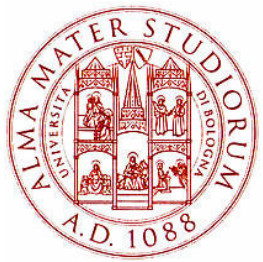
Sicurezza 2006 - 2007

Lezione 2: Natura ed evoluzione del fenomeno hacking

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

05/10/2007, Bologna

Scaletta della lezione

- Definizione del termine hacker
- Definizione del termine cracker
- Etica hacker (by Levy)
- Frutti concreti del fenomeno hacking
- Profilo di un hacker
- Come si diventa hacker?
- Profilo di un cracker
- Tassonomia (Halleck)
- Cracker bravi o fortunati?

Definizione del termine hacker

- **Chi è un Hacker:** *è una persona interessata a conoscere nei minimi dettagli gli aspetti più nascosti e reconditi delle funzionalità di un sistema informatico*

  - Gli hacker sono studiosi, veri esperti di sistemi operativi, linguaggi, reti… hardware
  - Nella maggior parte dei casi gli hacker sono seri professionisti, programmatori, sistemisti
  - Sono continuamente alla ricerca di nuova conoscenza che condividono gratuitamente con tutti
  - Non danneggiano mai, volontariamente, le informazioni

Definizione del termine cracker

- **Chi è un Cracker:** *è una persona che volontariamente viola la integrità di sistemi agendo con intenti maligni*
  - Spesso agiscono per carpire informazioni riservate, distruggere dati importanti ed eventualmente impedire l'accesso a utenti legittimi
  - Agiscono **non** per il fine di conoscere o comprendere ma per danneggiare o per trarne un vantaggio strettamente personale (molto spesso economico o facilmente monetizzabile)

The basic difference is this: hackers build things, crackers break them

Eric S. Raymond

Etica hacker secondo Steven Levy

- Access to computers -- and anything which might teach you something about the way the world works -- should be **unlimited** and **total**
- Always yield to the **Hands-On Imperative**
- All information should be **free**
- Mistrust authority--promote decentralization
- Hackers should be judged by their hacking
- You can create art and beauty on a computer
- Computers can change your life for the better

Frutti concreti del fenomeno hacking

- **Personal Computer** (Jobs, Wozniac)
- **UNIX** (Ritchie, Thompson, Kernighan)
- **C Language** (Ritchie)
- **GNU-Linux** (Stallman, Torvalds)
- **Memoria Virtuale** (Joy, Babaoglu)
- **Napster** (Fanning)
- **Gnutella** (Kan)
- **Virtualizzazione di sistemi e di reti** (?)
- ...

Profilo di un hacker

Un hacker è quindi uno studioso che:

- Applica tecniche tipiche della ricerca e investigazione scientifica alla conoscenza del funzionamento di apparati hardware e sistemi software (non sempre seguendo i metodi più ortodossi o “tipici”)
- Desidera (o dovrebbe desiderare) la vera conoscenza, non si limita a quella funzionale al proprio lavoro. La curiosità è quindi una componente essenziale della sua esistenza
- È quasi sempre “computer addicted”, è fiero ed orgoglioso della propria conoscenza al punto di farne una vera e propria identità

Come si diventa hacker?

To follow the path:

look to the master,

follow the master,

walk with the master,

see through the master,

become the master.

(poesia Zen)

“How to become an Hacker” (Eric Steven Raymond)

Autore di "Jargon File“ e “The Cathedral and the Bazaar"

Profilo di un cracker

Non c'è una singola tipologia di cracker, possono infatti avere diversi scopi per il loro cracking:

- Conquistare un rango fra i “cracker”
- Soddisfare il proprio io
- Divertimento
- Motivi “morali”: combattere battaglie in nome dell'etica, dell'ecologia, di una idea politica o in nome dell'hacking
- Avere accesso gratuito a contenuti “protetti”
- Per denaro
- Per noia

Tassonomia (by Gurney Halleck)

- La “**vecchia scuola**”: hacker che per il desiderio di conoscenza hanno varcato la soglia e hanno compiuto azioni illegali. Non danneggiano ma si limitano ad osservare per comprendere. Sono esperti
- La “**nuova scuola**”: giovani cracker che spesso sono riuniti in gruppi e svolgono competizioni per compiere azioni vistose: “gradassate informatiche” (es. **defacing**). Hanno limitate competenze tecniche legate principalmente ai mondi Windows e più raramente Apple
- Lo “**Script Kiddie**” (il ragazzotto degli script). Trova istruzioni per violare sistemi e prova come sia facile entrare negli elaboratori altrui (soprattutto grazie all’imperizia di tanti amministratori)

Tassonomia (by Gurney Halleck)

- Il “**Warez Kid**”. Ha il solo scopo di scambiare software, musica, film pirata. Elimina protezioni e scopre codici di attivazione. È spesso un ottimo giocatore di videogame
- Il “**Phreaker**” (da phone + freak). È il pirata dei sistemi telefonici. Un tempo usava fischietti e scatolette magiche ora riprogramma i centralini aziendali per poter fare chiamate gratis o per spiare telefonate
- Il “**Glam Hacker**”. Tatuato e con piercing, si presenta ai media come hacker e fornisce l'icona distorta del fenomeno (che però soddisfa il pubblico e questo è sufficiente). Normalmente non ha alcuna reale competenza di hacking ma vuole solo apparire

Tassonomia (by Gurney Halleck)

- I “**cracker etici**”: agiscono per motivi etici in modo illegale. Distruggono in nome di una (per loro) “giusta causa”
- I **ciarlatani**: essere un hacker o un cracker può dare occasioni professionali o lustro nel gruppo. Costoro mentono sulle loro esperienze e azioni
- Le **spie** (governative/industriali)
- I **free-lance**: da assoldare
- I **creatori di virus** (che fanno molto comodo ai fornitori di antivirus)
- Gli “**ingegneri sociali**”: carpiscono informazioni usando la parte più debole dei sistemi: le persone (tecniche di **social engineering**)
- I **cyberpunk**: vogliono (tra l’altro) rompere i metodi crittografici

Cracker bravi o fortunati?

Se i cracker sono così impreparati perché riescono a bucare i sistemi?

- Gli utenti sono quasi sempre estremamente ignoranti, spesso lo sono anche gli amministratori (che è ovviamente ancor più grave)
- Sistemi proprietari (che non si sa come siano fatti) scarsamente documentati, aggiornati e protetti
- Sistemi e programmi mai o scarsamente aggiornati (la paranoia da aggiornamento continuo non è la soluzione corretta a questo problema)
- Uso di password banali: parole di senso compiuto (da dizionario) o semplici anagrammi/combinazioni di esse
- Sistemi monoutente senza protezione di memoria usati in ambiente professionale (soprattutto in passato)
- Trasmissione di dati sensibili in chiaro sulla rete (es. molti degli instant messenger, webmail ecc), soprattutto nel caso del wireless
- Fiducia nella sicurezza “plug'n play”, che ovviamente non esiste!

Riflessioni

- Negli ultimi decenni lo scenario informatico è cambiato in maniera radicale, ma molti dei problemi di sicurezza sono rimasti quasi del tutto invariati. Perché? Cosa significa?
- Qual'è il ruolo della tecnologia in questa "**insicurezza diffusa**", è una sua colpa oppure quanto necessario per costruire sistemi sicuri esiste già ma andrebbe applicato?
- Esiste una **reale esigenza di sicurezza** oppure si tratta di una percezione distorta di alcuni paranoici?
- Qual'è il reale costo della sicurezza soprattutto se confrontato al costo della violazione di un sistema? Questo costo risulta **sostenibile**?
- Dati i sistemi attuali, quasi sempre altamente insicuri, quali sono **scenari realistici** per la loro evoluzione e messa in sicurezza?

Bibliografia

- Anonymous: “**Maximum Security**” SAMS NET
- Eric Steven Raymond: “**How To Become A Hacker**”
  - http://www.tuxedo.org/~esr/faqs/hacker-howto.html
- Eric Steven Raymond: “**A Brief History of Hackerdom**”
  - http://tuxedo.org/~esr/writings/hacker-history/hacker-history.ps
- Peter Seebach: “**Hacker FAQ**”
  - http://www.plethora.net/~seebs/faqs/hacker.html
- Richard Stallman: “Free as in Freedom”
  - http://www.faifzilla.org/
- Gurney Halleck: “**A Hacker Taxonomy**”
  - http://www.blackknife.com/Papers/HackerTaxonomy.html

Ringraziamenti

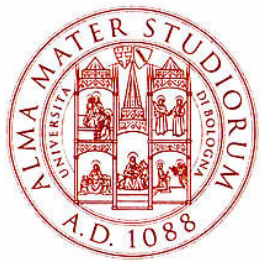
- Gran parte di questi lucidi sono direttamente tratti o “ispirati” da un lavoro precedente del Prof. Renzo Davoli e del Prof. Alberto Montresor, si ringrazia sentitamente

- In ogni caso la responsabilità di qualsiasi eventuale errore rimane integralmente dell’autore di questa lezione

Sicurezza 2006 - 2007

Lezione 2: Natura ed evoluzione del fenomeno Hacking

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