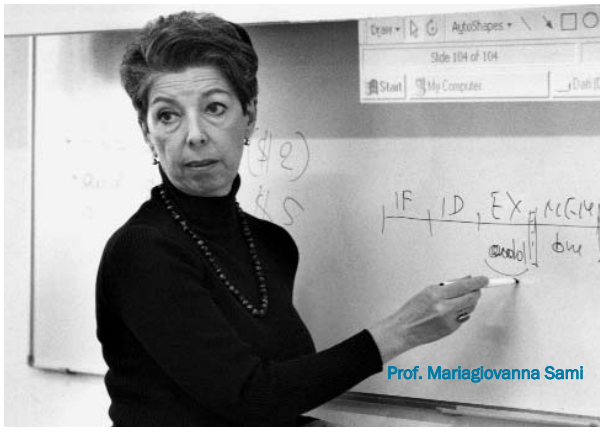
Sicurezza per la comunicazione mobile

"Essere connessi" è oggi una priorità, come mostra la crescente diffusione di sistemi di comunicazione senza fili (computer portatili, telefoni cellulari, palmari). Un requisito importante per i sistemi senza fili è la tutela dei dati personali. L'Istituto ALaRI dell'Università della Svizzera italiana (USI) e il Laboratorio di Microelettronica della SUPSI hanno sviluppato il progetto di ricerca "Security for mobile systems", finanziato dalla Fondazione Gebert Rüf, che presenta soluzioni innovative al problema della sicurezza nei sistemi mobili.

Il problema della sicurezza dei dati esiste da quando l'uomo archivia e trasferisce informazioni. Da allora gli esperti si sono cimentati in una duplice sfida con opposti obiettivi: inventare sistemi di protezione sempre più sicuri e coltivare l'estro necessario per accedere alle informazioni senza conoscere la chiave di entrata. Con l'esplosione dei sistemi di comunicazione senza fili la tutela delle informazioni è divenuta prioritaria. Quasi ogni giorno abbiamo notizia di pirati informatici che accedono a dati riservati, o che si impadroniscono di numeri di carte di credito, facendo irruzione anche nei dati archiviati in computer personali. Già una semplice connessione può essere utilizzata dai pirati informatici per accedere a informazioni protette. Reazione immediata a tale fragilità è stata l'adozione di soluzioni crittografiche che permettono di proteggere le informazioni scambiate attraverso i sistemi di comunicazione senza filo. Tuttavia lo sviluppo di un algoritmo crittografico non permette da solo di risolvere tutti i problemi. Il funzionamento di un codice sofisticato richiede un microprocessore potente. Di conseguenza ogni volta che l'utente desidera un sistema affidabile, ne ottiene uno che sarà sì più sicuro, ma anche più lento; solo i computer più veloci potranno eseguire il processo di codifica e decodifica in tempi ragionevoli. Il problema si complica quando i sistemi di sicurezza devono essere incorporati in dispositivi mobili che presentano una serie di fattori limitanti in termini di dimensione, costi, microprocessori e batterie. Il progetto sviluppato congiuntamente dall'istituto ALaRI dell'USI e dal Laboratorio di Microelettronica della SUPSI ha cercato di rispondere a questa esigenza. Tenendo conto dei problemi particolari dei dispositivi mobili, la strategia è stata di sviluppare dei circuiti integrati e dei programmi specifici in modo da ottenere il miglior sistema di sicurezza possibile senza compromettere il funzionamento o la rapidità degli apparecchi. Il progetto, finanziato dalla Fondazione Gebert Rüf e conclusosi nel corso del 2003, ha aperto una linea di ricerca essenziale per lo sviluppo delle reti senza filo e che offrirà al mercato nuove applicazioni e agli utenti più sicurezza.



L'Istituto ALaRI dell'USI

L'istituto ALaRI (Advanced Learning and Research Institute), fondato nel 1999, è un istituto dell'Università della Svizzera italiana specializzato nella ricerca e programmazione di sistemi embedded, piccoli dispositivi elettronici che dotano d'intelligenza le strutture più diverse, nelle quali vengono inseriti. Una particolare attenzione è data agli studi sulla sicurezza per sistemi mobili e sul "pervasive computing". Le collaborazioni con i politecnici di Milano e Zurigo e i progetti di ricerca in corso, finanziati dall'Unione Europea e dal Fondo nazionale svizzero, hanno permesso ad ALaRI di creare un ponte fra le tecnologie informatiche e quelle elettroniche. Fiore all'occhiello dell'istituto ALaRI è l'Advanced Master of Engineering in Embedded Systems Design, corso internazionale post-laurea dedicato a neolaureati, giovani ingegneri e professionisti che intendono specializzarsi nel campo degli embedded systems. Il successo, conseguito dall'Advanced Master, consentirà di offrire la prima laurea specialistica (Master nella terminologia europea) della nuova facoltà di Scienze informatiche dell'USI: il Master of Science in Embedded Systems Design, accessibile a chi possiede una laurea triennale (Bachelor nella terminologia europea) in facoltà tecniche o scientifiche.

I piccoli sistemi mobili alla ricerca di una grande sicurezza

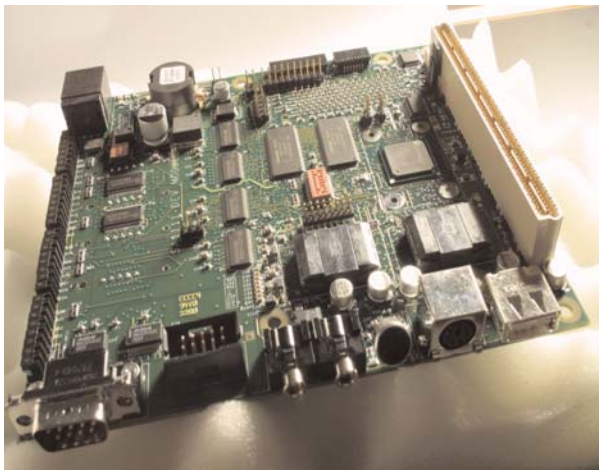
Quali soluzioni concrete si possono sviluppare per la sicurezza dei piccoli sistemi mobili? I ricercatori dell'Istituto ALaRI dell'USI e del Laboratorio di Microelettronica della SUPSI hanno considerato due diversi aspetti strettamente correlati: inserire negli apparecchi mobili degli adeguati sistemi di sicurezza (algoritmi) che rispondessero al meglio alle esigenze di questi piccoli apparecchi, senza dimenticare di adattare la struttura hardware per sostenerne il funzionamento. I ricercatori hanno dapprima analizzato i più recenti algoritmi crittografici, hanno quindi selezionati i sistemi più veloci e li hanno adattati alle esigenze dei sistemi mobili. La seconda parte del progetto consisteva nello sviluppare dei circuiti integrati adatti per supportare lo svolgimento delle operazioni. Le soluzioni proposte dal team di ricerca dell'Istituto AlaRI sono state infine verificate grazie ai prototipi hardware sviluppati presso il Laboratorio di Microelettronica della SUPSI.

Il laboratorio di microelettronica della SUPSI

Il Laboratorio di Microelettronica (LME) della SUPSI si occupa di sviluppo di circuiti microelettronici e di applicazioni microprogrammate. Il LME partecipa a progetti di ricerca applicata (nazionali ed europei) ed ha una funzione di supporto per l'industria locale mediante studi di fattibilità e consulenze. Ha partecipato al programma MICROSWISS 1992-1999 e partecipa alla rete nazionale di competenza ed eccellenza MICROSWISS Network.

La sfida dei ricercatori è stata quindi di trovare il giusto equilibrio fra due alternative difficilmente conciliabili: la sicurezza e l'operatività del sistema. Tanto più complesso è un algoritmo crittografico, quanto più sicuro è il sistema mobile. Un sistema troppo complesso rallenta tuttavia considerevolmente l'operatività.

Tenendo conto di questi fattori, un buon algoritmo crittografico, associato ad un efficiente sistema hardware-software, garantisce agli utenti una completa sicurezza? *"In questa fase di forte espansione dei sistemi di comunicazione mobili* - afferma la prof. Mariagiovanna Sami - *le soluzioni sviluppate dovranno essere continuamente ridefinite. La protezione dei dati sarà sempre un equilibrio che si giocherà tra sistemi semplici, rapidi e poco sicuri e sistemi complessi e che richiedono uno sviluppo attento di hardware e software."* In altri termini, non esiste una soluzione definitiva e per ogni apparecchio o situazione si dovrà trovare e ritrovare il giusto equilibrio. Per questa ragione i ricercatori hanno anche sviluppato delle linee guida sulla sicurezza applicabili alla maggior parte dei sistemi mobili e leggeri. I risultati ottenuti sono stati promettenti, consentendo la continuità della ricerca e il perseguimento di nuovi importanti obiettivi: lo sviluppo di soluzioni proponibili al mercato e l'estensione dei sistemi di sicurezza anche ai più piccoli e diffusi dispositivi digitali: i telefoni cellulari.



Nella foto: sviluppando specifici algoritmi crittografici e opportuni circuiti integrati è possibile rendere sicuri anche i piccoli sistemi mobili.

Informazioni
Prof. Mariagiovanna Sami
Università della Svizzera italiana
Advanced Learning and Research Institute (ALaRI)
Tel.: + 41 91 912 47 06
e-mail: sami@alari.ch

Indirizzi Web:
Università della Svizzera italiana: www.unisi.ch
Istituto ALaRI: www.alari.ch
Laboratorio di Microelettronica (LME): www.dti.supsi.ch
Gebert Rüf Stiftung: www.grstiftung.ch

I M P R E S S U M

Il progetto del mese
No. 7 - febbraio 2004
on-line: http://www.ticinoricerca.ch/progettomese.htm

via Lambertenghi 10a, CH- 6904 Lugano
Tel. +41 91 912 46 17; e-mail: sr@unisi.ch