Galdus CFP

Bryan Garcia Martinez Adonay

Classe 3B info

Tesi Tecnica

Sicurezza e attacchi informatici

**Capitolo 1**

La Sicurezza Informatica

(Generale, passiva e attiva)

**Sicurezza Generale**

La sicurezza informatica è un problema sempre più sentito in ambito tecnico-informatico per via della crescente informatizzazione della società e dei servizi (pubblici e privati) in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o hacker.L’interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività. Molti ex-[hacker](http://it.wikipedia.org/wiki/Hacker)/[cracker](http://it.wikipedia.org/wiki/Cracker) sono oggi dirigenti di società di sicurezza informatica o responsabili di questa in grandi multinazionali. Ciò sembra mostrare che per capire le strategie migliori di sicurezza informatica è necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolare le mosse.Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: resistenza del [software](http://it.wikipedia.org/wiki/Software) di base e applicativo, [affidabilità](http://it.wikipedia.org/wiki/Affidabilit%C3%A0) delle apparecchiature e degli ambienti in cui essi sono collocati.Il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia da eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo i [server](http://it.wikipedia.org/wiki/Server) in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica" è sempre il caso di far notare come spesso il fatto di adottare le tecniche più sofisticate generi un falso senso di sicurezza che può portare a trascurare quelle semplici.Il secondo livello è normalmente quello logico che prevede l'[autenticazione](http://it.wikipedia.org/wiki/Autenticazione) e l'[autorizzazione](http://it.wikipedia.org/wiki/Autorizzazione_(informatica)) di un'entità che rappresenta l'utente nel sistema. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate in [file](http://it.wikipedia.org/wiki/File) di [log](http://it.wikipedia.org/wiki/Log). Questo processo di monitoraggio delle attività è detto [audit](http://it.wikipedia.org/wiki/Audit_(informatica)) o [accountability](http://it.wikipedia.org/wiki/Accountability).

Per evitare invece gli eventi accidentali, non esistono soluzioni generali, ma di solito è buon senso dell’utente fare una copia di [backup](http://it.wikipedia.org/wiki/Backup) del sistema, fare backup periodico di dati e applicazioni, com'è tipico delle procedure di [disaster recovery](http://it.wikipedia.org/wiki/Disaster_recovery), in modo da poter fronteggiare qualsiasi danno imprevisto.

**Sicurezza passiva**

Per sicurezza passiva normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

**Sicurezza attiva**

Per sicurezza attiva si intendono, invece, tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi ([confidenzialità](http://it.wikipedia.org/wiki/Confidenzialit%C3%A0)), sia dalla possibilità che un utente non autorizzato possa modificarli ([integrità](http://it.wikipedia.org/wiki/Integrit%C3%A0_dei_dati)). È evidente che la sicurezza passiva e quella attiva siano tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema. Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, realizzando più barriere fra l'attaccante e l'obiettivo. Spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, quanto piuttosto dai dati in essi contenuti, quindi la sicurezza informatica deve preoccuparsi di impedire l'accesso ad utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a certe operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati. Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di [identità digitale](http://it.wikipedia.org/wiki/Identit%C3%A0_digitale) o di [file](http://it.wikipedia.org/wiki/File) riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc. La sicurezza informatica si occupa anche di prevenire eventuali situazioni di [Denial of service](http://it.wikipedia.org/wiki/Denial_of_service) (DoS). I DoS sono attacchi sferrati al sistema con l'obiettivo di renderne inutilizzabili alcune risorse in modo da danneggiare gli utenti del sistema. Per prevenire le violazioni si utilizzano strumenti [hardware](http://it.wikipedia.org/wiki/Hardware) e [software](http://it.wikipedia.org/wiki/Software).

**Capitolo 2**

Sicurezza dei programmi &

Programmi virus

Il problema della [sicurezza dei programmi](http://it.wikipedia.org/wiki/Sicurezza_dei_programmi) e soprattutto dell'invio e ricezione di dati confidenziali protetti, si è posto all'attenzione degli sviluppatori di [software](http://it.wikipedia.org/wiki/Software) come conseguenza della sensibile crescita dell'uso degli strumenti informatici e di [internet](http://it.wikipedia.org/wiki/Internet). Per quanto riguarda la produzione di software "protetti" possiamo partire col definire il concetto disicurezza come l'assenza da condizioni conflittuali capaci di produrre danni mortali o irreparabili ad un sistema. Nella progettazione di [software](http://it.wikipedia.org/wiki/Software) è quindi fondamentale raggiungere il compromesso più funzionale tra l'efficienza d'uso del [programma](http://it.wikipedia.org/wiki/Programma_(informatica)) in questione e la sua capacità di "sopravvivenza" ad attacchi esterni e ad errori più o meno critici. Il livello base della sicurezza dei programmi è fornito dalla [sicurezza del sistema operativo](http://it.wikipedia.org/wiki/Sicurezza_dei_sistemi_operativi) su cui si appoggiano i programmi applicativi.

**Caratteristiche di sicurezza**

Due caratteristiche fondamentali esplicano il concetto di sicurezza:

* **Safety** (sicurezza): una serie di accorgimenti atti ad eliminare la produzione di danni irreparabili all'interno del [sistema](http://it.wikipedia.org/wiki/Sistema);
* **Reliability**(affidabilità): prevenzione da eventi che possono produrre danni di qualsiasi gravità al [sistema](http://it.wikipedia.org/wiki/Sistema).

Un [software](http://it.wikipedia.org/wiki/Software) (o [programma](http://it.wikipedia.org/wiki/Programma_(informatica))) è tanto più sicuro quanto minori sono le probabilità che si verifichi un guasto e la gravità del danno conseguente al guasto stesso. Possiamo ora vedere, in ordine crescente, i possibili effetti dei guasti in cui può incorrere un [software](http://it.wikipedia.org/wiki/Software):

* Nessun effetto
* Rischio trascurabile
* Rischio significativo
* Rischio elevato
* Rischio catastrofico.

**Controllo della sicurezza di un programma**

Una volta prodotto il [software](http://it.wikipedia.org/wiki/Software) si procede alla verifica del suo comportamento, in modo tale da effettuare una ricerca estesa dei difetti presenti, per passare poi alla loro eventuale eliminazione. Esistono diversi modelli di sicurezza per il controllo dei programmi basati su due metodi differenti:

-**Semantic-based** security model (modelli di sicurezza basati sulla semantica): la sicurezza del [programma](http://it.wikipedia.org/wiki/Programma_(informatica)) controllato viene esaminata in termini di comportamento del programma

-**Security-typed language** (modelli di sicurezza basati sul linguaggio): i tipi delle variabili sono seguiti dall'esplicazione delle politiche adottate per l'uso dei dati battuti.

Per essere efficace un [programma](http://it.wikipedia.org/wiki/Programma_(informatica)) deve essere controllato nelle sue specifiche e deve essere privo di difetti nel codice, a questo fine viene effettuato un controllo delle specifiche del programma e delle prestazioni correlate all'affidabilità, in secondo luogo viene analizzata ogni parte di [codice](http://it.wikipedia.org/wiki/Codice_sorgente) e funzione del [sistema](http://it.wikipedia.org/wiki/Sistema).

**Errori di programma**

L'[IEEE](http://it.wikipedia.org/wiki/IEEE) (Institute of Electrical and Electronics Engineers) ha catalogato gli errori nel software in tre diverse voci a seconda della natura degli errori stessi. Esse sono:

 -**Error**: è un errore umano verificatosi durante il processo di interpretazione delle specifiche oppure durante l'uso di un metodo o nel tentativo di risoluzione di un problema

-F**ailure**: è un comportamento del software imprevisto ed incongruo rispetto alle specifiche del [programma](http://it.wikipedia.org/wiki/Programma_(informatica)) stesso

-**Fault**: è un difetto del codice sorgente.

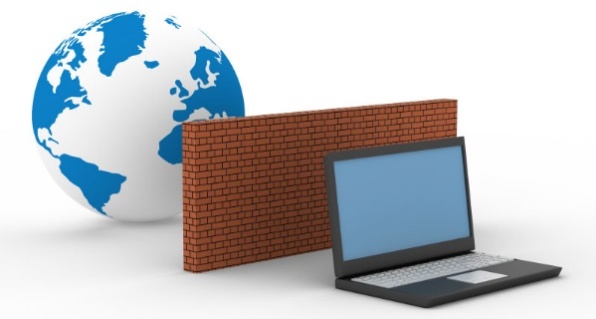
Gli errori di [programma](http://it.wikipedia.org/wiki/Programma_(informatica)) non nocivi, come ad esempio gli [spyware](http://it.wikipedia.org/wiki/Spyware) ed il [buffer overflow](http://it.wikipedia.org/wiki/Buffer_overflow) hanno la caratteristica di non modificare i [file](http://it.wikipedia.org/wiki/File) di [sistema](http://it.wikipedia.org/wiki/Sistema) e non recare danno alle caratteristiche del sistema stesso. Troviamo qui sotto elencati una serie di errori e di attacchi al software di differente entità.

**Principali tecniche di attacco**

* [Exploit](http://it.wikipedia.org/wiki/Exploit)
* [Buffer overflow](http://it.wikipedia.org/wiki/Buffer_overflow)
* [Shellcode](http://it.wikipedia.org/wiki/Shellcode)
* [Cracking](http://it.wikipedia.org/wiki/Cracking_(informatica))
* [Backdoor](http://it.wikipedia.org/wiki/Backdoor)
* [Port scanning](http://it.wikipedia.org/wiki/Port_scanning)
* [Sniffing](http://it.wikipedia.org/wiki/Sniffing)
* [Keylogging](http://it.wikipedia.org/wiki/Keylogger)
* [Spoofing](http://it.wikipedia.org/wiki/Spoofing)
* [Trojan](http://it.wikipedia.org/wiki/Trojan)

**Capitolo 3**

Principali tecniche di difesa

* [Antivirus](http://it.wikipedia.org/wiki/Antivirus): consente di proteggere il proprio personal computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l’utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti floppy), per verificare la presenza di virus, worm. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall’antivirus correttamente configurato a tale scopo.
* [Antispyware](http://it.wikipedia.org/wiki/Antispyware): software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato un utilissimo tool per la rimozione di “file spia”, gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell’utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
* [Firewall](http://it.wikipedia.org/wiki/Firewall): installato e ben configurato un firewall garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall’esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell’utente.
* [Backup](http://it.wikipedia.org/wiki/Backup" \o "Backup): più che un sistema di difesa si tratta di un utile sistema per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell’esecuzione di una copia di sicurezza dei dati di un personal computer o comunque di dati considerati importanti onde evitare che vadano perduti o diventino illeggibili.
* [Honeypot](http://it.wikipedia.org/wiki/Honeypot): un honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici. Solitamente consiste in un computer o un sito che sembra essere parte della rete e contenere informazioni preziose, ma che in realtà è ben isolato e non ha contenuti sensibili o critici; potrebbe anche essere un file, un record, o un indirizzo IP non utilizzato.
* [Network Intrusion Detection System](http://it.wikipedia.org/wiki/Network_Intrusion_Detection_System) (NIDS): sono degli strumenti informatici, software o hardware, dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche. I più comuni NIDS sono composti da una o più sonde dislocate sulla rete, che 
* comunicano con un server centralizzato, che in genere si appoggia ad un Database. Fra le attività anomale che possono presentarsi e venire rilevate da un NIDS vi sono: accessi non autorizzati, propagazione di software malevolo, acquisizione abusiva di privilegi appartenenti a soggetti autorizzati, intercettazione del traffico (sniffing), negazioni di servizio (DoS).
* [Sistema di autenticazione](http://it.wikipedia.org/wiki/Sistema_di_autenticazione): potrebbe rivelarsi utile, in particolare nelle aziende, l’utilizzo di software per l’autenticazione sicura con un secondo elemento di autenticazione basato su un insieme di caratteri disposti in uno schema suddiviso in file e colonne conosciute dall’utente che dovrà poi inserirle in una combinazione di valori per dimostrare di essere in possesso dei dati corretti. Altro sistema, più sofisticato, è quello del riconoscimento dell’utente tramite l’utilizzo dell’impronta digitale come forma di autenticazione.

**Capitolo 4**

Hacking e le sue tipologie

Il termine Hacking nel gergo informatico è spesso connotato da un'accezione negativa, in quanto nell'immaginario collettivo identifica una tipologia di operazioni e comportamenti del tutto illegali. Tuttavia l'Hacking comprende in realtà una serie di attività perfettamente lecite, svolte anche a livello professionale: i sistemi informatici vengono infatti sottoposti a specifici e costanti test al fine di valutarne e comprovarne la sicurezza e l'affidabilità (i risultati di questi test non possono comunque provare l'assoluta robustezza del sistema, ma soltanto il fatto che in un ristretto periodo di tempo chi ci ha lavorato non è riuscito a scoprire alcuna vulnerabilità). Altre attività di Hacking sono poi svolte di routine da chi si occupa dell'amministrazione di sistemi informatici, nonché da chi ne cura lo studio e lo sviluppo.

In ogni caso, l'opinione pubblica spesso associa al termine Hacking la pratica di accedere illegalmente a sistemi altrui, allo scopo di carpire dati riservati o danneggiarne il funzionamento: tale pratica è più propriamente denominata [cracking](http://it.wikipedia.org/wiki/Cracking_(informatica)) (che si può tradurre in questo contesto come intaccare con l'obiettivo di rompere, distruggere), sebbene utilizzi metodi e tecniche hacker.

#### **Incremento di prestazioni (hardware)**

I circuiti fisici di un computer funzionano secondo le leggi dell'[elettronica](http://it.wikipedia.org/wiki/Elettronica): è possibile alterarne il funzionamento al fine di ottenere un incremento delle prestazioni. Nella pratica vengono apportati miglioramenti che, non essendo stati ancora sperimentati dal produttore, non possono essere inclusi nel prodotto al momento della vendita.

In passato è stato possibile imporre a [masterizzatori](http://it.wikipedia.org/wiki/Masterizzatore) di [CD](http://it.wikipedia.org/wiki/Compact_disc" \o "Compact disc) di lavorare al doppio della velocità, semplicemente rimuovendo un [resistore](http://it.wikipedia.org/wiki/Resistore). Esempi più frequenti riguardano alcune schede di [personal computer](http://it.wikipedia.org/wiki/Personal_computer) sulle quali, tramite la modifica di connettori detti jumper, si potevano alterare i parametri di [frequenza](http://it.wikipedia.org/wiki/Frequenza) del [processore](http://it.wikipedia.org/wiki/CPU) installato, facendo sì che questo lavorasse a maggiori prestazioni: tale pratica viene chiamata [overclocking](http://it.wikipedia.org/wiki/Overclocking) (i jumper sono stati sostituiti, nelle moderne schede madri, da apposite funzioni software del[BIOS](http://it.wikipedia.org/wiki/BIOS)). L'incremento di prestazioni può tuttavia comportare un surriscaldamento eccessivo delle componenti.

#### **Rimozione di limitazioni al funzionamento**

I produttori di componenti elettronici (l'[hardware](http://it.wikipedia.org/wiki/Hardware)) o di applicazioni (il [software](http://it.wikipedia.org/wiki/Software)) possono aggiungere ai loro prodotti funzioni, non necessariamente documentate in fase di vendita, che limitano l'utilizzo dei prodotti stessi in specifiche situazioni: ad esempio, possono essere inseriti meccanismi atti a impedire l'aggiunta al sistema di componenti non certificati, oppure atti a controllare l'originalità dei programmi utilizzati. L'elusione di tali limitazioni rientra nelle attività di Hacking: in taluni casi è assolutamente legale (nel caso, ad esempio, in cui si richiedano permessi di amministrazione per accedere a tutte le funzionalità del sistema operativo mobile [Android](http://it.wikipedia.org/wiki/Android" \o "Android)), in altri casi viene svolta in maniera illecita per aggirare l'acquisto delle licenze ([pirateria informatica](http://it.wikipedia.org/wiki/Pirateria_informatica)).

#### **Alterazione della struttura di un programma**

Un [sistema operativo](http://it.wikipedia.org/wiki/Sistema_operativo) o, in generale, un qualsiasi software, si basa su una strutturata sequenza di operazioni da far compiere all'elaboratore elettronico su cui viene installato; nel caso dei programmi [open source](http://it.wikipedia.org/wiki/Open_source) questa sequenza di operazioni è volutamente resa nota e in vari casi è anche alterabile liberamente, ma nel software cosiddetto protetto oproprietario non viene autorizzata nessuna possibilità di intervento, nemmeno al fine di correggere malfunzionamenti. Nella pratica è però possibile modificare il software portandolo ad eseguire le operazioni in una sequenza diversa da quella scelta dal produttore fino ad ottenere il "salto" (cioè la mancata esecuzione) di alcune operazioni; programmi specificatamente realizzati per alterare la struttura di un software provocando il salto delle operazioni che dovrebbero verificare l'originalità della [licenza](http://it.wikipedia.org/wiki/Licenza_(informatica)) di un'[applicazione](http://it.wikipedia.org/wiki/Applicazione_(informatica)) vengono ad esempio chiamati [crack](http://it.wikipedia.org/wiki/Cracking_(informatica)).

#### **Aggiunta di funzioni ad un programma**

Come ad un software possono essere tolte delle funzioni, così possono esserne aggiunte di nuove; anche in questo caso sul software protetto o proprietario tale operazione non è consentita, ma nella pratica questa operazione è possibile. Un esempio può essere l'aggiunta della funzione di "ballo jazz" ad un cane [robot](http://it.wikipedia.org/wiki/Robot) distribuito da una nota casa produttrice di materiali ludici, che può essere eseguito tramite inserimento di nuove parti al programma di controllo delle funzioni di questo [giocattolo](http://it.wikipedia.org/wiki/Giocattolo).

**Capitolo 5**

Heartbleed

  
Heartbleed (cuore che sanguina in inglese) non è un "virus da computer": è un **vulnerabilità informatica.** In pratica, una falla in una componente chiave dei sistemi che garantiscono la sicurezza delle comunicazioni su Internet.   
Quindi, non siamo protetti per il semplice fatto di avere l'antivirus installato.  
**Quando si è diffuso e quando è stato comunicato**   
La falla esiste dal **dicembre2011**. È stata scoperta e comunicata lunedì 7 aprile da **NeelMetha**, ingegnere di Google, che ha creato una pagina web con tanto di logo "carino". È la prima volta che si comunica una criticità così grave.

**Che cosa fa Heartbleed**  
Colpisce una funzionalità di **OpenSSL**, un tipo di sistema di cifratura (SSL) delle comunicazioni online usato, si stima, da **due terzi dei server**del pianeta.   
Semplificando all’osso, OpenSSL si preoccupa di codificare quello che “esce” da un computer e viaggia nella rete per raggiungere un altro computer (il nostro o un server): qui, OpenSSL esegue il processo inverso e ci permette di leggere i dati. È un processo che, di solito, noi non percepiamo. Succede, per esempio, ogni volta che vediamo un lucchetto in alto a sinistra nella barra degli indirizzi del browser: significa che un SSL è abilitato.

**Chi ha colpito**  
Tutti i server che utilizzano OpenSSL, a patto che abbiano il tool "heartbeat installato e funzionante. Si stima siano i due terzi del totale.

Tra questi ci sono **Google,Facebook, Dropbox** e **Yahoo.**   
Non sono invece affetti (perché non usano il sistema Open SSL)**Microsoft, Amazon, Linkedin**e**PayPal.**   
**Apple**e**Twitter** non dichiarano quale SSL usano, quindi non è dato sapere se sono affetti o no.   
Non sono a rischio neppure i siti di home banking, protetti solitamente da protocolli proprietari.   
**Che cosa dobbiamo fare noi per essere protetti**  
Un solo consiglio: è meglio **cambiare le password**di Google, Facebook e Yahoo, dato che hanno dichiarato di aver corretto la falla. Nel dubbio, è preferibile cambiare anche quelle di Twitter e Apple.   
La mail, in particolare, va sempre **protetta al massimo**: dalla nostra mail si possono ottenere le password per quasi tutte le altre applicazioni, dalla banca ai dati più sensibili. «Cambiare le password è una operazione sempre consigliabile, che andrebbe fatta comunque di tanto in tanto» spiega Antonio Forzieri.   
Va fatto, però, nel **modo giusto**. «Evitando i comportamenti critici: non bisogna scriversi la password da qualche parte, non usare date di nascita o squadre di calcio ed evitare di usare la stessa per tutte le applicazioni» dice Forzieri.   
Attenzione, però: «Nel caso specifico di Heartbleed, prima di cambiarla è bene **chiedere all’operatore se la falla di OpenSSL è stata corretta**: altrimenti il cambiamento è inutile».