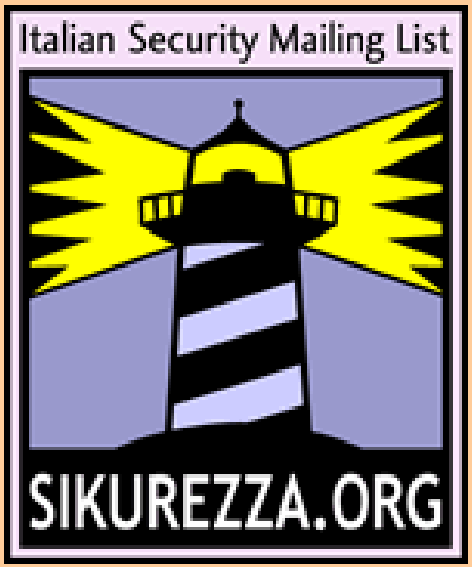
Webbit 2004

Padova, 8 maggio 2003

Secure by default?



Relatore: Igor Falcomatà - koba@sikurezza.org

Secure by default?
Ovvero? E' possibile? Ce ne sono?

audience: livello tecnico basso

in questa presentazione analizzeremo

- **le principali problematiche di sicurezza nei sistemi operativi “tradizionali”**
- **alcune delle soluzioni proposte da ricercatori e sviluppatori**
- **alcune soluzioni “out-of-the-box” basate su sistemi operativi open source**

Le ultime novità nell'information security. Anno 1975. Pianeta terra.

- “Economy of mechanism: Keep the design as simple and small as possible.” (KISS)
- “Fail-safe defaults: Base access decisions on permission rather than exclusion.”
- “Complete mediation: Every access to every object must be checked for authority.”
- “Open design: The design should not be secret”
- “Separation of privilege: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.”

Least privilege: minor privilegio, minor danno

- **“Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.”**

The Protection of Information in Computer Systems
JEROME H. SALTZER, SENIOR MEMBER, IEEE
MICHAEL D. SCHROEDER, MEMBER, IEEE
Proceedings of the IEEE. Vol. 63, No. 9 (September 1975), pp. 1278-1308

http://www.cap-lore.com/CapTheory/ProtInf/

Nel 2004, cosa sarebbe logico aspettarsi parlando di information security?

La teoria c'è. Da anni. Adesso ci si mettono pure le leggi...

- **Utilizzare reti, sistemi operativi, software e protocolli che garantiscano la riservatezza dei miei dati e delle mie comunicazioni**
- **che garantiscano l'identità delle persone e dei sistemi con cui scambio i miei dati e che garantiscano a loro la mia**
- **che siano facili da installare, configurare e mantenere, senza perdere i requisiti di cui sopra; possibilmente ben documentati e supportati**
- **che mi proteggano quanto più possibile da incidenti e mi consentano di continuare/riprendere a lavorare**

La fiera delle ovvietà?

Può essere...

- **Ricordatemi, quando concluderò la prima parte di questa presentazione, di invitarVi a citare un sistema operativo qualsiasi che soddisfi “by default” tutti i requisiti “ovvi” che sto illustrando...**
- **magari anche uno che li soddisfi con un minimo di configurazione**
- **quando per “un minimo” si intende senza impiegare ore di lavoro e/o svariati consulenti da mille-mila euri al giorno**

Nel 2004, cosa sarebbe logico aspettarsi accendendo il peecee?

Un sistema che protegga la privacy dei miei dati.
E' opinione comune che l'unico sistema per proteggere i dati da compromissione in caso di furto o possesso fisico, sia utilizzare la crittografia.

- **Nessun sistema operativo server/workstation/pda adotta, di default, meccanismi di cifratura del disco/file system.**
- **alcuni OS, sia free che commerciali, permettono di utilizzare funzionalità di questo genere, almeno sui “dati”**
- **molti OS non permettono di utilizzare (facilmente) queste funzionalità sui dischi di “boot”**
- **molti OS non hanno questa funzionalità nativamente**

E dopo averlo acceso?

Un sistema che almeno provi a proteggere la privacy dei miei dati chiedendo delle credenziali di accesso;
un sistema che, in caso di compromissione delle mie credenziali, non fornisca il controllo completo del sistema.

- **Alcuni OS "vecchiotti" (no, non antecedenti al 1975) tuttora diffusi, non prevedono credenziali di accesso locali**
- **alcuni OS non forzano l'utente ad impostare credenziali di accesso durante l'installazione**
- **alcuni OS, seguendo l'installazione standard, forniscono all'utente un ambiente di lavoro (posta, navigazione, programmi d'ufficio, etc.) con privilegi di amministrazione**

E dal mio sistema installato “by default” cosa potrei ancora pretendere, nel 2004?

- che impedisca ad utenti non privilegiati di creare file e directory all'esterno della loro “home” o di appositi spazi
- che impedisca ad altri utenti del sistema di accedere ai miei dati, visualizzare le mie connessioni di rete, i siti che ho visitato, la mia posta, i programmi in esecuzione, i nomi dei file che apro, ...
- che mi permetta di effettuare facilmente copie di sicurezza dei miei dati e del sistema operativo stesso, con strumenti di recovery rapido
- che mi permetta di aggiornarlo in maniera comoda e sicura
- che sia supportato per un tempo ragionevole dal produttore

Mi rendo conto, mi sto allargando, ma vorrei un sistema...

- che abbia un design ragionevolmente sicuro verso attacchi di utenti non privilegiati mirati ad ottenere il controllo del sistema o renderlo inefficiente
- che verifichi l'integrità di software ed eseguibili installati; almeno quelli base
- che mi permetta di capire cosa sta succedendo ed effettuare monitoraggio, diagnostica e debug adeguati
- che registri le attività e gli errori di sistema, in particolar modo quelli legati a potenziali violazioni della sicurezza (se poi volesse anche avvisarmi di sua iniziativa di attività anomale, non mi dispiacerebbe)
- che abbia log e messaggi di errori comprensibili e documentabili (ho sfortunatamente dimenticato il sanscrito antico appreso a scuola)

E se avessi la malaugurata idea di attaccarlo ad una rete?

- beh, almeno che aspetti che sia io ad attaccarlo ad una rete e non decida lui arbitrariamente di mettersi in rete con qualcun'altro (bello il wireless, eh? chiedetelo al vostro vicino...)
- che non fornisca a tutti quelli che sono in rete con me “porte” di accesso a software/servizi che non uso (e magari neanche conosco)
- che non fornisca “porte” di accesso a software/servizi. PUNTO. Sono grande e vaccinato e se ho bisogno di un software che fornisca servizi alla rete, posso cliccare un checkbox ed abilitarlo ESPLICITAMENTE. Se proprio esistono dei servizi “di default”, che almeno si possano disabilitare e abbiano dei settaggi “ragionevoli”
- vogliamo parlare delle vulnerabilità dei client di rete (web, posta, etc.)? Soprattutto quando vengono usati da un utente con privilegi elevati...

Si è fatta una certa... non parleremo della sicurezza dell'infrastrutta di networking

- autenticazione sulle porte di rete
- autenticazione per accedere alla rete
- protocolli di comunicazione “in chiaro”
- password in chiaro
- nessuna possibilità di identificare il mittente dei pacchetti
- nessuna possibilità di assicurare l'integrità del traffico
- estrema facilità nel portare attacchi DoS

Principali categorie di attacchi

- attacchi fisici
  accesso illegale ad infrastrutture (locali, stazioni e terminali, cablaggio); furto di beni (pda, portatili, media, dispositivi di accesso, hw in genere, ...); etc.
- attacchi alla componente umana
  social engineering; abuso di buona fede; raccolta informazioni; truffe; minacce e rapimenti; etc.
- attacchi alla rete e sue componenti
  analisi, modifica ed intercettazione del traffico, sabotaggio e DoS, attacchi a router, switch ed altre apparecchiature di networking e sicurezza (load balancer ed accelleratori, firewall, ids, ..), ...
- attacchi a componenti di telecomunicazione
  ras, modem ed apparecchiature, telefoni, centralini e pbx, cellulari, fax, etc.
- attacchi ai sistemi server ed alle relative applicazioni
- attacchi alle stazioni client ed alle relative applicazioni
- attacchi ad altre apparecchiature
  stampanti, fax, allarmi, rilevazione presenze, dispositivi di archiviazione e storage, webcam, scanner, macchine del caffé, etc.

Cosa intendiamo con “secure by default”?

- secure by design: least privilege, etc. (vedi slide 3)
- nessun servizio attivo
- nessun account/password prevedibile/preimpostato
- software (server, client, locali) in esecuzione con i privilegi minimi necessari
- configurazioni (servizi, ACL, kernel) che “by default” garantiscano un livello di sicurezza ragionevole (vedi least privilege)
- supporto nativo per crittografia dei dati sul file system e per le connessioni di rete; obbligatorio per accesso remoto ed amministrazione
- strumenti di logging, monitoraggio e diagnostica adeguati

Cosa intendiamo con “secure by default”?

- strumenti di aggiornamento e patch management adeguati
- interoperabilità, supporto per varie tipologie di autenticazione centralizzata
- strumenti di rilevamento (e blocco) degli attacchi più comuni
- strumenti di verifica dell'integrità del sistema
- codice sviluppato utilizzando principi di sicurezza/ingegneria del software adeguati
- verifica estensiva della sicurezza del codice

- capabilities/MAC/RSBAC/trusted system

Ed il supporto?

- documentazione adeguata
  - hardenening
  - corretta configurazione e best pratices
  - diagnostica
- protocolli e standard aperti
- disponibilità dei sorgenti
- responsività nel risolvere le problematiche di sicurezza
- advisor/patch
- supporto

Allora?

Vi invito a citare un sistema operativo qualsiasi che soddisfi “by default” tutti i requisiti “ovvi” che ho illustrato.

...parlatene con il vostro vendor...

Domande?

- **Un ringraziamento particolare a Guido Bolognesi (Zen), la seconda parte del seminario verrà tenuta utilizzando la presentazione_**
  Free & Secure, una panoramica delle feature di sicurezza moderne nei sistemi operativi OpenSource.
  http://www.kill-9.it/slides/unibo03.pdf

Alle 17, LAB3, Laboratorio “run secure || die”
come realizzare in modo sicuro una piccola infrastruttura per fornire servizi (web, mail) in modo sicuro.

<free advertising>
http://www.sikurezza.org - Italian Security Mailing List
</free advertising>