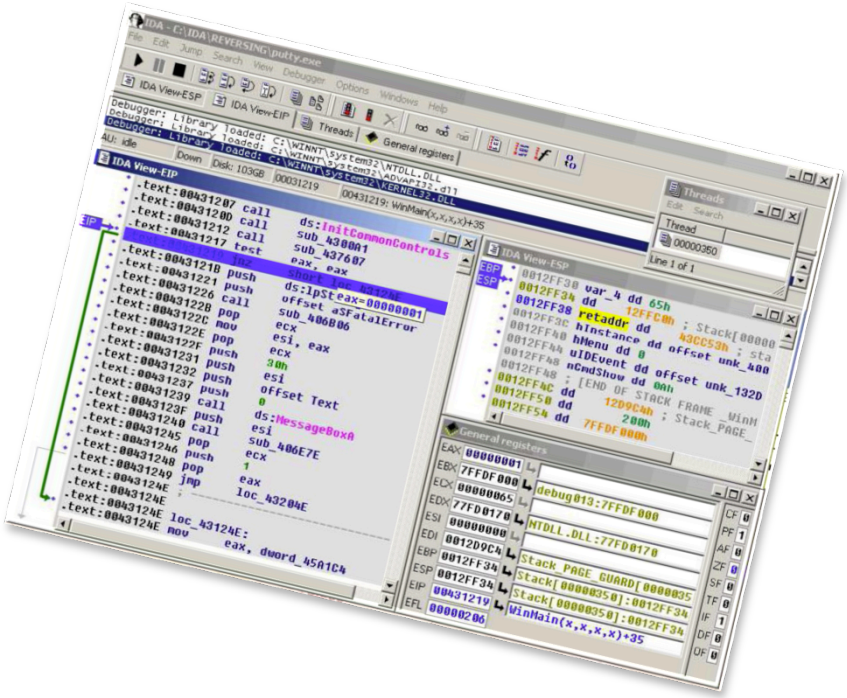




- **Eliminare o limitare i bug**
- **Ricavare proprietà dei programmi**
- **Prevenire esecuzioni pericolose**

PROTEZIONE DEL CODICE





- **Proteggere diritti e copyrights**
- **Debugging e disassembling**
- **Malware e vulenrabilità**

Ingegneria del Software e sicurezza

Crittografia

Roberto Segala
Dipartimento di Informatica, Università di Verona

Aula Gino Tessari, Mercoledì 25 Gennaio 2012, 16:30-19:10

Obiettivi del corso

Il corso si propone di far acquisire le competenze di base relative

- agli strumenti computazionali per la criptazione dei dati,
- all'uso di tali strumenti per la gestione di comunicazioni sicure, e
- ai problemi legati all'implementazione di primitive crittografiche.

Viene data enfasi sia alla struttura dei principali algoritmi e protocolli crittografici che agli aspetti definizionali dei problemi e agli strumenti formali per la loro analisi.

Syllabus

- Crittografia a chiave simmetrica (DES, AES)
- CBC
- crittografia a chiave pubblica (Diffie-Hellman, RSA, BBS, El Gamal)
- provable security e critto sistemi provable secure
- funzioni one way trapdoor
- generazione di bit e funzioni pseudo casuali
- protocolli di firma digitale (RSA)
- funzioni hash collision free (MD5, SHA1)
- bit commitment
- verifiable secret sharing
- Zero-Knowledge
- autenticazione di messaggi
- autenticazione di agenti
- modelli di specifica ed analisi (computazionale, giochi, Dolev-Yao) e loro relazioni