Ridisegnare i Sistemi Operativi per una Nuova Sicurezza

Sommario

I nuovi strumenti informatici, dagli smartphone ai tablet che tanto ci sono utili nella vita di tutti i giorni, portano con se non solo nuove funzionalità ma anche nuovi rischi. La gestione di questi rischi richiede l'introduzione di nuove misure di sicurezza informatiche ma sta diventando sempre più evidente che per implementare queste nuove misure di sicurezza potrebbe essere necessario ridisegnare l'approccio ai sistemi di sicurezza informatica a partire dalle primitive hardware e dei Sistemi Operativi.

Come tutti ben sappiamo, gli ultimi anni hanno portato una nuova rivoluzione nell'ICT con una ulteriore diffusione e massificazione dell'uso degli strumenti informatici a qualunque livello e quasi per qualunque scopo.

Allo stesso tempo vi è stata una rivisitazione di architetture e sistemi ICT antichi e che ben conosciamo. Il paradigma “Cloud” comporta l'esistenza di sistemi centrali sui quali risiedono i dati ed avvengono le elaborazioni, mentre l'utente ha a disposizione uno o normalmente più terminali per l'accesso ai dati e ai servizi. Se l'architettura a grandi linee è quella dei vecchi sistemi centrali, ad esempio dei Mainframe, le tecnologie adottate, gli impieghi e gli utilizzatori sono completamente diversi.

Lo scenario di oggi è quello di un utilizzatore privato o aziendale che utilizza per lo più dei device mobili, dallo smartphone al tablet, per accedere a diverse applicazioni e dati residenti su diversi sistemi remoti. La principale novità è che l'utente oggi accede alle stesse applicazioni e dati da terminali diversi e ad applicazioni e dati diversi da ogni terminale. Anni fa ogni terminale era connesso direttamente ad un singolo server centrale e le applicazioni sul server centrale gestivano gli stessi dati per tutti gli utenti.

Come ben sappiamo, la sicurezza dei sistemi ICT non è un fatto od una misura isolata, ma una catena che non deve avere punti deboli. Per implementare misure di sicurezza che proteggano i dati e i servizi degli utenti finali, è necessario che tutta la catena ICT, dalle applicazioni che interagiscono con gli utenti all'hardware, forniscano le funzionalità necessarie.

Se negli ultimi 10 anni molto è cambiato nell'ICT, ben poco è cambiato nell'approccio alla sicurezza

nei livelli più bassi della catena ICT, ovvero l'hardware e i sistemi operativi. E' necessario perciò chiedersi se le funzionalità utili e necessarie a garantire la sicurezza fornite dall'hardware e dai sistemi operativi di oggi siano in grado di soddisfare le esigenze dei mutati utilizzi da parte delle applicazioni e degli utenti oppure se dobbiamo ridisegnarle.

Il punto di vista del server

Per capire meglio cosa è cambiato e di cosa abbiamo bisogno dobbiamo analizzare più nel dettaglio gli scenari usuali e quelli nuovi partendo dal punto di vista del server centrale. Lo scenario che ben conosciamo e sul quale abbiamo costruito la base della sicurezza ICT consiste in un server centrale nel quale risiedono i dati e le applicazioni che li gestiscono. Al server accedono direttamente gli utenti che possono interagire solo con il server e direttamente con esso. In questo scenario sono da rimarcare alcune assunzioni importanti:

- è il server che autentica direttamente gli utenti;
- gli utenti tramite quei terminali non si possono connettere direttamente ad altri server: le connessioni ad altri server sono possibili solo attraverso il proprio server;
- la gestione e protezione dei dati e delle applicazioni è in carico completamente al server, gli utenti non posso utilizzare loro applicazioni, indipendenti da quelle presenti sul server, per gestire i dati;
- il sistema operativo, le applicazioni eseguite sul server ed i dati sono considerati “sicuri” perché gestiti unicamente dal server.

I principali obiettivi della sicurezza sono:

- garantire l'identificazione degli utenti;
- verificare, limitare e controllare l'accesso ai dati, risorse e applicazioni degli utenti;
- verificare, limitare e controllare l'accesso ai dati, risorse e applicazioni delle applicazioni.

Questi obiettivi sono raggiunti utilizzando le primitive di sicurezza, in particolare quelle di “Access Control”, fornite dai sistemi operativi.

Lo scenario odierno lato server, ad esempio in un ambiente “Cloud”, è per molti aspetti simile a quello tradizionale. La principale differenza architetturale è che possiamo distinguere tra il livello di infrastruttura e quello di servizio. A livello di infrastruttura è presente l'hardware e il software di base, i sistemi Host di virtualizzazione, che forniscono i servizi a sistemi applicativi diversi e ne devono garantire l'isolamento. In linea di principio le ben note primitive di “Access Control” dovrebbero essere in grado di gestire l'isolamento tra macchine virtuali diverse e anche se oggi non molto è stato ancora fatto su questo punto, è possibile che a breve con la maturazione delle

tecnologie di virtualizzazione, i sistemi di sicurezza intrinseci agli Host di virtualizzazione forniranno le necessarie funzionalità di sicurezza.

I sistemi che forniscono i servizi, tipicamente chiamati Guest virtualizzati, ospitano normalmente una sola applicazione composta da molte componenti, e da questo punto di vista sono più semplici dei precedenti sistemi centrali (come i Mainframe). Come nello scenario precedente, l'obiettivo principale è quello di controllare l'accesso ai dati ed alle risorse da parte delle componenti delle applicazioni (date per "sicure") e soprattutto degli utenti. Anche se gli utenti accedono ai dati con modalità pratiche e protocolli nuovi, lo scenario è abbastanza simile a quello che già conosciamo e per il quale di nuovo le primitive di "Access Control" opportunamente aggiornate dovrebbero essere sufficienti a permetterci di implementare le misure di sicurezza necessarie.

In conclusione, dal punto di vista del server pur essendo completamente cambiate le tecnologie e le modalità di utilizzo dei sistemi, l'approccio che ben conosciamo per fornire la sicurezza a partire dall'hardware e dai sistemi operativi dovrebbe continuare ad essere efficace.

Il punto di vista del terminale utente

Invece se consideriamo i nuovi device che tanto ci appassionano e ci sono utili, il punto di vista del terminale utente è del tutto mutato. L'accesso ai servizi e ai dati è oggi fatto da terminali utenti quali smartphone, tablet e PC personali. Questi strumenti hanno in comune varie caratteristiche e in primo luogo il fatto di essere (nella maggioranza dei casi) sotto il completo controllo dell'utente. In molti casi, i terminali sono dell'utente stesso che li utilizza sia per lavoro (il BYOD, Bring Your Own Device) che privatamente. E' sempre l'utente che li sceglie e decide quali applicazioni installare, quando fare update e aggiornamenti. Lo stesso terminale è utilizzato normalmente per accedere ad applicazioni e dati diversi, sia personali che lavorativi. Il terminale accede ai dati ed ai servizi offerti dal server o tramite un browser web che svolge il ruolo di interfaccia applicativa generica, oppure tramite specifiche "App" (applicazioni software) che svolgono il ruolo di interfacce dedicate.

Le principali differenze con lo scenario classico e i punti di attenzione sono:

- il terminale è sotto il controllo dell'utente e non più dell'amministratore del server;
- tipicamente ogni terminale è univocamente assegnato e utilizzato da un utente, e quindi non vi è necessità di controllo e separazione tra utenti a questo livello;
- l'utente utilizza il terminale per scopi diversi con applicazioni diverse di sua scelta che agiscono su diversi set di dati e interagiscono con server diversi;
- dal punto di vista del server, le applicazioni ed il software del terminale non possono più

essere considerati “sicuri” visto che non ne ha alcun controllo.

L'ultima affermazione è forse quella più critica, il server, e quindi chi lo gestisce e ha competenze tecniche per farlo, anche nel campo della sicurezza, ha poche o nulle possibilità di controllare i terminali e in particolare gestirne la sicurezza.

In questo nuovo scenario i server, le applicazioni e i dati che risiedono sui server sono “sicuri”, mentre lo stesso non si può dire dei terminali, delle “App” e dei dati che transitano sui terminali.

Di questo abbiamo esempi quotidiani con la presenza di malware sui terminali utenti, ovvero “App” malevole, che intercettano e modificano i dati e le comunicazioni delle altre “App”.

Questa è una situazione nuova per la sicurezza dei dati e delle informazioni. I modelli teorici su cui ci siamo basati per tutti questi anni partono dall'assunto che il rischio provenga dall'esterno, un altro utente o un altro sistema, e non che sia interno ai dati ed alle applicazioni dell'utente stesso. In questa situazione, i tradizionali modelli di “Access Control” che sono basati fondamentalmente sull'identificazione dell'utente (sia esso persona o server), non ci sono molto utili.

Quali nuove primitive di sicurezza?

Cosa possiamo fare per implementare della sicurezza sui terminali utenti nel mondo “Cloud”? E' chiaro che non possiamo delegare l'utente alla gestione della sicurezza, visto che non possiamo pretendere competenze di alcun tipo dall'utente finale. Già oggi gli utenti finali sono raggiunti da messaggi contrastanti e non chiari: da una parte vi sono i messaggi che sconsigliano di installare nuove “App” o di accedere a servizi se non si è assolutamente certi della loro provenienza, dall'altra parte quasi quotidianamente compaiono nuove applicazioni online e nuovi mercati di “App” che attirano gli utenti all'utilizzo di nuove funzionalità. L'utente finale non ha le competenze per poter distinguere tra tutte queste applicazioni quali sono a rischio e quali rischi comporti il loro utilizzo.

Non possiamo neanche delegare la gestione della sicurezza unicamente alle “App” o ai browser, visto che oggi una “App” malevola può accedere ai dati ed alle funzioni delle altre applicazioni.

E' necessario quindi che le funzionalità di sicurezza siano implementate ad un livello inferiore, tipicamente a livello di Sistema Operativo o, nel caso ad esempio di Browser web, dell'ambiente all'interno del quale vengono eseguite le applicazioni.

E' per questo che recentemente sentiamo tanto parlare di “Sandboxing”, ovvero l'esecuzione di applicazioni isolate dal resto del sistema e dei dati. Implementare correttamente una “Sandbox” non è però facile se l'ambiente che ospita l'esecuzione dell'applicazione, alla fin fine sempre il Sistema Operativo, non offre primitive che permettono di implementare i necessari controlli.

Implementare efficacemente queste primitive richiede però un drastico cambio di approccio nel disegno dei Sistemi Operativi. Come detto, sinora lo scenario di riferimento utilizzato per disegnare

i sistemi di sicurezza dei Sistemi Operativi è sempre stato quello di difendersi da attacchi esterni e di separare utenti diversi assumendo che le applicazioni fossero "sicure". Invece nello scenario nuovo abbiamo un solo utente con uno o più set di dati ed applicazioni a priori "non sicure" che devono essere isolate tra di loro pur fornendo i propri servizi allo stesso utente e accendendo in parte agli stessi dati.

E' quasi una rivoluzione Copernicana in quanto invece di doversi difendere da attacchi esterni, ora dobbiamo implementare delle difese da attacchi interni, e ben sappiamo come sia molto più difficile la difesa da nemici interni che esterni.

Non solo, l'implementazione di queste nuove primitive può richiedere anche la modifica dell'hardware con l'aggiunta di funzioni opportune, come già capitato recentemente con il supporto implementato direttamente nei processori per la virtualizzazione.

Sandboxing

L'idea della "Sandbox" è abbastanza semplice e potente e potrebbe indicare la strada da percorrere. Il Sistema Operativo, o comunque l'ambiente di esecuzione delle "App", deve garantire un isolamento ragionato tra le varie "App". L'isolamento deve essere implementato almeno nelle seguenti direzioni:

- per l'accesso diretto all'hardware: dalle comunicazioni in rete, al microfono, altoparlante, camera, dispositivi di memorizzazione dati ecc.;
- per l'accesso ai dati: dai file personali residenti sul filesystem ai parametri di configurazione del sistema quali ad esempio indirizzi IP, versione del Sistema Operativo, applicazioni ecc.;
- per l'accesso alle altre "App" presenti sul device e il dialogo diretto tra applicazioni.

Il problema principale è che le "App" devono accedere all'hardware, ai dati e alle altre "App" e quindi non è possibile pensare ad un completo isolamento. Se fossimo costretti a duplicare tutti i dati per ogni "App" come se avessimo un terminale dedicato per ognuna di esse, il tutto diventerebbe velocemente non utilizzabile. Al contrario è necessario che l'inserzione o l'aggiornamento di un dato comune a molte "App" sia fatto una volta sola dall'utente per tutte le "App".

Dobbiamo quindi disegnare ed implementare un ambiente nel quale siano possibili accessi a hardware, dati e servizi tra "App" solo se autorizzati, necessari e a basso rischio. Il tutto tenendo sempre conto che non possiamo contare sulla competenza dell'utilizzatore finale il che richiede che le interfacce di gestione siano intuitive e semplici.

Conclusioni

La problematica discussa in questo articolo non è totalmente nuova, in quanto è ormai da almeno un paio di anni che se ne discute. Quello che però sta emergendo adesso, si veda ad esempio [1], è la consapevolezza che non basta aggiungere qualche nuova funzionalità tradizionale a quelle già esistenti per risolvere il problema della sicurezza dei nuovi strumenti e terminali utenti. E' invece molto probabilmente necessario ripensare da capo e dal basso l'implementazione stessa dei Sistemi Operativi in modo che i nuovi scenari siano compresi e supportati direttamente dall'hardware e da ogni livello software.

Al momento non è ancora chiaro cosa sia necessario fare per affrontare queste problematiche né tanto meno quali siano le soluzioni possibili. Molti però se ne stanno occupando: tra i primi ad affrontare queste problematiche sono stati i produttori di browser [2] e di smartphone, e sono nati anche progetti quali [3] e [4] il cui approccio invece parte dal Sistema Operativo.

Riferimenti

[1] Intervista a Robert Watson in IEEE Spectrum
http://spectrum.ieee.org/podcast/computing/software/computers-its-time-to-start-over

[2] Si consideri ad esempio questa valutazione sullo stato di implementazione delle sandbox nei maggiori browser nel 2011: http://www.accuvant.com/capability/accuvant-labs/security-research/browser-security-comparison-quantitative-approach
http://www.theregister.co.uk/2011/12/09/chrome_ie_firefox_security_bakeoff/

[3] Qubes http://qubes-os.org/trac

[4] Bromium http://www.bromium.com/

Andrea Pasquinucci (PhD CISA CISSP) si occupa prevalentemente di progetti ICT innovativi ed avanzati e in particolare di sicurezza ICT, audit, compliance, governance e formazione ICT per il management ed il personale tecnico. E' esperto di sicurezza delle reti e dei servizi web, dei sistemi operativi e di crittografia.