Sicurezza e Crittografia
Introduzione al Corso

Ugo Dal Lago
Dipartimento di Scienze dell'Informazione
Università degli Studi di Bologna
`dallago@cs.unibo.it`

28 settembre 2009

Cosa?

- L'obiettivo del corso è quello di studiare la **sicurezza informatica**, concentrandosi sugli aspetti più teorici.
- In particolare, il corso è suddiviso in due parti:
  - Inizialmente si parlerà di **crittografia moderna**.
  - In un secondo momento, verranno illustrate alcune tecniche per la **verifica** (automatica o semi-automatica) di correttezza per **protocolli di sicurezza**.
- **Crittografia Moderna**
  - La crittografia occuperà almeno 2/3 del corso.
  - Si studieranno alcuni risultati teorici che hanno permesso alla crittografia di diventare una **scienza**.
    - Fino alla metà degli anni Ottanta, la crittografia era un'**arte**.
    - Non esistevano, in particolare, definizioni precise del concetto di **sicurezza** per codici, protocolli, etc.
    - La crittografia, in altre parole, consisteva in una collezione di tecniche **presumibilmente** sicure (che spesso si scoprivano essere **insicure**).
  - Si procederà quindi in due fasi:
    - Si **definiranno** formalmente le proprietà di sicurezza.
    - Si **dimostrerà** poi come sia possibile (sotto certe ipotesi) costruire tecniche crittografiche sicure.
  - Si procederà in questo modo parlando di crittografia a chiave simmetrica e a chiave asimmetrica, di autenticazione di messaggi e (tempo permettendo) di firma digitale.
  - **Strumento** teorico fondamentale sarà la **pseudocasualità**.
    - Requisiti: **calcolo delle probabilità**, **teoria degli algoritmi**.
- **Verifica di Correttezza di Protocolli di Sicurezza**
  - Questa seconda tematica occuperà al più 1/3 del corso.
  - Esistono **moltissime** tecniche per la verifica automatica o semi-automatica di proprietà di sicurezza.
    - **Model-checking**.
    - **Dimostrazione assistita**.
    - **Interpretazione astratta**.
    - **Programmazione logica**.
    - ...
  - Ci concentreremo su un **caso di studio concreto**, ovvero sul tool `proverif`:
    `http://www.proverif.ens.fr/`

Chi?

- Questo corso è pensato per gli studenti della Laurea Magistrale in Informatica.
  - E' un insegnamento del **Gruppo A**.
  - Può essere seguito anche dagli studenti della "vecchia" Laurea Specialistica in Informatica.
  - Per studenti di altri corsi di laurea, si contatti il docente.
- Il docente è **Ugo Dal Lago**.
  - Email: `dallago@cs.unibo.it`
  - Ufficio: **via Malaguti, 1/D**
  - Ricevimento Studenti:
    - Su appuntamento (via posta elettronica).

Come?

- Il corso prevede 40 ore di lezioni teoriche.
- Orario delle lezioni:
  - **Lunedì**: 16.30-18-30 (Arzelà).
  - **Giovedì**: 16.00-18:30 (Arzelà).
- La lezione del giovedì inizierà talvolta alle 16:30.
- Modalità d'esame:
  - **Approfondimento.**
    - Lo studente sceglie, su suggerimento del docente, una tematica di ricerca inerente il corso.
    - Legge poi uno o più articoli di ricerca relativi alla tematica.
    - Scrive quindi una breve relazione (10-15 pagine) sul materiale studiato.
    - Presenta infine al docente e agli altri studenti ciò di cui si è occupato (in un seminario).
  - **Esame orale.**
- Per la parte relativa alla crittografia moderna, il testo di riferimento sarà:
  - *J. Katz and Y. Lindell.* **Introduction to Modern Cryptography**. Chapman & Hall, 2007.
- Altri testi interessanti sono i seguenti:
  - *D. O Goldreich.* **Foundations of Cryptography I: Basic Tools**. Cambridge University Press, 2001.
  - *D. O Goldreich.* **Foundations of Cryptography II: Basic Applications**. Cambridge University Press, 2004.
  - *D. R. Stinson.* **Cryptography: theory and practice**. Chapman & Hall, Third Edition, 2006.
- Nella seconda parte utilizzeremo alcune note reperibili sul web.
- La pagina web del corso è:

  `http://www.cs.unibo.it/~dallago/SEC0910/`
- Il newsgroup del corso è:

  `unibo.cs.informatica.sicurezzacrittografia`