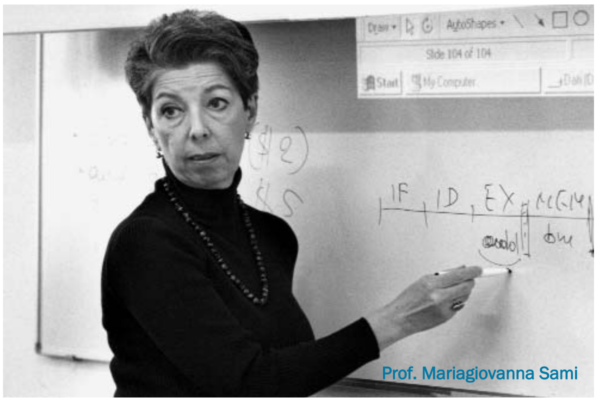
Is there security in mobile communication?

"Only connect" may be said to be today's motto. The next stage after the cell phone is the wireless network, through which we can link up to the Internet wherever we are. An essential desideratum when a wireless system is created is the guarantee of personal data protection. Security in mobile systems is one problem tackled by AlaRI, an institute of the Università della Svizzera italiana (USI) and by the Microelectronics Laboratory at SUPSI. Together, and with the support of the Gebert Rüf Stiftung, they have developed a project that puts forward innovative solutions.

Data security has been a major concern ever since man first started record keeping and information transfer. Since that time, in fact, experts have taken it in turn to play two ostensibly antithetical roles: inventing safer and safer protection systems and perfecting the knack of accessing information by breaking the code (without knowing the password). With the escalation of wireless communication systems, the need to assure confidentiality of information has become essential. Day in day out, we hear of hackers who get through to secret information, who get hold of credit card numbers, or even raid documents archived on personal computers. The simple fact of being on-line makes you prone to this sort of assault. Cryptography has been seen as the immediate answer to this, a solution that grants security to information exchanged over a wireless system. However, developing a cryptographic algorithm is not the final key to all such problems. For a sophisticated code to work, a very powerful microprocessor is required. Therefore each time a user is looking for a reliable system he will indeed get one that is more secure, but slower; only the fastest computers can carry out the coding and decoding processes in reasonable time. The whole situation is further complicated as soon as security systems are to be built into mobile devices (portable PCs, cell phones and Personal Digital Assistants) that are limited in terms of size, cost, microprocessors and batteries. All of these factors put a damper on any security system. Set up by AlaRI (an institute of the University of Lugano - USI) in association with the Microelectronics Laboratory, SUPSI, the project has attempted to overcome this limitation. Bearing in mind the peculiar features of mobile devices, the strategy has been aimed at developing integrated circuits and specific programmes so as to obtain the best possible security system without endangering the working and speed of the devices. The recipient of financial backing from the Gebert Rüf Foundation, this project was completed during 2003. It has pioneered a new line of research that is essential to the development of wireless networks, providing the market with new applications, and the user with better security.


Prof. Mariagiovanna Sami

The ALaRI Institute, USI

Established in 1999, ALaRI (Advanced Learning and Research Institute) is an institute of the Università della Svizzera italiana specialising in research into, and design of, embedded systems, minute electronic devices capable of endowing with intelligence the most disparate structures into which they are fitted. Its investigations bear more particularly on the security of mobile systems and on pervasive computing. Through its collaborative links with Milan's Politecnico and the Federal Institute of Technology, Zurich, as well as its active research programmes (supported by European funding and by the Swiss Science Foundation), ALaRI has been able to bridge the gap between information technologies and electronic technologies. AlaRI takes particular pride in its Advanced Master of Engineering in Embedded Systems Design, an international graduate programme addressing young engineers and professionals wishing to acquire specific skills in the field of embedded systems. In the wake of the success enjoyed by the Advanced Master's programme, USI's new Faculty of Informatics will launch the academic degree programme, Master of Science in Embedded Systems, intended for candidates holding a Bachelor's degree from a technical or science Faculty.

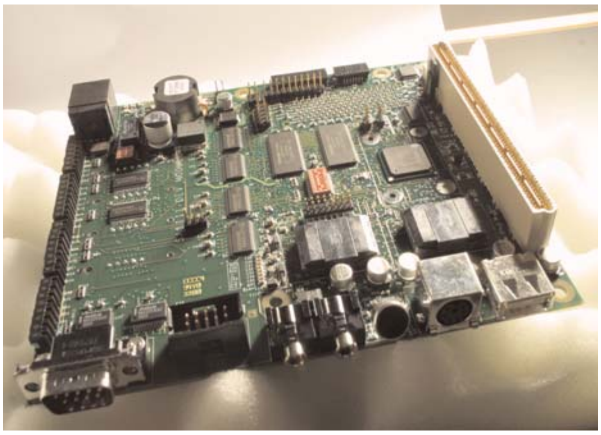
Little "mobile systems" in search of greater security

What concrete solutions can we think up to make small mobile systems secure? Researchers at the ALaRI Institute, USI, and at the Microelectronics Laboratory, SUPSI, have contemplated two separate but closely interdependent aspects. One operation consists in installing into the mobile devices appropriate security systems (algorithms) that best answer the needs of these tiny mechanisms. The second attempts to adjust the hardware structure in order to support its functioning. Researchers first analysed the latest cryptographic algorithms; then they picked the fastest systems and adapted them to the needs of the mobile systems. The second part of the project was devoted to building integrated circuits well-equipped to facilitate their operations. The solutions put forward by the ALaRI research team were checked against the hardware prototypes developed at the Microelectronics Laboratory, SUPSI.

The Microelectronics Laboratory, SUPSI

The Microelectronics Laboratory (LME), SUPSI, deals with the creation of microelectronic circuits and micro-programmed applications. LME takes part in applied research projects (on a national and on a European scale) and acts in a support role to local industry by providing feasibility studies and consultancy services. It participated in MICROSWISS 1992-1999 and is an active member of the national centre for competence and excellence known as MICROSWISS Network.

The tough challenge facing the researchers was therefore to strike a fair balance between two scarcely compatible alternatives: a cryptographic algorithm becomes safer the moment it grows more complex; yet an overly complex system is bound to slow down a mobile system's operability quite considerably. The end result was the simultaneous creation of a particular integrated circuit suitable to perform with the most advanced algorithms hand-picked especially for mobile systems. Given these premises, does a good cryptographic algorithm, matched up with an efficient hardware-software system, guarantee its users full security? "*At a time when mobile communication systems are thriving and booming* - answers Mariagiovanna Sami - *whatever solutions we work out must be continuously re-defined. Data protection will continue to play a* In *hard game of balance between simple, fast and small secure systems and complex systems requiring a careful and subtle development of hardware and software. "Put it another way, there is no hard and fast rule; but one must struggle to achieve the right balance for every appliance or situation anew. This is why one of the tasks that our researchers have had to take up has been the drafting of guidelines on security to cover most mobile and lightweight systems."*



Small-sized mobile systems can be made secure by developing specific cryptographic algorithms and appropriate integrated circuits.

The results achieved have been so promising as to ensure continuity in research along the same path. The team members are confident that they can now aim for viable solutions suitable for the market; and so broaden the proposal for security systems and extend it to smallest and widespread digital devices: namely cell phones.

For more details, please contact:

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

Web addresses:

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

IMPRESSUM

Project of the month
No. 7 - February 2004
on-line: http://www.ticinoricerca.ch/progettomese.htm

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