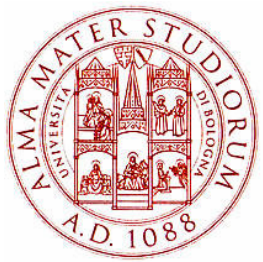
Sicurezza 2006 - 2007

Lezione 1: *Principi fondamentali di sicurezza informatica*

Gabriele D'Angelo
<*gda@cs.unibo.it*>
http://www.cs.unibo.it/~gdangelo/



Master universitario in
Tecnologia del Software Libero
e Open Source
Università di Bologna

07/09/2007, Bologna

Scaletta della lezione

- Alcuni principi fondamentali della sicurezza informatica:
  - **Principio numero 1**: inesistenza di sistemi sicuri
  - **Principio numero 1 corollario**: complessità dei sistemi
  - **Principio numero 2**: entità componenti di un sistema
  - **Principio numero 3**: sicurezza = conoscenza
- Sicurezza di un crittosistema
- Paranoia & sicurezza

Principi fondamentali: sistemi sicuri

- **Principio numero 1:**

NON ESISTONO SISTEMI SICURI

- Il software può non essere perfetto (e usualmente non lo è), allo stesso modo ci possono esserci errori di progettazione nei protocolli che usiamo normalmente
- Il mito del sistema inviolabile deve essere assimilato a quello del caveau non svaligiabile o della nave inaffondabile (es. Titanic)
- Il **grado di sicurezza** è dato dal tempo necessario per violare il sistema, dall'investimento necessario e dalla probabilità di successo

Cosa stiamo proteggendo, da **chi** e **perché**?

Principi fondamentali: complessità

- **Principio numero 1 corollario:**

  UN SISTEMA PIÙ È COMPLESSO PIÙ È INSICURO

- Empiricamente si nota come la crescita di complessità porti necessariamente alla creazione di sistemi insicuri. Inoltre risulta evidente come la funzione sia più che proporzionale!
- Un buon punto di partenza per la creazione di sistemi sicuri è l'applicazione metodica della **KISS rule**: *Keep It Simple and Stupid*
- Questo NON significa che i sistemi da proteggere non possano essere molto complessi o articolati ma che il sistema di protezione deve essere quanto più semplice possibile, se possibile estremamente semplice ("*Quello che non c'è non si rompe*")
- Tutta la complessità che non è necessaria implica possibili errori (di progettazione o implementazione) e le conseguenti falle nel sistema

Principi fondamentali: entità componenti di un sistema

- **Principio numero 2:**

  LE ENTITÀ CHE COMPONGONO UN SISTEMA SONO 3

  1. **HARDWARE**
  2. **SOFTWARE**
  3. **HUMANWARE**

- La componente umana non deve mai essere sottovalutata

- **La sicurezza è un processo**: senza un continuo apporto di lavoro e di educazione nessun sistema può essere ragionevolmente sicuro. Un sistema considerato sicuro oggi può non esserlo domani (molto probabilmente non lo sarà), ad esempio per la scoperta di un difetto del sistema. I sistemi che non vengono aggiornati in modo continuo ed attento divengono quindi fragili e insicuri

Principi fondamentali: sicurezza = conoscenza

- **Principio numero 3:**

  SICUREZZA = CONOSCENZA

- Nessun sistema sconosciuto può essere considerato sicuro
- Quali implicazioni ha questa affermazione sul tema del software **Open Source vs. Closed Source**, **Sistemi Aperti vs. Sistemi Chiusi**?
- In questi due casi distinti, potenzialmente abbiamo la possibilità di un diverso livello di analisi del sistema?
- Atto di fiducia nei confronti di una comunità vs. di un'azienda
- L'educazione degli utenti è una forma di conoscenza fondamentale (es. percezione dell'importanza del tema sicurezza, pratiche comunemente diffuse ma altamente insicure, resistenza ideologiche o per semplice abitudine ecc.)

Principi fondamentali: crittografia

- Questo principio della sicurezza informatica può essere assimilato ad un principio della crittografia che è molto noto:

  La sicurezza di un crittosistema non deve dipendere dalla segretezza dell'algoritmo usato, ma solo dalla segretezza della chiave

  (Kerckhoffs. La criptographie militaire, 1883)

- NOTA BENE: questo NON significa che diffondere tutti i dettagli sul proprio sistema sia una buona pratica di sicurezza, anzi, è un primo passo per rendere il proprio sistema insicuro! (e non ha praticamente nulla a che fare con la **security through obscurity**)

La paranoia nella sicurezza [informatica]?

- Ma ricordate sempre che:

"Only the paranoids will survive"

Andy Grove

Ringraziamenti

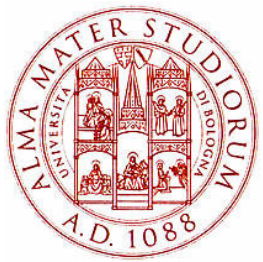
- Gran parte di questi lucidi sono direttamente tratti o “ispirati” da un lavoro precedente del Prof. Renzo Davoli, si ringrazia sentitamente

- In ogni caso la responsabilità di qualsiasi errore o imprecisione è da imputare esclusivamente all’autore di questa lezione

Sicurezza 2006 - 2007

Lezione 1: *Principi fondamentali di sicurezza informatica*

Gabriele D'Angelo
<*gda@cs.unibo.it*>
http://www.cs.unibo.it/~gdangelo/



Master universitario in
Tecnologia del Software Libero
e Open Source
Università di Bologna

07/09/2007, Bologna