Project Number:	IST-2001-32603
Project Title:	6NET
CEC Deliverable Number:	32603/Partner/DS/3.5.1/A1
Contractual Date of Delivery to the CEC:	December 31st 2002
Actual Date of Delivery to the CEC:	October 8th 2003
Title of Deliverable:	Implementation of Security Plan (v1 & v2)
Work package contributing to Deliverable:	WP3
Type of Deliverable*:	R-Report
Deliverable Security Class**:	PU-Public
Editors:	G. Koutepas
Contributors:	Georgios Koutepas, Athanassios Liakopoulos, Carlos Friacas

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Abstract:

This Deliverable describes the implementation plan of the 6NET security policy. The document, as part of Activity 3.5: Network Security, examines security measures at each level of the 6NET network infrastructure, as well as the supporting security policy. Actions suggested in this document will be tested for the most appropriate configurations and the results published as part of the Security Cookbook (D3.1.2).

This Deliverable is a merger of D3.5.1 v1 and D3.5.1 v2.

Keywords:

Executive Summary

The main objective of Deliverable 3.5.1 is the definition of appropriate security policies for 6Net and their implementation plan. It tries to identify the problem, i.e. possible security threats, and examines the most suitable counter-measures. Actions suggested in this document will derive from tests performed within 6Net in order to gain practical experience of IPv6 environments.

In the context of WP3, there was considerable effort on routing and multicast implementation, testing, and debugging that recently resulted in a stable networking environment. The next logical step is to undertake other activities that will complete the functionality of the 6Net infrastructure, such as IPv6 security. The latter is an activity that can be examined and configured effectively only when the network architecture and services running have been finalized. 6Net is currently a network under continuous development, e.g. new functionality is added to the core/access network and more IPv6 implementations are made available for end users. This prevents the assessment of the main security issues as conditions constantly change. Also, increased amount of traffic is essential to define the normal operational conditions and thus be able to determine the anomalous situations.

Complementary of having fully operational conditions, a comprehensive testing plan has to be developed to assess the security characteristics of this new novel network under special (still possible during security incidents) circumstances. As the network continuously changes, it wasn't possible to define a complete security policy that will preserve the efficiency of the network operations while protecting it from threats. In the current (intermediate) stage of 6Net, the existing IPv4 operational experience is the only base for implementing network device configuration. Obviously, some of the IPv6 threats were envisaged and corresponding measures are taken. However, in this stage it isn't possible to validate these measures for their effectiveness. Also, so far, there is a lack of observed security events that could stimulate the need for deploying immediate measures. Finally, the lack of appropriate detection tools for IPv6 limits the ability to identify malicious traffic and thus to restrict it.

Due to the importance of security, it is suggested that Deliverable 3.5.1 is completed and it should offer comprehensive guidance on security policies and methodologies for 6Net. It should be the result of a series of practical tests that will take place within 6Net later in its development process. The appropriate timeframe could be 1Q2004 which will give some time for the needed tests and development of procedures.

Table of Contents

1. INTRODUCTION 4

1.1. THE NEED FOR SECURITY IN 6NET 4
1.2. IPV6 SECURITY CHARACTERISTICS 4

2. 6NET SECURITY ASSESSMENT 5

2.1. DESCRIPTION OF THE 6NET NETWORK 5
2.2. PRESENTATION OF MAIN ARCHITECTURE PLAYERS; CORE, ACCESS, NRNS, 3RD PARTIES 5
2.3. DESCRIPTION OF MAIN NETWORK LAYERS 5
2.3.1. Physical 5
2.3.2. Routing 6
2.3.3. Access control 6
2.3.4. Management 6
2.3.5. Testing facilities 6
2.4. MAIN INFRASTRUCTURE THREATS: THREATS TO THE NETWORK 6
2.5. MAIN LOGICAL THREATS: THREATS TO THE NODES AND SERVICES SUPPORTED BY THE NETWORK 6
2.6. THE ASSOCIATION OF LAYER2 - IPV6 ADDRESSING: POSSIBLE DANGERS 6
2.7. CURRENT 6NET SECURITY MEASURES IN OPERATION 7
2.8. SECURITY EVENTS ALREADY OBSERVED 7

3. 6NET SECURITY PLAN (ACROSS ALL PLAYERS) 7

3.1. SECURITY MEASURES TO BE TAKEN AT THE PHYSICAL LAYER 7
3.2. SECURITY MEASURES TO BE TAKEN AT THE ACCESS CONTROL LAYER 7
3.2.1. Access procedure/Servers on IPv6 and ways of controlling router and other active device access 7
3.2.2. Access control for mobility services 7
3.3. SECURITY MEASURES TO BE TAKEN AT THE ROUTING LAYER 7
3.3.1. Methods of control that can be implemented: 7
3.3.2. Routing Protocol secure configurations 8
3.3.3. Standard security configurations for routers and other devices 8
3.4. SECURITY MEASURES TO BE TAKEN AT THE SUPPORT SERVICES LAYER 8
3.4.1. Security of Network services (DNS, NTP, ssh, Looking Glasses etc.) 8
3.4.2. Security of informational servers 8
3.5. SECURITY MEASURES TO BE TAKEN AT THE MANAGEMENT LAYER 9
3.5.1. Network operations associated with security, to be controlled from the management layer 9
3.5.2. Description of IDSes and other security tool deployment 9
3.6. SECURITY MEASURES TO BE TAKEN FOR TESTING FACILITIES 9

4. SECURITY POLICY 9

4.1. ACCESS POLICY FOR EACH PLAYER (ACCEPTABLE USE POLICY) 9
4.2. ROUTER TRAFFIC CONTROL RULES 9
4.3. SECURITY INCIDENT RESPONSE 9

5. BIBLIOGRAPHY 9

1. Introduction

1.1. The need for security in 6NET

6Net is a production network that introduces native IPv6 connectivity at a high scale. The implications of having a relatively new and not thoroughly tested (some times even not perfectly understood) technology, implemented on a full scale production network make security a high priority. Although the assets at risk are academic networks and the operation of experimental services, security problems can escalate to the universities' internal networks, possibly creating problems there, but also may disrupt experiments and other evaluation processes of 6Net itself. Furthermore since 6Net is also a demonstration project the security requirements will guarantee the public's trust in the value and especially reliability of the new technology.

6Net with its high bandwidth network lines also offers a very efficient infrastructure for the malicious users that will manage to utilize it in order to attack any of its nodes or targets outside of it. 6to4 facilities provide the possibility of an attack "spill-over" to more critical IPv4 production and even commercial networks. It is critical to address security issues early in the design and implementation process for embedding security in every step of the process. Policies, methodologies, configurations and the general security lessons learnt from 6Net will prove a useful and substantial contribution to the IPv6 community and future deployments.

1.2. IPv6 security characteristics

Most of the people talking about IPv6 security focus on its two main features that provide authentication and encryption:

- The "Authentication Header", provides authentication and integrity (without confidentiality) to the IPv6 datagrams. It is an extension to the IP header and offers support for many different authentication techniques.
- The "Encapsulating Security Header" provides integrity and confidentiality to the IPv6 datagrams. In fact IPsec was initially proposed as a feature of IPv6 and was transferred to IPv4.

Security in IPv6 however has many more parts:

A wide range of addresses makes host and port scanning difficult, however it may also be very effective in concealing malicious users and their operation within a LAN

Intrusion detection systems and especially NIDS have to be adjusted to the new type of IP packets. Although a number of security products right now provide this capability, IPv6 provides extra difficulties for any security assessment based on traffic analysis; there is extra CPU overload associated with the analysis of the bigger IPv6 packets. The IPv6 packet embedding within UDP or other encapsulation methods will also prevent direct examination of the packets.

The CPU overload problem is also an issue when setting up Access Control Lists at routers or when they come under direct Denial of Service (DoS) attacks. The Routing Header feature of IPv6 can also provide the opportunity for indirect attacks since it can be used to conceal the real destination of the IP datagram.

Another security issue is created by the automatic IPv6 configuration feature. Specifically, automatic address allocation when misconfigured may reveal important assets of the network due to pattern repetition. The same technique may also be initiated by malicious users in order to reserve specific IPs and prevent legitimate address allocation.

2. 6net Security Assessment

2.1. Description of the 6Net network

Short description of 6Net topology and operational characteristics

2.2. Presentation of main architecture players; Core, Access, NRNs, 3rd parties

In this section we present the main parts of the 6Net networking infrastructure and their implications in security issues.

As explained in Deliverable 6.1.1 (6Net Network Management Architecture) the architecture of the network can be divided in 3 major components:

- the core backbone, composed of the 6Net PoP routers,

It is here that the network is implemented and the routing decisions are made. Management there is centralized which makes security configuration and reactions to incidents easy to decide and implement through a common policy. The main threats in this section are (a) unauthorized access to the core routers that could allow altering the routing tables, (b) direct attacks on the routers making use of vulnerabilities presented by their current operating systems (these attacks may be attempts to gain access or simply exploits to make them stop their operation - Denial of Service) and (c) possible mis-configurations. Due to the high bandwidth backbone links direct Distributed Denial of Service attacks against them are unlikely; however there is the risk that these links will be used as a passageway for such attacks against the 6Net infrastructure or other connected networks.

- the NREN networks,

These are the 6Net client networks. Although there are common policies that determine the methodology of connectivity of the NRENs to the 6Net backbone, as well as common directives for the internal operation of services (e.g. multicast) each NREN implements its own internal security policy. Thus, security in this case is both a technical and political issue.

- the users, connected to 6Net via their National Research and Education Network

Currently, IPv6 protocols are supported on most platforms and operating systems. It often requires a single command to get connected with the IPv6 network via auto-configuration mechanisms. IPv6 connectivity can be achieved without the system administrators being aware of it. Therefore, it presents a security factor that has to be considered. Also, users or system administrators overlook the dangers, which derive from the de-facto IPv6 connectivity.

2.3. Description of main network layers

2.3.1. Physical

The characteristics of the physical layer that can play a security role, e.g.:

- Security of IPv4-to-IPv6 migration mechanisms (comments on Deliverable 6.2.1). For example, tunnel brokers may be used for gaining anonymous access to IPv6 networks. Tunnel brokers (outside the control of 6Net network administrators) provide connectivity to

requesting hosts. It's therefore difficult to identify an attacker, connected via a tunnel broker service to the network.

- Having (unauthorized) IPv6 access via tunnels may overcome security measures that depend on traffic analysis, such as firewalls or Network Intrusion Detection Systems. Moreover legitimate users are subjected to threats that can pass the security systems undetected.

2.3.2. Routing

- Problems that can result from router mis-configurations
- Router problems/vulnerabilities in IPv6
- Problems that can be solved through router rate limiting mechanisms and access lists (e.g. ICMP rate limiting)

2.3.3. Access control

Areas of 6Net that require secure access; ways to achieve this through policies and technical measures:

- Wireless/mobile access
- Active network components, e.g. routers, switches etc.
- Ssh remote access
- Dial-in threats

2.3.4. Management

Management informational services, 6Net tools (http://6nettools.dante.net), weathermap (http://netmon.grnet.gr/6net.html) etc.

The need for secure management information dissemination.

2.3.5. Testing facilities

As there is a need for network testing in 6Net, these should be conducted in a way that will not disrupt the overall security. Additionally, a testing security policy must be developed and applied. For example, during testing access permissions are granted for some network operators that should be revoked after the end of the tests.

2.4. Main infrastructure threats: threats to the network

Denial of Service (DoS) attacks, aiming at component vulnerabilities and Distributed DoS (DDoS) attacks aiming at exhausting the network and computing resources.

2.5. Main logical threats: threats to the nodes and services supported by the network

2.6. The association of layer2 - IPv6 addressing: possible dangers

Threats that derive from the use of MAC addresses for dynamic assignment of the IPv6 address.

For example, the EUI64 standard methodology for address allocation may protect privacy of end users but may also be exploited by attackers to prevent their tracking.

2.7. Current 6Net security measures in operation

Describe the ad-hoc security measures that have been implemented during the initial set up of the 6Net backbone and NREN/University networks.

2.8. Security events already observed

So far there haven't been observed any security events originating from the 6Net infrastructure. Currently, there is no policy on the reporting procedure for such events.

It should also be noted that security tools for identifying incidents have not been widely deployed on 6Net. Some proven tools are under development to support IPv6 and are expected to yield results after the start of their operation.

3. 6net Security Plan (across all players)

3.1. Security measures to be taken at the physical layer

Physical security and redundancy measures across the network are to be defined through the security policy.

3.2. Security measures to be taken at the access control layer

3.2.1. Access procedure/Servers on IPv6 and ways of controlling router and other active device access

What should be the appropriate access procedure, rights granting (through policy).

Which should be the most suitable access server deployment to ensure availability of service and adequate protection.

A large group of network administrator are still using command line interfaces nowadays to access routers/switches/... A secure way of updating active equipments' configuration should be used when it is available. Today, Cisco already has Secure Shell servers running on its equipments, and command line users might use it instead of the old and insecure telnet tool. An alternative way of controlling such devices would be through a console server, which also should permit secure communications to the network administrator's client.

3.2.2. Access control for mobility services

Describe the architecture for supporting secure access of mobile users / mobility services (comment on relevant MIPv6 documents, e.g. corresponding 6Net deliverable). More specifically, threats involving false Binding Updates (traffic redirection, man-in-the-middle, DoS) will be analyzed and the solutions chosen by 6Net will be presented.

3.3. Security measures to be taken at the routing layer

3.3.1. Methods of control that can be implemented:

Route filtering implemented at the border, will prevent mostly configurations errors made in other autonomous systems to affect our network. It can be done using as-path access-lists, prefix-lists, or some other form of preventing the entrance of unwanted BGP information in our routing tables. Route filtering implemented in the IGP (Interior Gateway Protocol) will also prevent configuration mistakes and might also prevent somebody from introducing undesired routes into the IGP tables.

Today, mobile networks are emerging, and there is the possibility that someone will try to use a device (connected within the same network) to inject some routes into an unprotected IGP setup.

It may be helpful to filter packets at the network access points in order to recognise incoherent source addresses coming from a customer network. Packet filtering (per protocol/per port/...) is sometimes the only way to stop Worms and DDoS attacks. Rate limiting is also another option, which may provide a helpful mechanism against some Virus/Worms and DDoS attacks. However, it is very difficult to completely eliminate these incidents.

3.3.2. Routing Protocol secure configurations

Usage of authentication mechanisms in BGP sessions and IGP protocols (ospf/is-is/...) will increase network security, and stop any man-in-the-middle attacks (regarding BGP) and the appearance of new network members in one's backbone.

3.3.3. Standard security configurations for routers and other devices

To be determined after some testing

3.4. Security measures to be taken at the support services layer

3.4.1. Security of Network services (DNS, NTP, ssh, Looking Glasses etc.)

DNS service is a critical part of a network operational infrastructure. The version information (version directive in the options section of named.conf -- in BIND) should be made stealth. This may prevent revealing the version information that will allow potential attackers to exploit well-known bugs of older software versions. Also allowing zone transfers from unidentified places should be considered a bad practice.

Initially, 6net used IP based authentication for managing zone transfers for the 6net.org and sixnet.org zones. Secondary name servers, for example, could get updated zone information only if their IPv6 address matched the addresses stated within the primary DNS configuration files. Currently zone transfers use symmetric keys for authentication and authorazation, namely TSIG authentication. This improved significantly the overall security of the whole procedure.

The NTP service has a growing importance, and its integrity has become crucial because of the need for synchronization by some applications. The best practice regarding this service is to protect the access to the highest stratum servers (stratum 1) by using access control lists.

Looking Glasses are very useful tools, and their public availability helps with the debugging of routing problems. However, this information may need to be restricted from the public as well as authenticated for its source and accuracy. A best practice solution would be to use of Secure HTTP (https://) to provide authorization and authentication.

3.4.2. Security of informational servers

Input required by WP5 partners in order to list the applications that have been developed under 6Net and provide methods for securing them. Practices derived from their implementations of these services could generally be applied for securing 6Net information/other application servers.

3.5. Security measures to be taken at the management layer

3.5.1. Network operations associated with security, to be controlled from the management layer

Traffic measurement: Information collected via Netflow could be used to identify anomalies in network traffic. Sharp increases in the number of packets of traffic volume usually reveal attacks. Additionally, offline examination of collected traffic information could be used to identify small scale attacks or follow step-by-step the path of a DDoS attack.

3.5.2. Description of IDSes and other security tool deployment

A number of IPv6 tools that either test vulnerabilities or initiate attacks have to be tested. The results from these tests may administrators to increase the security level of the network against common threats. As part of the security policy a comprehensive methodology of using such tools has to be developed.

3.6. Security measures to be taken for testing facilities

"Environmental control" of testing facilities will guarantee that the any tests will not interfere with the normal production services. One issue usually related to testing is the end-of-life of each setup. Each new setup shouldn't inherit security data from previous test setups. Security data (as well as other information, e.g. temporary access passwords) must be removed after the test setup is dismantled.

4. Security policy

This section deals with the security procedures that should be followed in everyday network operations.

4.1. Access policy for each player (acceptable use policy)

These policy recommendations for each partner connected to the 6Net can be incorporated in the AUP. Examples of such recommendations are: Egress/ingress ACLs, routing filters, access control on active network components, and list of best practices.

4.2. Router traffic control rules

Tests or theoretical analysis may determine optimal routing rules, security-wise (e.g. preventing spoofed packets from sources they are not expected to initiate). In addition to those there will be recommendations on the actions to be taken when dealing with specific type security incidents (e.g. how to identify an ongoing DDoS attack, how to determine its type, and a suggested malicious traffic filtering policy)

4.3. Security incident response

Variations to the helpdesk problem resolving procedure followed now and described in deliverables D6.1.1 (6NET Network Management Architecture) and D6.3.1 (6NET IPv6 Network Management Cookbook).

5. Bibliography

[1] Michael Behringer, "Tracing DoS Attacks," Hi Tech 2002 Workshop, Limmerick, IE, June 2002

[2] Internet Security Systems, "Security Implications of IPv6", white paper, http://documents.iss.net/whitepapers/IPv6.pdf