SICSI

VIII CICLO

EVOLUZIONE DEI MECCANISMI PER LA SICUREZZA DEI SISTEMI INFORMATICI

Corso di:
Storia dell'informatica e
del calcolo automatico

Esposito Vincenzo

Sommario

Introduzione

- Primi Anni 60 , nasce il problema della sicurezza dei sistemi di calcolo e fanno la loro apparizione meccanismi appositi per garantire la sicurezza informatica degli stessi.
- Vengono riportati i primi casi di frode informatica e per la prima volta, sulle riviste specializzate si possono leggere i primi contributi scientifici che definiscono il problema della sicurezza informatica ed individuano possibili soluzioni.

Hacker/Prima generazione /1

- Perché il problema della sicurezza informatica risale ai primi anni 60 ?
- Perché proprio in quegli anni nasce:
  LA PRIMA GENEARZIONE DI HACKER definiti come EROI DELLA RIVOLUZIONE INFORMATICA:
- Ne facevano parte:

1. **Peter Samson**
2. **Alan KotoK**
3. **Marvin Minsky**
4. **Richard Greenblatt**

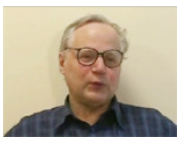
…ed altri

Figura 1

Peter Samson

Marvin Minsky

Ala kotok



Richard Greenblatt

Hacker/Prima generazione /2

- PETER SAMSON /1

Figura 2
Peter Samson

Fu uno dei primi a mutare la personalità del computer Ibm 704 situato nella stanza EAM (Electronic Account machinery) nel seminterrato del palazzo 26 uno degli edificio più recenti del MIT (Massachussetts institute of technology).
Egli si accorse che tale stanza non era sorvegliata di notte e con un gruppo di suoi amici sfruttando anche la presenza di uno strumento per perforare schede chiamato 407 , creò schede perforate che una volta inserite nella macchina gli avrebbe fatto fare di tutto….

Hacker/Prima generazione /3

- Fu un passo casuale e spensierato ma tipico del modo in cui una sottocultura nasce e diventa un fenomeno underground di rilievo per trasformarsi in una cultura che sempre sarebbe stata l'ánima maleducata e non autorizzata del mondo del computer.

Era una delle primissime incursioni degli Hacker……..

Figura 3
IBM 704
Situato al primo piano del palazzo 26, e' stato il primo computer violato dagli hacker.

Sistemi Multiutente e Primi Meccanismi di Sicurezza

- Ancora agli inizi degli anni '60...
- Con l'introduzione dei "Sistemi Multiutente", arrivano i primi meccanismi che migliorano la sicurezza di un calcolatore.
- L'obiettivo di tali meccanismi era riconducibile allo svolgimento di due funzionalità:

1. Consentire l'accesso ad un calcolatore ai soli utenti autorizzati detti "Meccanismi di sicurezza"
2. Evitare che utenti autorizzati utilizzassero risorse ad essi non assegnate detti "Meccanismi di protezione"

Meccanismi di protezione/1

- Molta enfasi fu data ai Meccanismi di protezione realizzati sulla base di due assunzioni ben precise:

1. Proteggere fisicamente il sistema
2. Ogni entità attiva presente nel sistema veniva preventivamente riconosciuta ed identificata.

- La realizzazione di tali presupposti è stata facile poiché in quel periodo l'informatica si sviluppava con l'uso di grossi calcolatori centrali noti come "mainframe" situati in locali ben protetti ed accessibili solo a poco personale e facilmente identificabili.

- Quindi la prima assunzione la si otteneva imponendo rigide procedure per l'accesso ai locali in cui era situato il calcolatore.

Meccanismi di protezione/2

- Il secondo, cioè l'autenticazione di un utente venne ottenuto con l'introduzione del noto meccanismo di sicurezza: le password. Tale meccanismo opera in questo modo:
  - Ad ogni utente autorizzato ad accedere al calcolatore viene comunicata una parola di accesso che l'utente deve impegnarsi a mantenere segreta.
  - Quando un utente intende usare un calcolatore gli viene chiesto di digitare il suo nome e la parola segreta associata al suo nome.
  - Se la parola digitata è uguale a quella memorizzata nel calcolatore l'utente può usare il calcolatore. In caso contrario gli viene negato l'accesso.

Meccanismi di protezione/3

- Inefficienza delle Password:
  - Le password non venivano però considerate un meccanismo sufficientemente affidabile in ambienti in cui la confidenzialità delle informazioni giocava un ruolo determinante quali gli apparati militari o sistemi bancari.
  - Come si legge nell'introduzione dell'Orange Book* [cfr. 6], già a partire dal 1968 il Ministero della Difesa Americana si poneva il problema della sicurezza delle informazioni sensibili memorizzate su computer che consentivano accessi remoti a più utenti ed istituiva commissioni per l'individuazione di nuovi meccanismi e metodologie.
  - Il problema resta relegato a tali ambiti sino agli anni '80.

*L'orange Book, ovvero i Trusted Computer Systems Evaluation Criteria, è una raccolta di criteri di valutazione della sicurezza informatica principalmente orientata alla valutazione dei sistemi operativi multiutente (così chiamato in relazione al colore della copertina del volume che lo contiene).

Definizione di Sistema di Calcolo Sicuro/1

- Infatti solo alla fine degli anni '80 si arriva ad una definizione universalmente accettata di sistema di calcolo sicuro.

Tale definizione è riportata nel manuale ITSEC* [cfr. 4] e può essere così sintetizzata:

> **"Un sistema di calcolo viene considerato sicuro quando è in grado di garantire il soddisfacimento delle proprietà di confidenzialità, integrità e disponibilità".**

* ITSEC è l'acronimo di Information Technology Security Evaluation Criteria (Criteri per la valutazione della sicurezza della tecnologica informatica)

Definizione di Sistema di Calcolo Sicuro/2

- In altre parole il sistema è in grado di garantire che:
  - ogni utente può accedere esclusivamente alle informazioni di sua competenza (confidenzialità)
  - ogni utente può modificare solo informazioni di sua competenza (integrità)
  - ogni azione intrapresa da persone non autorizzate che miri ad impossessarsi di una qualunque risorsa del sistema, sia preventivamente bloccata.
- La nozione di sistema sicuro è strettamente correlata a quello di privacy, un sistema che voglia garantire la riservatezza dei dati in esso contenuti deve, essere sicuro.

Dai MainFrame alle Reti/1

- Sempre negli Anni 80, a seguito di un forte calo dei costi di produzione dell'hardware e della diffusione delle prime tecnologie di interconnessione, inizia per l'informatica una fase di trasformazione ...
  - Smembramento dei grandi centri di calcolo,
  - sostituzione dei "mainframe" con le "reti di calcolatori".
- Questo fa si che la realizzazione di una rete vista come un unico calcolatore diventa quindi il nuovo paradigma di calcolo.
- La diffusione di Internet contribuisce a rafforzare tale paradigma.

Dai MainFrame alle Reti/2

- Questo trasformazione rende non più affidabili le misure di sicurezza fin ora adottate infatti,
  - le password non erano più in grado di garantire la corretta autenticazione di un utente in rete
  - vengono meno i presupposti che garantivano la sicurezza fisica del sistema
- Risulta estremamente difficile garantire la sicurezza fisica di tutti i calcolatori di una rete che sono dislocati in siti geograficamente dispersi.
- E' altrettanto difficile controllare con precisione chi tenta di accedere a questi computer.

Caso Robert Moriss/1

- La prova di queste constatazioni si ebbe il 2 Novembre 1988 quando uno studente dell'Università di Cornell , Robert Morris attraverso un programma da lui scritto riuscì a guadagnare l'accesso ad alcune migliaia di calcolatori operanti in Internet . L'attacco noto come Internet Worm, mise fuori uso calcolatori appartenenti a università, laboratori di Ricerca, enti Governativi e industrie.

Figura 4
Figlio di un agente dell'NSA, ha scritto il primo worm della storia, mettendo ko un 25% dell'allora internet.

Caso Robert Moriss/2

- ...Morris sfrutto due elementi per sferrare il suo attacco...
  1. L'assoluta inaffidabilità del meccanismo della password per lo svolgimento della procedura di autenticazione,
  2. la presenza di errori (bug) nei programmi utilizzati dal calcolatore per il suo funzionamento.
- Tali errori in alcuni casi consentono di bypassare il meccanismo di autenticazione e guadagnare comunque l'accesso al sistema.

Misure Organizzative

- A partire dal 1988 si moltiplicano da una parte gli attacchi ai sistemi informatici e dall'altra le iniziative di ricerca per individuare le misure di sicurezza necessarie per rendere un sistema sicuro: il problema sicurezza informatica va affrontato su due fronti:

  1. Manageriale organizzativo
  2. tecnologico

- Un requisito fondamentale per la sicurezza è la definizione e la stesura di una "politica di sicurezza".
- Sul punto di vista tecnologico vanno individuati i mezzi più appropriati da utilizzare per la difesa del sistema.

M. O. – Il Ruolo della Tecnologia/1

- Intorno al 1988 si diffondono una serie di prodotti di supporto ai system manager che contribuiscono ad aumentare il livello di sicurezza.

  Tali strumenti, realizzati come freeware, consentono la gestione delle password utenti, il logging, la configurazione di sistema, il controllo degli accessi ecc.

- Di seguito si esporrà l'evoluzione degli elementi più caratteristici di un moderno sistema di sicurezza.

M. O. - Dalle pw ai certificati digitali/1

- Per far fronte all'inefficienza delle password sono stati individuati dei meccanismi di autenticazione basati principalmente sull'utilizzo di dispositivi quali smart card o calcolatori tascabili che sono in grado di generare una password che identifica correttamente l'utente.

- I più noti sono:
- One time password
- Certificati digitali.

M. O. - Dalle pw ai certificati digitali/3

- One time password...
- Il meccanismo delle one-time password

Figura 5
Token crittografico

è basato sull'uso di password che possono essere utilizzate una sola volta (usa e getta) e generate ad esempio mediante token

Le one-time password consentono di debellare i problemi derivanti dall'uso di "sniffer"

Cosa è lo Sniffing???

- Sniffing: l'attività di monitorare i pacchetti di rete che arrivano al proprio computer
- Password sniffing: si esaminano i pacchetti in cerca di coppie user - password
- Per ottenere le password dobbiamo sniffare i pacchetti...

M. O. – Dalle pw ai certificati digitali/4

- Certificati Digitali…
- Questo meccanismo è stato realizzato sulla scorta dei risultati della crittografia a chiave asimmetrica [cfr. 5].

  In tale ambito ogni utente viene fornito di almeno una coppia di chiavi (pubblica e privata) che lo identificano.

  La chiave pubblica viene inserita in un certificato digitale, emesso da un ente preposto denominato Certificatore, che ne attesta inequivocabilmente l'appartenenza all'utente stesso.

  La chiave privata viene invece custodita segretamente dall'utente.
- La particolarità di tale coppia di chiavi è che ogni messaggio cifrato con la chiave pubblica può essere correttamente decifrato solo con la corrispondente chiave privata.

M. O. – Dalle pw ai certificati digitali/5

- Per verificare l'identità di un utente gli viene dato un numero scelto a caso e cifrato con la chiave pubblica che trova sul certificato associato all'utente.
- Se l'utente contattato sarà in grado decifrare il contenuto del messaggio significa che possiede la relativa chiave segreta e quindi è esattamente chi dichiara di essere.
- Tale meccanismo è utilizzato per realizzare la "firma digitale" di documenti.
- Questo sarà il meccanismo di autenticazione che sostituirà le password per evitare ogni coinvolgimento dell'utente nella fase di autenticazione.

M. O. - Dalla crittografia alle PKI /1

- Agli inizi degli anni '90, Phil Zimmermann sviluppava un prodotto noto come PGP acronimo di Pretty Good Privacy [cfr. 7]. PGP era basato sui principi della "crittografia a chiave pubblica " e consentiva a tutti gli utenti di cifrare il contenuto dei messaggi che inviavano in rete, al fine di renderne comprensibile il contenuto al solo destinatario. In breve tempo PGP divenne uno standard per la salvaguardia della privacy personale.

Figura 6
Phil Zimmermann

M. O. - Dalla crittografia alle PKI /2

- Lo sviluppo di nuove applicazioni quali l'home banking e il commercio elettronico impongono, la realizzazione di quelle che vengono definite PKI (Public Key Infrastructure).
- PKI consentono di utilizzare una serie di funzionalità permesse dalla crittografia a chiave pubblica quali la firma digitale, il non ripudio dei messaggi, l'autenticazione, la confidenzialità e l'integrità.
- I principali compiti istituzionali di una PKI sono:

1. L'emissione dei certificati digitali,
2. la gestione di un archivio costantemente in rete che contiene tutti i certificati emessi
3. la revoca dei certificati
4. la gestione di un archivio dei certificati revocati.

M. O. – Dalla crittografia alle PKI /3

- Il PKI risolve in modo definito i problemi legati alla confidenzialità delle informazioni memorizzate nei sistemi.

  Ma ciò non basta a caratterizzare un sistema sicuro.

  Vanno infatti rese le necessarie misure affinché il sistema goda anche delle proprietà di integrità e disponibilità.

  Le quali sono le più difficile da garantire e attualmente per esse non si conoscono sinora soluzioni definitive…

M. O. – Dai Firewall agli Intrusion Detection System /1

- Uno dei primi problemi affrontati per la realizzazione di sistemi più sicuri fu l'individuazione di strumenti per la protezione di una rete "aziendale" connessa ad Internet da intrusori esterni.

  Era necessario che la rete "aziendale" avesse un unico punto di accesso da e verso internet sul quale veniva installato un dispositivo, per analizzare tutti i messaggi che transitavano in tale punto e bloccare tutti quelli che non rispettavano certi requisiti, cioè effettuare il packet filtering (Filtraggio di pacchetti).

  Tali dispositivi vennero denominati Firewall e fecero la loro comparsa nella loro versione più semplice (indicata con il termine tecnico di screening router) intorno al 1990

M. O. - Dai Firewall agli Intrusion Detection System /2

- Dal 1990 a oggi i firewall si sono notevolmente evoluti [cfr. 1] per consentire un controllo sempre più dettagliato sul traffico e quindi effettuare distinzioni sempre più sofisticate tra traffico ammesso e traffico bloccato e migliorare le proprie prestazioni.
- Ai firewall è stata poi data la possibilità di verificare la presenza di virus o più in generale di codice dannoso.
- L'idea su cui si basano i firewall è quella di controllare tutto il traffico in ingresso ad una rete mediante un'analisi sintattica, cioè la presenza o meno in un pacchetto di certe sequenze di bit predefinite.

M. O. - Dai Firewall agli Intrusion Detection System /3

- L'ultimo ritrovato in termini di misure per la sicurezza sono gli "Intrusion Detection System", prodotti essenzialmente software, che analizzano il traffico di rete che entra in un host ed individuano attraverso un'analisi semantica, eventuali attacchi in corso, e provvedono a segnalare tempestivamente l'evento.
- La loro applicabilità è limitata, in particolare possono solo rilevare intrusioni note al momento del loro rilascio, nulla possono fare contro tecniche di intrusione introdotte successivamente

M. O. - Antivirus /1

- I computer virus, sono programmi scritti per causare un danneggiamento a un computer o a una rete di computer.
- Un computer virus effettua due funzioni di base:

  1. Infetta altri computer
  2. Svolge all'interno del sistema le azioni per cui è programmato

- Queste azioni provocano la modifica e/o la cancellazione di alcuni file presenti sull'hd, l'alterazione del contenuto del video o delle impostazioni hardware della tastiera.
  Alcuni esempi di computer virus sono: trojan horses, worm e bombe logiche...

M. O. - Antivirus /2

- A partire dagli anni '60 furono sviluppate tecniche per la creazione di programmi in grado di replicarsi. Nel 1981, si assiste alla prima diffusione di un software rispondente alle caratteristiche di un virus.

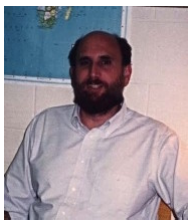


Figura 6
Frederick Cohen

Il programma in questione, "Elk Cloner", infettava il settore di boot dei dischetti dell'Apple II e prevedeva numerosi payload: ad esempio faceva lampeggiare il testo presente a video e a volte lo invertiva con un effetto a specchio.
Nel 1983, Frederick Cohen usò per la prima volta pubblicamente il termine virus, ma fu solo nel 1986 che i virus informatici iniziarono a guadagnarsi gli onori della cronaca.

M. O. – Antivirus /3

- Per difendersi da i virus bisogna installare sui calcolatori di ogni utente prodotti antivirus che effettuano un'analisi preventiva dei programmi al fine di individuarne la presenza di virus ovviamente noti.
- La NCSA (National Computer Secutiy Association) ha individuato una serie di criteri che possono aiutare l'utente a individuare il prodotto a lui più confacente.
  Un antivirus è in grado di debellare solo i virus che sono noti alla data del suo rilascio. Va quindi "costantemente aggiornato" al fine di mantenerne l'efficacia dello stesso.
- Si stima che in un mese sono prodotti più di 250 nuovi virus.

M. O. – Network Scanner/1

- Un'altra attività che produce molti problemi alla sicurezza dei sistemi è l'installazione e la configurazione dei prodotti software.
- Infatti anche un minimo errore in questa fase può trasformare ad esempio un firewall, in un prodotto che compromette ogni misura di sicurezza del sistema.
- A partire dal 1990 la comunità scientifica si è quindi preoccupata di realizzare dei tool che fossero di supporto all'installazione di tali prodotti.
- Il primo di questi prodotti è COPS (Computer Oracle and Password System), un prodotto che verifica se tutta una serie di parametri riguardanti l'installazione di sistemi UNIX erano correttamente settati.

M. O. - Network Scanner/2

- Nel 1993 COPS viene sostituito con un prodotto più sofisticato, TIGER e successive versioni.
- Nel 1994, fanno la loro comparsa dei tool più orientati alla verifica dei sistemi e dei servizi di rete.

  Il primo di questi tool è Internet Security Scanner seguito nel 1995 dal più famoso SATAN (Security Administrator Tool for Analyzing network).

  Cê da dire che tali strumenti sono stati utilizzati in molti casi per effettuare intrusioni su sistemi.
- Infatti SATAN contrariamente a COPS e TIGER consentiva anche quello che in gergo è definito lo scanning di un sistema remoto ed ottenere un dettagliato rapporto degli eventuali punti deboli di quest'ultimo.

M. O. - Network Scanner/3

- Tutti i prodotti sinora menzionati erano disponibili come freeware all'intera comunità.
- Nel giro di pochi anni questi prodotti sono diventati obsoleti e le idee che sottostavano alla loro realizzazione così come le loro capacità di individuare "bachi" sono stata assorbite da prodotti commerciali, noti con il termine di "Network Scanner"
- In particolare ai prodotti che operano per gli ambienti UNIX in questi ultimi anni si sono aggiunti anche prodotti per il sistema NT, per il quale incominciano ad affiorare un numero non trascurabile di security bug.

Bibliografia Essenziale

- [1] S.M. Bellovin e W.R. Cheswick, Firewalls & Internet Security, Addison Wesley, 1994
- [2] B. Fraser, "Site Security Handbook", RFC 2196 (Obsoletes RFC1244),
- [3] 5. Garfinkel e G. Spafford, Pratical Unix and Internet Security, 2 Edition O'Reilly & Associates, 1996
- [4] ITSEC Information Technology Security Evaluation Criteria.
- [5] B. Schneier, Applied Cryptography 2 Edition, John Wiley & Sons, 1996
- [6] TCSEC Trusted Computer System Evaluation Criteria.
- [7] Philip R. Zimmermann, The Official PGP User's Guide, MIT Press Book, 1995