

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

UPGRADE is the anchor point for UPENET (UPGRADE European NETWORK), the network of CEPIS member societies' publications, that currently includes the following ones:

- **Mondo Digitale**, digital journal from the Italian CEPIS society AICA
- **Novática**, journal from the Spanish CEPIS society ATI
- **OCG Journal**, journal from the Austrian CEPIS society OCG
- **Pifororiki**, journal from the Cyprus CEPIS society CCS
- **Pro Dialog**, journal from the Polish CEPIS society PTI-PIPS

Publisher

UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by **Novática** (<http://www.ati.es/novatica/>), journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática* <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by **Novática**, and in Italian (summary, abstracts and some articles online) by the Italian CEPIS society ALSI (<http://www.alsi.it/>) and the Italian IT portal **Tecnoteca** (<http://www.tecnoteca.it/>)

UPGRADE was created in October 2000 by CEPIS and was first published by **Novática** and **INFORMATIK/INFORMATIQUE**, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

Editorial Team

Chief Editor: Rafael Fernández Calvo, Spain, rfoalvo@ati.es

Associate Editors:

François Louis Nicolet, Switzerland, nicolet@acm.org
Roberto Carniel, Italy, carniel@dgt.uniud.it
Zakaria Maamar, Arab Emirates, Zakaria.Maamar@zu.ac.ae
Soraya Kouadri Mostéfaoui, Switzerland, soraya.kouadrimostefaoui@unifr.ch

Editorial Board

Prof. Wolfried Stucky, CEPIS Past President
Prof. Nello Scarabottolo, CEPIS Vice President
Fernando Piera Gómez and Rafael Fernández Calvo, ATI (Spain)
François Louis Nicolet, SI (Switzerland)
Roberto Carniel, ALSI – Tecnoteca (Italy)

UPENET Advisory Board

Franco Filippazzi (Mondo Digitale, Italy)
Rafael Fernández Calvo (Novática, Spain)
Veith Risak (OCG Journal, Austria)
Panicos Masouras (Pifororiki, Cyprus)
Andrzej Marciniak (Pro Dialog, Poland)

English Editors: Mike Andersson, Richard Butchart, David Cash, Arthur Cook, Tracey Darch, Laura Davies, Nick Dunn, Rodney Fennemore, Hilary Green, Roger Harris, Michael Hird, Jim Holder, Alasdair MacLeod, Pat Moody, Adam David Moss, Phil Parkin, Brian Robson

Cover page designed by Antonio Crespo Foix, © ATI 2005

Layout Design: François Louis Nicolet

Composition: Jorge Llácer-Gil de Ramalos

Editorial correspondence: Rafael Fernández Calvo rfoalvo@ati.es

Advertising correspondence: novatica@ati.es

UPGRADE Newslist available at

<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

Copyright

© Novática 2005 (for the monograph and the cover page)

© CEPIS 2005 (for the sections MOSAIC and UPENET)

All rights reserved. Abstracting is permitted with credit to the source. For copying, reprint, or republication permission, contact the Editorial Team

The opinions expressed by the authors are their exclusive responsibility

ISSN 1684-5285

Monograph of next issue (June 2005):
"Free Software Engineering"
(The full schedule of UPGRADE is available at our website)

Monograph: IPv6 - More than A Protocol (published jointly with Novática*)

Guest Editors: *Jordi Domingo-Pascual, Alberto García-Martínez, and Matthew Ford*

- 2 Presentation
IPv6: A New Network Paradigm — *Jordi Domingo-Pascual, Alberto García-Martínez, and Matthew Ford*
- 5 IPv6 Deployment State 2005 — *Jim Bound*
- 9 Internet Protocol version 6 Overview — *Albert Cabellos-Aparicio and Jordi Domingo-Pascual*
- 15 Transition of Applications to IPv6 — *Eva M. Castro-Barbero, Tomás P. de Miguel-Moro, and Santiago Pavón-Gómez*
- 19 Service Deployment Experience in Pre-Commercial IPv6 Networks — *Rüdiger Geib, Eduardo Azañón-Teruel, Sandra Donaire-Arroyo, Aurora Ferrándiz-Cancio, Carlos Ralli-Ucendo, and Francisco Romero Bueno*
- 27 Security with IPv6 — *Latif Ladid, Jimmy McGibney, and John Ronan*
- 31 Tools for IPv6 Multihoming — *Marcelo Bagnulo-Braun, Alberto García-Martínez, and Arturo Azcorra-Saloña*
- 36 NEMO: Network Mobility in IPv6 — *Carlos J. Bernardos-Cano, Ignacio Soto-Campos, María Calderón-Pastor, Dirk von Hugo, and Emmanuel Riou*
- 43 IPv6 Status in The World and IPv6 Task Forces — *Jordi Palet-Martínez*

MOSAIC

- 49 Mobile Networks
QoS and Micromobility Coupling: Improving Performance in Integrated Scenarios — *Luis-Angel Galindo-Sánchez and Pedro-Manuel Ruiz-Martínez*
- 56 Performance Analysis
The Design of A Dynamic Zero-Copy Communication Model for Cluster-Based Systems — *Appolo Tankeh and Dominique A. Heger*
- 64 News & Events: European Commission; ECDL; EUCIP - AICA, Italy; IPv6 Summit - ATI, Spain

UPENET (UPGRADE European NETWORK)

- 66 From **Pro Dialog** (PTI-PIPS, Poland)
IT Teaching
Today's Concepts of Teaching Computer Science Basics and Occupational Profile of Software Engineer — *Henryk Budzisz, Krzysztof Kadowski, and Walery Susłow*
- 73 From **Novática** (ATI, Spain)
Information Society
Beyond The Internet: The Digital Universal Network — *Fernando Sáez-Vacas*

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>, and in Italian (online edition only, containing summary, abstracts, and some articles) by the Italian CEPIS society ALSI (*Associazione nazionale Laureati in Scienze dell'informazione e Informatica*) and the Italian IT portal Tecnoteca at <http://www.tecnoteca.it/>.

Security with IPv6

Latif Ladid, Jimmy McGibney, and John Ronan

This paper presents an argument for the deployment of IPv6 (Internet Protocol version 6) as the key enabler for restoration of the end-to-end model, and how this impacts the current state of network security, so that IPv6 security issues can be understood in this context. It introduces IPsec (Secure Internet Protocol) and discusses its impact and the benefits it brings, and briefly discusses some security aspects of IPv4 (Internet Protocol version 4) and IPv6 co-existence.

Keywords: IPsec, IPv6, Security.

1 Introduction

The Internet today provides generic communication infrastructure for packet-based communications. Several edge networks that carry both business and non-business oriented traffic communicate with each other via this public infrastructure. This infrastructure is based on an agreed suite of protocols, generally denoted TCP/IP (Transmission Control Protocol/Internet Protocol) [1][2] in reference to the two most significant of these protocols.

Currently, version 4 of the Internet Protocol (known as IPv4) is the *de facto* standard for Internet connectivity. Internet standards emerged from research work in the United States, sponsored by DARPA (Defense Advanced Research Projects Agency), a US defense research agency. TCP/IP became popular in universities and was incorporated into the UNIX family of operating systems used in university computer science faculties. Over time TCP/IP became a worldwide network linking universities and research bodies, and became the foundation for the web.

With IPv4, there have been a variety of exploits on end and intermediate systems due to protocol design as well as implementation problems resulting in substantial loss of revenues. IPv4 has therefore been supplemented by the IPsec (Secure Internet Protocol) protocols to provide for security needs at the network layer. The new version of the Internet Protocol, IPv6 (Internet Protocol version 6) [3], by contrast, has mandated support for IPsec as part of its basic design.

IPsec helps serve the data privacy and integrity needs of the data in transit across the Internet in addition to providing authenticity of the data's origin. Traditionally, following the definitions of ITU (International Telecommunications Union [4]), the term security addresses requirements of *privacy* (the protection of the association of the identity of users and the activities performed by them), *data confidentiality* (the protection against unauthorized access to data contents), *authentication* (proof that the claimed identity of an entity is true), *integrity* (that data have not been altered in an unauthorized manner) and *availability* (no denial of authorized access). At the network layer, IPsec provides for the first four of these needs. Consequently, IPv6 provides for these requirements too.

This paper is structured as follows: Section 2 describes IPsec along with an overview of the current state of the IP protocol and the advantages IPv6 has to offer over IPv4 (Internet Protocol version 4), from a security perspective. The next section presents a brief discussion of security as-

pects of IPv4-IPv6 coexistence, and we finally draw conclusions in Section 4.

2 Security Challenges

As computing and computer-based communications gain an ever-increasing foothold in our lives, the need for security is paramount. The field of security incorporates con-

Latif Ladid is the current Chair of the European IPv6 Task Force, President of the IPv6 Forum, Trustee of the Internet Society – ISOC and a Researcher on multiple European Commission IST projects focused on Next Generation Technologies. Latif has worked in various managerial and marketing positions at Nixdorf Computers in Germany, and Hewlett-Packard in the Middle East, as International Sales Manager at ComputerLand Europe in Luxembourg, and as Managing Director of ComputerLand Switzerland. From 1992 to 1998, he was with the Canadian Internet and internetworking specialist, DEVELCON, where he served as Vice President of Sales and Business Development. In 1998, Latif joined Telebit Communications A/S as Vice President, Sales EMEA. He has also served, from 1996 to 1998, as chairman of Global-ISDN. He holds an ESCAE (France), and did post-graduate work in business and administration in the UK. <latif.ladid@ipv6forum.com>

Jimmy McGibney is a lecturer in Applied Computing at Waterford Institute of Technology, Ireland, where he gives courses in security and distributed systems and carries out research with the Telecommunications Software & Systems Group. He is also studying for a PhD at University College Dublin on service models for intrusion detection. He received his BE in 1992 from University College Dublin and his MEng in 1995 from Dublin City University. Between 1994 and 2000, he worked in the telecommunications industry, both as a software developer as a researcher on collaborative projects. <jmcgibney@tssg.org>

John Ronan is a Researcher in the Telecommunications Software & Systems group in Waterford Institute of Technology, Ireland. He received his BSc from Waterford Institute of Technology in 1998 and his Masters Degree in 2000. Since then he has worked on several IST and Irish Government funded projects in the areas of Network Security, IPv6, Wireless Network Technologies, Network Testbeds & Advanced Grid systems and development of Billing and Security mechanisms for IP services. He also lectures in the Computing Department on Networks and Communications. <jronan@tssg.org>

cepts of authentication (including identification and trust), confidentiality, integrity, availability, access control and non-repudiation. ITU defines security services along these lines. In general, such security requirements are critical for enterprises that use the Internet or Internet-like infrastructure for their day-to-day business.

It is fair to say that a constant war is being waged between those who own and manage systems and those who wish to attack them. Access to the Internet is relatively easy and cheap, with users enjoying a high level of anonymity if desired. In many ways, those who wish to breach security have all the aces:

- The standards used for basic Internet protocols are public. This means that attackers know much more about how the Internet works than they would if a closed network were used.
- Even though the number and diversity of systems is increasing, as is their complexity, the level of technical sophistication required to carry out attacks is falling [5].
- Modern systems in general are very complex, operating at several layers. Complexity usually makes for bad security. The sheer number of ways in which modern systems can be used makes comprehensive testing an extremely difficult problem, and production systems almost inevitably have flaws.
- The speed of development of the Internet has been huge. This means that much of the software used was developed with its main functionality in mind, with less thought being given to the security aspects. The most secure systems are those that were designed with security in mind from the start. IPv4, for example, was not designed with security as a priority.
- The trend toward code mobility in the past decade has provided all sorts of opportunities for the development of viruses and worms, which are in effect autonomous agents that, once released, can reproduce. The resulting combinatorial explosion allows the attacker's wishes to be carried out on a very large scale.

These attacks manifest themselves as identity impersonation (referred to as spoofing), loss of privacy, loss of data integrity (e.g. credit card transaction details being modified in transit), communications monitoring, and denial-of-service. Such attacks are the result of discovering exploits that emerge from the flaws in the basic protocol design (e.g. WEP, Wired Equivalent Privacy, in IEEE 802.11, also known as WiFi, Wireless Fidelity) or from the incorrect implementation of protocols, applications, and operating systems (e.g. not enforcing the use of strong encryption in a WiFi network, or the selection of a weak cipher on an encrypted communications link). Exploiting such discoveries will remain as long as protocol implementations do.

Defenses available to those charged with managing computer systems include the strict enforcement of a comprehensive security policy (the importance of having a policy and enforcing it cannot be overstated), avoidance of insecure technologies and protocols where possible, use of the best available and most secure technologies, and keeping up to date with events in the world of security, especially in order to patch systems when a new exploit is discovered. Just as attackers quickly share information about new flaws

using the Internet, system administrators can be warned almost immediately and patches disseminated quickly.

3 Network Layer Security

3.1 IPsec Overview

The term IPsec refers to a suite of protocols from the IETF (Internet Engineering Task Force) providing network layer encryption and authentication for IP-based networks. The objective of IPsec is to authenticate and/or encrypt all traffic at the IP level. As it operates at the IP level, it is independent of applications and transport.

IPsec first arose from a workshop held by the Internet Architecture Board (IAB) in 1994 on security in the Internet architecture, from which recommendations were published in RFC 1636. The key IPsec specifications are provided in:

- RFC 2401 (Security architecture).
- RFC 2402 (Authentication).
- RFC 2406 (Encryption).
- RFC 2408 (Security Associations & Key management).

The main present-day use of IPsec is in establishing virtual private networks for connecting remote offices and users to the enterprise using the public Internet, for low-cost remote access for teleworkers (via local call to ISP, Internet Service Provider) and for extranet connectivity (secure communication with partners, suppliers and so on).

IPsec is implemented by means of one of two alternative IP header extensions. The first, Authentication Header (AH) [6], provides authentication but not privacy. The alternative, Encapsulating Security Payload (ESP) [7], provides packet encryption and, optionally, authentication. AH adds an additional header field to the traditional IP packet, normally based on a message authentication code (key-based hash of the packet data). With ESP, the content is encrypted and encapsulated between header and trailer fields.

To use IPsec, a pair of hosts must first negotiate a Security Association (SA). This acts as a virtual connection, for which various attributes are set such as the type of protection, keys, and cryptographic algorithms to be used. An SA specifies a one-way relationship, so two SAs are required for a duplex connection. An SA caters for AH or ESP.

IPsec can be deployed in either transport mode or tunnel mode. Transport mode is typically used for end-to-end communication and protects the IP packet payload only – a consequence of this is that the traffic pattern between hosts is not protected, but there is no need for involvement of intermediate devices (that may not be trusted). Tunnel mode, by contrast, is typically used for connecting secure gateways (e.g. firewalls or routers) and protects the entire IP packet, including the header. A significant advantage of tunnel mode is that hosts do not need to be IPsec-enabled, which will often be the case in mixed IPv4-IPv6 environments.

Cryptographic key management is a significant issue with IPsec – i.e. how to generate and distribute secret keys? Within a small organization, the system administrator can do this manually, but it does not scale well. A number of automated approaches exist, most notably Internet Security Association and Key Management Protocol (ISAKMP) [8] and Internet Key Exchange (IKE) [9].

While the objective of introducing security mechanisms

like IPsec is to ensure data privacy and authenticity, the mere usage of such mechanisms may not render the security at other layers (application, transport, etc.) redundant and ensure end-to-end communications are fully secure, forever. The framework provided by IPsec is generic enough to allow additional complementing security mechanisms (like PGP, S/MIME, etc.).

In conclusion, it can be said that IPsec provides a level of security for all applications and hosts and allows the deployment of new applications and the addition of new on-site hosts without needing any extra configuration. It also readily supports the secure addition of off-site users and partners. A further benefit of IPsec is that the architecture is independent of specific cryptographic methods and new, stronger, algorithms can be used as they become available. Note though that IPsec cannot strictly provide user level authentication, but rather packet source (i.e. host) authentication. This is not a concern if the user is working, say, at a Windows desktop, but would be an issue with a multi-user OS.

It is worth noting that, though IPv6 mandates support for IPsec, particular performance-sensitive IPv6 deployments may choose not to use IPsec or just to use it for authentication. Security always involves some kind of trade-off; the benefits of IPsec should be weighed against resulting throughput or processing overhead to assess needs for each situation.

3.2 Security with IPv6

IPsec is mandated in the protocol. Every implementation claiming support for IPv6 is expected to provide IPsec as part of the protocol.

To effectively use IPsec, there is a need for a key management framework (ISAKMP and IKE) to make an end-to-end secure communication truly happen. Such key management mechanisms, though used extensively with IPsec, are independent and are not a part of IPv6. Therefore, Public Key Infrastructures (PKIs) are required for wide scale deployment. PKIs function as authoritative sources for certified keys of hosts and services on the Internet and are somewhat similar operationally to the Domain Name Service (DNS). There is no accepted standard for PKI, yet. It is also very unlikely that there will be a single PKI for the entire Internet; it is neither acceptable operationally nor does it go with the Internet philosophy. Present day implementations use static key allocations and often do a manual exchange of keys.

An alternative for the provision of public-key authentication for IP addresses without relying on any trusted third parties, PKI, or other global infrastructure, is the use of Cryptographically Generated Addresses (CGAs). CGAs are currently under investigation in the IETF, and provide an intermediate level of security below strong public-key authentication and above routing-based methods. The idea is to form the last 64 bits of an IPv6 address, the interface identifier, by computing a 64-bit one-way hash of the node's public signature key. The node signs its data with the corresponding private key and sends the public key along with the signed data. The recipient hashes the public key and compares the hash to the interface identifier of the source IP address before verifying the signature on the transmitted data.

This prevents anyone except the node itself from sending data for its address. As only IPv6 addresses have a 64-bit interface identifier, CGAs consequently can only be used with IPv6.

In many instances, a constant 64-bit interface identifier is used to form a global IPv6 address (stateless address auto configuration). In the event that secure transfers are not using tunnel mode, the IPv6 source and destination addresses are visible rendering the fact that the occurrence of the session itself can be noticed by an intermediate snooper. In cases where the devices move between networks, it then becomes possible to track the movement of the device and hence the sessions it participates in.

This is considered a serious threat to privacy, especially for mobile and wireless users. RFC 3041 is proposed as a solution to this. The solution involves the use of a pseudorandom number as an interface identifier that changes over time, to generate an IPv6 address. This makes it difficult for an eavesdropper to correlate activity based on an address and hence makes it extremely difficult (if not unfeasible) for an eavesdropper to detect or track a given device (and thus potentially a user).

One somewhat subtle aspect of the security of IPv6 lies in the greatly expanded address range. With IPv4, scanning a network or subnet is very straightforward; all the attacker with access needs to do is find the network address and scan all available hosts. With widely available tools, such as *nmap*, he or she can quickly build up a profile of machines running, their operating systems and the services that are running on them, including proxies, weak services and back doors. As well as manual attacks, many automated attacks use scanning – in particular recent worms like Blaster and Slammer have propagated by scanning the network for specific vulnerable ports through which to gain access.

The reason this can be done quickly is that the range of addresses to be scanned is quite small. With IPv6, by contrast, this kind of "brute force" scanning is impossible in practice. If addresses are distributed sparsely over the allocated range, the sheer number of addresses allocated to a network segment means that any scanning tool will get bogged down simply searching for an address that responds. This should make scanning worms infeasible.

4 IPv4-IPv6 transition

The transition from IPv4 to IPv6 will not of course happen overnight. Organizations that are adopting IPv6 are generally doing so piecewise, largely due to the need to support legacy systems and applications. As with any new technology adoption, it is prudent to proceed with caution and first select pilot portions of the network for transition. The effect is that IPv4 and IPv6 will need to coexist for a considerable period of time. This means a dual-stack approach for systems, as well as extensive use of tunneling to deliver IPv6 packets over IPv4 networks (and vice versa). This coexistence phase presents several security challenges.

One of the greatest enemies of security is complexity. In general, the more complex a system is, the greater the risk of human error and the more opportunities exist for attack. For example, dual IPv4-IPv6 routers need more configuration than IPv4-only or IPv6-only routers. [10] report a 50% increase in the number of lines of a typical

firewall configuration when IPv6 is added. The bigger it is, the greater the chance of misconfiguration. In addition, there are now two distinct protocols that can be attacked rather than just one.

Existing IPv4 systems have deployed security technologies that are well understood. Problems have been ironed out over time based on experience. Very strict change control is required as IPv6 is rolled out as experimental deployment can provide ways for long-established safeguards to be bypassed. In fact it is difficult to secure new IPv6 deployments on existing networks as some network protection mechanisms like intrusion detection systems may not yet support IPv6.

5 Conclusion

All end-to-end security models today inherently imply security above the transport layer. PGP, S/MIME and SSL secure higher layer objects and hand them down to the lower layers. Additionally, link layer security mechanisms ensure privacy on the physical communications link, hop-by-hop. IPsec in IPv6 implies security at the network layer. It complements the security mechanisms at the other layers and does not eliminate the need for them.

Users are becoming increasingly mobile and are demanding increasing flexibility, making perimeter security (firewalls, etc) less effective for organizations. In a world where applications are increasingly developed as Web services and port tunneling techniques are well advanced, firewalls, once seen as critical to system security, are increasingly perceived as having limitations [11].

Business applications will benefit by taking advantage of the IPv6 security infrastructure. There is an implicit need here for confidentiality as well as authentication. While security mechanisms today provide for confidentiality of objects, data in transit (transport payload) as well as link layer encryption, there is no specific security mechanism in widespread use at the network layer. The most important benefits for such a specific community are twofold. All sources of data can be authenticated and data confidentiality can be provided with the use of IPsec. Given that such a community most likely already has a specific PKI developed for its own use, deployment of IPsec with this PKI becomes simply a matter of integration of the two.

Network management data is collected to analyze and monitor the traffic across the network. This information is strategic to decision makers in the corporate entity in order to provision a network for future growth. This data could be perceived as commercially sensitive and hence there is a need to secure such data. From the service provider perspective, the capability to collect accurate billing data is critical. This data needs to be secure and authentic; otherwise it could result in inappropriate, inaccurate or non-existent billing with consequent revenue losses (this is perceived to be especially important in the 3G wireless context).

To ensure that every end-to-end session is private in the real sense of the word, a large support infrastructure to support security is required. A public key infrastructure (PKI) is required with the objective of providing certified public keys for every potential IPv6 host. An IPv6 host that intends to communicate securely with a remote host will require to have the latter's public key to begin secure communication.

Alternatively, with the use of CGAs, IPv6 can provide a level of security even without these supporting infrastructures.

In the current Internet scenario, conservative address allocation policies as well as asymmetric user traffic characteristics have resulted in the widespread use of network address translation devices. NATs have broken the peer-to-peer model of the Internet. With its huge address space, IPv6 is expected to re-enable transparent end-to-end applications and services over the Internet. Security will play a vital role in sustaining this attribute.

It is worth concluding with two final remarks. Firstly, despite the promise of a secure world of mobile IPv6-enabled devices communicating end-to-end, facilitated by IPsec, it is important to recognize that no security technology is a panacea – rather, security technologies are only useful in the context of a good, frequently-updated, security policy that is adhered to. For example, having a highly secure IPsec connection will not protect a host against Internet worms if they have penetrated the corporate network [12]. The worm will quite happily make its way down the 'secure' tunnel and attempt to infect the host. Secondly, it should also be recognized that there is no such thing as perfect security – there will always be a need to balance security requirements with business and user demands for flexibility and freedom to get on with what they are doing. The key to effective security is to understand where to strike this balance.

References

- [1] J. Postel. "Internet Protocol", RFC 791, September 1981.
- [2] J. Postel. "Transmission Control Protocol", RFC 793, September 1981.
- [3] S. Deering, R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [4] ITU-T. Security in Telecommunications and Information Technology, International Telecommunication Union, Geneva, 2003.
- [5] C. Manikopoulos, S. Papavassiliou. "Network Intrusion and Fault Detection: A Statistical Anomaly Approach", IEEE Communications Magazine, October 2002.
- [6] S. Kent, R. Atkinson. "IP Authentication Header", RFC 2402, November 1998.
- [7] S. Kent, R. Atkinson. "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
- [8] D. Maughan et al. "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
- [9] D. Harkins, D. Carrel. "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
- [10] S. Convery, D. Miller. "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation", v1.0, Cisco Systems Technical Report, March 2004.
- [11] A. Singer. "Life without firewalls", USENIX ;login: magazine, December 2003.
- [12] A. Vives, J. Palet, P. Savola. "IPv6 Security Problem Statement", draft-vives-v6ops-ipv6-security-ps-02.txt, October 2004.