Internet Engineering Task Force
Internet-Draft
Expires: August 24, 2005

A. Vives
J. Palet
Consulintel
P. Savola
CSC/FUNET

February 20, 2005

IPv6 Security Problem Statement
draft-vives-v6ops-ipv6-security-ps-03.txt

Status of this Memo

Copyright Notice

Abstract

Today, each network is often secured by a unique device (i.e. security gateway or firewall) that becomes a bottleneck for the end-to-end security model with IPv6. The deployment of IPv6 enabled devices and networks bring some issues, which must be addressed by

security administrators in order to guarantee at least the same level of security that is obtained nowadays with IPv4 and network-based (including perimeter-based) security schemes, allowing at the same time all the IPv6 advantages.

The most important issues are the rediscovery of end-to-end communications, the availability of IPsec in all IPv6 stacks, the increase in the number and type of IP devices and also the increase in the number of nomadic devices, connecting to different networks that could have different security policies.

The security policies and architectures currently applied in Internet with IPv4 do no longer apply for end-to-end security models which IPv6 will need. This document outlines the advantages and drawbacks of both security schemes: network/perimeter-based and distributed.

This document aims to identify IPv6 issues that justify the need of a distributed security model for IPv6, that is, simply to show that a security problem will arise with the deployment of IPv6 networks if nothing is done.

Table of Contents

1. Introduction

This document will cope only with IPv6 issues related to security, i.e., it will try to answer the following question: How would the deployment of IPv6 affect the security of a network? This network could be a dual-stack network with IPv6 traffic from IPv6 capable nodes, or an IPv6 only network.

The deployment of IPv6 enabled devices and networks forces the security administrator to consider several issues:

- The rediscovery of end-to-end communications.
- The availability of IPsec in all IPv6 stacks.
- The increase in the number and type of IP devices.
- The increase in the number of nomadic devices, connecting and moving between different networks.

The security policies and architectures currently applied in Internet with IPv4 no longer apply for end-to-end security models which IPv6 will enable. This document outlines the advantages and drawbacks of both the security schemes: network/perimeter-based and distributed.

Also IPv6 issues will be identified that justify the need of distributed security for IPv6, that is, simply to show that a security problem will arise with the deployment of IPv6 networks if traditional schemes are used.

The following issues are out of scope of this document and will be addressed elsewhere:

- State the security requirements for the described IPv6 scenarios.
- Propose a solution or architecture to address the problem stated in this document.
- To address security problems derived from the use of transition mechanisms.

Last but not least, this document contains a brief definition of what we understand by "security". We use security in the "big scope" of the word, trying to include as much as possible. In other words, a host, a network or some information, will be secure when no attacks could succeed against them. A success will mean compromise of availability, integrity, confidentiality or authenticity. The realistic objective is to be as much secure as possible in a precise

moment. It will be part of the requirements to establish which kind of security is given using a number of mechanisms.

For clarity, in the rest of this document, network-based security includes also the perimeter-based model.

2. Network-based versus Host-based Security

In this section two different approaches are analyzed to be used later in the rationale about the security problems that IPv6 could introduce

2.1 Network-based Security

This is the most used scheme, where the security of a host depends on the point of the network it is connected to.

The perimeter scheme is the simplest one (see Fig. 1) and is based in the topology of the network. The security policy is enforced in a central host or firewall (FW), which provides secure network connectivity to one or more network segments. The FW will be what an "outside" host sees when tries to attack the network. Attacks coming from the same LAN segment are not protected by the FW. Different nodes (even different addresses in the same node) may have different policies.

In a more advanced form of perimeter security, the different networks could be protected from each other, or a number of internal firewalls could be used as well. This way some networks could be protected from hosts in other internal network

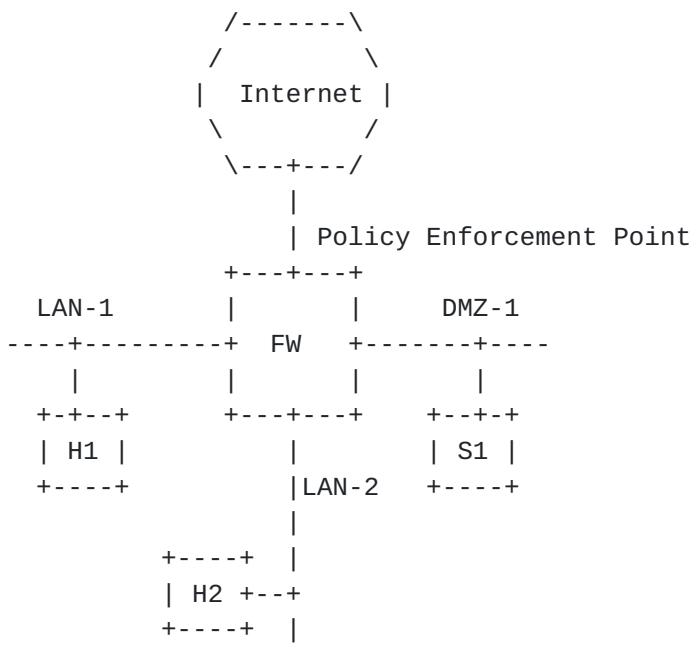

Figure 1: Perimeter Security

This model is based on the following assumptions:

- The threats come from "outside" the FW, basically the Internet.
- Everybody from the same LAN segment is trusted.
- The protected nodes won't go "outside" where FW won't be able to protect them.
- There are no backdoors on the network (modem, WLAN, other connections).
- The hosts will not need to be accessed directly from outside (at least in a general manner, i.e., potentially all ports on all hosts).

The main advantage of this scheme is its simplicity and easiness as the elements and points of configuration are reduced to the minimum, requiring few/no protocols and mechanisms to implement the security.

In case of a more complex configuration, where multiple FW are deployed within an organization network, the complexity will increase.

The drawbacks of this model are:

- This is a centralized model: Single point of failure for both

performance and availability. If the FW fails, then all the networks connected to it loose network connectivity unless specific fail-over techniques are applied.

- A big percentage of the threats come from inside the FW, and are not addressed by this security model, especially when internal firewalls are not deployed.

- The most dangerous threats, in the sense that one may not be able to protect from them, come from inside the FW.

- The FW usually acts as NAT and/or proxy box, interfering or even disallowing end-to-end communications. In complex configurations, even more than one level of NAT/proxy could appear.

- Transport mode secured communications (using IPsec ESP for example) need special solutions ([1]).

- The same security policy may be enforced for all the nodes of each network connected to the FW, but it is also possible to have separate policies for all hosts. In any case, an error in the FW will equally expose all hosts in a network.

- Virtual organizations, for example those using GRID models, don't work with traditional centralized security models.

- The lack of secure end-to-end prevents innovation.

2.2 Host-based Security

Host based security model, already introduced by [2], is based on the idea of enforcing the security policy in each network host from a central control point.

The three main elements identified in the distributed security model are:

- Policy Specification Language.

- Policy Exchange Protocol.

- Authentication of Entities.

The basic idea is simple: the Security Policy is centrally defined using the Policy Specification Language and distributed to each host by means of the Policy Exchange Protocol. The Network Entities need to be authenticated in order to be trusted, for example to allow an

incoming connection or to trust the received Security Policy.

The biggest challenge, however, is trusting that the hosts comply to the rules they've received, for example that the user can't just disable the firewall if (s)he dislike the policy; of course, this only can happen in the case (s)he has administrative rights for that (often not the case in non-personal systems, those not owned by the end user). It seems that one ore more network entities would have to keep watch over the hosts in order to detect if they are not following the received policy. At first look the more appropriated entity seems to be one that knows the security policy, for example the one that distributes it.

From a security point of view this model somehow eases the work to the "enemies", putting the Policy Enforcement Point in their hands. So not only mechanisms to prevent direct attacks to the security solution must be developed but mechanisms to minimize the consequences.

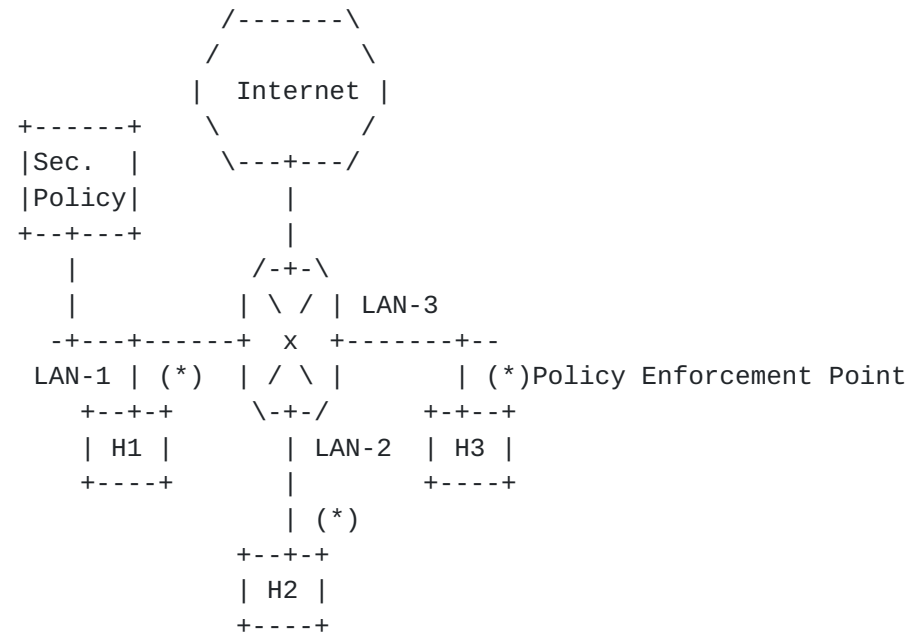

Figure 2: Host-based Security

This model is based on the following assumptions:

- Each host can be uniquely and securely identified.
- The security policy could be applied in one or more of the following levels: network, transport and application.

- The threat comes from anywhere in the network.
- The intruder has no physical access to the protected network hosts (what about malicious users? See other topics section).
- "Outside" hosts may be able to access all hosts "Inside", depending on the policies.

The advantages of this model are:

- The security policy can be host-specific.
- A host can take better decisions as it knows what it is doing or trying to do, that means it can better detect strange packets. For example, it could allow mail traffic to only one application on the system.
- Enables the usage of end-to-end applications level security (e.g., web services security standards).
- Enables better protection from attacks by the "internal" users, and possibly even to a degree from those in the local segment. For example address spoofing can be detected and avoided coming from the same LAN segment, without router participation.
- Can protect a host independent of the topology, i.e., wherever the host is connected.
- Does not need specific devices to secure a host (consider the case of a single host with a CPE (Customer Premises Equipment), if the CPE has no (user-controllable) firewall functions).
- Can control the outgoing attempts from each host, avoiding local network misbehavior or malicious practices.
- The collection of audit information could be more complete in a distributed model, despite the processing of that information is done in a distributed or centralized fashion.
- It maintains the centralized control of the security policies, from where they are distributed to each host (central decisions, local enforcement).

The drawbacks of this model are:

- It is more complex than the perimeter one.
- The uniqueness and secured identification of hosts is not trivial,

for example using certificates [2].

- The hosts must be trusted (or designed appropriately) so that they will operate according to the policy. For example, it must be impossible to disable the firewall functions or if the policy is not followed network communication is not allowed.

- A host that becomes compromised or infected with a worm or virus in any case can't be trusted to operate according to the policies, as the worms/viruses probably first create holes or disable the protections if they can.

- It may be challenging to design the system so that policy updates are made available to the nodes which may not be network-reachable all the time.

- It may be difficult to distinguish a misbehaving application from a legitimate application (for example, many email worms may be channeled through the MUA which must be authorized to send the mails to operate correctly).

- Because of having a centralized Policy Decision Point (PDP) from where the Security Policies are distributed a weakness is introduced in form of a central point of failure unless more complexity is added, for example with a distributed/replicated system.

- The host security is in some sense 'server-dependant'. It must be able to detect the lost of connectivity with the PDP and act in consequence. It also seems that being disconnected from the PDP for a long period could be dangerous.

3. IPv6 Issues

When IPv6 is deployed, either in an existing IPv4 network or in a new IPv6-only network, the security administrator must take into account that IPv6 traffic will be different from the IPv4.

IPv6 enabled nodes will likely have global addresses, which means they may be reachable from any other IPv6 node in the Internet. A security administrator can prevent this by using local addressing and/or firewalls, but the benefits of IPv6 may not be fully realized if so.

The differences between IPv4 and IPv6 change the type of attacks which IPv6 networks are likely to see.

Also mention that there are studies that conclude that the rollout of dedicated IPv4 firewalls in the internal network to regulate internal network communication causes the same work that dedicated firewalling on hosts.

3.1 End-to-End

The global availability of end-to-end communication is one of the benefits of IPv6, and provides the required framework for further innovation, where technologies like P2P and GRID, among others, can be widely spread with no problems in a seamless way. However, end-to-end communication also means that every host should be reachable from any other host, including the ones from "outside". It can lead to an increase in the possibility of being attacked, such as cracking, DoS, etc.

In the network-based security model, these threats are normally solved by disabling every end-to-end communications between inside and outside, but this is not a solution for those who want to use end-to-end communications.

Some possible solutions to cracking are outlined in [3], one of them being a host firewall.

Several researches are ongoing regarding DoS prevention, and some of these solutions need to be adopted to provide security for such end-to-end communications.

3.2 IPsec-encrypted ESP-traffic in transport mode

As stated in [3], section 5, there is a problem with the IPv6 encrypted traffic (IPsec ESP mechanism in transport mode, for example) and the network-based security model.

The idea is that a host inside the network can establish an encrypted communication channel with other host outside of the network. A middlebox (for example the perimeter firewall) won't be able to inspect the contents of such a communication.

In [3] some possible solutions are outlined, one of them being a host firewall.

3.3 Mobility

In parallel to the increase in the number of devices, IPv6 facilitates that those devices are "mobile", that is, can easily move from one network to another using Mobile IPv6 or just disconnecting from one and connecting to another.

Because of the amount of addresses available and the facilities given by Autoconfiguration mechanisms together with the mentioned rise of the number of IP devices, this kind of behavior should be taken into account by the security administrator, as these devices will be connected to networks where they have no control and consequently, no responsibility.

A possible solution for these devices is the use of host based security, enabled in every network it is connected. The policies and mechanisms should be described elsewhere.

3.4 Addresses

Regarding the addresses in IPv6 must be taken into account that:

- The amount of addresses is much bigger for a given network.
- Each host will have more than one address which are probably globally routable.
- An IPv6 node can use randomly generated addresses [4].
- The IPv6 addresses are more human error prone that the IPv4 ones.

That means:

- To scan a given network whole range of addresses and ports will take a really big effort [5]. It would be easier to do that by sniffing a LAN segment looking for existent addresses.
- The common way of identifying a host by means of its IP address will be more difficult to use.
- If a host uses randomly generated addresses [4], it could be problematic to identify a host using its IP address for security policy matching purposes.
- The Security Administrator should be careful when establishing, for example, an ACL (Access Control List) as the common practice is to use raw IP addresses (instead of DNS names). Some mechanism would be desirable to prevent these mistakes.

Regarding the scan of addresses, [5] demonstrates that the "brute force" scanning would make no sense for an IPv6 address range, typically a minimum of /64.

A host based security scheme would protect the other hosts from the compromised one.

The idea behind all this is that the new IPv6 address scheme and mechanisms will somehow protect from existent attack techniques but we can be sure that they will adapt themselves to the new scheme and we have to act consequently being prepared.

The IPv6 addressing scheme eases the work of identifying a user host, becoming a privacy threat. There are two IPv6 features to be considered, the host identifier created from the MAC address by the address autoconfiguration and the user network prefix.

The first one could be used to identify a user independently of the network to which it is attached. As a solution the randomly generated addresses were defined.

The second one refers to the fact that every user will receive at least a /64 prefix and so all the hosts coming from one user network could be identified by the network prefix. In IPv4 it is common to use a temporary address assignment scheme for the home user, resulting in changes of its assigned address.

3.4.1 Link-local addresses

In IPv6 we have got the link-local addresses that allows a host that connects to a network to have IP connectivity without any external help.

Even if this is quite useful, also represents a security problem because allows a host to attack the network it is connected to. This must be taken into account by the security administrator.

As a guideline, we should not simply rely on trusting by default those sessions which are from link local addresses. It is better to restrict to use link local address to some fundamental services, until the host is trusted.

3.4.2 New Multicast addresses

In IPv6 new multicast addresses are defined than identifies resources in a well known manner. This can enable an enemy to locate and attack those key resources with no need of a time consuming address search.

This kind of addresses have an scope field. This means that many of such services would have either link-local scope. Note that these addresses are used for the protocol itself, for example in the autoconfiguration process. This kind of addresses must be taken into account by a security solution that addresses inside attacks.

There are also global-scope addresses that must be published to the outside. This kind of services must be protected and monitored by a security solution that addresses outside attacks.

For an updated IPv6 multicast addresses list see [6].

3.5 Multihoming

As said above the IPv6 capable interface could have more than one IPv6 global address. This will be the case in multihomed networks, where more than one network prefix could be used to have access to the IPv6 world.

If the security policy is based on rules which use IP addresses as an identifier, it must be taken into account that a single host could be behind different addresses with different prefixes.

Also the case of a host with more than one interface, each one with one or more different addresses should be taken into account. If more than one interface is using the network infrastructure with different addresses, the Security Administrator should be able to identify that the same host is behind all these addresses.

3.6 Randomly Generated Addresses

Whatever security model is being used, in case of using randomly generated addresses, the host identifier part is randomly generated by the host to be used temporarily [4].

The consequence is that it will be harder for a security administrator to define a policy rule (access rule) in the security enforcement point to identify end nodes in all cases. For example a node could generate a DoS attack generating a lot of traffic using a random source address. The security administrator could not just block the host's network prefix because there could be other valid hosts within that network. Even in the case of a detection mechanism, the attacking node could change its random source address.

So the Security Administrator should take into account the randomly generated addresses when receiving incoming packets from outside of its security domain. Its decision could be for example to allow access to public services, like web servers, but not to allow or put special attention to connections to end nodes inside its network. To put special attention could be for example, to inspect packets up to application level or to dedicate more IDS resources.

3.7 Neighbor Discovery Weakness

As said above, one of the assumptions of the host-based security model is that all hosts in the network are non trusted, the possible threats coming from the same LAN segment must be taken into account, in this case the ones coming from Neighbor Discovery (ND) [7][8].

Note that this is not possible within the network-based security model, although some detection mechanism could be implemented, nothing can be done to protect the hosts.

There are some ways to interfere in the normal behavior of the autoconfiguration process, causing redirection of traffic and/or DoS (Denial of Service).

Special attention must be put on Router Advertisement (RA), Router Solicitation (RS), Neighbor Solicitation (NS), Neighbor Advertisement (NA) and Redirect messages. See [9] for a detailed explanation of possible threats.

Using host firewalls and/or IDS (Intrusion Detection Systems) for protecting hosts against these threats is very likely a wrong approach, as that would basically imply reinventing SEND [10][11]; it is better to use SEND instead.

There is no easy protection against these threats as the ND features (e.g., using link-local or the unspecified addresses) are needed before a host can authorize itself to the other network components.

3.8 Routing Header

IPv6 protocol defines some extension headers, among them is the Routing Header [12]. All IPv6 endpoints are required to process this header resulting in the forwarding of the IPv6 packet.

Using the routing header a list of one or more nodes through which the packet must pass, in its path from source to destination, is created. Basically what happens is that the destination address is changed in each host where the routing header is processed. This mechanism, for example, could be used to reach hosts beyond network-based security mechanisms.

The security administrator should establish, in the Security Policy, which hosts, if any, are allowed to forward IPv6 packets with routing header. The security solution must be able to assure that this policy is accomplished by all the hosts under its control. This can be achieved, for example, by disabling IP stack processing of routing headers or by filtering packets with routing headers in each host.

The routing header is used in Mobile IPv6. If this functionality is allowed in the network the Security Administrator must take it into account. For example, if administrators filter packets with routing-header, but don't filter ICMPv6 packets regarding Return-Routability, Mobile IPv6 will succeed in route-optimization but can't make the communication because packets with routing-header are rejected. Hence, Mobile IPv6 does not work at all in such configuration.

3.9 Home Address Option

IPv6 protocol defines some extension headers, among them is the Home Address [13]. All IPv6 endpoints should accept this header.

Basically what happens is that the source address of the packet is changed by the Home Address option's address. It is used in a packet sent by a mobile node while away from home, to inform the recipient of the mobile node's home address. This could be used for spoofing.

Because this option was defined for Mobile IPv6 use, the security administrator should reject the packet with home address option unless Mobile IPv6 is allowed.

3.10 Embedded Devices

With the deployment of IPv6 we can expect the avenue of a big amount of new IPv6-enabled devices with few resources, low computing capacity, even low battery capacity. In some cases, this kind of devices will not be able even to perform the minimum set of functions required by the Host-based Security Model.

It also should be taken into account that the convergence of both the IPsec capability of every IPv6 stack and the avenue of small devices with few CPU resources could be used for DoS attacks.

This should be taken into account when the security requirements are outlined and by the proposed solutions.

4. Other Issues

Further elaboration is required (TBD) on:

- Malicious users: We can't protect the network from malicious users that have physical access to network hosts in the protected network. The objective is to minimize the danger they can cause.

- In the host-based security, the host that stores and distributes the security policies seems to be the best option to be the one

that acts as IDS information collector.

5. Security Considerations

This document is concerned entirely with security.

6. Acknowledgements

The authors would like to acknowledge the inputs of Brian Carpenter, Satoshi Kondo, Shinsuke Suzuki, Peter Bieringer and the European Commission support in the co-funding of the Euro6IX project, where this work is being developed.

7. References

7.1 Normative References

7.2 Informative References

[1] "IETF midcom WG", <http://www.ietf.org/html.charters/midcom-charter.html>.

[2] Bellovin, S., "Distributed Firewalls", November 1999, <http://www.research.att.com/~smb/papers/distfw.pdf>.

[3] Savola, P., "Firewalling Considerations for IPv6", Internet-Draft draft-savola-v6ops-firewalling-02, October 2003.

[4] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[5] Chown, T., "IPv6 Implications for TCP/UDP Port Scanning", Internet-Draft draft-chown-v6ops-port-scanning-implications-01, July 2004.

[6] "IANA's IPv6 Multicast Addresses List", <http://www.iana.org/assignments/ipv6-multicast-addresses>.

[7] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[8] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[9] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[10] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", Internet-Draft draft-ietf-send-ndopt-06, July 2004.

[11] Aura, T., "Cryptographically Generated Addresses (CGA)", Internet-Draft draft-ietf-send-cga-06, April 2004.

[12] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[13] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

Authors' Addresses

Alvaro Vives Martinez
Consulintel
San Jose Artesano, 1
Alcobendas - Madrid
E-28108 - Spain

Phone: +34 91 151 81 99
Fax: +34 91 151 81 98
Email: alvaro.vives@consulintel.es

Jordi Palet Martinez
Consulintel
San Jose Artesano, 1
Alcobendas - Madrid
E-28108 - Spain

Phone: +34 91 151 81 99
Fax: +34 91 151 81 98
Email: jordi.palet@consulintel.es

Pekka Savola
CSC/FUNET
Espoo
Finland

Email: psavola@funet.fi

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.