PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 774 di martedì 13 maggio 2003

Firma digitale: un attacco simulato rileva alcune debolezze del sistema

Il Laboratorio di Sicurezza e Reti del Dipartimento di informatica e comunicazione dell'Universita' degli Studi di Milano ha condotto la prima realizzazione pratica a livello mondiale di attacco riuscito a un dispositivo di firma digitale.

Danilo Bruschi, docente al Dipartimento di scienze dell'informazione dell'Università di Milano, Presidente del CLUSIT e coordinatore del CERT-IT già citato più volte su PuntoSicuro (vedi numero 481 di giovedì 24 gennaio 2002), nell'ambito di un programma di ricerca mirato a verificare la robustezza delle applicazioni di firma digitale, ha coordinato un test di attacco a un'applicazione di firma digitale distribuita da un certificatore iscritto all'albo dell'Autorita' Informatica per la Pubblica Amministrazione nell'ambito di una ricerca del Laboratorio di Sicurezza e Reti del Dipartimento di informatica e comunicazione dell'Università degli Studi di Milano.

I risultati sono piuttosto allarmanti dato che, stanti le dichiarazione del Dr. Bruschi "L'attacco ha consentito a un intruso di ottenere documenti digitalmente firmati da un utente, all'insaputa dello stesso".
La modalità tecnica per l'attacco è stata quella di un virus informatico, inviato a un utente attraverso un attachment di posta elettronica. L'attachment, una volta aperto ha attivato la procedura di infezione del sistema ospite, consistente nell'esecuzione di un codice maligno che ha preso il controllo del dispositivo di firma (smart card piu' relativo lettore).

Da quel momento, ogni volta che un utente sottoponeva un documento al processo di firma, il codice maligno poteva sottoporne altri il cui contenuto era stato preventivamente deciso da chi ha realizzato il virus, ovviamente il tutto all'insaputa dell'utente.

Per la realizzazione dell'attacco sono state sfruttate alcune debolezze di sicurezza dell'ambiente Java, quando eseguito su sistemi operativi configurati senza opportuni accorgimenti di protezione, insieme ad alcune debolezze dell'applicazione attaccata. Questo attacco, sempre a detta dei ricercatori, solleva alcune perplessità sul sistema preposto alla gestione della firma digitale nel nostro paese.
