Valutazione di sistemi operativi sicuri

Lezione 21 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2008-9

Indice

fiducia e garanzia

il problema oggetto delle due lezioni precedenti è stato quello di **come progettare** un sistema operativo "sicuro", o più precisamente "***trusted***", cioè **degno di fiducia**

ci si pone ora un problema correlato, ma ben diverso:

come mostrare che un sistema operativo è degno di fiducia

ovvero il problema di come offrire una credibile **garanzia** della sua sicurezza

gli utenti possono ottenere tale garanzia in tre modi:

fiducia nelle dichiarazioni del costruttore

valutazione propria delle caratteristiche di sicurezza del sistema

valutazione da terzi indipendenti, esperti in sicurezza dei sistemi informatici

varie norme tecniche per la valutazione di sicurezza dei sistemi informatici sono state prodotte e pubblicate nell'ultimo trentennio

la prossima lezione ne presenta una breve rassegna

fonti di vulnerabilità dei sistemi operativi

un buon punto di partenza per la valutazione dell'effettivo livello di fiducia accordabile a un sistema operativo è la conoscenza delle fonti delle vulnerabilità più frequenti in tali sistemi

una *checklist* per l'orientamento nella ricerca di lacune e punti deboli:

elaborazione dell'I/O

→ da sottosistemi hardware intelligenti, spesso esterni al KdS

→ da *driver* di periferica, spesso più difficili da verificare

→ spesso in concorrenza con altre funzioni del sistema operativo

ambiguità nella *policy* di autorizzazione degli accessi

tradeoff prestazionali

→ difetti di completezza della mediazione nel controllo di accesso

open endedness della piattaforma

installabilità di software di terzi, integrabile nel sistema operativo:

può introdurre *trapdoor*, e talvolta richiede esecuzione privilegiata

metodi di valutazione della sicurezza

in una lezione precedente si è già avuta una introduzione generale ai principali metodi di valutazione della sicurezza dei sistemi informatici:

- validazione dei requisiti e del software
- revisione e ispezione formale del software
- verifica formale
- collaudo

tutti questi metodi sono utili alla valutazione di sicurezza dei sistemi operativi

i metodi delle prime due categorie sono di largo impiego in metodologie di

- **progettazione partecipativa**

questa ha diverse modalità operative

- in particolare a seconda che il software sia *open source* o meno

open source: una questione aperta

è molto dibattuta, e ormai da lungo tempo, la questione dei meriti relativi del software *open source* e del software proprietario a sorgente chiuso, riguardo alla sicurezza

- Unix e successori, segnatamente Linux, sono il caso di riferimento per i sistemi operativi *open source*

le ragioni generali in favore dell'adozione di software *open source* sono molteplici:

- costo nullo o molto basso
- controllo pubblico di qualità
- supporto aperto agli utenti (fornitori di supporto mediante forum, etc.)
- estendibilità, sviluppo aperto agli utenti

la seconda delle suddette ragioni è un argomento in favore di migliori garanzie di sicurezza

la pubblicità del sorgente dà tuttavia più agio alla ricerca di vulnerabilità a fini maligni

(Anderson 2002, 2005) ha prodotto un modello statistico di affidabilità che dà sostanzialmente lo stesso tasso di errore dopo il collaudo per le due categorie di software

- la differenza più evidente sta probabilmente più nella disponibilità di **antidoti** al codice maligno che nel tasso di vulnerabilità

standard di valutazione della sicurezza

la progettazione partecipativa coinvolge utenti e/o acquirenti dei sistemi informatici, tuttavia...

la maggioranza di questi non sono abbastanza esperti di sicurezza dei sistemi informatici da poter valutare in proprio il livello di fiducia accordabile al prodotto

> il ricorso alla valutazione indipendente da terzi esperti è necessario quando le garanzie offerte dal costruttore non bastano

gli standard di valutazione della sicurezza hanno un duplice fine, cioè permettere:

> ai **costruttori** di disporre di linee-guida e criteri di valutazione per progettare sistemi sicuri, e di fare riferimento a norme tecniche nella presentazione di garanzie di sicurezza a utenti e/o acquirenti
> ad **esperti indipendenti** di mettere in opera procedure di valutazione standard per fornire i loro servizi, e quindi **certificare** il livello di fiducia del sistema valutato in base a scale di valutazione standard

riferimenti

Anderson (2002) :
Security in Open versus Closed Systems - The Dance of Boltzmann, Coase and Moore,
at: *Open Source Software: Economics, Law and Policy*, Toulouse (F), 20-21 June 2002.
http://www.cl.cam.ac.uk/~rja14/Papers/toulouse.pdf

Anderson (2005) :
Open and Closed Systems are Equivalent (that is, in an ideal world),
Chapter 8 in: Feller *et al.* (Eds.),
Perspectives on Free and Open Source Software, MIT Press, June 2005.