Sicurezza nei Sistemi di Gestione dell'Informazione

Claudio Ferretti
DISCo – Univ. Milano-Bicocca

- Princìpi
- Esempi
- Attacchi
- Difese

Principio base

- Un problema di sicurezza, o vulnerabilità, può essere in generale inteso come una ...

Via Alternativa

- Quando il sistema è complesso:
  - Le vie "alternative" sono troppe

Un esempio non informatico

- Un cassetto con serratura si può aprire con:
  - La chiave, oppure...
  - Rompendo la serratura
  - Sollevando la copertura del cassetto, liberando il chiavistello
  - Aprendo il retro del mobile
  - Aprendo il cassetto sopra a quello chiuso
  - ...

Informatica = Complessità

- Il problema è particolarmente evidente nei sistemi informatici:
  - Software composti da milioni di righe di codice
  - Applicazioni che si basano sul sistema operativo
  - Sistema operativo che si basa su infrastrutture di rete (hardware e software)
- Osservazione: Eterogeneità del problema

Vulnerabilità / Exploit

- Un programma ha un difetto = vulnerabilità
- ...però:
- l'attaccante è l'utente del programma
- può attaccare solo comunicando dati al progr.

  (come ogni utente)
- se nel programma i dati utente non giungono al punto difettoso l'attacco non può avere successo!

Exploit

- Scelta di dati e sequenza operativa pratica
- in grado di far eseguire al programma

  la parte vulnerabile...
- ...E ANCHE usarla per far danno

Tipi di attacchi

- Per far breccia in questa complessità possiamo immaginare alcuni tipi di attacchi, ad esempio:
  - Ricerca di errori nel software
  - Penetrazione tramite infrastrutture di rete
  - "Social Engineering"
  - Preliminare: Raccolta di informazioni tecniche
  - Puramente negativo: Denial of Service (DOS)

Errori nel software

- Errori di progettazione
- Errori del programmatore
- Errori nella produzione del programma (compilazione)
  - "Buffer Overflow"

Infrastrutture di rete

- Se controllo i dati in transito posso penetrare in un sistema
  - Posso fingermi di essere una macchina autorizzata
  - Posso sostituirmi ad un utente remoto, dopo che si e' autenticato
  - Posso spiare informazioni in transito

Social Engineering

- Sfruttare comportamenti contrari a principi di sicurezza:
  - "PostIt" con password
  - Fidarsi di telefonate presumibilmente autorevoli
  - Carta straccia
  - ...

Raccolta informazioni

- Ha lo scopo di favorire un successivo attacco
  - Nomi utenti (ricerca password)
  - Versioni del software installato
  - Esistenza di macchine
  - Strutturazione dei nodi della rete

Denial of Service

- Ha l'obiettivo di bloccare il funzionamento di un elaboratore
  - Solo per infliggere un danno
  - Per fiancheggiare un attacco informatico
  - In generale difficile da evitare

Alcune difese

- Crittografia
  - E' uno strumento rigoroso ma adatto solo ad alcune funzioni
- Aggiornamento dei pacchetti installati
- Filtraggio delle comunicazioni via rete
- Rilevamento intrusioni
- Procedure
- Semplicità

Crittografia: esempio PGP

- Trattamento posta elettronica:
  - Una email è sempre “spiabile” sui nodi di suo transito
  - Il mittente può spedire il suo messaggio dopo averlo crittato con strumenti appositi come PGP
  - La email rimane spiabile, ma ciò che viene visto è un mucchio di caratteri senza senso, se non decrittati

Aggiornamento del software

- Importantissimo
- Qualità del fornitore/produttore
- Scelta delle applicazioni critiche

Filtraggio su rete (firewall)

- Se non posso avere controllo completo sullo stato di sicurezza delle macchine personali, frappongo un filtro tra la rete esterna e quella interna
  - Posso filtrare in base a identità delle macchine
  - Posso filtrare limitando il tipo di comunicazione
  - Posso filtrare in base al contenuto dei pacchetti (virus, ...)

Rilevamento Intrusioni

- Osservo il traffico sulla rete
- Verifico una lista di vulnerabilità note
- Utile sia in tempo reale, sia per analisi post-mortem, per determinare i danni e per prevenire ripetizioni

Procedure – Semplicità

- Criteri non tecnici, non informatici:
  - Regole di attribuzione delle password
  - Distruzione documenti
  - Divieti sulle comunicazioni non affidabili
  - Divieti di installazione software su personal
  - Divieto di uso di alcune apparecchiature (es. wireless)
- Semplicità: favorisce l'analisi dello stato di sicurezza, sia nel software come nelle procedure