Breve introduzione alla sicurezza informatica

Gabriele D'Angelo
gdangelo@cs.unibo.it

Dipartimento di Scienze dell'Informazione
Università di Bologna

13/05/2004

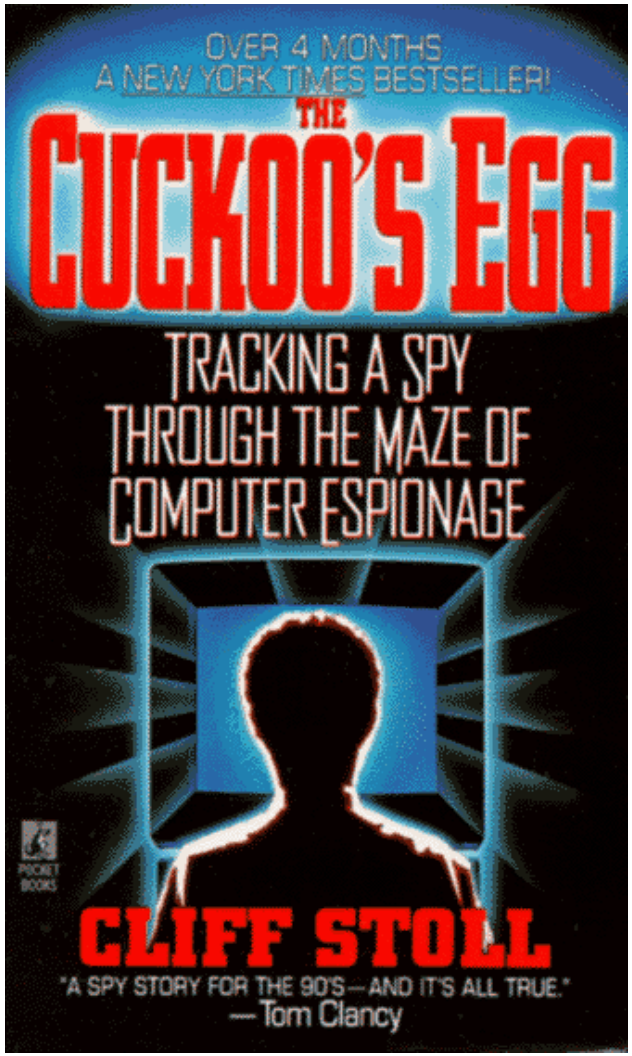
Sicurezza informatica

Che cos'è la sicurezza informatica?

- Host security
- Home network security
- Internet security

I sistemi attuali sono ragionevolmente sicuri?

Sicurezza o insicurezza?



Non c'è nulla da proteggere?

- **Cosa** vogliamo proteggere e **da cosa** vogliamo proteggerci?
- Obiettivi:
  - Data **confidentiality** vs. Exposure of data
  - Data **integrity** vs. Tampering with data
  - System **availability** vs. Denial of Service
- In alcuni casi vogliamo proteggere il nostro nome e **rispettabilità** (ad esempio non incorrere in problemi legali), non diffondere **dati sensibili** (informazioni mediche, religiose, politiche ecc.) e non vedere i nostri dati **modificati** senza autorizzazione. In altri casi vogliamo semplicemente avere il sistema **a disposizione** quando ne abbiamo bisogno!

Le parole sono importanti

Hacker vs. Cracker

- **Hacker**: "a person who enjoys **exploring the details** of programmable systems and how to stretch their capabilities, as opposed to most users, who perfer to learn the minimum necessary […]"

- **Cracker**: "One who breaks security on a system […] Most crackers are only **mediocre** hackers"

Fonte: The Jargon Dictionary [http://info.astrian.net/jargon/]

Autenticazione

La base di ogni sistema di sicurezza è solitamente centrata su autenticazione / identificazione

- Alternative di identificazione:
  - qualcosa che l'utente **conosce** (es. meccanismi basati su **password**)
  - qualcosa che l'utente **ha** (es. **oggetto fisico**)
  - qualcosa che l'utente **è** (es. meccanismi **biometrici**)
- Vantaggi e svantaggi dei vari meccanismi

Confidenzialità

Il commercio elettronico, molte interazioni su Internet e la conservazione dei dati non possono prescindere dal principio di **confidenzialità**

- Crittografia **simmetrica** (DES) ed **asimmetrica** (RSA)
- La crittografia è "per sempre" o è a "scadenza"?
- Esempio pratico: Secure Socket Layer (World Wide Web)
  - É sufficiente che l'algoritmo crittografico sia "buono" per garantire la sicurezza di una transazione?
  - Quali altri elementi entrano in gioco?

Due parole sui firewall

- Il termine firewall significa "muro di fuoco"? NO!!!
- La traduzione corretta è "**muro taglia fuoco**"
  - Un **firewall** può avere un'architettura decisamente complessa ma usualmente è composto da almeno due moduli parzialmente distinti:
    - **packet filtering** (livello rete)
    - **proxy** (livello applicazione), application gateway
  - Un firewall può essere utilizzato non solo per dividere/proteggere da Internet ma anche per ridurre in comparti la rete interna
- VPN (Virtual Private Network), estensione del concetto di rete privata

Attacchi dall'esterno e rischi vari

- **Intrusione**: cosa significa nella pratica "**bucare un server**"?
  - Prenderne il controllo
  - Nel caso di un server WWW modificare l'homepage (defacement)
  - Interrompere il servizio
  - …
- Il concetto di **vulnerabilità**
  - Il software non è perfetto, non è esente da **errori**
  - Facendo leva su alcuni errori è possibile **compromettere** un server
  - Il problema dei **buffer overflow**: molte vulnerabilità derivano da errori di progettazione o da **banali errori di programmazione**. L'errore più diffuso è un'errata **gestione della memoria e degli input** (es. dimensionamento dei buffer)

Virus e Worm

- Spesso si parla indistintamente di Virus e di Worm, con molta confusione, ma sono due concetti differenti:
  - **Virus**: parte di un programma che, mimando i virus biologici, cerca di infettare altri programmi (usualmente all'interno dello stesso host, ultimamente il termine si applica anche per le infezioni tra computer diversi collegati in rete)
  - **Worm**: programma in grado di replicarsi che, sfruttando vulnerabilità dei sistemi, cerca di diffondersi infettando vari host su Internet
- Per colpa di un worm è possibile che Internet collassi?

Il famoso “Internet Worm”

- Crash della rete? É già successo in passato!!!

- “The first worm to attract wide attention, the Morris worm, was written by Robert Tappan Morris, Jr. at the MIT Artificial intelligence Laboratory. It was released on November 2, **1988**, and quickly infected a great many computers on the Internet at the time. It propagated through a number of bugs in BSD Unix and its derivatives. Morris himself was convicted under the US Computer Crime and Abuse Act and received 3 years’ probation, community service and a fine in excess of $10.000” [www.wikipedia.org]

- Potrebbe succedere nuovamente oggi?

- Come è cambiato lo scenario Internet rispetto al 1988?

Cavalli di troia

- Non sempre le apparenze corrispondono a verità, anche in questo caso il software non fa eccezione
- Chi ci assicura che il software che compriamo o che scarichiamo gratuitamente da Internet non si comporti in maniera diversa da come ci aspettiamo?
- Software "**closed source**" -> ci fidiamo del **produttore**, del suo buon nome, della sua voglia di mantenersi "**rispettabile**"
- Software "**open source**" -> usualmente ci fidiamo della "**comunità**", teoricamente sarebbe possibile controllare tutto. Non si può escludere che siano compromessi i binari o la fonte di distribuzione

Denial of Service (DoS)

- Spesso l'obiettivo di chi attacca non è l'intrusione ma semplicemente causare un **disservizio** parziale o totale
- Esistono varie forme di Denial of Service, alcune sono realizzate sfruttando la natura distribuita della rete:

  Distributed Denial of Service (DDoS)
- Esempio: molte richieste di connessione contemporanee possono rendere irraggiungibile un sito WWW. Certi DDoS sono stati creati attraverso la diffusione mirata di worm/virus
- In alcuni casi non esiste nessun tipo di difesa attuabile

SPAM – SPiced hAM

- Dalla carne in scatola (di bassa qualità) alle e-mail di massa e indesiderate
- Parlare di Spam come attacco esterno alla sicurezza è "piuttosto ridicolo". Ma nella pratica grandi quantitativi di Spam possono **consumare risorse**, **rendere inservibile** un servizio o complicato **filtrare** i contenuti che non sono Spam
- Come si **combatte** lo Spam?
  - Buonsenso e un po' di attenzione
  - Tecnologia (filtri bayesiani, blacklist ecc.)
  - Collaborazione da parte degli Internet Service Provider
  - Nuovi protocolli per la gestione della mail?

Security by obscurity

- La **segretezza** rende un sistema **sicuro**?
- Meglio tenere **nascoste** le informazioni su un sistema oppure una loro diffusione garantisce un **migliore controllo** e una **risposta più veloce** alle vulnerabilità?
- Il caso della crittografia (principio di Kerckhoff): tutto è noto agli attaccanti ad esclusione della chiave di crittazione.

  "**The enemy knows the system**" (C. Shannon)
- Sarebbe preferibile evitare un approccio **dogmatico**: spesso la security by obscurity è inutile, in altri casi può migliorare in maniera notevole la sicurezza di un sistema

Altri strumenti per l'attacco: conoscere per evitare

- Social Engineering: molto spesso è sufficiente **chiedere per ottenere**, magari millantando di essere chi in realtà non si è. Fidarsi spesso è male (esempio: finti amministratori che chiedono password)
- Eavesdropping: guardare in giro (o fare vero e proprio sniffing) può rivelare informazioni molto delicate
- Backdoor: molti programmatori/sistemisti hanno la pessima abitudine di lasciare qualche ricordo indesiderato. Quello che sembra segreto non è sempre destinato a rimanerlo, soprattutto ad occhi interessati, esperti ed attenti (esempio: molti prodotti per il networking)

La sicurezza è un processo continuo

- Soprattutto in presenza di scenari complicati (es. ambienti di lavoro formati da molti utenti) cercare una buona sicurezza significa un processo continuo di **educazione** e **attenzione**
- La realtà mette di fronte alla scelta di un **compromesso** tra **sicurezza** e **facilità d'uso**. Un sistema troppo complicato e quindi scomodo da utilizzare spesso diventa insicuro perchè le policity concordate **non** vengono rispettate
- La sicurezza rappresenta un **costo finanziario** molto tangibile, sia quando tutto funziona correttamente, sia in presenza di incidenti

Internet: anonimi o riconoscibili?

- Collegato ad Internet, nascosto dietro un video, quindi anonimo:

  assolutamente falso

- La mole di informazioni che rilasciamo più o meno inavvertitamente sulla rete è notevole, queste potrebbero essere riutilizzate anche contro di noi per attacchi, profilazione ecc.

- Problema **privacy**: quanto sono sicuri i dati sensibili contenuti nel nostro computer?

- Gli spyware sono programmi che hanno lo scopo di carpire informazioni sul nostro comportamento e le nostre abitudini

Contromisure

- Prevenzione (sistemi **aggiornati** con attenzione)
- Informazione (**conoscere il problema** e seguirlo passo passo)
- Detection: molto spesso non ci si accorge delle intrusioni. Chi si vanta di non aver mai subito un'intrusione probabilmente non si è mai accorto dell'intrusione
- In alcuni casi la reazione è molto complicata. Ad esempio come si può reagire ad uno **zero-day exploit** (un exploit che si basa su una vulnerabilità appena scoperta/annunciata)?

Frequently Asked Questions (FAQ)

Domande banali passate per la testa più o meno a tutti:

- Qual'è il sistema operativo più sicuro?
- Qual'è il firewall più sicuro? Il mio firewall è "buono"?
- Se non apro le mail posso lo stesso prendere un virus?
- É meglio avere un IP statico o dinamico per la sicurezza?
- Ho appena installato il firewall e vedo centinaia di attacchi, cosa devo fare?
- Per Linux non ci sono virus (diffusi) perchè lo usano in pochi?
- La sicurezza non mi interessa, è così noiosa, perchè devo preoccuparmi?
- …. ???

Bibliografia

- Wikipedia — http://www.wikipedia.org
- SecurityFocus — http://www.securityfocus.com
- BugTraq — **mailing list**
- A tour of the worm — http://world.std.com/~franl/worm.html
- Slashdot — http://www.slashdot.org

- **A. S. Tanenbaum. Modern Operating Systems.**
- **E. Zwicky, S. Cooper, D.B. Chapman. Building Internet Firewalls.**
- **S. Garfinkel. G. Spafford. Practical UNIX and Internet Security**