

Calipso RFP – Research Proposal sami20030514

Abstract

IPSec is an important part of the Mobile IPv6 protocol that can be used to provide security services for the IP datagrams being sent over the network. The aim of this project is to provide a set of guidelines for IPSec configuration and to study possible optimizations of the protocol in a Mobile IPv6 environment. To provide an experimental basis for definition of such guidelines, a test network made of Intel SA-1110 boards equipped with wireless cards will be built and specific performance figures will be collected.

Project description

Introduction

The proposal focuses on a relevant aspect of mobile IPv6, namely security. While the security layer (IPSec) is not necessarily used in all applications of IPv6, its relevance – in particular where mobile systems are concerned – is ever increasing, and in fact its implementation may be critical for large segments of users.

The subject of the present proposal deals with the Security layer IPSec in the Mobile IPv6 environment. IPSec is an important and mandatory-to-implement part of IPv6; it is devised to protect and authenticate – respectively through encryption and digital signature functions – the IP datagrams sent over the network. Security is increasingly relevant for large numbers of users, due to transmission of sensitive data over the Internet in applications that go from e-commerce to e-banking, from e-health care to e-government, just to mention a few instances. The use of mobile systems further enhances the critical importance of security, since such systems will be used most often in “unprotected” environments where malicious attacks are most likely. Unluckily, enabling IPSec may lead to severe device performance degradation, due to the computational load introduced by the crypto-algorithms used in the protocols, such as to make the solution scarcely acceptable to end users; the negative impact on battery life cannot be ignored as well. Achieving higher performances even in the presence of cryptographic techniques involves a number of aspects, from efficient algorithm implementation to adoption of ad-hoc hardware and to efficient protocol design. A further problem relates to interoperability of the various IPv6 implementations – and in particular of the IPSec protocol suite: interoperability can be evaluated through accurate tests in mixed environments (i.e. in environments containing devices with different operating systems and implementations of the protocol). In the case of mobile systems, heterogeneity of the devices is an intrinsic characteristic of the operating environment even for the individual user who may switch from a laptop to a hand-held device and the requirement that security be maintained through the various implementations is mandatory.

A further aspect of interest where IPSec is concerned arises when one considers the possible use of IPComp, i.e. the Ipv6 protocol providing the capability of compressing prior to transmission over the network. Evaluating the overall impact of this protocol can be very important for mobile systems, not only from the performance (network/device) stand point, but in particular with reference to the relationships between encryption and compression, in order to check on their mutual impact as well as on the global impact on the application.

Aim of the project

The present proposal fit in a wider research carried out at ALaRI with final goal of defining hardware-software architectures leading to optimized implementation of the IPSec protocol, through actions both at the operating system level and at the coprocessor (hardware accelerator)

level. The present proposals focus on mobile systems and are more limited in scope and duration (one year). The main figure of merit envisioned for optimization where networking is concerned is that of *network performances*; while of course even in the case of mobile systems network performances are very relevant, we will here take into account also other considerations, such as *power consumption* and the relatively limited capacity of the involved CPU (at least for some of the mobile systems), making it mandatory to find manageable *configurations* of IPSec capable of granting high security while not saturating the device's capacities. In the project proposal here presented, we focus more specifically on software aspects, from optimization of encryption/decryption algorithms to operating system's support of communications between CPU and crypto accelerators present in the hardware architecture and to evaluation of the effects of IPComp on security. Relating to *mobile* systems will lead to taking into account the characteristics of both the hardware that may be typically used in such systems and of the operating systems (e.g., Windows CE.NET) adopted.

As a first step of the project, a critical analysis will be carried out to evaluate performances of IPSec in various conditions (such as, for example, bandwidth available, alternative encryption techniques adopted, etc.). Previous experience on this point has been obtained at ALaRI with reference to IPSec for an IPv4 network. Within the project here proposed, a testbed for Mobile IPv6 will be created, consisting of a small network on which it will be possible to evaluate and optimize some of the most relevant parts of Mobile IPv6. The testbed network will be created based on Intel SA-1110 boards on which Microsoft Windows CE.NET operating system will be installed. Wireless devices will be introduced to configure the wireless network (the network devices may be the same Intel boards equipped with wireless network cards). Choice of the Intel SA-1110 board is due to the experience developed thanks to collaboration with Intel (Intel donated the boards) during which, in particular, optimization of crypto algorithms and analysis on OS requirements for security were carried out. The testbed will support IPComp evaluation as well as IPSec evaluation.

Using such testbed network the following experiments will be performed:

- Profiling various IPSec configurations in the Mobile IPv6 environment. This will allow evaluating the security/performance tradeoffs of said configurations, including the use of different encryption algorithms proposed at international level and of various optimizations of such algorithms. The results of this part of the project will be a set of configuration proposals for different use cases. The profiling phase will also provide the necessary information to specify functional and non-functional requirements of possible hardware accelerators.
- Evaluating the interoperability of different IPSec stack implementations. This requires setting up some parts of the system with different operating systems (with particular attention to embedded and mobile solutions, these being the envisioned target systems). Simultaneously, policies for hardware accelerator management by the operating system will be defined and evaluated by simulation¹
- Evaluating the impact of the IPComp compressibility test on the system performance/power consumption, also with relation to IPSec actions and performances. This should allow verifying whether it is necessary to develop a "smarter" method for deciding a priori which data payloads should be compressed, rather than the present trial-and-error approach.

¹ While implementation of a crypto-coprocessor by means of an FPGA is within the ALaRI projects, it is not part of the present proposal and its completion is not envisioned within the project's timeline.

At the end of this project, a set of guidelines for optimum configuration of IPSec in a mobile environment and for related hardware accelerator management will be available. The analysis will also provide an evaluation of actual usability of IPSec in the case of relatively small devices.

Resources

The ALaRI Institute, presenting proposal **sami20030514.doc**, is a research and training Institute at the University of Lugano (Switzerland), specifically dealing with problems in Embedded Systems design and providing a Master in Embedded Systems Design. The initiative sees the collaboration of a number of European and US Universities (including in particular Politecnico di Milano, Italy, and the Federal Technical Universities of Zurich and Lausanne, Switzerland) as well as of Research centers and high-tech companies. Since its opening in September 2000, ALaRI has been particularly active in the area of security; in this domain, two patents have been filed and some papers have been published. A list of publications and patents is appended.

The project will be developed under the supervision of the ALaRI Scientific Director, prof. Mariagiovanna Sami, and of lecturers belonging to the ALaRI international faculty (specifically, prof. Breveglieri of Politecnico di Milano and prof. Parr of Bocum University, lecturing on security and guiding students' research on this subject); activities will be carried out by a PhD student, as well as by four Master students whose Master projects will focus on this particular subject. Actually, the project will involve interaction also with other groups active within ALaRI on research in the area of security, in particular where definition and design of crypto-coprocessors is concerned.

Hardware resources necessary for development of the project are already available in the ALaRI laboratory (Intel SA-1110 boards with the relative companion boards (SA-1111), switches, PCs).

Development of the project will require availability of source code of the network stack (including the Mobile IPv6 layer) and of the Windows CE.NET operating system.

Deliverables

A final report plus source code and configuration files. Intermediate reports can be provided upon request.

Timeline

July – October 2003: documentation and training phase for the master students (who will come at mid-September: four students provided with basic knowledge necessary to start with the project will be immediately identified). Simultaneously, the possible hw/sw architectures supporting efficient implementations of IPSec will be explored.

November 2003 - February 2004: network setup and testing. Optimization of security algorithms and theoretical aspects of impact of compression on security will be studied.

March – June 2004: IPSec configurations will be evaluated and problems related to interoperability will be taken into account. Interaction between CPU and a possible crypto-coprocessor will be defined, and support by the operating system will be designed.

Contacts

Research proposal **sami20031405** is submitted by Prof. Mariagiovanna Sami as Scientific

Director of ALaRI.

Application contact details are:

E-mail: sami@ALaRI.CH

Phone: +41 91 9124706

Fax: +41 91 9124647

Mail address: ALaRI, University of Lugano
Via Lambertenghi 10 A

ALaRI Relevant Publications

A. Bona, ALaRI, CH, M. Sami, D. Sciuto and V. Zaccaria, Politecnico di Milano, IT, C. Silvano, Milano U, IT: R. Zafalon, STMicroelectronics, IT: "An Instruction-level Methodology for Power Estimation and Optimization of Embedded VLIW Cores", *proc. DATE 2002, Paris, March 4-8 2002*

W. Fornaciari, F. Salice, Politecnico di Milano, IT, U. Bondi, ALaRI, CH, E. Magini, Omnitel, IT: "Development cost and size estimation starting from high level specifications", *proc. Ninth IEEE International Symposium on Hardware Software Codesign, Copenhagen, April 25-27 2001*

M. Macchetti, and S. Marchesin, ALaRI, CH, G. Bertoni, L. Breveglieri Politecnico di Milano, IT, P. Fragneto, STMicroelectronics, IT: "Efficient Software Implementation of AES on 32-bits Platforms", *Proc. CHES 2002, Redwood Shores, August 13-15 2002*

Antonio Minosi, Aris Martinola, Srinivas Mankan, ALaRI, CH, Mauro Prevostini, Università della Svizzera Italiana, Lugano, CH: "System-level design of embedded applications by UML: the Wireless Meter Reading case", *Proc. MSy'02 Workshop, Winterthur, October 3-4 2002*

M. Macchetti, ALaRI, CH, G. Bertoni, Politecnico di Milano, IT: "Hardware Implementation of the Rijndael Sbox: a Case Study", To be published, *ST Journal of System Design*

F. Cassoli, F. Polloni, S. Marchesin, M. Macchetti, ALaRI, CH, G. Bretoni, L. Breveglieri, Politecnico di Milano, IT, P. Fragneto, STMicroelectronics, IT: "Efficient C implementation of the ECC and AES cryptographic systems" *Proc. Technology Leadership Day organized by the MicroSwiss Network, Fribourg, October 10 2001*

Umberto Bondi, Giuseppe Saraceno, ALaRI, CH, Luca Mazzoni, ACCENT, Agrate, IT: "The «Smart Card System» project: From «plastic money» to mobile transaction support" *Proc. Technology Leadership Day organized by the MicroSwiss Network, Fribourg, October 10 2001*

A. Bircan, M. Macchetti, ALaRI, CH, G. Bertoni, L. Breveglieri, V. Zaccaria, Politecnico di Milano, IT, P. Fragneto, STMicroelectronics, IT: "About the Performances of the Advanced Encryption Standard in Embedded Systems with Cache Memory" To be presented at the *IEEE International Symposium on Circuits and Systems, Bangkok, May 25-28 2003*

L. Salvemini, M.G. Sami,; D. Sciuto, C.Silvano, C.; Zaccaria, R.Zafalon: "A Methodology for efficient architectural exploration of energy-delay trade-offs for embedded systems", *Proc. SAC 2003, Melbourne, FLA, March 2003, pp. 672-678*
