PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 244 di venerdì 15 dicembre 2000

Controllati...a tempo

E' stato messo a punto da due ricercatori di Princeton un sistema che consente di appurare, senza inviare cookies, se il visitatore di un sito abbia visitato anche siti della concorrenza...

Non sara' impresa facile individuare in tempi brevi un metodo efficace per proteggere la privacy degli utenti della rete dai "timing attack". Ad affermarlo sono gli autori stessi della nuova tecnica, due ricercatori della Universita' di Priceton.

Ormai i cookies "invadenti", cioe' i file che inviati sul computer del visitatore di un sito possono registrarne le abitudini, sebbene insidiosi per la privacy dell'utente, possono essere conosciuti e scovati dalla maggior parte degli utenti della rete.

Quella del "timing attack" e' invece una tecnica nuova, che nulla lascia sul computer dell'utente, e per questo ancor piu' subdola e difficilmente individuabile.

Ma di cosa si tratta? Chi potra' servirsene?
Il sistema si basa sulla presenza sui computer di una zona di memoria, detta cache, nella quale sono temporaneamente salvate le pagine visualizzate, allo scopo di consentire una navigazione piu' veloce.
Quando si richiama una pagina gia' visualizzata in precedenza, il computer la ritrova nella sua memoria e la rende disponibile piu' velocemente.

"Timing attack" sfrutta proprio questa caratteristica.
Quando l'utente giunge sul sito "spione", il server invia oltre alla pagina da visualizzare un programmino in java che, senza essere installato sul computer, chiede al browser di cercare alcuni oggetti, quali ad esempio logo o immagini presenti su siti della concorrenza.

Il software in java allora misura il tempo impiegato dal browser a trovare l'oggetto presente su un determinato sito: se lo rende disponibile immediatamente significa che e' presente nella cache del computer e che pertanto l'utente ha visitato negli ultimi giorni tale sito.
E i passi della navigazione dell'utente sono cosi' svelati...

La precisione del sistema e' del 98% e potrebbe essere utilizzato da chiunque possieda un sito.

E se l'utente decide di disabilitare la funzionalita' java dal suo computer? "Timing attack" non si ferma innanzi a questo ostacolo, ma effettua la ricerca mediante comandi HTML e, con una precisione del 94%, effettua i medesimi controlli.
