La minaccia dei sistemi di protezione hardware.

Alessio Frusciante

algol@firenze.linux.it

Sicurezza

Gli attuali computer non sono pensati per essere sicuri.

Internet è un luogo pieno di pericoli.

Esempio di programmi insicuri: telnet, che manda le password in chiaro.

Bug che portano vulnerabilità. Classico esempio: buffer overflow.

Soluzioni?

Una soluzione proposta dall’industria hardware e software:

Il "computer fidato"

Computer fidato

TCG (Trusted Computer Group), presentato ad aprile 2003

TCPA (Trusted Computing Platform Alliance)

Consorzio di quasi 200 aziende il cui scopo è produrre hardware che permetta di ottenere un "computer fidato".

In particolare, non ridisegnando tutto, ma aggiungendo componenti ad un normale PC.

Da chi è formato il TCG?

Alcuni nomi di aziende facenti parte del consorzio:

Produttori di microprocessori: Intel, AMD

Produttori di chipset per schede madri: Ali, SiS, Via

Microsoft, IBM, HP, Sony, ...

Alcuni aspetti del progetto TCPA

Gestione hardware della crittografia. C’è una chiave "master" che non esce mai dal chip (TPM, Trusted Platform Module)

La modalità fidata può essere disattivata (si può avviare il computer in modalità inaffidabile).

"trusted boot". Il computer viene avviato con una sequenza di passi. Al termine di ciascun passo si controlla che ciò che verrà eseguito è quello che ci si attende (non è stato modificato).

TCPA è una realtà

Esistono già dei chip che rispettano le specifiche TCPA

Atmel - AT97SC3201
Infineon - SLD 9630TT11
National Semiconductor - Safekeeper

Prospettive e domande

Scopo dichiarato: "ubiquità", ossia sostituire tutte le macchine attuali con macchine "fidate"

Perché tutta questa preoccupazione per la nostra sicurezza, quando per anni l’attenzione alla sicurezza era delegata al singolo?

Perché proprio *questo* modo di affrontare il problema della sicurezza?

Problemi

Qualche preoccupazione

Ogni chip ha un identificativo. Possibilità di essere riconosciuti.

Non è detto che si possa conoscere il codice microprogrammato nei chip

Se il codice nel chip ha dei bug come si patcha?

Non è la prima volta.

Precedenti di soluzioni hardware che tolgono controllo all'utente.

PSN (Personal Serial Number) su Pentium III
Ritirato per le proteste.

HDCP (High-bandwidth Digital Content Protection)

CPRM (Content Protection for Recordable Media)
Poi non entrato nella specifica ATA

Software

NGSCB (Next-Generation Secure Computing Bases)

Palladium

Documentazione non chiarissima.

Soluzione software, che necessita di una base hardware adatta.

TCPA per ora non basta. In realtà Intel ha annunciato LaGrande che sembra avere le caratteristiche necessarie.

Che cosa consente Palladium?

DRM (Digital Rights Management). Passaggio da acquisto al pay-per-view.

Controllo di che cosa gira su un computer (solo i programmi "certificati" possono girare)

Revoca documenti. Mando un’email che dopo 10 giorni non si può più leggere (si può ricondurre al DRM).

Lock-in grazie ai formati (non sono in grado di leggere i *miei* documenti se non con un programma dato).

Pericoli

Centralizzazione dei controlli. Da una parte Microsoft, dall'altra i detentori dei diritti d'autore possono conoscere e limitare il modo in cui usufruiamo del sistema.

Protezione dell'utente dai pericoli esterni o protezione di terze parti dagli utenti?

Di chi è il mio computer?

Sviluppi futuri

Controllo totale del sistema da parte di terzi

Copertura legale negli USA. Il senatore Hollings è proponente di una legge (SSSCA-CBDTPA) per cui i computer non fidati sono illegali.

Conclusioni

Vale la pena aumentare la sicurezza a questo prezzo?

Che sicurezza si può avere senza privacy?