InfoCom

IPv6 security models and dual stack (IPv6/IPv4) implications

A whitepaper

Authors :   Karl Mayer and Wolfgang Fritsche, IABG

Table of Contents

1 Scope and objectives

This whitepaper outlines the IPv6 security models and dual-stack (IPv6/IPv4) implications, which have been identified and analyzed within a study contracted by the European Commission to IABG and EADS. It expresses the opinions of the authors and not necessarily reflects the views of the European Commission.

The scope of the study was to provide an analysis and evaluation of emerging and existing private and business user scenarios regarding

- new security models and architectures made possible by the use of IPv6 or in the face of IPv6-IPv4 coexistence as well as
- IPv6 security vulnerabilities, advantages and shortcomings.

After having identified vulnerabilities and research gaps, recommendations for future activities were to be identified.

During the study, stakeholders and experts from various research and business areas have been involved via direct contacts and via two workshops for enrichment and validation of the study results.

2 Definition, evaluation, and selection of scenarios

Initially, the following business and private user scenarios that benefit from IPv6 have been identified and described:

- **Scenario "E-government":** A government network comprises interconnections of various government departments and central services networks, offering services for internal clients as well as citizens (e.g. online voting, tax declaration, car registration, etc.). By removing NAT, IPv6 is expected to foster e-government services and to facilitate management of the network.

- **Scenario "Mobile User":** Users of mobile devices (e.g. a business man on a trip) expect to stay connected without interruption while roaming between different access networks and service providers. Therefore Mobile IP has been standardized. Since IPv6 provides sufficient addresses and advanced features, it is expected that a mobility service will be based on Mobile IPv6.

- **Scenario "Public Safety"**: Public safety organizations call for IP-based broadband communication (e.g. exchange of videos, pictures, documents, messages, etc) on-site as well as with the command control centre. The IPv6 benefits in this scenario are autoconfiguration, enhanced mobility, and easier interworking between different organisations.

- **Scenario "Direct secure end-to-end communication":** Users of mobile devices expect to get access to their corporate network or to work with (maybe also mobile) co-workers while being mobile and remote. In this scenario, Mobile IPv6 route optimization could be deployed in order to

provide a direct end-to-end link between mobile device and its peer without inefficient triangular routing over a mobility anchor point.

- **Scenario "Corporate network":** Corporate networks are evolving from border-protected sets of internal resources to an extended enterprise architecture. Imminent IPv4 address shortage and possible benefits of IPv6 (huge address space, simplified management, new services, lifetime) demand for IPv6 migration.

- **Scenario "Personal Area Network (PAN)":** Users may carry several devices (phone, laptop, sensors, input devices) and one of the devices could provide access to the Internet (via WLAN, 3G), providing mobility service for the PAN via IPv6-based network mobility (NEMO).

- **Scenario "Access security":** IEEE 802.1X is deployed to control access to a network. Once connected, however, an infected or malevolent node is able to target its neighbours. In IPv6, secure neighbor discovery (SEND) can prevent this type of attack.

- **Scenario "Car-to-car communication":** The Car2Car communication consortium is standardizing the communication between different cars (e.g. exchange of sensor data) as well as communication between a car and road side units, the Internet, or the car manufacturer (e.g. for maintenance). Thereby, IPv6 is the IP version in scope for the network layer.

- **Scenario "Home network connectivity and networked gaming":** Networked games are becoming more and more popular. IPv6 would provide a transparent network layer without NAT boxes that would facilitate the deployment of networked games, especially peer-to-peer games, requiring the users to have IPv6 connectivity at home.

- **Scenario "Collective transports":** Collective transport (e.g. a plane) provides Internet connection to passengers, airline applications and aircraft applications. IPv6-based network mobility (NEMO) provides address stability in case various upstream technologies are used.

After having performed an initial investigation of these 10 scenarios, the scenarios have been assessed concerning benefit of IPv6 security vs. IPv4 security, maturity of technologies and components involved, market relevance, grade of potential impact of study, potential stakeholder involvement, and feedback of stakeholders. The first 5 scenarios given above have been ranked highest and selected for a detailed analysis, discussed in the following.

3 Investigation of scenarios regarding IPv6 security aspects

For each of the five selected scenarios the IPv6 security architecture has been compared with an IPv4 one and advantages, shortcomings, and challenges have been identified. Furthermore, issues especially in case IPv6 and IPv4 are run in parallel have been identified. Since some issues are applicable for all scenarios, those aspects are given in a separate section (next section).

3.1   Security aspects valid for all scenarios

Switching from IPv4 to IPv6 will not be possible in an instant way but over a period of migration with IPv4/IPv6 coexistence. During this phase, migration techniques like dual-stack, tunnelling, and translation have to be deployed. Where possible, dual stack nodes and networks (supporting IPv4 and IPv6) should be used. Where not, tunnelling mechanisms could be deployed to interconnect IPv6 nodes/networks over IPv4-only networks. These transition mechanisms, however, introducing certain issues, discussed in this section:

- **Issues of tunneling mechanisms:** Various tunnel mechanisms have been defined, some used for interconnection of IPv6 sites over IPv4 networks (e.g. 6in4, 6to4, 6rd) or for providing individual dual-stack hosts connectivity to an IPv6 network (e.g. 6over4, ISATAP, Teredo).

  Tunnel mechanisms are vulnerable to packet injection (e.g. for a reflection DoS attack). A countermeasure is the setup of appropriate filtering at the tunnel end-points (TEPs), e.g. regarding the source IPv4 and IPv6 address, or the deployment of IPsec for all tunnel traffic. Furthermore, some tunnel mechanisms (6to4, 6rd, ISATAP and Teredo) are vulnerable against DNS attacks in case tunnel end-points are discovered via DNS.
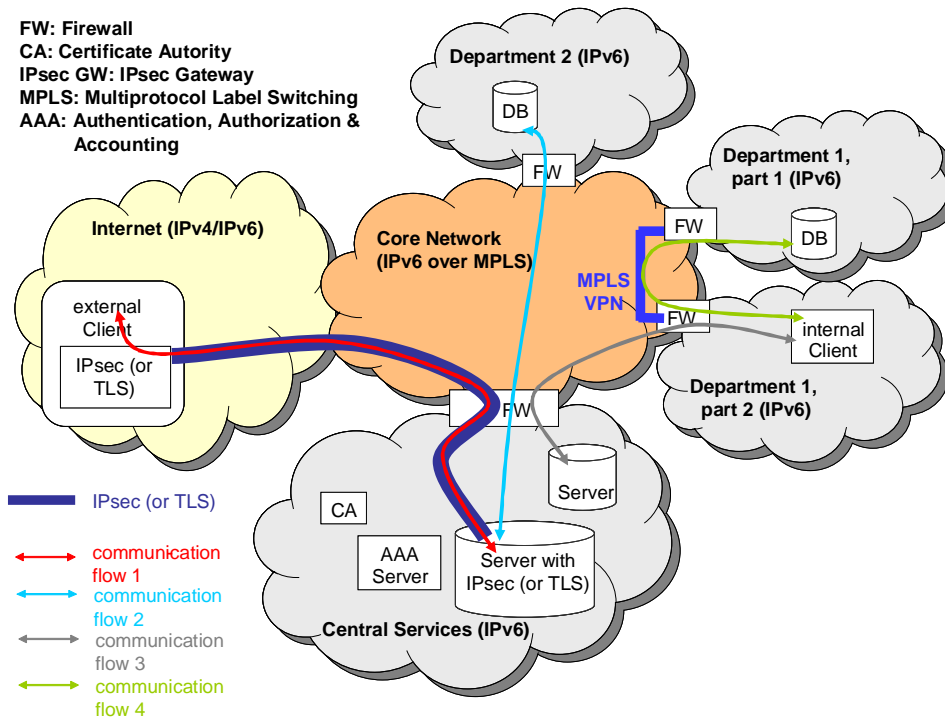
  Teredo provides connectivity for a dual-stack node stuck behind a NAT box. However, its usage has to be done carefully since Teredo requires opening a port in the network firewall that could be used for attacks unless a Teredo-aware firewall or an appropriately configured personal firewall are in place.

- **Vulnerabilities of operating systems:** Several dual-stack bugs in major operating systems for hosts and router have been identified in the past. For example, there has been a remote code execution vulnerability exploited via a specially crafted ICMPv6 Router Advertisement or ICMPv6 Router Information packet. Also a device could crash in case a specially crafted IPv6 Type 0 Routing Header is received. Bug fixes are available meanwhile, but upgrade depends on awareness of users and more bugs/vulnerabilities may just be discovered via a large scale deployment.

- **Missing awareness of IPv6:** Several operating systems enable IPv6 by default, e.g. Microsoft Vista (2007), Linux 2.6 kernel, Apple OS/10.3 (2002), etc. Users/administrators may not be aware of this so protection against IPv6 attacks may not be in place. This demands for an immediate training of users/administrators accompanied with hands-on experiences.

- **Dual-stack attacks:** During the transition phase, one has to consider both, IPv4 and IPv6 issues/attacks. Generally, a worm that has infected a host searches for other vulnerable hosts on the same LAN/subnet. In case of IPv4 this is achieved by a brute force scan. In case of IPv6 a brute force scan is not possible but a worm could use an IPv6 multicast ping (ICMPv6 echo request to multicast address, e.g. FF02::1) to discover on-link nodes. Hence, the spreading of a dual-stack worm could even be faster in a dual-stack network than in a native IPv4 network. A countermeasure would be to filter ICMPv6 echo requests with a multicast destination address in each node.

- **Translation technique NAT-PT:** A protocol translation (provided by NAT-PT) between IPv6 and IPv4 is required in case an IPv6-only node intends

to communicate with an IPv4-only node. NAT-PT incorporates some deployment issues. For example, converting IP headers is not sufficient in case IP addresses are used in high layer protocols (e.g. SIP or SDP), requiring Application Layer Gateways for each of these protocols collocated with the NAT-PT functionality. However, ALGs cannot operate on traffic protected by either IPsec or TLS.

3.2 Scenario "E-government"

A government network consists of networks of different governmental departments, of the central services, and the core network that interconnects those networks. Internal communication is required between different internal clients (flow 4), between internal clients and servers (flow 3), and between servers and other servers or databases (flow 2). External communication is deployed between external clients (citizen hosts) and the e-government servers (flow 1).

Figure 3-1: IPv6 security architecture of e-government scenario

The IPv6 security architecture (depicted in Figure 3-1) and the IPv4 security architecture of the e-government scenario offer a similar security level. In the core network IPv6 or IPv4 over MPLS VPNs is deployed, respectively, and the networks are protected by firewalls (FW). In case of IPv6, citizens can use IPsec/IKE for securing the connection to the e-government server, which is cumbersome in IPv4 due to NAT traversal. Alternatively or in case of IPv4, the connection between citizen host and server could be protected by TLS-based security (e.g. HTTPS integrated in common browsers).

The effort/costs for introduction and management of security are medium for both security architectures. While in case of IPv6 firewall configuration is more complex and has to consider IPv6 specifics (discussed in section 4), in case of

IPv4 the management and maintenance of NAT boxes and security mechanisms in the face of NAT boxes is extensive and cumbersome.

IPv6 is expected to foster e-government services due to end-to-end transparency; however, acceptance of citizens requires user-friendly security software (e.g. this is a problem with the electronic ID card DNIe in Spain). There are new trends regarding user authentication to make it more user-friendly, e.g. smartcards with USB interface, smartcards with TCP/IPv6 stack (for provider access, e.g. doing an update), or mobile devices with security built-in the processor for e-government and e-business applications.

3.3   Scenario "Mobile user"

This scenario is about realizing an operational mobility service by deploying Mobile IP. The mobility anchor points, the home agents, are operated by a mobility service provider, which may or may not be the same as the mobility service authorizer for a specific mobile node (a mobile device like a laptop, PDA, or smart phone).

One key advantage of Mobile IPv6 compared to Mobile IPv4 is a standardized secure bootstrapping process of Mobile IPv6 parameters. Thereby, the mobile node learns automatically the home agent address (selected by the mobility service provider due to internal policy), home address (the stable IP address), and security credentials. Furthermore, for Mobile IPv6, standardized AAA interfaces and protocol messages are specified that allow the deployment of Mobile IPv6 for an operational mobility service.

In contrast, with Mobile IPv4, inflexible static configuration of bootstrapping parameters would be required or to do extensive standardization work. Furthermore, in case of Mobile IPv6 the deployment of IPsec (which is highly secure, field-proven, and provides encryption) together with IKE have been standardized for protection of the signaling between mobile node and home agent while in Mobile IPv4 signaling protection is provided by a specific Authentication Extension (which does not provide encryption and is not as field-proven as IPsec).

Moreover, in case of Mobile IPv6 a home agent reliability protocol is currently under standardization and a load sharing mechanism has been developed, providing robustness against failures and attacks (e.g. denial of service attacks against home agents).
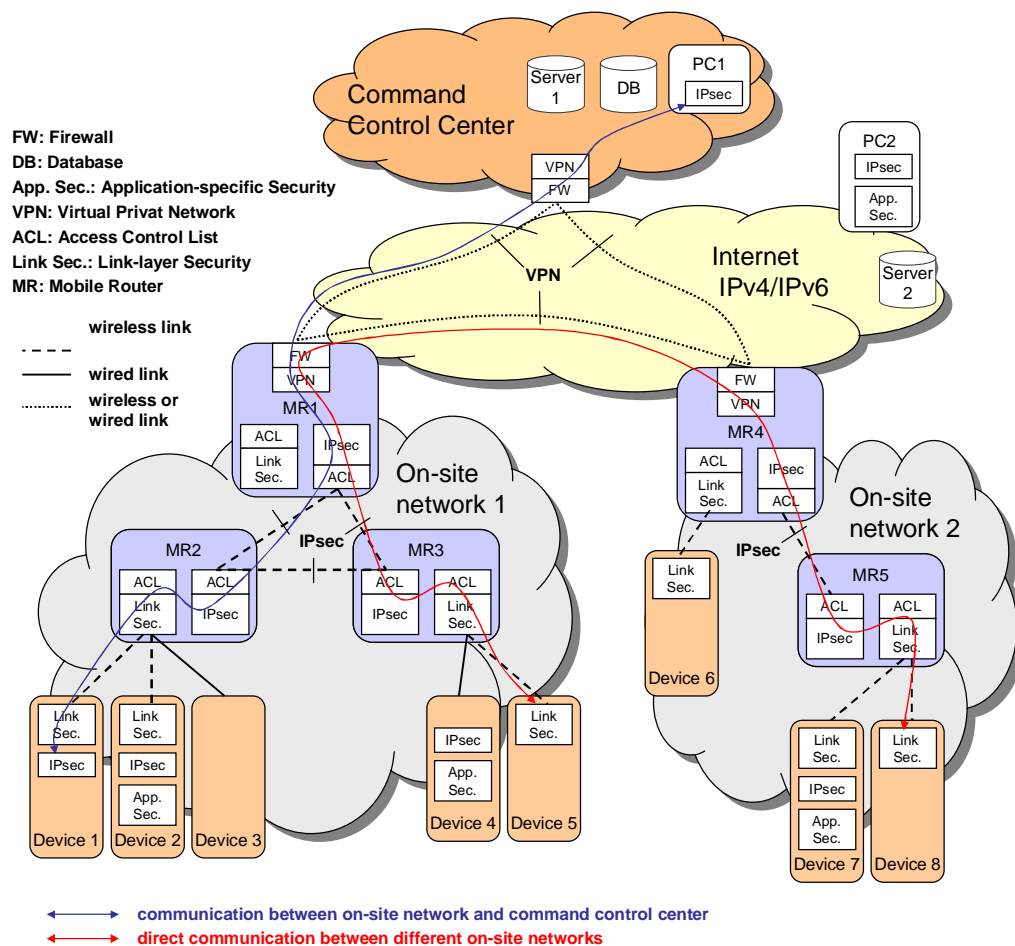
IPv6/IPv4-coexistence is given in case a mobile node is connected to an IPv4-only access network while the mobility service is based on Mobile IPv6. Dual Stack Mobile IPv6 (DSMIPv6) is a standardized solution for this scenario. In case DSMIPv6 is deployed in a NAT traversal scenario, the protocol is vulnerable against a man in the middle manipulating the outer IPv4 header for performing a redirection attack. However, this vulnerability is given for MIPv4 NAT traversal as well so it is not an IPv6 issue.

3.4   Scenario "Public safety"

The IPv6 security architecture of the public safety communication scenario is depicted in Figure 3-2. As example, the network comprises two on-site

networks (e.g. of two different public safety agencies possibly at different locations), the network of the command control center, and the Wide Area Network (the Internet). Each on-site network includes several different user devices (e.g. laptops, PDAs, sensors, cameras, etc.), interconnected via a mobile ad-hoc network (MANET) comprising several Mobile Routers (MRs). One of the MRs per on-site network represents the gateway to the Wide Area Network.

The main difference between IPv6 and IPv4 security architecture is that in case of IPv4 the public safety network parts are addressed by IPv4 private addresses, requiring NAT boxes at the perimeter (e.g. in the gateways). This complicates the deployment of security mechanisms for protection of the data exchanged between different on-site networks (red flow) or between on-site network and command control centre (blue flow). Although some IPsec-based VPN software is available with support for NAT traversal, using IPsec in a NAT environment increases complexity. Alternatively, software based on TLS (e.g. OpenVPN or GnuTLS) could be used as well, providing similar security than IPsec but no protection of the IP and the transport header.

Figure 3-2: IPv6 security architecture of public safety scenario

IPv6 is advantageous concerning robustness against failures. In case the gateway node between on-site network and wide area network fails, a smooth gateway failover would be possible (if a backup gateway is available) since no NAT state has to be synchronized.

In IPv4, when the address ranges are conflicting, a direct communication between different on-site networks is not possible (red flow). Consequently the communication has to be routed via some kind of rendezvous point, e.g. located at the command control center. This means that in case one of the links between an on-site network and the command control center is failing, no direct communication between the two on-site networks is possible. In contrast, in IPv6 no rendezvous point is required and direct communication is possible even without communication with the command control center.

Public safety applications may require the communication between IPv4-only nodes (e.g. a display that has not yet migrated) and IPv6-only nodes (e.g. a 6lowpan sensor). Hence, protocol translation via NAT-PT is required, but NAT-PT has its own security issues (described in 3.1).

3.5 Scenario "Direct secure e2e communication"

This scenario is about deploying Mobile IPv6 route optimization in order to provide a direct link between mobile device (using Mobile IP) and its peers (e.g. a node in the corporate network or the host of a remote co-worker) without inefficient triangular routing over a mobility anchor point (the home agent of a mobility service). Unlike Mobile IPv6, Mobile IPv4 does not provide an integrated route optimization solution to support direct E2E communications. Even in case the communicating peers are not mobile, due to IPv4 private addressing direct E2E communication requires some kind of rendezvous mechanism (e.g. STUN), but this has never been deployed on a large scale. These external rendezvous points create additional states in the network (hence reducing resilience) and increase the attack possibilities against the infrastructure.

While in IPv4 the predominance of applications rely on a Client/Server model (e.g. the clients setup a security association with a server they trust in), with the recovery of end-to-end transparency in IPv6 networks it is expected for E2E services to gain momentum pushing the deployment of some global credential services. At the moment, this is what some Certificate Authorities partially provide. However, a limiting factor for the deployment is that common central services (e.g. gmail, twitter, amazon, facebook, etc.) do not provide the ability for clients to authenticate using certificates.

3.6 Scenario "Corporate network"

After IPv6 migration of a corporate network, every corporate network node can benefit from global addressing capabilities. The related security perimeter shift from company boundary to host boundary would disclose the internal network topology as well. Hence, appropriate filtering of IPv6 traffic at the company boundary is still required in order to protect the corporate network e.g. from DoS attacks. Filtering could even benefit from IPv6 by sharing filtering between perimeter firewalls and personal firewalls (section 4 discussed this hybrid approach).

IPv6 introduces the concept of address scopes (link-local, unique local, and global), which can be used to help applying defence in depth principle: link-local interactions are performed using non routable addresses which results in the inability for remote attackers to subvert these functions. Unique local addresses allow administrators to naturally reduce the reachability of their devices to the corporate network scope.

A huge difference between IPv6 and IPv4 is associated with the replacement of ARP by IPv6 Neighbor Discovery protocol. Nonetheless, on security aspects, all the existing threats known against ARP (spoofing, redirection, etc.) still exist (in a different form though) on IPv6 subnets. However, the countermeasures defined by Secure Neighbor Discovery (SEND) – developed for IPv6 networks - and its initial availability on recent network equipments from major vendors (Cisco and Juniper) could provide additional security in the long term. Still missing are, however, SEND products for hosts (e.g. for Windows).

Migration will temporarily increase the workload for administrators and network teams. A higher number of protocols/features/devices to handle will result in reduced time to spend on each, leaving more room for mistakes and increased response times (e.g. in face of an attack).

During the phase of migration, IPv6 and IPv4 will run in parallel. Besides the issues addressed in section 3.1, network monitoring and management tools may not be as efficient for IPv6 protocol as for IPv4, requiring additional field tests.

4 Best practice firewall guidelines for the scenarios

IPv6 is expected to shift the security model from a network-centric to a host-centric one. In a **network-centric model** security enforcement (firewall, VPN, etc.) is performed within the network, e.g. at the perimeter between internal and external network. The advantages are: a small number of security enforcement points to be managed, security enforcement points are under full control of the administrators, and perimeter firewalls are anyway required to cope with DoS attacks from outside. However, this model misses protection against attacks from inside, e.g. virus or worm, and the security policies affect all hosts in the internal network and therefore administrators are very conservative in opening certain firewall wholes (e.g. a port for a new service). Also many attacks to hosts from outside cannot be prevented at the boundary to the external network, as they are inherent to end user applications like HTTP, Skype, etc.

In a **host-centric model** security enforcement is performed at the hosts, e.g. via a personal firewall or local VPN software. Since the number of IP-enabled mobile devices is growing (IPv6 will accelerate this) that get connected to untrusted networks (e.g. a hotspot) host-centric security policies become more and more important. Attacks from inside the network as well as external attacks inside end user applications can be prevented by this model. However, host-centric security cannot cope with DoS attacks. Therefore, it is expected

that a **hybrid security model** will be deployed, with basic policies at the perimeter (e.g. just IPsec/TLS traffic is allowed to traverse) and fine-grained policies at the hosts (e.g. opening of a certain port for a certain user group). A hybrid model, however, requires standardization of policy specification languages and tools as well as commercially available distribution, enforcement, and monitoring mechanisms for host-centric policies.

In the following, we will discuss filtering policies especially required to achieve IPv6 working correctly in the five selected scenarios:

- **Filtering for scenario "E-government":** Beside various other applications that are not possible to specify a priori, VoIP is expected to be deployed, so SIP, SDP, and RTP messages have to pass through firewalls. The default SIP/SDP port is 5060, while the RTP port is negotiated via SIP.

    Regarding external communication, the traffic is either protected by IPsec/IKE or HTTPS/TLS. IPsec traffic is identified by AH or/and ESP headers, IKE uses port 500 (or 4500), and HTTPS uses port 443.

- **Filtering for scenario "Mobile user":** Messages that have to traverse firewalls are Mobile IPv6 signaling messages (BU and BA protected by IPsec), IKE messages (port 500 or 4500), AAA messages (e.g. RADIUS (port 1812) or Diameter (port 3868)), and packets of user data. A general problem in this scenario are unsolicited messages (a message from outside without a prior request) which could be a problem for stateful firewalls that just allow traffic that is solicited, i.e. the firewall creates a state for an outgoing message and just allows an incoming message it has a state for.

- **Filtering for scenario "Public Safety":** Firewalls are given at the perimeter of the on-site networks as well as the command control network towards the wide area network. The wide area links are usually protected by VPNs based on IPsec/IKE or TLS. IPsec packets can be identified by AH and/or ESP headers and IKE uses UDP port 500 (or 4500). In case of TLS, setting filter rules a priori is more difficult since the port is not predefined and could be set by the user. Hence, coordination is required. The default port is 1194 for OpenVPN and 5556 for GnuTLS, for instance.

- **Filtering for scenario "Direct secure e2e communication":** Additional to the aspects discussed for the "Mobile user" scenario, in this scenario Mobile IPv6 route optimization is considered. Hence, the respective messages (HoTI, HoT, CoTI, and CoT) have to pass through firewalls.

- **Filtering for scenario "Corporate network":** Beside HTTP (port 80) and HTTPS (port 443), several other applications demand for firewall pass through. Hence, specific policies have to be defined per company in order to allow the right set of applications and block the rest. Certain IPv6 extension headers (e.g. AH, ESP, mobility header, routing header, etc.) may have to be allowed. A key difference applies to filtering of ICMP messages, which is common in IPv4. For instance, IPv6 requires proper working of the Path MTU Discovery mechanism, which requires successful transmission of ICMPv6 Packet Too Big messages. Moreover, several mechanisms are based on multicast so multicast traffic should not be blocked by default.

5 Summary and conclusions

- IPv6 and IPv4 are using the same security mechanisms with regard to IPsec. However, regarding deployment, IPv6 is more efficient, e.g. IPv6 provides end-to-end (e2e) transparency that facilitates e2e security models (e.g. using IPsec/IKE end-to-end) without NAT traversal issues, more fine grained security policies and filtering rules can be applied due to unique end system addresses, and IPv6 offers the possibility of end-to-end identification and authentication.

- Some security tools and software are partly not IPv6-ready or not field-proven (e.g. firewalls for handhelds or network monitoring and auditing tools), which demands for development work and careful testing (e.g. in an IPv6 pilot project).

- IPv6 requires changing of firewall policies, e.g. multicast and ICMP traffic should not be blocked by default. Moreover, several operating systems enable IPv6 by default but users/administrators may not be aware of this, leaving temporarily room for IPv6 attacks. This requires starting training of network administrators now in order to get appropriate protection in place.

- For migration, where possible, dual stack nodes/networks should be used. Where not, tunnelling mechanisms could be deployed to interconnect IPv6 nodes/networks over IPv4-only networks. During the migration phase, users and administrators have to consider IPv4 and IPv6 issues and attacks. For IPv6, multicast pings should be filtered to hinder the spreading of worms. In order to make tunnelling mechanisms secure, proper filters should be setup at tunnel end-points and Teredo should be selected just in case NAT traversal is required and a Teredo aware firewall is setup.

- The growing number of IP-enabled mobile devices (IPv6 is expected to accelerate this), higher flexibility (e.g. user specific security policies), and better protection against internal attacks (e.g. against viruses and worms) demand for a hybrid security policy approach with coarse-grained security policy enforcement at the perimeter (e.g. via a perimeter firewall) and fine-grained security policy enforcement at the hosts (e.g. via personal firewalls).

- Some scenarios show specific advantages of IPv6 security. For instance, the "Mobile user" scenario benefits from IPv6 via standardized secure bootstrapping processes and defined interfaces between Mobile IPv6 and AAA infrastructure. In the "Public Safety" scenario, IPv6 is advantageous regarding robustness and failover mechanisms. Corporate networks would benefit from SEND. SEND implementations for hosts (e.g. for Windows) are missing so far.

- IPv6 will facilitate/accelerate the deployment of e2e services (e.g. e-government services), requiring user-friendly security mechanisms (e.g. user authentication via certificates). Moreover, peer-to-peer based services (between unknown parties) demand for a global credential service with support for certificates.

6 Recommendations for future activities

The findings of the study identified the following key activities in order to close IPv6 security gaps and to accelerate the deployment of IPv6:

- **Development work:** There are still some areas requiring development work, e.g. development of tools and mechanisms for distribution and enforcement of host-centric security policies, development of user-friendly certificate-based authentication products, and development of SEND implementations for hosts.

- **Training:** Users, operators, and administrators have to be trained now regarding IPv6-specific security policies. Thereby, the training should include hands-on experiences in an IPv6 environment.

- **IPv6 deployment:** IPv6 deployment is necessary in order to proof security policies and software (e.g. IPv6 stacks, security protocols, and security monitoring and auditing tools) in the field and to give users, administrators, and operators hands-on experiences.

- **Dissemination:** Raising awareness among users, administrators, operators, and decision makers is required regarding IPv6 security advantages as well as challenges, e.g. via presentations in conferences related to networking (e.g. related to security and/or IPv6), articles in relevant journals, or articles in well-known portals related to networking (e.g. www.heise.de).

These activities would benefit from support by the European Commission, involving a critical mass of IPv6 security experts, users, administrators, and decision makers. Such activities could establish e.g. pilots related to certain business scenario, e.g. a secure e-government service, a secure mobility service for business and private users, or a secure public safety communication scenario.

7 Acknowledgements