calabria ora
sabato 5 luglio 2008
pagina 12

la ricerca

Firma digitale a rischio "pirati"

Uno studio condotto dalla Mediterranea ha scoperto nuovi pericoli

REGGIO CALABRIA Tecnologia al servizio dei cittadini sì, ma meglio se senza rischi. Un'affermazione condivisa certamente da tutti e anche dalla legge dello Stato che, con l'avanzare della ricerca in campo scientifico e le sue applicazioni nella vita quotidiana, si è trovata di fronte alla necessità di adeguare la normativa vigente in funzione delle nuove procedure, spesso informatiche, che da anni regolano il funzionamento della società. Tra queste, diventata ormai prassi, la firma digitale. Con la necessità di sostituire i faldoni e i documenti cartacei degli uffici di tutto il mondo, oggi è possibile sottoscrivere un atto con una "autografo" informatico, che mette in soffitta la "vecchia" stilografica. La firma digitale è una sequenza di bit generata a partire da un documento attraverso una smart card, un dispositivo molto simile ad una carta di credito che è in possesso esclusivo del sottoscrittore che la abilita attraverso l'inserimento di un pin. A partire da questa sequenza di bit è possibile verificare se è stata prodotta da una certa smart card, e di conseguenza da un certo utente, e se il documento è stato modificato successivamente alla firma.

Con l'introduzione della firma digitale anche la giurisprudenza si è dovuta aggiornare con norme che ne tutelino l'utilizzo e tengano lontani speculazioni e reati. Ma se fino a qualche tempo fa le "debolezze" della sigla elettronica potevano essere connesse a fattori di rischio quali lo smarrimento della smart card, l'"infezione" di virus informatici in grado di alterare il comportamento dei software di firma, e l'inserimento di "macro-istruzioni" in grado di trasformare l'atto nel tempo, grazie ad uno studio (www.unirc.it/firma) portato avanti dall'università Mediterranea di Reggio Calabria, si è scoperto un nuovo concreto pericolo legato all'applicazione della firma digitale.

La scoperta verrà presentata ad agosto a Tripoli in un convegno

Una minaccia che, per i riverberi sul piano della normativa tecnica, è oggi attualmente allo studio degli esperti del Centro Nazionale per l'Informatica della Pubblica Amministrazione (CNIPA).

La ricerca, diretta dal professor Francesco Buccafurri, è stata effettuata in collaborazione con gli ingegneri Gianluca Lax e Gianluca Caminiti, tutti reggini, del laboratorio di Ingegneria Informatica della Facoltà di Ingegneria.

«Lo studio ha mostrato la possibilità di creare documenti informatici che hanno un comportamento polimorfo – spiega il professor Buccafurri – cioè tale da presentare un contenuto diverso, a seconda dell'applicazione con la quale il documento viene visualizzato. Tale comportamento permane anche quando al documento venga apposta la firma digitale».

«Infatti – aggiungono Lax e Caminiti – l'attacco viene realizzato senza modificare i bit del documento dopo l'apposizione della firma, ma solo attraverso la modifica del nome del file (più precisamente della sua estensione), una volta che il file è stato opportunamente predisposto. Sarà l'applicazione associata alla nuova estensione a visualizzare un contenuto diverso da quello sottoscritto», conclude Buccafurri.

In breve il creatore della firma digitale ha garantito l'immutabilità dei bit del documento, ma non il senso che ad essi deve essere attribuito.

Il lavoro compiuto nei laboratori della Mediterranea sarà presentato nel mese di agosto a Tripoli in un convegno internazionale sulle applicazioni delle tecnologie digitali.

EMANUELA MARTINO
e.martino@calabriaora.it

TRIS D'ASSI Il professor Buccafurri e gli ingegneri Lax e Caminiti che hanno lavorato al progetto che ora è sotto esame al C. N. I. P. A.