| | |
|---|---|
| Project Number: | **IST-2000-25187** |
| Project Title: | **TORRENT** |
| Deliverable Security*: | **RE** |
| CEC Deliverable Number: | **D3.3** |
| Project Document Number: | 01-031-v005-wp3-RE-R-d3.3 |
| Contractual Date of Delivery to the CEC: | **31.05.2002** |
| Actual Date of Delivery to the CEC: | **22.09.2003/14.02.04** |
| Title of Deliverable: | **Security Aspects and Features of the TORRENT Test-bed** |
| Work package contributing to the Deliverable: | **WP3** |
| Type of Deliverable**: | **R** |
| Editor: | J. Rossebø (Telenor), J. Ronan (WIT-TSSG) |
| Contributors: | J. Rossebø, S. Houmb (Telenor), J. Ronan, Kristian Walsh, Jerry Horgan (WIT-TSSG) |

* Security: PU – Public, PP - Restricted to other programme participants (including the Commission Services)
RE - Restricted to a group specified by the consortium (including the Commission Services)
CO - Confidential, only for members of the consortium (including the Commission Services)
** Type: R - Report, P - Prototype, D - Demonstrator, O - Other

**Abstract:**
The TORRENT system security architecture and features have been refined throughout the project, through the detailed analysis of the requirements of users, and the network operators and service providers. This Deliverable has been used as a *living document* within the project to document the current view of the security features of the system. A final version of this deliverable, including the results of work during the last quarter of the project is presented to the final audit.

**Background:**
The whole spectrum of user requirements were identified in D1.1: “User Requirements”, and the full-scale capabilities of the system to meet these requirements were described in D1.2: “Requirements for Service Providers, Network Operators, Manufacturers”. This includes the security requirements. In addition, a threat analysis has been carried out to determine which security services and mechanisms are required to bring the risks to an acceptable level, so that the TORRENT system may fulfil the users requirements.

**Keywords:**
security, access network technologies, local access point, residential gateway, home networks, terminals, applications, Firewall, IDS, Authentication, PKI,

**TABLE OF CONTENTS**

**Executive Summary**

This Deliverable now focuses on describing the TORRENT security aspects and features as are being implemented in the testbed system. Recommendations and descriptions of security services and mechanisms that should be implemented in commercial products based on the TORRENT system are also addressed. The security requirements, as recognised by TORRENT, have been identified by a threat analysis (Ref. Appendix C of this document). The TORRENT security features have been, first and foremost, to satisfy the security requirements of the residential customer while also protecting business interests of the Service Providers and Network Operators. For example, it is important to maintain the integrity of the LAP and the networks of the Network Operators and Service Providers.

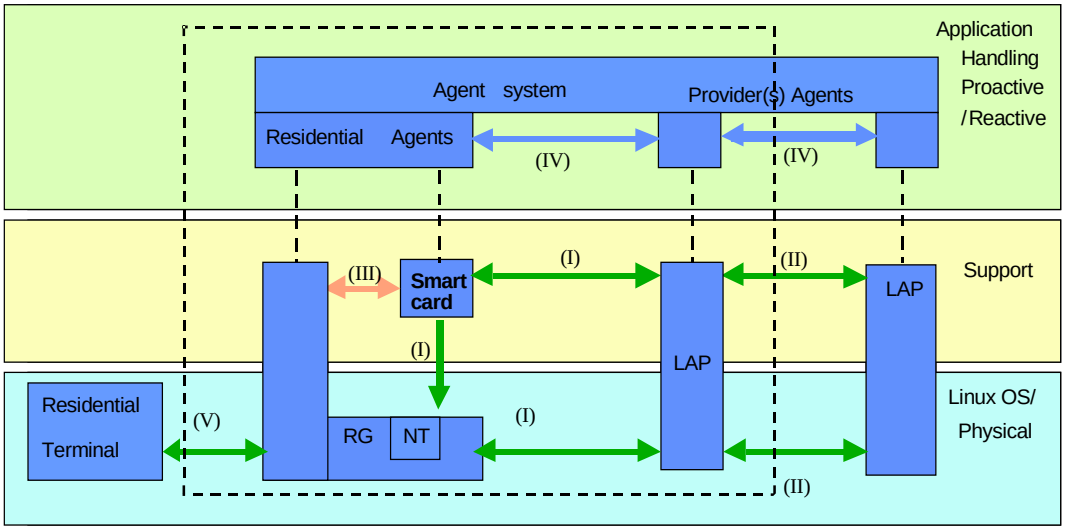
# 1. Introduction

This document has been produced by WP3: Service to Resource Management.

As several papers have been published (and some have recently been submitted) describing different security services and features of the TORRENT system, the form of this deliverable is as follows: Introduction and summary of the threat analysis followed by recommendations. A section will be devoted to each of the recommended security services and mechanisms. The papers will be inserted appropriately. The threat analysis is inserted as Appendix C.

## *1.1 TORRENT security architecture*

During the first year of TORRENT, a security specification was worked out, indicating which security services and mechanisms should be addressed in the project. This included a security architecture for the TORRENT system as shown in the figure below.[1]




Scope of the field trials = - - - - - -

Abbreviations: NT = ISDN NT1 with S interface to the customer
RG = Residential Gateway; LAP= Local Access Point

***Figure 1: TORRENT Security Architecture as Initially Proposed***

The scope of the field trials is shown within the dashed box. The interfaces indicated in the figure are categorised according to the security features pertaining to a particular interface and are defined as follows:

(I): Network access security - The set of security features that protect the access link between the RG and the LAP and subsequently provide users with secure access to TORRENT services;
Examples of features that may be provided are as follows:

- Authentication of the LAP by the RG
- Authentication of the RG by the LAP
- Authentication of the user by the agent system (e.g. for access to the "User Service Profile Modification" procedure)

Note that authentication services may be implemented as a token based hardware mechanism (smartcard), using asymmetric or symmetric keying, and keys stored in a smartcard issued to the subscriber and inserted in the RG. Alternatively, static keying may be used with keys stored directly in the RG and LAP

- Encryption of the link between the RG and the LAP using an IPsec VPN. Static keying may be used or smartcard based authentication for key agreement
- Stateful firewall on the LAP
- Access Control Lists (ACLs).
- Intrusion Detection: An active Intrusion Detection system may be used to (for example) track breaches of security policy and fraudulent activities.

(II): Network domain security - The set of security features that enables LAPs in the provider(s) domain(s) to securely exchange signalling data, and protect against attacks on the network; this is outside the scope of the TORRENT field trials.

(III): User domain security - This is an issue that is represented by the set of features that secures the user access to the RG. This may be implemented depending on who is allowed to access (e.g. to configure) the RG, and how tightly the RG needs to be controlled.

(IV): Application domain security - The set of security features that:

- Enables agents in the user and in the provider(s) domain(s) to securely exchange messages (e.g. for negotiation)
- Protects the negotiation process in the agent system, e.g. to protect against malevolent agents being injected into the system.

(V): Visibility and configurability of security - The set of features that enables the user to be informed whether a security feature is in operation or not, and whether the use and provision of services should depend upon the security feature.

### *1.2 TORRENT security features*

Based on the work done in the TORRENT Deliverables D1.1 and D1.2, the following specification for the implementation of security services in TORRENT was created and presented at the first annual TORRENT review:

- Network security
  - Stateful Firewall on the LAP (part of the agent policy engine)
  - Active Intrusion Detection System
  - Peer to peer authentication: This should be implemented as hardware token-based (mutual) authentication of (for example) RG-LAP, or LAP-LAP
  - IPsec VPN for encryption of the link between the RG and the LAP.
- Agent system security
  - Protection against malevolent agents being injected into the system must be provided, e.g. via encryption of the communication between the agents.
- User/client security (protection)
  - Strong (PKI-based) authentication, e.g. for accessing the Web-based user interface and making subscription changes via the Web interface
  - Recommendations for security in the home network

### *1.3 TORRENT threat analysis*

In order to determine and select the appropriate security services and mechanisms that shall be implemented in the TORRENT system, a risk analysis has been conducted, based upon the security specification.

Based upon the proposed TORRENT general architecture, hardware architecture, and the software architecture, a threat analysis was conducted, to identify the risks to the system. From the entire list of threats and resulting risk assessment, a number of major threats were identified. The following is a list of threats to the TORRENT system that must be minimized with high priority:

- General Threats:
  - Denial of Service (DoS) attacks that cause a noticeable effect on the responsiveness of services to the users
  - Flooding of the network causing a noticeable reduction of throughput at the LAP
  - Access to the Emergency Telephone Service is denied
- Threats related to functions provided by the LAP:
  - Unauthorised access to the User Preferences database
- Threats related to RG/RG owner:
  - Masquerading as a LAP (e.g., to gain access to users info and/or to divert user access to services) or perform “man-in-the-middle attacks”. The attacker may perform this attack on a large number of users quite easily.
- Threats related to service provisioning:
  - The emergency call system is not accessible due to a flaw in the TORRENT system
  - Manipulation of the data sent between agents

The following is a list of countermeasures to the above threats that have been identified and which will be implemented:

- Mutual authentication of the RG and LAP
- Stateful Firewall in the LAP
- IDS tracking/actively blocking
- Access Control Lists (ACLs)
- The Emergency Telephone Service will be provided through the PSTN/ISDN. It will be ensured that the service is available even though the RG and LAP are powered down or unavailable
- Encryption and authentication of communication between agents
- In addition the following countermeasures should be implemented:
  - Strong Mutual authentication of LAP - RG
  - Encrypt the link between the LAP and RG
  - Strong authentication for user access to services
  - Strong user authentication for administrative access to the LAP
  - Strong user authentication for access to the agent system

- Provide TORRENT users with information about how to protect themselves from attacks. For example, provide information about anti-virus protection and advice all users to install anti-virus protection (and possibly, if the Service Provider wishes, to offer antivirus protection as a service)
- Rules and routines for administrators (e.g. separation of data/limited accessibility)
- Don't store sensitive information on the LAP in an unencrypted form
- Encrypt the link between the LAP and Terminal (e.g. SSL/TLS or IPsec)
- Require user authentication using PKI (X.509 certificates) e.g. via SSL from the user's terminal for access to the Web interface (e.g. the "View User Preferences Home Page function")
- Intelligence should not be located on the RG,
- Procedure for authentication of agents
- Authentication of agents with limited access time to the particular service and encryption of communication

### *1.4 Revised TORRENT security specification*

A revision of the TORRENT proposed security features has been created, placing the security features in two categories:

(i) priority 1 for the set of all features that must be implemented for the field trials, and

(ii) priority 2 for the features that must be implemented for a commercial version of the TORRENT RG and LAP.

The revised TORRENT proposed security services and mechanisms are as follows. These features have been prioritised for implementation:

- Network security:
  - Priority 1 features:
    - Mutual authentication of the LAP and RG
    - Stateful Firewall on the LAP (part of the agent policy engine)
    - Active Intrusion Detection System
    - The Emergency Telephone Service must be provided through the PSTN/ISDN. It must be ensured that the service is available even though the RG and LAP are powered down or unavailable
  - Priority 2 features:
    - Peer to peer authentication: Hardware token-based (mutual) authentication of (e.g.) RG-LAP, LAP-LAP
    - IPsec VPN for encryption of the link between the RG and the LAP
    - Sensitive information should not be stored on the LAP; an encrypted version of it can be stored instead
    - Calculate a Hash using an appropriate algorithm (e.g. MD5) of user Web pages hosted on the LAP for integrity checks, e.g. to identify replacement of content of user Web pages on LAP
    - A policy with rules and routines for administrators should be drawn up (e.g. for separation of data/limited accessibility). (Including Access Control Lists)
- Agent system security
  - Priority 1 features:
    - Protect against malevolent agents being injected into the system by encryption and authentication of communication between agents

- User/client security (protection)
  - Priority 2 features:
    - Strong (PKI-based) authentication e.g. for access to "View User Preferences Home Page function". Use of electronic signature may also be implemented for signing user subscription changes via the Web interface.
    - Recommendations for security in the home network. Provide TORRENT users with information about how to protect themselves from attacks. For example, provide information about anti-virus protection and advice all users to install anti-virus protection

The security aspects of the TORRENT test-bed will be addressed in more detail in the following chapters.

## 2. Authentication

The authentication requirements for the TORRENT system have been determined by the threat analysis. (Ref. Appendix C of this document) It was determined that the threats of masquerading by LAP or RG can be mitigated by mutually authenticating the LAP and the RG. Authentication is important e.g. to ensure that the authorised customer behind an RG is getting the QoS that was requested, to reduce the likelihood of fraud and also as a baseline for avoiding repudiation of messages e.g. payments. Users and providers of networks and services will thus benefit from this security service.

It is a requirement of TORRENT to protect residential users and business interests (Network Operators and Service Providers) by mutually authenticating the RG and the LAP. It is also a requirement to authenticate users accessing the system e.g. to make changes to the user profile and user preferences (service subscription, QoS, cost, etc.) It can be foreseen that if a hardware (HW) token were used as key holder of the authentication exchange, then this HW token could also be used for user authentication (of the RG user) and eCommerce applications. The same token could be used for authentication and key exchange for an IPsec VPN tunnel service. Certificates and associated private keys for authentication and encryption of agents and agent communication could also be stored on the HW token. In fact, certificates and associated private keys for the services of user authentication, electronic signature, and encryption can be reused by TORRENT's agent-based Service to Resource Management system for authentication of the user agents.

### *2.1 Summary of Authentication paper*

The TORRENT system allows residential customers to choose amongst a variety of service offerings, over a range of Core Networks and subject to user requirements such as QoS, mobility, cost and availability. These issues place requirements on authentication for network access, with a need for mutual authentication of the RG and the LAP. This paper [2] examines the authentication issues for the TORRENT system and presents a public key based authentication protocol for mutually authenticating the RG and LAP.

## 3. Internet Firewall

In theory, an Internet firewall serves to prevent the dangers of the Internet from spreading to your internal network [3] In practice, an Internet firewall is more like a moat of a medieval castle: It has the following attributes:

- It restricts people entering your network to one carefully controlled and monitored (see §5 and Appendix A) point.
- It prevents attackers from getting close to other defences.
- It restricts people to leaving the network at a carefully controlled point.

An Internet firewall is most often installed at the point where the internal network connects to the Internet. As can be seen from the torrent architecture (See D3.2 Figure 1), this obviously happens at the Local Access Point.

All traffic coming from the internet or going out from the internal network (access network/RGs) passes through the firewall. Because the traffic passes through it, the firewall has the opportunity to make sure that this traffic is acceptable.

"Acceptable" in the TORRENT case means that it is either Domain Name System (DNS) traffic, which is required as users generally do not think of hosts in terms of IP addresses or any traffic that enters or leaves the LAP in accordance with the SRM functionality (See D3.2 §5), and indeed, by the policy the operator of the LAP wishes to implement.

Appendix A in this document outlines the characteristics of DNS, FTP and http traffic in a firewall context and how these protocols will be dealt with in TORRENT.

## 4. Encryption of the link between the RG and the LAP

The threat analysis revealed that it would be desirable for LAP operators to offer a VPN service which consisted of a secure communications channel between a Residential Gateway (RG) and a LAP. In time, this led to an evaluation of the performance implications of using IP security (IPsec) (Ref Appendix D) to achieve this goal. Several different VPN scenarios have been tested, measured and analysed. The tests were performed on IPv4 and IPv6 networks and results were collected for several client enumerations in both IPv4 and IPv6 control scenarios in addition to the IPv6 enciphered scenarios.

### *4.1 Summary of VPN Overhead paper*

Virtual Private Networks (VPNs) use the Internet or other network service as a backbone to provide a secure connection across a potentially hostile WAN. Such security guarantees provide the motivation for VPN deployment. This security does, however, come at a performance cost brought about by the increased processing overhead. This paper presents an investigation into these overheads. In particular, this investigation will consider the server side overhead for VPN deployments and seek to establish a relationship between this overhead and the number of clients being serviced.

### *4.2 Main Findings*

IPsec could be deployed as an encryption and authentication service in the TORRENT architecture, without hitting any significant performance bottlenecks. If the algorithms deployed are AES for encryption and HMAC-MD5 for authentication then one LAP could support upto 90Mbps of traffic from the access network.

As software is a repidly moving target, this topic will, hopefully, be re-visited before the end of the project, possibly with a comparison done between a hardware based IPsec accelerator Card versus the current software based implementation. Based on previous experience[4], we would assume that a hardware based cccellerator card would reduce the load on the LAP by a significant amount, thus allowing each LAP to service more RG's.

In the second trial, tests were done between the LAP and the RG in the lab in UST (Appendix E). In summary, the findings show that there is a penalty to be paid in terms of processing overhead, this is most obvious on the lower powered RG, the symptoms of which are both lower throughput, and hugely increased processor overhead but most likely, Moore's Law, and more efficient IPsec implementations will remove this obstacle in time.

# 5. Intrusion Detection System

## *5.1 Intended role of IDS*

The Intrusion Detection System (IDS) is intended to provide the following functionality:

1. To protect the LAP by detection of malevolent traffic from both the Internet and the RGs.
2. To protect the RGs from such traffic coming from the Internet and from other RGs.
3. To monitor such traffic generated by the RGs.

By malevolent traffic we mean Internet worms, some viruses, hacking attempts and other malicious uses of the network.

The IDS will monitor all traffic passing through the LAP. If some of the traffic matches certain 'rules' or patterns the IDS can be configured to send an alert to the operator, log the traffic and, depending on the deemed severity of the attack, drop all traffic from the source address. If the traffic was not considered a threat the 'event' will be logged for later analysis. This active monitoring, in conjunction with a tightly configured firewall will deliver a high level of security to the torrent testbed by:

- Protecting the Users of the system from each other.
- Protecting the Users of the system from others on the Internet.
- Protecting the LAP from Crackers both inside and out.

The most important IPv4 Intrusion Detection Systems are:

- Dragon
- Network Flight Recorder
- Cisco IDS
- Snort
- RealSecure

The Intrusion Detection System of choice for our investigations was the open source tool, Snort [5].

## *5.2 Difficulties faced*

Currently Snort does not support the monitoring of IPv6 traffic (this is a Work In Progress by the Snort development team). This makes the IDS only useful for monitoring IPv4 traffic.

The main issue with deployment of an IDS in the Flextel LAP is the fact that in order for Snort to operate it needs to 'see' all traffic passing through all interfaces, in general this is a small monitoring nightmare as in a typical scenario a 'sniffer' would be required on every network interface that a RG is connected to and every interface that a 'core' network is connected to.

## *5.3 Possible solutions*

Conveniently however, the Flextel LAP architecture neatly provides a possible solution. As all traffic from the access network(s) to the core network(s) passes across the IPB, this is the place to place the Snort 'sniffer'.

However due to the current (rapidly prototyped) CLIP implementation on the LAP Snort can only 'see' one side of the conversation, this is enough to allow snort to monitor traffic and generate 'alerts' though we would like to working towards a more complete solution.

The underlying software that Snort relies on, tcpdump, is fully IPv6 aware. As Snort is 'open source' it is possible to generate code required to get Snort monitoring IPv6 traffic.

Tests were performed on the WIT-TSSG testbed (which is the similiar hardware to the LAP). The Inter Processor Bus architecture of the Flextel LAP allows a common point for 'sniffing' all traffic that passes through the system from access to core networks. Flextel term this feature "IP Carbon Copy"

The SNORT IDS has been installed in the WIT-TSSG test-bed and tested in order to evaluate its IPv6 capabilities. The result is that the version under test, 2.0.0 has still very few IPv6 capabilities compared to the rich feature set provided for IPv4. This applies especially concerning the analysis and decoding of IPv6 packets, which is already possible with genuine packet analysers, ethereal and tcpdump.

The test was set up as follows:

- Three dual processor blades, representing:
  - Core
  - Access
  - IDS
- All traffic between the Core and Access blades was configured to be sent to the IDS blade.
- Netperf was used to send the maximum amount of IPv4 traffic possible across the Inter Processor Bus and hence maximise the processor load on the IDS blade.

Results:
Using snort, and a configuration (Appendix B) commensurate with the services offered by TORRENT, the processor load on the IDS blade averaged 85% while monitoring the traffic passing. This does show that there is a very large processing requirement for IDS deployment. That said, this 85% overhead figure is only reached by saturating the IPB. So may not be a realistic deployment scenario, but more of an indicator of the scalability of the system.

When doing the above tests, we initially received anomalous throughput figures across the IPB (throughputs ranging from 70 to 150Mbps, and overheads ranging fro 20-60%). After much testing, debugging and discussing the problem with Flextel, they supplied us with a revised version of the IPB firmware which fixed the problem completely.

### 5.3.1 Recommendations for Network IDS configuration.

We recommend that the operator:

- Forbid and log all telnet access attempts.
- Log all ftp 'root' logins and brute force attacks
- Log and block all port scan attempts including TCP connection scans, SYN FIN scan, NULL scan, XMAS scan and nmap XMAS scan.

We also recommend that the IDS is configured to detect, log and 'blackhole' all ip addresses that attempt common attacks such as:

- Scanning of critical services such as finger, systat, ttymux, netstat
- All portmap access and RPC service attacks
- Shell execution attacks
- DoS attacks
- *Land* attacks
- *IP Spoofing* attacks
- FTP specific attacks (looking for passwd file, etc)

Web server attacks such as:

- Searching for vulnerable CGI scripts
- Shell execution attacks
- *Passwd* and *shadow* file access attempts

DNS Server attacks

- TCP transfer requests from unauthorised hosts
- BIND version requests from unauthorised hosts
- IQUERY requests from unauthorised hosts

e-mail Server attacks

- Server scans using EXPN and VRFY commands
- Sendmail exploit scans
- Corrupt MAIL and RCPT commands sent to smtp server.

## 6. Summary of Agent Security Paper

FIPA is one of the main standards available within the software agent domain today. FIPA agents, which are part of the software agent domain are based on the concept of the distributed intelligent agent domain and requires secure and fair negotiation between agents. The TORRENT QoS negotiation agent system is based on the concepts of FIPA and requires secure and fair negotiation between agents. In order to achieve this we need to, for example, ensure the availability of agent system services for authorized users and avoid the insertion of malevolent agent into the system. However, the main focus within the FIPA domain has not been on security issues but on development and testing. Since FIPA agents operate in an open environment they are vulnerable to security attacks and one should consider security issues, such as the problem of authentication of agents, securing communication, and preventing unauthorised activity from hackers or malevolent agents. This work focus on security issues in FIPA agent systems by giving overviews of software agent technologies and IT security before discussing and highlighting security issues in FIPA agent systems in general and the TORRENT agent system in particular. A threat analysis including an assessment of these threats was carried out as part of the TORRENT project. In this paper we present a subset of the results from this analysis and a security framework that meets some of these security challenges.

The TORRENT agent system consists of several agents, but in the threat analysis we considered the agent system as a whole and where interested in general threats. Threats to the agent system where identified according to three categories:

1. Threats to the agent system during initialising and starting of the agents.
2. Threats to the agent system during run-time.
3. Threats to the agent system when terminating agents.

The risk scale used was low, moderate, serious, and extreme. Threats identified in category 1 were;

a. Unauthorised start of agent.
b. Authorised start of agent failing.
c. Uncontrolled start of agent with the risk values of serious, moderate and low.

Threats identified in category 2 were;

d. Masquerade of agent.

e. Eavesdropping of data from agent.
f. Spoofing of an agent.
g. Manipulation of data sent between agents

Threats identified in category 3 were
h. Unauthorised termination of agent.
i. Authorised termination of agent fails.
j. Uncontrolled termination of agent.

Risks in need of treatment were defined to be risks with a value equal to moderate or higher. One important issue to note is that the risk values are individual for each system and each case even though the threats are general for FIPA agent systems.

The FIPA Agent security framework is designed based on the security requirements identified in the risk analysis. These requirements are derived from the result of the risk analysis and proposed as treatment options for the risks having the risk value medium or higher. In order to meet the requirements the FIPA agent security framework needs to cover authentication of users, authentication of agents, and encryption of communication between user and agent and between agents

This paper has recently been submitted to AAMAS 2004.

## 7. Home Network Security

Recommendations for security in the home network have been provided in D1.1, and D3.1. In addition to the information that we have provided, the CERT® Coordination Centre (CERT/CC), provides an extensive guide to home computer security which is available from [6]. There is also a very useful guide to home network security available again from Cert[7].

## 8. Recommendations for future systems

It is our recommendation that any future system supports at a minimum, both the priority 1 and priority 2 feature set mentioned in §1.4. This would allow for a reasonably secure deployment, by operators, of services to a customer base whereby both operators and users of the system could be reasonably confident of secure, confidential access to services.

It must also be acknowledged that IPv4s days are numbered, there is no need for a single "flag day" for conversion from IPv4 to IPv6 in existing networks. An enterprise or service provider/operator will progressively introduce IPv6 connectivity and services, until eventually they become the normal way of doing business and IPv4 becomes a legacy.

Universal connectivity will simplify end-to-end security, without preventing conventional firewall, proxy and intrusion detection techniques, and will simplify application-level security. None of this will invalidate the work done in TORRENT.

### *8.1 The Evolutionary aspects of the TORRENT security architecture*

In the age of full IPv6 deployment, the following can be envisioned: Privacy can actually be much easier. Today, with unlisted numbers, as soon as the number becomes known, it has to be changed. With IPv6, and certificates, IP addresses can be public, but the certificate governs what traffic is allowed in, and what traffic should be prohibited. Only users with approved certificates can reach the destination IP address. Privacy can

also be established as certificate standardisation progresses. The X.500 catalogue containing the certificate and public key can be designed in such a way that personal info is only transmitted according to policy.

## 9. Conclusions

This document has been produced by WP3: Service to Resource Management.

The initial role of WP3 was to develop the Service to Resource Management Software

WP3 also identified, through a rigorous threat analysis several areas of the system that needed to be addressed.

This document has concentrated on WP3s effort in dealing with the issues revealed in the threat analysis.

Each security service has been evaluated in its respective chapter. The evaluation is intended to show that the technique is feasible and that the hardware and software operates in accordance with the user requirements

The TORRENT system security architecture and features have been refined throughout the project, through the detailed analysis of the requirements of users, and the network operators and service providers. This final version of the Deliverable documents the current view of the security features of the system.

## 10. Abbreviations

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| ASP | Application Service Provider |
| ASP | Application Service Provisioning |
| ATM | Asynchronous Transfer Mode |
| BER | Bit Error Rate |
| BRI | Basic Rate Interface |
| CATV | Cable TV |
| CE | Compact Edition |
| CEC | Commission of the European Community |
| CLID | Calling Line Identification |
| CLID | Calling Line Identity |
| CoS | Class of Service |
| CPU | Central Processing Unit |
| CSCW | Computer-Supported Collaborative Work |
| dB | decibel |
| DBS | Direct Broadcasting Satellite |
| DECT | (digital wireless technology) |
| DiffServ | Differentiated Service |
| DS | Differentiated Service |
| DSCP | Differentiated Services Code Point |
| DSLAM | Digital Subscriber Line Access Multiplexer |
| DVD | Digital Video Disk |
| ERLE | Echo Return Loss Enhancement |
| ETSI | European Telecommunications Standards Institute |
| FEC | Forwarding Equivalent Class |
| fps | frames per second |
| FTTC | Fibre-to-the-Curb |
| FTTCab | Fibre to the Cabinet |
| FTTH | Fibre-to-the-Home |
| FYTTB | Fibre-to-the-Building |
| GSM | Global System for Mobile |
| H/W | hardware |
| HAVi™ | Home Audio Visual interface |
| HDTV | High Definition TV |
| IEEE | Institution of Electrical and Electronic Engineers |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IrDA | Infrared Device Adapter |
| ISDN | Integrated Services Digital Network |
| ISP | Integrated Services Provider |
| ITU | International Telecommunications Union |
| ITU-T | International Telecommunications Union - Telecommunications |
| kbit/s | KiloBits/second |
| Khz | Kilo Herz |
| LAN | Local Area Network |
| LAP | Local Access Point |

| | |
|---|---|
| LCD | Liquid Crystal Display |
| LMDS | Local Multi-point Distribution Services |
| LSP | label switched path |
| MBit/s | Mega bits / second |
| MPEG | Motion Picture Experts Group |
| MPLS | Multi-Protocol Label Switching |
| ms | milli second |
| MUX | multiplexer |
| NFAS | Non-Facility Associated Signalling |
| NP | Network Performance |
| NT-1 | Network Termination 1 |
| NT-2 | Network Termination 2 |
| NVOD | near video on demand |
| OLT | Optical Line Terminal (located at central office or cable head-end) |
| ONU | Optical Network Units |
| OS | Operating System |
| OSGi | Open Systems Gateway initiative |
| PC | Personal Computer |
| PDA | Personal Digital Assistants |
| PHB | Per Hop Behaviour |
| PLC | Powerline Communication |
| PNNI | Private Network Node Interface |
| PON | Passive Optical Network |
| POTS | Plain Old Telephone Network |
| PRI | Primary Rate Interface |
| PSTN | Public Switched Telephony Network |
| QoS | Quality of Service |
| RG | Residential Gateway |
| RSVP | Resource Reservation Protocol |
| RTP | Real-Time Transport Protocol |
| SDH | Synchronous Digital Hierarchy |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SME | Small to Medium Enterprise |
| SS7 | Signalling System 7 |
| STB | Set Top Box |
| STM | Synchronous Transmission Mode |
| $T_a$ | Absolute delay |
| TA | Terminal Adapter |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TDM | Time Division Multiplexing |
| TE1 | Terminal Equipment 1 |
| TE2 | Terminal Equipment 2 |
| TELR | Talker Echo Loudness |
| TORRENT | Towards a Realistic End-User Testbed |
| $T_r$ | Round trip delay |
| TV | Television |
| UDP | User Datagram Protocol |

| | |
|---|---|
| UMTS | Universal Mobile Telecommunications System |
| USB | Universal Serial Bus |
| VC | virtual circuit |
| VCR | video recorder |
| VGA | Versatile Graphics Adapter |
| VOD | video on demand |
| VoIP | Voice-over-IP |
| VP | virtual path |
| WAP | Wireless Applications Protocol |
| WDM | Wavelength Division Multiplexing |
| WEPL | Weighted Echo Path Loss |
| WLL | Wireless Local Loop |
| WP | Work Package |
| xDSL | Generic term for Digital Subscriber Line technology - A/H/S/VDSL |

# References

(Former Appendix A)

1. 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects*; 3G Security; Security Architecture (Release 4)
2. Judith Rossebø, John Ronan, Kristian Walsh: Issues in Multi-Service Residential Access Networks. In Proceedings of the 6th IFIP/IEEE International Conference on Management of Multimedia Networks and Services, Belfast, Northern Ireland, Ireland, September 7-10, 2003
3. *Building Internet Firewall, second edition* by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, O'Reilly & Associates June 2000.
4. *Firmware Deployment of Strong Encryption an Investigation and Implementation* by John Ronan Bsc (Hons), submitted for MSc in computing by Research and Thesis October 2000.
5. *The Open Source Network Intrusion Detection System, **http://www.snort.org***
6. **Cert Coordination Center, Home Computer Security, http://www.cert.org/homeusers/HomeComputerSecurity/**
7. **Cert Coordination Center, Home Network Security, http://www.cert.org/tech_tips/home_networks.html**
8. **Euro6IX, D4.4A Report on the second year network and application research activities, http://www.euro6ix.org/documents/e_publics_deli.php**

# Appendix B Firewall Characteristics

## B.1 Firewall Characteristics & Snort Configuration

This document intends to be a short explanation of the low-level protocol issues that have to be dealt with in provisioning for a 'tight' firewall, while still allowing the system to be useable and useful. This section is largely taken from [6]

## B.2 Firewalls

### B.2.1 DNS

#### *B.2.1.1 Packet filtering characteristics of DNS*

There are two types of DNS network activities: lookups and zone transfers. We will deal with lookups here, as that is all our clients need to be able to do.

A DNS server uses well-known port 53 as its server port for TCP and UDP. It uses a port above 1023 for TCP requests. Some servers use 53 as a source port for UDP requests, while others will use a port above 1023. A DNS client uses a random port above 1023 for both UDP and TCP. You can thus differentiate between the following:

**A client-to-server query**

**Source port is above 1023, destination port is 53.**

**A server-to-client response**

**Source port is 53, destination port is above 1023.**

**A server-to-server query or response**

**At least with UDP on some servers where both source and destination port are 53; with TCP, the requesting server will use a port above 1023. Servers that do not use UDP source port 53 are indistinguishable from clients.**

| Direction | Source Addr. | Dest. Addr. | Protocol | Source Port | Dest. Port | ACK Set | Notes |
|---|---|---|---|---|---|---|---|
| In | Ext | Int | UDP | >1023 | 53 | [1] | Query via UDP, external client to internal server. |
| Out | Int | Ext | UDP | **53** | >1023 | [1] | Response via UDP, internal server to external client. |
| In | Ext | Int | TCP | >1023 | 53 | [2] | Query via TCP, external client to internal server |
| In | Int | Ext | TCP | 53 | >1023 | Yes | Response via TCP, internal server to external client |
| Out | Int | Ext | UDP | >1023 | 53 | [1] | Query via UDP, internal client to external server |
| In | Ext | Int | UDP | 53 | >1023 | [1] | Response via UDP, external server to internal client. |
| Out | Int | Ext | TCP | >1023 | 53 | [2] | Query via TCP, internal client |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | to external server |
| In | Ext | Int | TCP | 53 | >1023 | Yes | Response via TCP, external server to internal client. |

**[1] UDP has no ACK equivalent**
**[2] ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.**

### B.2.2 HTTP

#### *B.2.2.1 Packet filtering characteristics of http*

http is a TCP-based service. Clients use random ports above 1023. Most servers use port 80, but some don't. This complicates things considerably from a packet filtering point of view. If users wish to access a server running on a non-standard port, you have several choices.

- You can tell the users they cannot do it.
- You can add a special exception for that specific service to your packet filtering rules. This is bad as the users first have to recognise the problem and have to wait until you have fixed it.
- You can try and convince the servers owner to move to a standard port.
- You can proxy the connections from the client. This requires setup on the client end.
- You can filter on the ACK bit, you can allow all outbound connections regardless of destination port. This opens up a wide variety of services, including passive-mode FTP. It also is a noticeable increase in your vulnerability.

Your firewall should prevent people on the internal network from setting up their own servers at non-standard ports.

| **Direction** | **Source Addr.** | **Dest. Addr.** | **Protocol** | **Source Port** | **Dest. Port** | **ACK Set** | **Notes** |
|---|---|---|---|---|---|---|---|
| In | Ext | Int | TCP | >1023 | 80[1] | [2] | Request, external client to internal server. |
| Out | Int | Ext | TCP | 80[1] | >1023 | Yes | Request, internal server to external client. |
| Out | Int | Ext | TCP | >1023 | 80[1] | [2] | Request, internal client to external server. |
| In | Ext | Int | TCP | 80[2] | >1023 | Yes | Response, external server to internal client. |

1 80 is the standard port for http servers.
2 ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

#### *B.2.2.2 Proxying characteristics of http.*

Various clients support various proxying schemes. Some clients will allow you to use an http proxy for protocols other than http, and most of them depend on using CONNECT, which makes the http proxy into a generic proxy, though this is not a particularly secure way of using a proxy.

It is extremely important to prevent external users from connecting to your proxy server, as it could be used as a platform from which to attack internal servers. Even if the proxy server can't be used this way it can be used to attack third parties. It should be noted that apache2 does proxy IPv6 http traffic, including the CONNECT mode mentioned above.

#### *B.2.2.3 Network Address Translation Characteristics of http.*

http does not use embedded IP addresses as a functional part of the protocol, so network address translation will not interfere with http.

### B.2.3 FTP

#### *B.2.3.1 Packet filtering characteristics of FTP*

FTP uses two separate TCP connections: one to carry commands and results between the client and server (commonly called the command channel), and the other to carry actual files and directory listings transferred (the data channel). The command channel uses port 21 on the server end and a port above 1023 on the client. FTP has two different ways to set up the data channel, called normal mode and passive mode. In normal mode, the server uses port 20 for the data channel, while in passive mode it uses a port above 1023. The client always uses a port above 1023 for the data channel.

Passive mode is useful because it allows you to avoid start-of-connection filtering problems. In passive mode, all connections will be opened from the inside, by the client.

| **Direction** | **Source Addr.** | **Dest. Addr.** | **Protocol** | **Source Port** | **Dest. Port** | **ACK Set** | **Notes** |
|---|---|---|---|---|---|---|---|
| In | Ext | Int | TCP | >1023 | 21 | [1] | Incoming Ftp Request |
| Out | Int | Ext | TCP | 21 | >1023 | Yes | Response to incoming request. |
| Out | Int | Ext | TCP | 20 | >1023 | [1] | Data channel creation for incoming ftp request, normal mode |
| In | Ext | Int | TCP | >1023 | 20 | Yes | Data channel responses for incoming FTP request, normal mode. |
| In | Ext | Int | TCP | >1023 | >1023 | [1] | Data channel creation for incoming ftp request, passive mode. |
| Out | Int | Ext | TCP | >1023 | >1023 | Yes | Data channel responses for incoming ftp request, passive mode. |
| Out | Int | Ext | TCP | >1023 | 21 | [1] | Outgoing FTP request |
| In | Ext | Int | TCP | 21 | >1023 | Yes | Response to outgoing request. |
| In | Ext | Int | TCP | 20 | >1023 | [1] | Data channel creation for outgoing ftp request, normal mode |
| Out | Int | Ext | TCP | >1023 | 20 | Yes | Data channel responses for |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | outgoing FTP request, normal mode. |
| Out | Int | Ext | TCP | >1023 | >1023 | [1] | Data channel creation for outgoing ftp request, passive mode. |
| In | Ext | Int | TCP | >1023 | >1023 | Yes | Data channel responses for outgoing ftp request, passive mode. |

[1] ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

### *B.2.3.2 Proxying characteristics of FTP*

Because of problems with passive mode, and because of complications introduced in the DNS service, proxying is a particularly attractive solution for outbound FTP. Using normal-mode proxied client allows you to talk reliably to external servers without having to allow incoming TCP connections for the data channel to any host except the LAP. It should be noted that apache2 does proxy IPv6 ftp traffic.

### *B.2.3.3 Network Address Translation Characteristics of FTP*

FTP uses embedded IP addresses to set up the data connection and will not work with network address translation unless the translator modifies the contents of the packets.

### *B.2.3.4 Firewall Initialisation Script*

```
#!/bin/bash
#
#
# Firewall startup script.
# By Jerry Horgan.

FWVER=1.0
IPTABLES=/opt/torrent/local/iptables/sbin/iptables
IP6TABLES=/opt/torrent/local/iptables/sbin/ip6tables
INSMOD=/sbin/insmod
LSMOD=/sbin/lsmod
GREP=/bin/grep
AWK=/bin/awk

IFA="eth0"
IFB="hdlc1"

PROXY="localhost"


# Web Browsing Proxy Port
BROWS="8080"
# Web Downloading Proxy Port
DOWNL="8081"
# VideoLAN Proxy Port
VIDEO="8085"
# Audio over HTTP Proxy Port
AUDIO="8086"
```

```
GLOBAL="0.0.0.0/0"
GLOBAL_v6="::"

case "$1" in
  start)
      echo -e "\n\nLoading Firewall Rules version $FWVER..\n"
      echo " - Verifying that all kernel modules are ok"
      /sbin/depmod -a
      echo -en "      Loading Kernel Modules: "
      if [ -z "` $LSMOD | $GREP ip_tables | $AWK {'print $1'} `" ]; then
            echo -en "\n    ip_tables, "
            $INSMOD ip_tables
      fi
      if [ -z "` $LSMOD | $GREP ip_conntrack | $AWK {'print $1'} `" ]; then
            echo -en "\n    ip_conntrack, "
            $INSMOD ip_conntrack
      fi
      if [ -z "` $LSMOD | $GREP ip_conntrack_ftp | $AWK {'print $1'} `" ]; then
            echo -en "\n    ip_conntrack_ftp, "
            $INSMOD ip_conntrack_ftp
      fi
      if [ -z "` $LSMOD | $GREP iptable_nat | $AWK {'print $1'} `" ]; then
            echo -en "\n    iptable_nat, "
            $INSMOD iptable_nat
      fi
      if [ -z "` $LSMOD | $GREP ip_nat_ftp | $AWK {'print $1'} `" ]; then
            echo -en "\n    ip_nat_ftp, "
            $INSMOD ip_nat_ftp
      fi
      echo -en "\n      Done loading modules."

      echo " - Clearing any existing rules and setting default policy.."
      $IPTABLES -P INPUT ACCEPT
      $IPTABLES -F INPUT
      $IPTABLES -P OUTPUT ACCEPT
      $IPTABLES -F OUTPUT

      $IP6TABLES -P INPUT ACCEPT
      $IP6TABLES -F INPUT
      $IP6TABLES -P OUTPUT ACCEPT
      $IP6TABLES -F OUTPUT


      if [ -n "`$IPTABLES -L | $GREP drop-and-log-it`" ] ; then
            $IPTABLES -F drop-and-log-it
      fi

      if [ -n "`$IP6TABLES -L | $GREP drop-and-log-it`" ] ; then
            $IP6TABLES -F drop-and-log-it
      fi


      $IPTABLES -Z
```

```
$IP6TABLES -Z

echo " - Creating a DROP chain .. "
$IPTABLES -N drop-and-log-it
$IPTABLES -A drop-and-log-it -j LOG --log-level info
$IPTABLES -A drop-and-log-it -j DROP

$IP6TABLES -N drop-and-log-it
$IP6TABLES -A drop-and-log-it -j LOG --log-level info
$IP6TABLES -A drop-and-log-it -j DROP


echo " - Loading IPv4 INPUT Rulesets"
# loopback i/f valid
$IPTABLES -A INPUT -i lo -s $GLOBAL -d $GLOBAL -j ACCEPT
# Allow external ICMP pings
$IPTABLES -A INPUT -i $IFA -p ICMP -s $GLOBAL -j ACCEPT
$IPTABLES -A INPUT -i $IFB -p ICMP -s $GLOBAL -j ACCEPT
# Allow external ssh, smtp, http and https access
$IPTABLES -A INPUT -p tcp --dport 22 -i $IFA -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 22 -i $IFB -j ACCEPT
# Allow any related traffic coming back in
$IPTABLES -A INPUT -i $IFA -s $GLOBAL -m state --state RELATED,ESTABLISHED -j ACCEPT
$IPTABLES -A INPUT -i $IFB -s $GLOBAL -m state --state RELATED,ESTABLISHED -j ACCEPT
# DROP and log everything else
$IPTABLES -A INPUT -p all -i $IFA -j drop-and-log-it
$IPTABLES -A INPUT -p all -i $IFB -j drop-and-log-it

echo " - Loading IPv4 OUTPUT Rulesets"
# Allow all DNS requests out
$IPTABLES -A OUTPUT -p tcp --dport 53 -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 53 -i $IFB -j ACCEPT
$IPTABLES -A OUTPUT -p udp --dport 53 -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p udp --dport 53 -i $IFB -j ACCEPT
# Allow all Traffic out to the PROXIES
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $BROWS -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $DOWNL -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $VIDEO -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $AUDIO -i $IFA -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $BROWS -i $IFB -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $DOWNL -i $IFB -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $VIDEO -i $IFB -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $PROXY --dport $AUDIO -i $IFB -j ACCEPT
# Deny all other outbound traffic and log it
$IPTABLES -A OUTPUT -p all -j drop-and-log-it


echo " - Loading IPv6 INPUT Rulesets"
# loopback i/f valid
$IP6TABLES -A INPUT -i lo -s $GLOBAL_v6 -d $GLOBAL_v6 -j ACCEPT
# A6llow external ICMP pings
$IP6TABLES -A INPUT -i $IFA -p icmpv6 -s $GLOBAL_v6 -j ACCEPT
$IP6TABLES -A INPUT -i $IFB -p icmpv6 -s $GLOBAL_v6 -j ACCEPT
# Allow external ssh, smtp, http and https access
```

```
        $IP6TABLES -A INPUT -p tcp --dport 22 -i $IFA -j ACCEPT
        $IP6TABLES -A INPUT -p tcp --dport 22 -i $IFB -j ACCEPT
        # Allow any related traffic coming back in
        $IP66TABLES -A INPUT -i $IFA -s $GLOBAL_v6 -m state --state RELATED,ESTABLISHED -j ACCEPT
        $IPTABLES -A INPUT -i $IFB -s $GLOBAL_v6 -m state --state RELATED,ESTABLISHED -j ACCEPT
        # DROP and log everything else
        $IP6TABLES -A INPUT -p all -i $IFA -j drop-and-log-it
        $IP6TABLES -A INPUT -p all -i $IFB -j drop-and-log-it

        echo " - Loading IPv6 OUTPUT Rulesets"
        # Allow all DNS requests out
        $IP6TABLES -A OUTPUT -p tcp --dport 53 -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp --dport 53 -i $IFB -j ACCEPT
        $IP6TABLES -A OUTPUT -p udp --dport 53 -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p udp --dport 53 -i $IFB -j ACCEPT
        # Allow all Traffic out to the PROXIES
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $BROWS -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $DOWNL -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $VIDEO -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $AUDIO -i $IFA -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $BROWS -i $IFB -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $DOWNL -i $IFB -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $VIDEO -i $IFB -j ACCEPT
        $IP6TABLES -A OUTPUT -p tcp -d $PROXY --dport $AUDIO -i $IFB -j ACCEPT
        # Deny all other outbound traffic and log it
        $IP6TABLES -A OUTPUT -p all -j drop-and-log-it

        echo -e "\nFirewall Rules version $FWVER loaded.\n"
        ;;
  stop)
        echo -en "Flushing firewall rules .. \n"
        # Clear FireWall Rules
        $IPTABLES -F
        $IP6TABLES -F
        $IPTABLES -Z
        $IP6TABLES -Z
        ;;
  reload|restart)
        $0 stop
        $0 start
        ;;
  status)
        echo -en "Checking IPv4 firewall rules ..\n"
        $IPTABLES -L
        echo -en "Checking IPv6 firewall rules ..\n"
        $IP6TABLES -L
        ;;
  *)
        echo "Usage: /etc/init.d/firewall {start|stop|restart|reload|status}"
        exit 1
esac

exit 0
```

## B.3 Snort (IDS) Configuration

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.0.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
# $Id$
#
##################################################
# This file contains a sample snort configuration.
# You can take the following steps to create your
# own custom configuration:
#
#  1) Set the network variables for your network
#  2) Configure preprocessors
#  3) Configure output plugins
#  4) Customize your rule set
#
##################################################
# Step #1: Set the network variables:
#
# You must change the following variables to reflect
# your local network. The variable is currently
# setup for an RFC 1918 address space.
#
# You can specify it explicitly as:
#
# var HOME_NET 10.1.1.0/24
#
# or use global variable $<interfacename>_ADDRESS
# which will be always initialized to IP address and
# netmask of the network interface which you run
# snort at.  Under Windows, this must be specified
# as $(<interfacename>_ADDRESS), such as:
# $(\Device\Packet_{12345678-90AB-CDEF-1234567890AB}_ADDRESS)
#
# var HOME_NET $eth0_ADDRESS
#
# You can specify lists of IP addresses for HOME_NET
# by separating the IPs with commas like this:
#
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:
```

```
var HOME_NET any

# Set up the external network addresses as well.
# A good start may be "any"

var EXTERNAL_NET any

# Configure your server lists.  This allows snort to only look for attacks
# to systems that have a service up.  Why look for HTTP attacks if you are
# not running a web server?  This allows quick filtering based on IP addresses
# These configurations MUST follow the same configuration scheme as defined
# above for $HOME_NET.

# List of DNS servers on your network
var DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET

# List of web servers on your network
var HTTP_SERVERS $HOME_NET

# List of sql servers on your network
var SQL_SERVERS $HOME_NET

# List of telnet servers on your network
var TELNET_SERVERS $HOME_NET

# Configure your service ports.  This allows snort to look for attacks
# destined to a specific application only on the ports that application
# runs on.  For example, if you run a web server on port 8081, set your
# HTTP_PORTS variable like this:
#
# var HTTP_PORTS 8081
#
# Port lists must either be continuous [eg 80:8080], or a single port [eg 80].
# We will adding support for a real list of ports in the future.

# Ports you run web servers on
var HTTP_PORTS 80

# Ports you want to look for SHELLCODE on.
var SHELLCODE_PORTS !80

# Ports you do oracle attacks on
var ORACLE_PORTS 1521

# other variables
#
```

```
# AIM servers.  AOL has a habit of adding new AIM servers, so instead of
# modifying the signatures when they do, we add them to this list of
# servers.
var                                                                    AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.0/24,64.12.161.0/24,64.12.163.0/24,205.1
88.5.0/24,205.188.9.0/24]

# Path to your rules files (this can be a relative path)
var RULE_PATH ../rules

# Configure the snort decoder:
# ============================
#
# Stop generic decode events:
#
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
#
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
#
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
#
# config disable_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
#
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
#
# config disable_ipopt_alerts


# Configure the detection engine
# ==============================
#
# Use a different pattern matcher in case you have a machine with very
# limited resources:
#
# config detection: search-method lowmem


##################################################
# Step #2: Configure preprocessors
```

```
#
# General configuration for preprocessors is of
# the form
# preprocessor <name_of_processor>: <configuration_options>

# frag2: IP defragmentation support
# ------------------------------
# This preprocessor performs IP defragmentation.  This plugin will also detect
# people launching fragmentation attacks (usually DoS) against hosts.  No
# arguments loads the default configuration of the preprocessor, which is a
# 60 second timeout and a 4MB fragment buffer.

# The following (comma delimited) options are available for frag2
#    timeout [seconds] - sets the number of [seconds] than an unfinished
#                        fragment will be kept around waiting for completion,
#                        if this time expires the fragment will be flushed
#    memcap [bytes] - limit frag2 memory usage to [number] bytes
#                     (default:  4194304)
#
#    min_ttl [number] - minimum ttl to accept
#
#    ttl_limit [number] - difference of ttl to accept without alerting
#                         will cause false positves with router flap
#
# Frag2 uses Generator ID 113 and uses the following SIDS
# for that GID:
#  SID     Event description
# -----   -------------------
#   1       Oversized fragment (reassembled frag > 64k bytes)
#   2       Teardrop-type attack

preprocessor frag2

# stream4: stateful inspection/stream reassembly for Snort
#--------------------------------------------------------------------
# Use in concert with the -z [all|est] command line switch to defeat
# stick/snot against TCP rules.  Also performs full TCP stream
# reassembly, stateful inspection of TCP streams, etc.  Can statefully
# detect various portscan types, fingerprinting, ECN, etc.

# stateful inspection directive
# no arguments loads the defaults (timeout 30, memcap 8388608)
# options (options are comma delimited):
#   detect_scans - stream4 will detect stealth portscans and generate alerts
#                  when it sees them when this option is set
#   detect_state_problems - detect TCP state problems, this tends to be very
#                           noisy because there are a lot of crappy ip stack
#                           implementations out there
#
```

```
#   disable_evasion_alerts - turn off the possibly noisy mitigation of
#                       overlapping sequences.
#
#
#   min_ttl [number]       - set a minium ttl that snort will accept to
#                       stream reassembly
#
#   ttl_limit [number]     - differential of the initial ttl on a session versus
#                        the normal that someone may be playing games.
#                        Routing flap may cause lots of false positives.
#
#   keepstats [machine|binary] - keep session statistics, add "machine" to
#                     get them in a flat format for machine reading, add
#                     "binary" to get them in a unified binary output
#                     format
#   noinspect - turn off stateful inspection only
#   timeout [number] - set the session timeout counter to [number] seconds,
#                   default is 30 seconds
#   memcap [number] - limit stream4 memory usage to [number] bytes
#   log_flushed_streams - if an event is detected on a stream this option will
#                     cause all packets that are stored in the stream4
#                     packet buffers to be flushed to disk.  This only
#                     works when logging in pcap mode!
#
# Stream4 uses Generator ID 111 and uses the following SIDS
# for that GID:
#  SID    Event description
# -----   -------------------
#   1      Stealth activity
#   2      Evasive RST packet
#   3      Evasive TCP packet retransmission
#   4      TCP Window violation
#   5      Data on SYN packet
#   6      Stealth scan: full XMAS
#   7      Stealth scan: SYN-ACK-PSH-URG
#   8      Stealth scan: FIN scan
#   9      Stealth scan: NULL scan
#   10     Stealth scan: NMAP XMAS scan
#   11     Stealth scan: Vecna scan
#   12     Stealth scan: NMAP fingerprint scan stateful detect
#   13     Stealth scan: SYN-FIN scan
#   14     TCP forward overlap

preprocessor stream4: detect_scans, disable_evasion_alerts

# tcp stream reassembly directive
# no arguments loads the default configuration
#   Only reassemble the client,
#   Only reassemble the default list of ports (See below),
```

```
#   Give alerts for "bad" streams
#
# Available options (comma delimited):
#   clientonly - reassemble traffic for the client side of a connection only
#   serveronly - reassemble traffic for the server side of a connection only
#   both - reassemble both sides of a session
#   noalerts - turn off alerts from the stream reassembly stage of stream4
#   ports [list] - use the space separated list of ports in [list], "all"
#                  will turn on reassembly for all ports, "default" will turn
#                  on reassembly for ports 21, 23, 25, 53, 80, 143, 110, 111
#                  and 513

preprocessor stream4_reassemble

# http_decode: normalize HTTP requests
# ----------------------------------
# http_decode normalizes HTTP requests from remote
# machines by converting any %XX character
# substitutions to their ASCII equivalent. This is
# very useful for doing things like defeating hostile
# attackers trying to stealth themselves from IDSs by
# mixing these substitutions in with the request.
# Specify the port numbers you want it to analyze as arguments.
#
# Major code cleanups thanks to rfp
#
# unicode          - normalize unicode
# iis_alt_unicode  - %u encoding from iis
# double_encode    - alert on possible double encodings
# iis_flip_slash   - normalize \ as /
# full_whitespace  - treat \t as whitespace ( for apache )
#
# for that GID:
#  SID     Event description
# -----   -------------------
#   1       UNICODE attack
#   2       NULL byte attack

preprocessor http_decode: 80 unicode iis_alt_unicode double_encode iis_flip_slash full_whitespace

# rpc_decode: normalize RPC traffic
# ---------------------------------
# RPC may be sent in alternate encodings besides the usual
# 4-byte encoding that is used by default.  This preprocessor
# normalized RPC traffic in much the same way as the http_decode
# preprocessor.  This plugin takes the ports numbers that RPC
# services are running on as arguments.
# The RPC decode preprocessor uses generator ID 106
#
```

```
# arguments: space separated list
# alert_fragments - alert on any rpc fragmented TCP data
# no_alert_multiple_requests - don't alert when >1 rpc query is in a packet
# no_alert_large_fragments - don't alert when the fragmented
#                            sizes exceed the current packet size
# no_alert_incomplete - don't alert when a single segment
#                       exceeds the current packet size

preprocessor rpc_decode: 111 32771

# bo: Back Orifice detector
# -------------------------
# Detects Back Orifice traffic on the network.  Takes no arguments in 2.0.
#
# The Back Orifice detector uses Generator ID 105 and uses the
# following SIDS for that GID:
#  SID     Event description
# -----   -------------------
#   1       Back Orifice traffic detected

preprocessor bo

# telnet_decode: Telnet negotiation string normalizer
# ---------------------------------------------------
# This preprocessor "normalizes" telnet negotiation strings from
# telnet and ftp traffic.  It works in much the same way as the
# http_decode preprocessor, searching for traffic that breaks up
# the normal data stream of a protocol and replacing it with
# a normalized representation of that traffic so that the "content"
# pattern matching keyword can work without requiring modifications.
# This preprocessor requires no arguments.
# Portscan uses Generator ID 109 and does not generate any SID currently.

preprocessor telnet_decode

# Portscan: detect a variety of portscans
# ---------------------------------------
# portscan preprocessor by Patrick Mullen <p_mullen@linuxrc.net>
# This preprocessor detects UDP packets or TCP SYN packets going to
# four different ports in less than three seconds. "Stealth" TCP
# packets are always detected, regardless of these settings.
# Portscan uses Generator ID 100 and uses the following SIDS for that GID:
#  SID     Event description
# -----   -------------------
#   1       Portscan detect
#   2       Inter-scan info
#   3       Portscan End

# preprocessor portscan: $HOME_NET 4 3 portscan.log
```

```
# Use portscan-ignorehosts to ignore TCP SYN and UDP "scans" from
# specific networks or hosts to reduce false alerts. It is typical
# to see many false alerts from DNS servers so you may want to
# add your DNS servers here. You can all multiple hosts/networks
# in a whitespace-delimited list.
#
#preprocessor portscan-ignorehosts: 0.0.0.0

# arpspoof
#--------------------------------------
# Experimental ARP detection code from Jeff Nathan, detects ARP attacks,
# unicast ARP requests, and specific ARP mapping monitoring.  To make use
# of this preprocessor you must specify the IP and hardware address of hosts on # the same layer 2 segment as you.  Specify one host IP MAC combo per line.
# Also takes a "-unicast" option to turn on unicast ARP request detection.
# Arpspoof uses Generator ID 112 and uses the following SIDS for that GID:
#  SID    Event description
# -----   -------------------
#   1      Unicast ARP request
#   2      Etherframe ARP mismatch (src)
#   3      Etherframe ARP mismatch (dst)
#   4      ARP cache overwrite attack

#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Conversation
#----------------------------------------
# This preprocessor tracks conversations for tcp, udp and icmp traffic.  It
# is a prerequisite for running portscan2.
#
# allowed_ip_protcols 1 6 17
#      list of allowed ip protcols ( defaults to any )
#
# timeout [num]
#      conversation timeout ( defaults to 60 )
#
#
# max_conversations [num]
#      number of conversations to support at once (defaults to 65335)
#
#
# alert_odd_protocols
#      alert on protocols not listed in allowed_ip_protocols
#
# preprocessor conversation: allowed_ip_protocols all, timeout 60, max_conversations 3000
#
# Portscan2
```

```
#--------------------------------------------
# Portscan 2, detect portscans in a new and exciting way.  You must enable
# spp_conversation in order to use this preprocessor.
#
# Available options:
#       scanners_max [num]
#       targets_max [num]
#       target_limit [num]
#       port_limit [num]
#       timeout [num]
#       log [logdir]
#
#preprocessor portscan2: scanners_max 256, targets_max 1024, target_limit 5, port_limit 20, timeout 60

# Too many false alerts from portscan2? Tone it down with
# portscan2-ignorehosts!
#
# A space delimited list of addresses in CIDR notation to ignore
#
# preprocessor portscan2-ignorehosts: 10.0.0.0/8 192.168.24.0/24
#

# Experimental Perf stats
# -----------------------
# No docs. Highly subject to change.
#
# preprocessor perfmonitor: console flow events time 10

##################################################################
# Step #3: Configure output plugins
#
# Uncomment and configure the output plugins you decide to use.
# General configuration for output plugins is of the form:
#
# output <name_of_plugin>: <configuration_options>
#
# alert_syslog: log alerts to syslog
# ----------------------------------
# Use one or more syslog facilities as arguments.  Win32 can also
# optionally specify a particular hostname/port.  Under Win32, the
# default hostname is '127.0.0.1', and the default port is 514.
#
# [Unix flavours should use this format...]
# output alert_syslog: LOG_AUTH LOG_ALERT
#
# [Win32 can use any of these formats...]
# output alert_syslog: LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname, LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname:port, LOG_AUTH LOG_ALERT
```

```
# log_tcpdump: log packets in binary tcpdump format
# ----------------------------------------------
# The only argument is the output file name.
#
# output log_tcpdump: tcpdump.log

# database: log to a variety of databases
# ---------------------------------------
# See the README.database file for more information about configuring
# and using this plugin.
#
# output database: log, mysql, user=root password=test dbname=db host=localhost
# output database: alert, postgresql, user=snort dbname=snort
# output database: log, unixodbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test

# unified: Snort unified binary format alerting and logging
# -------------------------------------------------------------
# The unified output plugin provides two new formats for logging
# and generating alerts from Snort, the "unified" format.  The
# unified format is a straight binary format for logging data
# out of Snort that is designed to be fast and efficient.  Used
# with barnyard (the new alert/log processor), most of the overhead
# for logging and alerting to various slow storage mechanisms
# such as databases or the network can now be avoided.
#
# Check out the spo_unified.h file for the data formats.
#
# Two arguments are supported.
#    filename - base filename to write to (current time_t is appended)
#    limit    - maximum size of spool file in MB (default: 128)
#
# output alert_unified: filename snort.alert, limit 128
# output log_unified: filename snort.log, limit 128

# You can optionally define new rule types and associate one or
# more output plugins specifically to that type.
#
# This example will create a type that will log to just tcpdump.
# ruletype suspicious
# {
#   type log
#   output log_tcpdump: suspicious.log
# }
#
# EXAMPLE RULE FOR SUSPICIOUS RULETYPE:
# suspicious $HOME_NET any -> $HOME_NET 6667 (msg:"Internal IRC Server";)
#
```

```
# This example will create a rule type that will log to syslog
# and a mysql database.
# ruletype redalert
# {
#   type alert
#   output alert_syslog: LOG_AUTH LOG_ALERT
#   output database: log, mysql, user=snort dbname=snort host=localhost
# }
#
# EXAMPLE RULE FOR REDALERT RULETYPE
# redalert $HOME_NET any -> $EXTERNAL_NET 31337 (msg:"Someone is being LEET"; \
#   flags:A+;)

#
# Include classification & priority settings
#

include classification.config

#
# Include reference systems
#

include reference.config

##################################################################
# Step #4: Customize your rule set
#
# Up to date snort rules are available at http://www.snort.org
#
# The snort web site has documentation about how to write your own
# custom snort rules.
#
# The rules included with this distribution generate alerts based on
# on suspicious activity. Depending on your network environment, your
# security policies, and what you consider to be suspicious, some of
# these rules may either generate false positives ore may be detecting
# activity you consider to be acceptable; therefore, you are
# encouraged to comment out rules that are not applicable in your
# environment.
#
# Note that using all of the rules at the same time may lead to
# serious packet loss on slower machines. YMMV, use with caution,
# standard disclaimers apply. :)
#
# The following individuals contributed many of rules in this
# distribution.
#
# Credits:
```

```
#   Ron Gula <rgula@securitywizards.com> of Network Security Wizards
#   Max Vision <vision@whitehats.com>
#   Martin Markgraf <martin@mail.du.gtn.com>
#   Fyodor Yarochkin <fygrave@tigerteam.net>
#   Nick Rogness <nick@rapidnet.com>
#   Jim Forster <jforster@rapidnet.com>
#   Scott McIntyre <scott@whoi.edu>
#   Tom Vandepoel <Tom.Vandepoel@ubizen.com>
#   Brian Caswell <bmc@snort.org>
#   Zeno <admin@cgisecurity.com>
#   Ryan Russell <ryan@securityfocus.com>
#
#==================================================
# Include all relevant rulesets here
#
# shellcode, policy, info, backdoor, and virus rulesets are
# disabled by default.  These require tuning and maintance.
# Please read the included specific file for more information.
#==================================================

include $RULE_PATH/exploit.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/virus.rules
```

## Appendix C Threat Analysis

Attached to the .pdf version of this deliverable

## Appendix D VPN Overhead Paper

Attached to the .pdf version of this deliverable

## Appendix E UST IPSec Suitability Trial

Attached to the .pdf version of this deliverable

# Threat Analysis
# TORRENT

# Table of Contents

# 1 Objectives and Motivation

## *1.1 The objective of the risk analysis*

The objective is to perform a risk analysis, which proposes countermeasures and/or identifies where countermeasures must be implemented in order to ensure that the TORRENT system is designed in the best possible way to minimize the risks and insure that the system performs as required.

This risk analysis is performed for the service providers/network operators to ensure that the TORRENT system is designed to minimise the risks for the service provider/network operator while at the same time fulfilling the requirements for the users and ensuring that the risks for customers are minimised as incidents to customers will have a negative effect on the service providers reputation. This is also important to ensure that the service provider may conduct a profitable business.

During the first year of TORRENT a security specification indicating which security services and mechanisms should be addressed by TORRENT was worked out including conceptual security architecture for the TORRENT system. In addition, based on the security requirements given in the TORRENT deliverables D1.1 and D1.2, a specification for implementation of security services in TORRENT was developed and presented at the first annual TORRENT audit.

During the software design phase of the TORRENT system it was determined by TORRENT WP3 that a threat analysis should be carried out to identify the risks to the system and determine the countermeasures that are required to bring the risks to an acceptable level. Using the results of the threat analysis a revised specification for implementation of security services in TORRENT was then devised.

## *1.2 Analysis group*

Judith Rossebø, Telenor, leader

Siv Hilde Houmb, Telenor

Frank Hansen, Telenor

Inge Svinnset, Telenor

John Ronan, WIT

## 1.3 Choice of method

Semi-structured HAZOP risk analysis.

A (Hazard and Operability) HAZOP risk analysis is a qualitative technique that can be defined as a systematic study of how deviations from the design specifications in a system can arise, and what the consequences are. This technique is usually performed using a set of guidewords and from these guidewords; scenarios that may result in a hazard or an operational problem are identified. An analysis team is established, consisting of experts, and headed by a HazOp leader.

## 1.4 Definitions and abbreviations

| | | |
|---|---|---|
| ADSL | Asymmetric Digital Subscriber Line | |
| ASP | Application Service Provisioning | |
| ATM | Asynchronous Transfer Mode | |
| CATV | Cable TV | |
| CPU | Central Processing UnitDECT | (digital wireless technology) |
| DiffServ | Differentiated Service | |
| DS | Differentiated Service | |
| DSCP | Differentiated Services Code Point | |
| DSLAM | Digital Subscriber Line Access Multiplexer | |
| DVD | Digital Video Disk | |
| ftp | File Transfer Protocol | |
| GSM | Global System for Mobile | |
| H/W | hardware | |
| IP | Internet Protocol | |
| ISDN | Integrated Services Digital Network | |
| ISP | Integrated Services Provider | |
| LAP | Local Access Point | |
| LCD | Liquid Crystal Display | |

| | |
|---|---|
| LMDS | Local Multi-point Distribution Services |
| MPLS | Multi-Protocol Label Switching |
| ms | milli second |
| NP | Network Performance |
| NT-1 | Network Termination 1 |
| NT-2 | Network Termination 2 |
| NVOD | near video on demand |
| OS | Operating System |
| PC | Personal Computer |
| PDA | Personal Digital Assistants |
| PSTN | Public Switched Telephony Network |
| QoS | Quality of Service |
| RG | Residential Gateway |
| RSVP | Resource Reservation Protocol |
| RTP | Real-Time Transport Protocol |
| SDH | Synchronous Digital Hierarchy |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SME | Small to Medium Enterprise |
| SRM | Service to Resource Management |
| SS7 | Signalling System 7 |
| STB | Set Top Box |
| STM | Synchronous Transmission Mode |
| TA | Terminal Adapter |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |

| | |
|---|---|
| TDM | Time Division Multiplexing |
| TE1 | Terminal Equipment 1 |
| TE2 | Terminal Equipment 2 |
| TORRENT | Towards a Realistic End-User Testbed |
| UDP | User Datagram Protocol |
| UMTS | Universal Mobile Telecommunications System |
| USB | Universal Serial Bus |
| VC | virtual circuit |
| VCR | video recorder |
| VOD | video on demand |
| VoIP | Voice-over-IP |
| WP | Work Package |
| xDSL | Generic term for Digital Subscriber Line technology - A/H/S/VDSL |

# 2 Description of TORRENT

TORRENT is a test-bed for multi-service residential networks. It is a shared physical access network for a range of different service and traffic types. The network can be controlled intelligently and thus enable a home user's QoS expectations for particular range and combination of services to be met. This will be done in a transparent way, and can be observed by the ability to choose the most appropriate service level. TORRENT will use agent technology for the service to resource management (SRM) system. Agent technology reduces the need for centralised control and scales well with the size and capabilities of a communications network.

TORRENT will provide users with services (e.g. video streaming service, or FTP. "Typical multi-media services could be multi-media conferences or access to multi-media databases. The latter can comprise a number of phases, including browsing, download or replay in "real time") with a particular quality:

a) High

b) Medium

c) Low

(These 3 terms will be defined in user-understandable terms and also mapped to network performance parameters for each service).

The choice of the quality is controlled by network selection and prioritisation, based on QoS requirements defined by the user through either:

- The user's profile.
- Inputting specific requirement for the session that override the user profile.

The following is a list of the user profile characteristics/requirements:

- Easy interpretable by the users
- Are unique per user
- Can be updated and changed by user
- Enables application selections
- Allows setting of quality preferences (and/or maximum price)
- Optimisation criterion, i.e. either minimize price under quality constraints or maximize quality under price constraints
- Trader agent chooses network dependent on user preferences

For example, maybe the user is presented with an anticipated cost for the service according to his current profile settings, and can then decide whether to accept or choose a higher/lower QoS.

Functionality will include service negotiation, configuration and creation, control and re-negotiation. Re-negotiation may be in real-time.

In order to be supported by TORRENT a service must offer both adequate visibility of its packet-flows and some means of influencing the choice of network provider.

## *2.1 Needs which TORRENT shall satisfy*

### 2.1.1 User Requirements:

- All services desired by the user should be accessible (within the capabilities of the access network)
- QoS (and/or price) expectations for particular range and combination of services shall be met
- The most suitable core network should be chosen according to the service requirements and the current state of the network, QoS requirements and price.
- Emergency telephone service access is a necessity (a mandatory service)
- Feedback (monitoring capabilities, billing, notification of access network status, notification of changes in access and core network (e.g. pricing) conditions)

### 2.1.2 Requirements for Service Providers, Network Operators, Manufacturers

- To satisfy the user requirements in a fast and flexible manner, and for the least cost to the user.
- Network operator: Optimise the bandwith utilisation in existing access and core networks
- NO and SP: To be aware of the performance requirements of a TORRENT system

- M: +NO and SP: Be able to provide feedback to the users (monitoring capabilities, billing, notification of access network status, notification of changes in access and core network (e.g. pricing) conditions)

The selection of the appropriate networks may be influenced by:

- Location of the service host (It might not be accessible through all core networks, this will obviously influence the decision making process of the system and consequently, the outgoing and incoming interface to be used on the LAP) [The service portfolio must be stated in the SLA and hence be part of the input to the agent system when choosing the appropriate network]

- Comment: the terminal is not so relevant as a selection criterion. The user might stream video on the PDA, while sending an SMS from the TV-set. The SLA must also describe the terminal support for the provided services.]

- Current congestion status of the networks (access and core), and the predicted future state. [Performance monitoring] If the operator is responsible for access control, a “busy signal” must be included.

-

There is maybe a need for agents in the latter case, i.e. if the film lasts 2 hours; the network state for the whole 2 hours has to be controlled - to avoid inter-session re-routing. Ultimately, it is the network provider that has responsibility for how this should be implemented.

Critical success factors for satisfying needs

- The networks must be able to deliver the availability, QoS, uptime required by the user.

- The system must allow intelligent control, both for the customer and for the network operators and service providers.

- The home user must be able to choose the most appropriate level of service for their session in a simple and intuitive way.

- The service-to-resource mapping (SRM) must function adequately.

- Agent-based smart decisions about traffic flows require the ability to:

    - Observe the traffic flows

    - Relate the traffic flows

    - Identify the service (without explicit signalling) from the traffic flow

- Measure traffic flows
- Route traffic flows through a chosen network provider
- And block all unauthorised traffic

## 2.2 Description of the TORRENT System

### 2.2.1 The interaction between TORRENT and its surroundings

Overview of the Multi-Service Test-bed

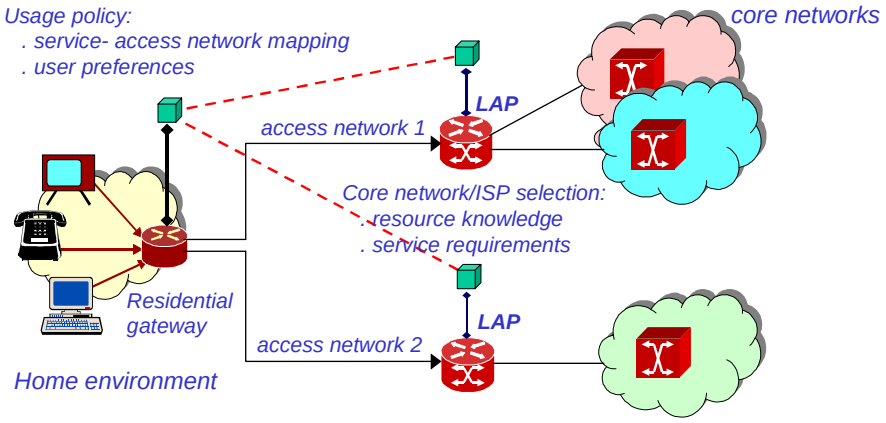



**Figure 2-1**

The architectural framework will consist of service-to-resource mapping (SRM) functionality, hosted in a user's residential gateway and one or more local access points, each of which in turn, communicates with a number of network operators and service providers.

A key feature of the SRM system will be the use of intelligent agent technology.

The local loop provides the interconnection between domestic users and the local access points. A wide variety of local-loop technologies, based on copper, coax, fibre and radio, are likely to coexist for some time. Copper-based ADSL is presently a strong contender for the support of multi-media services in the local loop.

The home network itself may be built on technologies based on Ethernet, (wired and wireless).

The Local Access Point (LAP) can be regarded as a high-technology local exchange. It will provide customer negotiation facilities and also host accounting and security functionality. It will be able to handle authorisation of access to the customer for tasks such as metering, security monitoring and activation of residential equipment and devices. The LAP will also support consumer applications such as Video-on-Demand. The LAP will have interfaces supporting several local-loop technologies and will serve many local residential customers. On the core network side, the LAP will enable access to several service providers and core networks. Each LAP will be made up from computer-controlled switching fabrics and host the most important parts of the service-to-resource-mapping system.

TORRENT will use agent technology for the SRM system. A software agent is a software entity that can act in an autonomous manner, can learn (be reactive) and be proactive. It can also interact with other agents, software systems and humans.

## 2.3 The basic TORRENT scenario

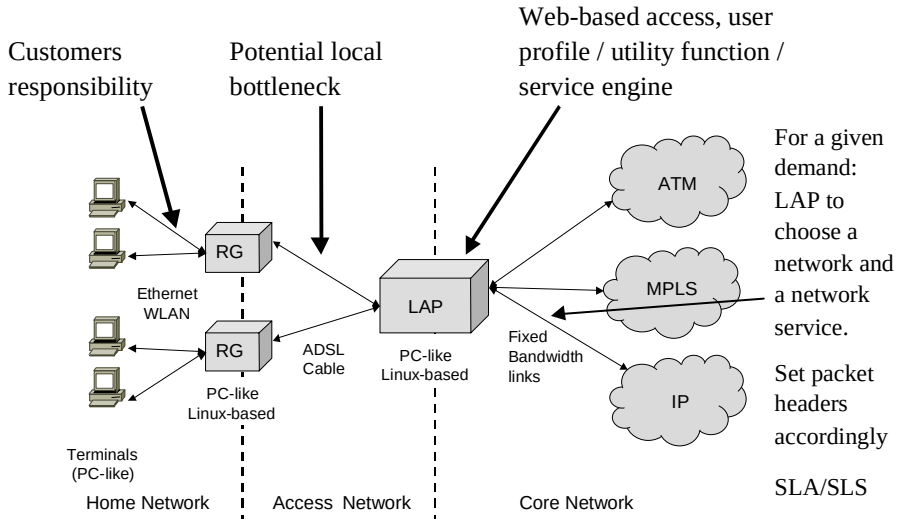



**Figure 2-2: The Basic TORRENT Scenario**

The focus of the software for the TORRENT system is the LAP.

Where no specific requirements are given, the TORRENT system will decide, based on the service selected, the status of the available networks, previous experience and personalised profiles. Examples of services are: ftp, http, VoIP, VoD (streaming), 2-way video. For some services it will be possible to choose between different quality levels.

As a background activity, the Agent system collects information about the NP/Network Services (transport services offered by NP)/Performance offered/ tariffs (SLA). From this accumulated information, the Agent system is able to associate each user service request with the appropriate network service, based on the user profile, which can be changed through a user-accessible web page.

Based on such information, a *Policy List* (Access List) is updated. This list gives the rules for the traffic handling of a given traffic demand; eg., which network and transport (quality) class to choose. In principle each user has his/her own Policy List.

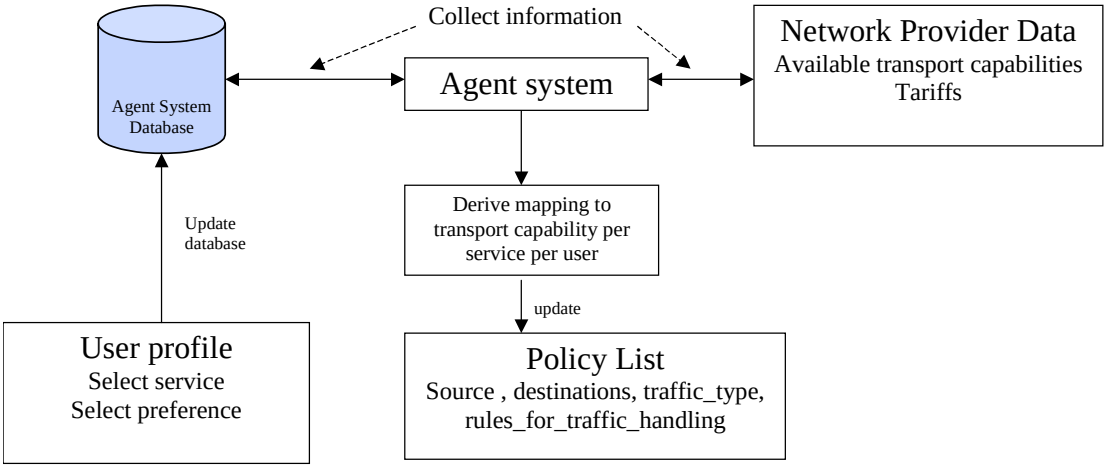



**Figure 2-3: Overall QoS model (LAP)**

### 2.3.1 User profile

In its simplest form the user profile interface will contain a list of accessible services with options for user to mark for preferred services and maximum tariffs. (The user should also specify what should be optimized (highest possible quality or lowest possible cost.) For some services, different quality levels could be distinguished. For example, for VoIP the quality will depend upon the codec, delay variation and loss rate. End-to-end delay is more or less given by the geographical location of the destination. Delay variation (jitter) and loss rate will depend upon the transport service used. By accepting a lower quality, a cheaper service can be expected.

### 2.3.2 Network Provider Data

This will typically be defined in terms of a set of Network (Transport) Services or Transport Capabilities. For each Network Service some requirement on the offered traffic will be given like traffic characteristic, rates, elasticity (TCP, UDP), etc. The Network Service will offer transport across a domain with certain performance characteristics such as maximum delay, delay variation, packet loss rate, throughput, network availability, etc. The Network Services will differ from operator to operator and from one transport technology to another (ie. ATM, IP DiffServ, MPLS)

Changes in tariffs are collected by the Agent system and stored in a database. Depending upon tariffs the optimal routing of a given demand may also depend upon the state of the LAP, since the already accepted traffic can have an impact on the price (eg. if the cost per unit decreases by volume).

Network conditions can change dynamically. For instance, a Network Service may be blocked due to temporarily overload. Such information is collected by the Agent system and the Policy List is updated accordingly.

(both offered/guaranteed parameters values as in SLA, but also real delivered values)

### 2.3.3 Agent System

The Agent system maintains an updated database of user profiles and Network Provider Data, etc. From this information (+ performance monitoring, ) a decision is made on how to route and mark a packet.

Some services will require that bandwidth is reserved in network. This implies signaling (eg. RSVP). Such process must communicate with the Agent system to cause an update of the Policy List. However, this feature will not be implemented in TORRENT, as we do not have access to any IPv6 signaling software.

### 2.3.4 Policy List

This list gives the rules for the traffic handling of a given traffic demand; e.g., which network and transport (quality) class to choose, given source address, destination address and some form of traffic type (ToS byte or port number, Ipv6 flow label, and current network state and tariffs)

### 2.3.5 The Service-Resource Mapping (SRM) software

Figure 2-4 SRM Software gives an overview of the TORRENT system Service-Resource Mapping (SRM) software.

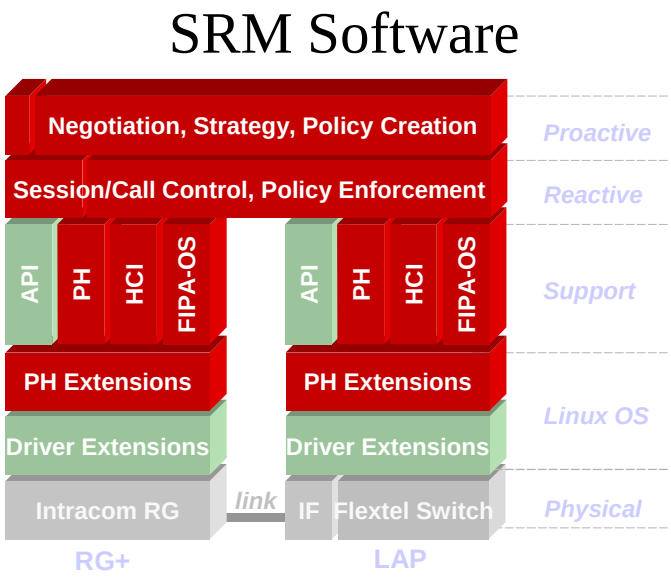



**Figure 2-4 SRM Software**

The mapping of services to resources is made according to default - or user selected - QoS requirements.

# 3 The scope of the threat analysis

This risk analysis focuses on the risks that the TORRENT system is exposed to. We will examine the risks that the TORRENT system is exposed to and for specific examples, we will examine the risks for the involved parties: home user (and owner of RG), Network Operator, LAP provider, and for Service Provider.

### 3.1.1 Division of TORRENT into components

We have divided the TORRENT system and it's surroundings into the following components:

- Home System (Network, terminals, servers, and other devices having communication capabilities) (a major growth area will be the networking of, and inter-working between residential equipment such as telephones, PCs, televisions, consumer equipment for heating, lighting and security.
- Residential Gateway (RG)
- Access network (ADSL and ISDN/PSTN, Cable and ISDN/PSTN)
- Local Access Point (LAP)
- Core network (ATM, MPLS, IP)
- Intelligent agent technology
- Network operators and service providers (this includes: their support functions (managers and management systems), network elements, servers, services, etc)
- Users =residents behind the RG.

### 3.1.2 Conditions and assumptions

- Assume a TORRENT RG – LAP system with at least 100 RGs connected
- Assume that the future will bring in more "critical" services than for example VoD. This is because it is very important to keep in mind that the TORRENT architecture should be designed in such a way that the countermeasures for more

"critical" measures are foreseen, and can be implemented without requiring a redesign of the entire system.

## 3.2 The threat analysis includes

In this threat analysis we have focused on the following components due to the scope of the risk analysis:

- Residential Gateway (RG)
- Local Access Point (LAP)
- Intelligent agent technology
- Network operators and service providers

## 3.3 The threat analysis does not include

Where possible, we exclude the risks involved with the core networks. E.g., the PSTN/ISDN, IP and MPLS networks and how they function are outside the scope of the analysis. The home network configuration and related risks involved are also outside of the scope. E.g., use of WLAN. Risks involved in using WLAN in the home are outside of the scope, however, information about this can be found at
http://www.cyberfrost.net/blogger/articles/HomeNetworks.htm

http://sourceforge.net/projects/wepcrack/

In this threat analysis we exclude the following due to the scope of the risk analysis:

- LAP to LAP scenario is excluded
- TORRENT system must provide continual access to the Emergency telephone services. However, threats involving use/misuse of this service are out of scope (Emergency service is provided by the primary PSTN/ISDN telephone operator.)
- Home network configuration is excluded
- The actual core network functions and services are excluded.

# 4 Scales for Consequence and Frequency

The threats were identified by first establishing what the general threats are, then going through one component of the system at a time and identifying possible threats related to confidentiality, integrity and availability for that particular component. Threats were also identified on the overall system level using the same method. The components were divided between the participants in the risk analysis such that the knowledge of the group where used efficiently. The risk analysis was carried out through several iterative stages where the different participants and a risk analysis expert who also guided the process gave feedback on the results obtained in order to make sure that all relevant aspects was covered.

## 4.1 Consequence value scale

**Table 1: Chosen consequence scale**

| | |
|---|---|
| **Catastrophic** | Death or extensive permanent invalidity due to lack of emergency service availability (the emergency call doesn't get through to the authorities).<br><br>Extensive financial losses (exceeding loss of annual budgeted profits for operators and service providers.)<br>Extremely reduced ability to provide all users with the access to available networks, applications according to user requirements.<br><br>Disclosure of subscribers' personal and private information e.g., incurring extensive monetary losses for a significant number of TORRENT subscribers (over 5000 Euros per subscriber).<br>Disclosure of subscribers' personal and private information e.g., incurring extensive monetary losses for more than 75% of TORRENT subscribers (1000-5000 Euros). |
| **Serious** | Loss of annual budgeted profits for operators and service providers.<br>Appreciably reduced ability to provide all users with the access to available networks, applications according to requirements.<br><br>Disclosure of subscribers' personal and private information e.g., incurring extensive monetary losses for (up to 75% of the) TORRENT subscribers (1000-5000 Euros).<br>Disclosure of subscribers' personal and private information e.g., incurring moderate monetary losses for (more than 75% of) the TORRENT subscribers (300-1000 Euros). |
| **Moderate** | The threat addresses the interests of providers/subscribers and cannot be neglected.<br>Reduced ability to provide a significant number of users with the access to available networks, applications according to requirements.<br><br>Disclosure of subscribers' personal and private information e.g., incurring moderate monetary losses for (up to 75% of) the TORRENT subscribers (300-1000 Euros).<br>A limited amount of Information in the system pertaining to a few customers is lost.<br>Disclosure of subscribers' personal and private information e.g., incurring minor monetary losses for more than 50% of the TORRENT subscribers (1-300 Euros) affected. |
| **Minor** | The concerned party is not harmed very strongly; the possible damage is low.<br>Minor or no influence on current business operations.<br><br>Disclosure of subscribers' personal and private information e.g., incurring minor monetary losses for (more than 25% of) TORRENT subscribers (1-300 Euros) affected. |

## 4.2 Chosen scale division for the frequency analysis

| | |
|---|---|
| **Very common** | *The event occurs routinely. More than one occurrence per week. Motivation for an attacker is very high. The means used to state this threat are readily available and it is easy to carry out the attack.* |
| **Common** | *There are no sufficient mechanisms installed to counter this threat, and the motivation for an attacker is quite high. The event occurs regularly and one has good experience both of the consequences and of how the situation shall be handled. More than one occurrence per month.* |
| **Can occur** | *The event occurs sporadically, and may happen at some time or other. More than one occurrence per year. The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.* |
| **Unlikely** | *It is not very likely that the event will occur. If it does, it is to be regarded as an isolated event. The event is unusual, and it is most probable that it will not occur. More than one occurrence per decade. According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.* |

**Table 2: Chosen scale of frequency (of threat occurrence - service deviation)**

## 4.3 Chosen scale division for risk level

| | | ***Frequency*** | | | |
|---|---|---|---|---|---|
| | | **Not very likely** | **Can occur** | **Common** | **Very common** |
| ***Consequence*** | **Minor** | *"Low"* | *"Low"* | *"Low"* | *"Moderate"* |

| | | | | |
|---|---|---|---|---|
| **Moderate** | *"Low"* | *"Low"* | *"Moderate"* | *"High"* |
| **Serious** | *"Moderate"* | *"Moderate"* | *"High"* | *"Extreme"* |
| **Catastrophic** | *"High"* | *"High"* | *"Extreme"* | *"Extreme"* |

**Table 1: Chosen designations of risk level**

### 4.3.1 The meaning of the designations of risk level

*The product of the occurrence likelihood and impact gives the risk, which serves as a measurement for the risk that the concerned management function is compromised. The result is classified into the following categories:*

| | |
|---|---|
| **Extreme** | *Extremely critical risks arise when motivation of a potential attacker is high and when the critical interests of the providers/subscribers are threatened. Extremely critical risks shall be minimized with utmost priority.*<br><br>*(high consequence and high frequency)* |
| **High** | *Critical risks arise, when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks shall be minimized with high priority.*<br><br>*(high consequence and moderate frequency) or*<br>*(moderate consequence and high frequency)* |
| **Moderate** | *Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimzed as soon as possible.*<br><br>*(high consequence and low frequency) or*<br>*(low consequence and high frequency) or*<br>*(moderate consequence and moderate frequency)* |
| **Low** | *Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats caused by minor risks have no primary need for counter measures.* |

| | |
|---|---|
| | *(moderate to low consequence and low frequency) or*<br>*(low consequence and moderate to low frequency)* |

**Table 2: Explanation of the designations of risk level**

# 5 Threat List

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 1 | **General Threats** | | | | | |
| 2 | Eavesdropping of user-id on interfaces or entities (RG, LAP) in order to masquerade as a real user | **Serious** | **Can occur** | **Moderate** | Encrypt the link between the LAP and RG; Strong authentication for user access to services available on the LAP; admin access rules. Use IDS and knowledge of which LAP interface(s) a user is conneted to and MAC addresses etc to discover masquerade. | |
| 3 | Eavesdropping on interfaces or entities (RG, LAP) in order to obtain user related information (user-id, credit card info, ) | **Serious** | **Can occur** | **Moderate** | Encrypt the link between the LAP and RG; Strong authentication for user access to services available on the LAP; admin access rules | |
| 4 | Eavesdropping interfaces or entities (RG, LAP) in order to conduct traffic pattern analysis and analyse which services are invoked by the user in order to attack the privacy of the user or DoS e.g. so a user is prevented from watching a film. For example, traffic analysis on shared media can be used to figure out what RG a neighbour (mac address) is using, then when he starts watching a film, DOS his RG | **Serious** | **Not very likely** | **Moderate** | Encrypt the link between the LAP and RG; Strong authentication for user access to services available on the LAP; admin access rules | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 5 | Subscription fraud: Customer (up to 25% /more than 25%) are subject to fraudulent activities such as hacker steals capacity/services from paying user, or e.g., hacker empties bank accounts. | **Serious/catastrophic** | **Can occur** | **Moderate/High** | Encrypt the link between the LAP and RG; Strong authentication for user access to services available on the LAP; However, if username and password authentication is implemented, once the fraud is detected, the user must be recompensed, passwords must be changed etc. Educate users on how to protect their passwords. | |
| 6 | DoS attack on user(s: up to 25 / more than 25)) | **Serious/catastrophic** | **Can occur** | **Moderate/High** | Firewall in LAP; IDS tracking/actively blocking Depending on the attack, QoS mechanisms may help. We will be making recommendations as to minimum configurations of the firewall, This would include several mechanisms for 'throttling' some of the standard DoS attacks. | |
| 7 | Flooding the network causing DoS (between 6 and 25/ more than 25 affected) | **Serious/catastrophic** | **Can occur** | **Moderate /High** | Firewall, ACLs. "Flood control" As per above. There is an issue if it is a shared access medium. | |
| 8 | Flooding the network causing degredation of service | **Moderate** | **Can occur** | **Low** | Firewall, ACLs. QoS mechanisms may help. The SLA will be the agreement of bandwidth also. So in theory, no user would be able to flood the network, as their total bandwitdh is limited. | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 9 | User terminals are infected by Virus (which subsequently spreads to other terminals through RGs connected to the LAP. Costs per user for disinfecting and if possible restoring valueable files is 1000 Euros and upwards. | **Serious** | **Can occur** | **Moderate** | Anti-virus protection at user terminals; As a preventative measure, the LAP provider can also use IDS services to identify infected terminals in the TORRENT system and stop spread of virus's to other terminals in the TORRENT system. | |
| 10 | Access to the Emergency Telephone Service (ETS) is denied. | **Catastrophic** | **Can occur** | **High** | Provide ETS through PSTN/ISDN. Ensure that service is available even though RG, LAP are powered down or unavailable. | |
| 11 | Social Engineering – apparently from the user side | **Moderate** | **Can Occur** | **Low** | Information/ Education Look at industry/academic best practice. | |
| 12 | Social Engineering – apparently from the operator side | **Serious** | **Can Occur** | **Moderate** | Information/ Education. To counter the case that someone is pretending to be the operator in order to get information to pretend to be a user that they are not, make the information/key/whatever dependent on a token of some sort. | |
| 13 | **Threats related to functions provided by the LAP** | | | | | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 14 | Administrator/Employee of network operator or service provider engages in fraudulent activities (e.g. obtaining customers credit card information from database) | Serious | Can Occur | Moderate | Rules and routines for administrators (e.g. separation of data/limited accessibility) Don't store the information, store a MD5 Hash of it. | |
| 15 | Unauthorized access to user related information such as user ID(s) and authentication information stored in the databases at the LAP | Serious | Can Occur | Moderate | Strong user authentication for access to the LAP; Administrative access requirements/rules/policy. Rules and routines for administrators (e.g. separation of data/limited accessibility) | |
| 16 | Masquerading as an RG (e.g. for fraudulent/unauthorized access to services available at the LAP) | Moderate | Can occur | Low | Mutual authentication of LAP – RG | |
| 17 | The LAP fails | Serious | Can Occur | Moderate | Provide duplication of the functions of the LAP | |
| 18 | The service to resource mapping (SRM) (agent system) malfunctions | Serious | Can Occur | Moderate | SLA; error handling measures; realiability functions | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 19 | Unauthorized access to agent system resulting in: fraud, DoS, Disclosure of subscribers' personal/private information | Serious | Can occur | Moderate | Strong user authentication for access to the LAP; admin access rules/policy. Provide hardware token-based authentication for access to services (e.g. PKI-based using smartcards) If the smartcard and pin are stolen then the certificate must be revoked. | |
| 20 | **Threats related to Service profile procedures** | | | | | |
| 21 | Eavesdropping of user information during Service profile access/change procedures assuming this info is transmitted e.g. as HTTP traffic to a WEB page on a terminal behind the RG. | Serious | Can occur | Moderate | Encrypt the link between the LAP and Terminal e.g., using SSL. | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 22 | Manipulation of transmitted information during service profile access/change procedures assuming this info is transmitted e.g. as HTTP traffic to a WEB page on a terminal behind the RG. (User Preferences Home page) | Serious | Not very likely | Moderate | Encrypt the link between the LAP and Terminal e.g., using SSL. | |
| 23 | Unauthorized access to service profile of somebody by unauthorized use of "View User Preferences Home page function" | Moderate | Can Occur | Low | Require strong authentication and encryption eg. using PKI (with X.509 certificates) and encrypt using SSL for access to the WEB interface | |
| 24 | Unauthorized access to, or unauthorized use of, the " User Service Profile Modification procedure" | Serious | Can occur | Moderate | Require strong authentication and encryption eg. using PKI (with X.509 certificates) and encrypt using SSL for access to the WEB interface | |
| 25 | **Threats to the RG /RG owner** | | | | | |
| 26 | Masquerading as a LAP (e.g., to gain access to users info and/or to divert user access to services) or perform "man-in-the-middle attacks" | Serious | Common | High | Mutual authentication of LAP - RG | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 27 | Manipulation/modification of the RG functionality | **Serious** | **Can occur** | **Moderate** | Authentication for access to the RG; Intelligence should not be located on the RG. | |
| 28 | The RG fails | **Moderate** | **Can Occur** | **Low** | Provide internet connection over ISDN even though the RG has failed. Configure the RG so that the PSTN/ISDN network is available even though the RG has failed. Ensure that Services can be provided via the PSTN/ISDN network even though the LAP has failed. | |
| 29 | **Threats related to service provisioning** | | | | | |
| 30 | A service is not available | **Moderate** | **Can Occur** | **Low** | SLA- Planned outage versus not planned outage. A service availability figure should be given in SLA. If not satisfied some form of compensation is natural. | |
| 31 | All Services are not available | **Serious** | **Can Occur** | **Moderate** | SLA- Planned outage versus not planned outage. Network availability figure should be given SLA. Should we add separate point: user profile not available | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 32 | The emergency call system is not accessible due to a flaw in the TORRENT system | Catastrophic | Can Occur | High | Provide ETS through PSTN/ISDN. Ensure that service is available even though RG, LAP are powered down or unavailable | |
| 33 | Feedback to users doesn't work | Moderate | Can Occur | Low | Provide information about faults via a WEB page. | |
| 34 | A service such as VoD is interrupted/stopped due to network problems | Moderate | Can Occur | Low | Compensate the User as per the SLA | |
| 35 | Failure to bar unauthorized traffic | Moderate/Serious | Can Occur | Low/Moderate | Update the SRM system to recognise the 'new or unknown' attack. | |
| 36 | The accounting functionality doesn't work | Serious | Can Occur | Moderate | Routines for test and monitoring | |
| 37 | Unauthorized access to the charging record DB (e.g to change billing records or obtain billing information) | Serious | Can Occur | Moderate | Strong authentication for access to the LAP; admin access rules | |
| 38 | The security functionality doesn't work | Serious | Can Occur | Moderate | Routines for test and monitoring | |
| 39 | **Threats against QoS architecture** | | | | | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 40 | An attacker allocates a substantial number of QoS enabled flows, which binds up the resources and degrades the performance for other users flows | **Serious** | **Can Occur** | **Moderate** | Access to the LAP and functions provided by the LAP must be protected. In the case of a distributed attack (from many false RGs) authentication of the RG and the user behind the RG for access to the user preferences GUI. Mechanisms to prevent attackers from inserting packets in the flows. Mutual authentication of the RG and LAP. | |
| 41 | An attacker attempts to get a higher QoS than agreed on. | **Moderate** | **Can Occur** | **Low** | Authentication and integrity protection (of QoS related data and signalling) (So that only the subscriber can make changes to QoS requirements and so that changes such as due to interception are discovered) SSL between the user terminal and the WEB server is also recommended. | |
| 42 | An attacker attempts to get QoS without paying for it | **Moderate** | **Can Occur** | **Low** | Authentication and integrity protection (of QoS related data and signalling) and encryption e.g. using SSL . | |
| 43 | An attack against the policy control/enforcer resulting in e.g. DoS | **Moderate** | **Can Occur** | **Low** | Authentication of agents and encryption of communication between agents. | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 44 | An attack against the policy control/enforcer resulting in manipulation of data (changes to QoS agreements) | Serious | Can Occur | Moderate | Authentication of agents and encryption of communication between agents. | |
| 45 | A customer gets higher QoS than agreed, but is required to pay for this | Moderate | Can Occur | Low | Price adjustment; SLA | |
| 46 | A customer gets lower QoS than agreed, but is required to pay for this | Moderate | Can Occur | Low | Price adjustment; SLA –agreed customer is compensated. This should be built into the SLA. | |
| 47 | Customer billing error; Price for QoS billed is different from price agreed. | Moderate | Can Occur | Low | SLA; Error handling measures and customer service | |
| 48 | The function " service negotiation, configuration and creation, control and re-negotiation" is not available | Serious | Can Occur | Moderate | SLA | |
| 49 | **Threats to the Agent System** | | | | | |
| 50 | **Threats related to the agent system during initialling and starting of agents** | | | | | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 51 | Unauthorised start of agent | Serious | Can occur | Moderate | The login procedure for users of the agent system needs to handle this threat. | |
| 52 | Authorised start of agent fail | Serious | Can occur | Moderate | Implement a timeout and send an error message to the service provider. | |
| 53 | Agent starts when it should not | Serious | Can Occure | Moderate | Need to check and test the code for errors or include a procedure to check whether or not the agent should actually start. However, this might introduce an increased time delay in the starting of the agents. (This issue is related to QoS. Having more routines when starting the agents will increase the probability of failures during startup and also the possibility of failing to fulfil the QoS contract.) | |
| 54 | Agent starts too late e.g., due to SW error or related to HW or communication error so that user does not receive the service requested. | Minor | Not very likely | Low | Implement a timeout. | |
| 55 | **Threats to the agent system after agents are initialised and started** | | | | | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 56 | Masquerading of an agent | **Serious** | **Common** | **High** | Authentication of agents before starting agents and during negotiation (to avoid problems do to malevolent agents) and timestamps to avoid the reuse of agents (masquerade). Example: Do an MD5 checksum of the original code and check at each stage of deployment. Authentication of users of agents, and encryption of communication between agents and users and agents. | |
| 57 | Eavesdropping of information from an agent | **Moderate** | **Can Occur** | **Low** | Encrypt communication between agents | |
| 58 | Spoofing of an agent | **Serious** | **Common** | **High** | Authentication of agents using a protocol such as Kerberos with limited access time to the particular service and encryption of communication between agents. | |
| 59 | Manipulation of data sent between agents | **Catastrophic** | **Common** | **Extreme** | Encryption of communication between agents and authentication of agents. | |
| 60 | **Threats to agent system when terminating agents** | | | | | |

| # | Scenario / threat | Risk assessment | | | Possible mitigating measures | Note |
|---|---|---|---|---|---|---|
| | | Consequence | Frequency | Risk level | | |
| 61 | Agent stop when it should not | Serious | Can occur | Moderate | Encryption of communication between agents and between user and agent, authentication of agents and users. | |
| 62 | Agent fail to stop when it should | Minor | Can occur | Low | Use a list to control which agents are initiated, started and stopped (not valid) and then use garbage collector to remove agents that fail to stop. | |

**Table 3: Threats and possible measures**

# 6 Risk Assessment

## 6.1 Risk Assessment for the TORRENT System

All threats with risk level “extreme” or “high” (critical risks) require countermeasures. Also threats with risk level “moderate” (major risk) shall be minimized as soon as possible. The according security requirements will be described in Deliverable 3.3. Security Aspects and Features of the TORRENT Test-Bed

All threats with risk level “extreme” or “high” must be properly treated before the TORRENT system can be a commercial product, see the following section. The risk level is reduced by a combination of

- Reducing the consequence
  - Isolating the threat to affect fewer users
  - Reducing the effect of the threat
- Reducing the frequency

## 6.2 Description of unacceptable threats

*“Describe the unacceptable threats in more detail than in the threat list.”*

From the entire list of threats and resulting risk assessment compiled, a number of major threats were identified. The following is a list of threats to the TORRENT system that are not accepted:

General Threats:

- Denial of Service (DoS) attack on the users affecting more than 25 users. An attacker may wish to degrade normal service use for the users and/or service providers. This can be done by manipulating information/communication within the agent system e.g. by modification of data, or by gaining access to the LAP. An attacker may use the approach of conducting a distributed DoS attack on all the RGs on a segment.
- Flooding of the network causing Denial of Service (DoS) for more than 25 users connected to the LAP.

- Access to the Emergency Telephone Service is denied. In European countries provision of emergency services is mandatory. Designing a RG as the access point to the home requires that access to the emergency telephone services is also provided. A system malfunction could cause the emergency service to be unavailable.

- Subscription fraud: Incurring disclosure of subscribers' personal and private information e.g., incurring extensive monetary losses for a significant number of TORRENT subscribers (over 5000 Euros per subscriber), or disclosure of subscribers' personal and private information e.g., incurring extensive monetary losses for more than 75% of TORRENT subscribers (1000-5000 Euros).

Threats related to functions provided by the LAP:

- Unauthorised access to the User Preferences DB. This can result in personal information being divulged to unauthorised persons. Unauthorised access to the User Preferences DB can also result in a DoS attack on the user, e.g., if user information is deleted from the database. An attacker (may also be the user) can also manipulate charging data in order to obtain free services.

Threats related to RG/RG owner

- Masquerading as a LAP (e.g., to gain access to users info and/or to divert user access to services) or perform "man-in-the-middle attacks". The attacker may perform this attack on a large number of users quite easily.

Threats related to service provisioning:

- The emergency call system is not accessible due to a flaw in the TORRENT system.

- Manipulation of the data sent between agents.

As a result, countermeasure must be implemented in the TORRENT system to bring the risks to an acceptable level.

The following lists the countermeasures that were identified and are required:

- Stateful Firewall in the LAP

- IDS tracking/actively blocking
- Access Control Lists (ACLs)
- The Emergency telephone service must be provided through the PSTN/ISDN. It must be ensured that the service is available even though RG, LAP are powered down or unavailable
- Encryption and authentication of communication between agents.
- Mutually authentication of the LAP and RG

In addition, the following threats shall be minimized as soon as possible:

General Threats:

- Eavesdropping of user-id on interfaces or entities (RG, LAP) in order to masquerade as a real user
- Eavesdropping on interfaces or entities (RG, LAP) in order to obtain user related information (user-id, credit card info, )
- Eavesdropping interfaces or entities (RG, LAP) in order to conduct traffic pattern analysis and analyse which services are invoked by the user in order to attack the privacy of the user or DoS e.g. so a user is prevented from watching a film. For example, traffic analysis on shared media can be used to figure out what RG a neighbour (mac address) is using, then when he starts watching a film, DOS his
- Subscription fraud: Customer (up to 25) are subject to fraudulent activities such as hacker steals capacity/services from paying user, or e.g., hacker empties bank accounts.
- User terminals are infected by Virus (which subsequently spreads to other terminals through RGs connected to the LAP. Costs per user for disinfecting and if possible restoring valueable files is 1000 Euros and upwards.
- Social Engineering – apparently from the operator side

Threats related to functions provided by the LAP:

- Administrator/Employee of network operator or service provider engages in fraudulent activities (e.g. obtaining customers credit card information from database)

- Unauthorized access to user related information such as user ID(s) and authentication information stored in the databases at the LAP

- Replace content of user web pages on LAP WEB server (e.g., with fraudulent/illegal/pornographic content) (WEB server located on LAP; Negative publicity for operator.User may choose to terminate subscription.)

- The LAP fails

- The service to resource mapping (SRM) (agent system) malfunctions

- Unauthorized access to agent system resulting in: fraud, DoS, Disclosure of subscribers' personal/private information

Threats related to Service profile procedures:

- Eavesdropping of user information during Service profile access/change procedures assuming this info is transmitted e.g. as HTTP traffic to a WEB page on a terminal behind the RG.

- Manipulation of transmitted information during service profile access/change procedures assuming this info is transmitted e.g. as HTTP traffic to a WEB page on a terminal behind the RG. (User Preferences Home page)

- Unauthorized access to, or unauthorized use of, the " User Service Profile Modification procedure"

Threats to the RG /RG owner:

- Masquerading as a LAP (e.g., to gain access to users info and/or to divert user access to services) or perform "man-in-the-middle attacks"

- Manipulation/modification of the RG functionality

Threats related to service provisioning:

- All services are not available

- Failure to bar unauthorised traffic

- The accounting functionality does not work

- The function " service negotiation, configuration and creation, control and re-negotiation" is not available
- Unauthorized access to the IPDR DB (e.g to change billing records or obtain billing information)
- The security functionality doesn't work

Threats against QoS architecture:

- An attacker allocates a substantial number of QoS enabled, which binds up the resources and degrades the performance for other users flows (between 6 and 25 users affected).
- An attack against the policy control/enforcer resulting in manipulation of data (changes to QoS agreements)
- The function " service negotiation, configuration and creation, control and re-negotiation" is not available

Threats to the agent system

- Authorised start of agent fails
- Masquerading of an agent
- Spoofing of an agent
- Agent stops when it should not
- Agent fails to stop when it should

The following countermeasures should be implemented in addition to the mandatory countermeasures:

- Strong, Hardware token based Mutual authentication of LAP - RG
- Encrypt the link between the LAP and RG
- Strong authentication for user access to services
- Strong user authentication for administrative access to the LAP

- Strong user authentication for access to the agent system
- Provide TORRENT users with information about how to protect themselves from attacks. For example, provide information about anti-virus protection and advice all users to install anti-virus protection
- Rules and routines for administrators (e.g. separation of data/limited accessibility)
- Don’t store sensitive information on the LAP, store a MD5 Hash of it.
- Encrypt the link between the LAP and Terminal (e.g., SSL).
- Require user authentication using PKI (X.509 certificates) e.g. via SSL from the user’s terminal for access to the WEB interface (e.g., the "View User Preferences Home page function”).
- Intelligence should not be located on the RG
- Update SRM system to recognise the “new or unknown” attack
- Routines for test and monitoring
- Procedure for authentication of agents
- Authentication of agents using a protocol such as Kerberos with limited access time to the particular service and encryption of communication

**Conclusion**

The TORRENT system is exposed to numerous risks. A threat analysis is helpful in determining how to bring the risks to an acceptable level.

# 7 References

[1] Levesen, Nancy G., SAFEWARE – System Safety and Computers, ISBN 0-201-11972-2, 1995.

[2] Pfleeger, C. P., Security in computing. Prentice Hall, Inc., ISBN 0-13-185794-0 (1997).

[3] Stallings, William, "Network Security Essentials", Pretence Hall, Inc., ISBN 0-13-016093-8, 2000.

[4] Picco, G.P., Understanding Code Mobility - Tutorial T18, 80 slides, ICSE'2000 / Univ. Limerick, June 2000.

[5] Sycara, K., Multi-agent Infrastructure, Agent Discovery, Middle Agents for Web Services and Interoperation. In Lecture Notes in Artificial Intelligence: Multi-Agent Systems and Applications, pp. 17-49, Springer-Verlage Berlin Heidelberg New York, ISBN 3-540-42312-5, 2001.

[6] Wayer, P., Agents Unleashed: A Public Domain Look at Agent Technology, Academic Press, Inc., ISBN 0-12-738765-X, 1995.

[7] Moreno, A., Isern, D., A first step towards providing health-care agent-based services to mobile users, Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 2, pages 589-590, ACM Press, ISBN 1-58113-480-0, 2002.

[8] Hu, Y.-J., Some thoughts on agent trust and delegation, Proceedings of the fifth international conference on Autonomous agents, pages 489-496, ACM Press, ISBN 1-58113-326-X, 2001.

[9] CORAS deliverable D2.1, WP2-WT1-del-001-v1.0, State-of-the-art and evaluation of established risk analysis methodologies for their applicability to security critical systems, 2001.

[10] IST-SHAMAN Deliverable D09: “Detailed Technical Specification of Security for Heterogeneous Access”, June 2002.

# Overhead Issues for Local Access Points in IPsec enabled VPNs

John Ronan, Paul Malone, Mícheál Ó Foghlú
*Telecommunications Software Systems Group (TSSG)*
*Waterford Institute of Technology, Ireland.*
*Email: {jronan, pmalone, mofoghlu}@tssg.org*

## Abstract

*Virtual Private Networks (VPNs) use the Internet or other network service as a backbone to provide a secure connection across a potentially hostile WAN. Such security guarantees provide the motivation for VPN deployment. This security does, however, come at a performance cost brought about by the increased processing overhead. This paper presents an investigation into these overheads. In particular, this investigation will consider the server side overhead for VPN deployments and seek to establish a relationship between this overhead and the number of clients being serviced.*

***Index Terms*—Communication System Security, Cryptography.**

## 1. Introduction

The results of this work comes from several different VPN scenarios which have been tested, measured and analysed. The tests were performed on IPv4 and IPv6 networks and results were collected for several client enumerations in both IPv4 and IPv6 control scenarios in addition to the IPv6 enciphered scenarios. Two different Linux kernel versions were used, firstly a *vanilla*[1] or stock kernel and secondly the USAGI[2] kernel which replaces the entire IPv6 stack with its own, more standards conformant version.

The results will demonstrate a relationship between the number of clients connected to a Local Access Point [3] (LAP – essentially a 'smart' router which sits between the access network and the core network) and the load placed upon the LAP. From this it should be possible to define limits to the number of clients that each LAP is capable of servicing while guaranteeing QoS requirements.

This work has evolved from an investigation within the TORRENT IST [4] project where it was deemed desirable to offer a service which consisted of a secure communications channel between a Residential Gateway (RG) and a LAP. In time, this led to an evaluation of the performance implications of using IP security (IPsec)[5] to achieve this goal. This, in turn, brought about a more detailed investigation as it became apparent that there were scalability issues involved. The results of this work will feed directly into the decision making process of the Agent Based SRM (Service Resource Management) system in TORRENT.

## 2. Context

### 2.1 TORRENT Overview

Among the expected outputs of the IST supported TORRENT project is a testbed providing for residential, multi-service access networks. This testbed (Figure 1) will allow the project to demonstrate the benefit of intelligent control, both for the customer and for the network operators and service providers.

An important additional need is to optimise the bandwidth utilisation in existing access and core networks, while at the same time meeting a user's requirements in an optimal manner. These requirements include Quality of Service (QoS), security, cost, and availability.

### 2.2 Motivation for IPsec deployment

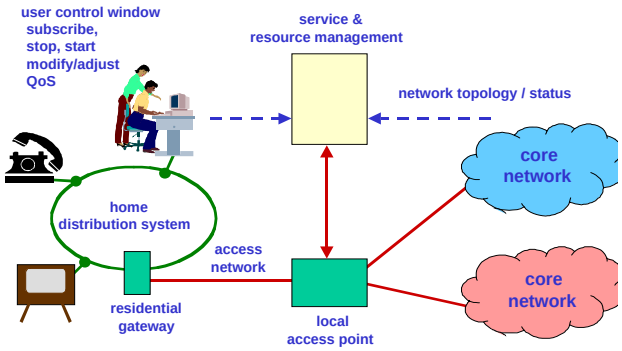



Figure 1 - TORRENT Architecture

It was proposed early in the TORRENT project lifecycle to integrate IPv6 as the transport protocol and IPsec as a service for securing the data between the RG and the LAP. It was understood that there would be performance implications arising from this, which were not quantified at the time. The work presented here is a result of a desire within TORRENT to gain an understanding of these performance implications.

## 3. IPsec Protocol Suite

IPsec is the security architecture for the Internet Protocol (IP). This protocol is applicable to both IPv4 and IPv6. The architecture is defined in [5] and addresses the following 4 elements:

A. *Security Protocols*: Authentication Header (AH) [6] and Encapsulating Security Payload (ESP)[7].

B. *Security Associations*: Definition, management and processing.[8]

C. *Key Management*: The Internet Key Exchange (IKE) [8],[9],[10],[11].

D. *Algorithms*: Requirements of the authentication and encryption algorithms.

### 3.1 Security Protocols

Traffic Security is provided by two security protocols:

- The *Authentication Header* protocol [6] provides connectionless integrity and data origin authentication. There is also an optional anti-replay service available.

- The *Encapsulating Security Payload* protocol [7] potentially provides two types of security service. The first being confidentiality via encryption and limited traffic flow confidentiality. The second type is connectionless integrity, data origin authentication and an anti-replay service.

Either of these protocols can be applied alone or in combination, thus providing the desired level of security. The IPsec security protocols are represented by headers that appear before the IP header in the IP packet.

### 3.2 Security Associations

The security protocol headers do not contain information pertaining to the cryptographic algorithms and the associated parameters. These representations are achieved through the transmission of a *Special Parameter Index* (SPI). This index combined with the destination IP addresses and the type of protocol header (AH or ESP) determines the parameters of the IPsec processing.

These parameters of a unidirectional security service are represented by a *Security Association* (SA). There are two types of SAs:

- *Transport Mode SA:* This is a security association between two hosts, generally used to secure the traffic of the upper layer protocols.

- *Tunnel Mode SA:* This is a security association in an IP-in-IP tunnel, generally used in connecting to security gateways.

### 3.3 Key Management

IPsec mandates support for two separate methods of cryptographic key and SA management: manual and automatic.

- *Manual Key Management:* This is the simplest form of key management and involves each IPsec connection to be configured manually on both hosts. While this is suitable in small static situations, it is unsuitable in larger deployment scenarios due to scalability problems.

- *Automatic Key and SA Management:* Larger deployment scenarios call for an Internet-standard, scalable and automated SA and key management protocol. This is provided by *Internet Key Exchange* (IKE). IKE is required to allow for use of anti-replay features of AH and ESP and to facilitate on-demand creation of SAs.

### 3.4 Algorithms

The IPsec protocol suite does not define the authentication and encryption algorithms used in implementations. These are defined in individual RFCs per algorithm. Algorithms used in these tests were:

DES [12]
AES [13]
HMAC-MD5 [14]

## 4. The WIT IPv6 IPsec Testbed

To perform the tests required to examine the performance of the various IPsec scenarios, a testbed was set up. All hosts were interconnected using a Cisco 2924 Ethernet switch using their own isolated VLAN.

A logical view of this testbed configuration is shown in Figure 2. This view shows all six test machines configured with IPv4 and IPv6 addresses. From a physical viewpoint, the testbed has at its core a Flextel WebVision 4012 (identical to the TORRENT LAP), which provides 12 multipurpose slots each of which can take processor cards or I/O carrier cards. Four of processor blades acted as hosts for the testbed. Each of these processor blades was equipped with dual Pentium III 850Mhz processors, 512 MB RAM and an Intel Ethernet Pro 100 network card integrated onto the motherboard. The other two hosts used in the testbed consist of two Dell PIII 500Mhz desktop machines with 100Mbit 3Com 3c905 Network Cards.

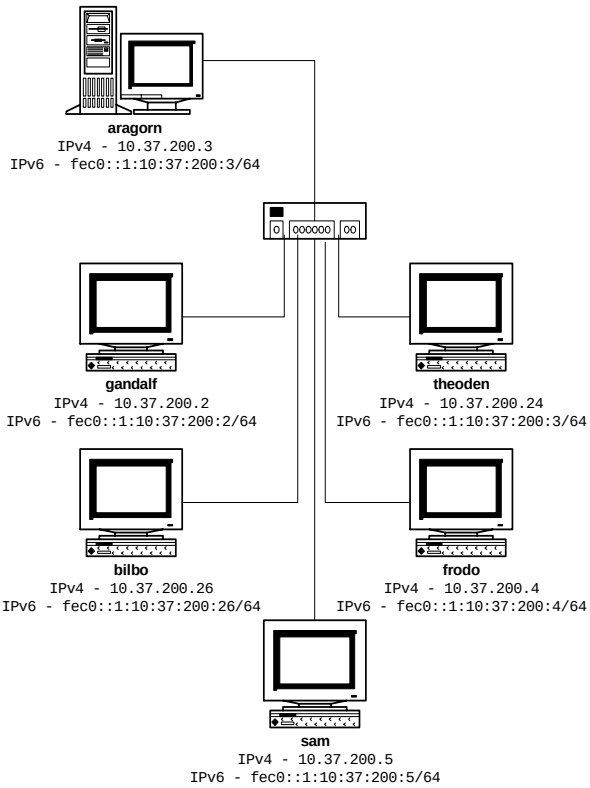



Figure 2 - Testbed configuration

### 4.1 Software

Each host was configured with the following software:

*Operating System:*

SuSE Linux 8.0 [15]

*Kernel Version:*

'Vanilla' Linux Kernel 2.4.19 [1]

USAGI Linux Kernel 2.4.19 [2]

In order to reduce the variables, we chose the 2.4.19 kernel as it was a relatively recent kernel and the USAGI stable Release 4, dated October 7 2002, which is based on this kernel.

*Network performance Benchmarking:*

Netperf version 2.2.pl2 [16]

Having searched for tools to do throughput testing that included metrics for CPU utilisation and also had IPv6 support. Netperf seemed to suit our needs after it had been patched with the KAME IPv6 patch [17].

*IPsec Software:*

The USAGI kernel and all its supporting utilities were compiled and installed as per the USAGI documentation. Pluto, the IKE daemon had to be patched [18] to allow for automatic usage of the AES algorithm as manual keying proved problematic.

## 5. The Tests and the Test Scenarios

Performance tests were organised as follows:

Host `aragorn` acted as the netperf server. This was invoked using the following command:

```
aragorn:#netserver -6
```

Where the –6 option enables IPv6 performance testing.

Scripts were written which ran Netperf User Datagram Protocol (UDP)[19] and Transmission Control Protocol (TCP) [20] stream tests. Each test was 4 minutes in length and was performed 3 times. The content of these scripts is shown in Listing 1 and Listing 2.

```
#!/bin/sh
#TCP Stream test
time=240

./netperf -H aragorn.tssg.org -t TCP_STREAM -C -c -l $time
./netperf -H aragorn.tssg.org -t TCP_STREAM -C -c -l $time
./netperf -H aragorn.tssg.org -t TCP_STREAM -C -c -l $time
```

Listing 1: Netperf TCP Stream test script

```
#!/bin/sh
#TCP Stream test
time=240

./netperf -H aragorn.tssg.org -t UDP_STREAM -C -c -l $time
./netperf -H aragorn.tssg.org -t UDP_STREAM -C -c -l $time
./netperf -H aragorn.tssg.org -t UDP_STREAM -C -c -l $time
```

Listing 2: Netperf UDP Stream test script

The purpose was to establish relationships between the performance overhead in the server (`aragorn`) and the number of clients being served. With this in mind, the above tests were first run sequentially on 1 client (`gandalf`), then on 2, 3, 4 and finally, all 5 clients.

The test start times were set up on each client using the standard unix job scheduler *cron*. All hosts times were synchronised to a local time-server using the *netdate* utility.

This test set was repeated for each of the following scenarios:

#### *5.1.1 Control Scenario: IPv4*

| *Protocol* | IPv4 |
|---|---|

| | |
|---|---|
| *IPsec* | No |
| *Kernel* | Vanilla 2.4.19<br>USAGI 2.4.19 |
| *Bandwidth Limited* | None |

This scenario (IPv4 tests with no IPsec VPN deployed) was used as a guide to throughput and overhead figures.

*5.1.2 Control Scenario: IPv6*

| | |
|---|---|
| *Protocol* | IPv6 |
| *IPsec* | No |
| *Kernel* | Vanilla 2.4.19<br>USAGI 2.4.19 |
| *Bandwidth Limited* | None |

This scenario was used as a guide to throughput and overhead for IPv6 with no IPsec VPN deployed.

*5.1.3 IPsec Scenario 1: IPv6*

| | | |
|---|---|---|
| *Protocol* | | IPv6 |
| *IPsec* | *SA* | Transport Mode |
| | *Auth* | HMAC-MD5 |
| | *Enc* | 3des-cbc |
| *Kernel* | | USAGI 2.4.19 |
| *Bandwidth Limited* | | None |

This scenario provided results for throughput and overhead for IPv6 tests with IPsec VPNs deployed using the 3des-cbc algorithm for encryption.

*5.1.4 IPsec Scenario 2:IPv6*

| | | |
|---|---|---|
| *Protocol* | | IPv6 |
| *IPsec* | *SA* | Transport Mode |
| | *Auth* | HMAC-MD5 |
| | *Enc* | aes-cbc |
| *Kernel* | | USAGI 2.4.19 |
| *Bandwidth Limited* | | None |

This scenario provided results for throughput and overhead for IPv6 tests with IPsec VPNs deployed using the AES algorithm for encryption.

## 6. Results

*Notes on the results:*

The results for IPv4 and IPv6 throughput with no encryption for both *vanilla* and USAGI kernels were extremely close (less than 1%), so for clarity they will not be shown here.

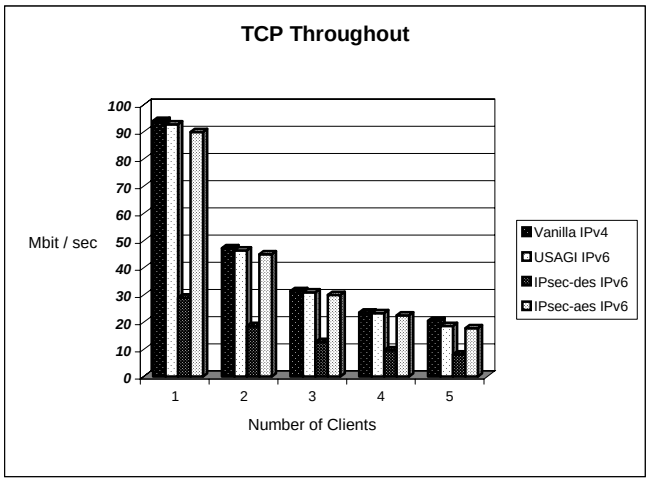



Figure 3 - TCP Throughput

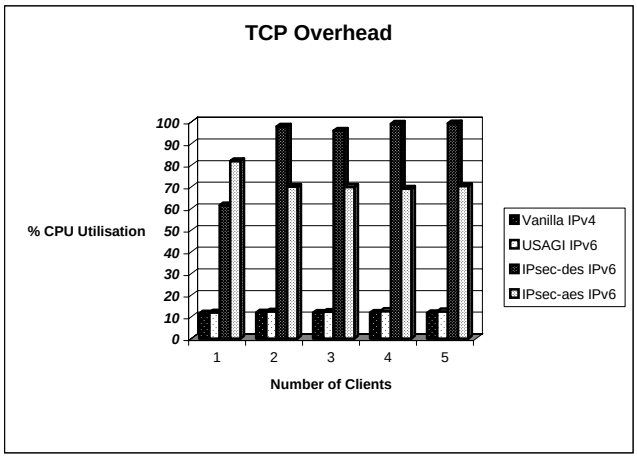



Figure 4 - TCP Overhead

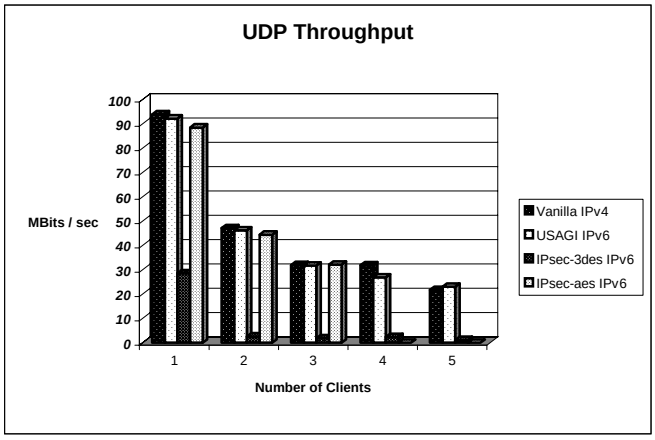



Figure 5 – UDP Throughput

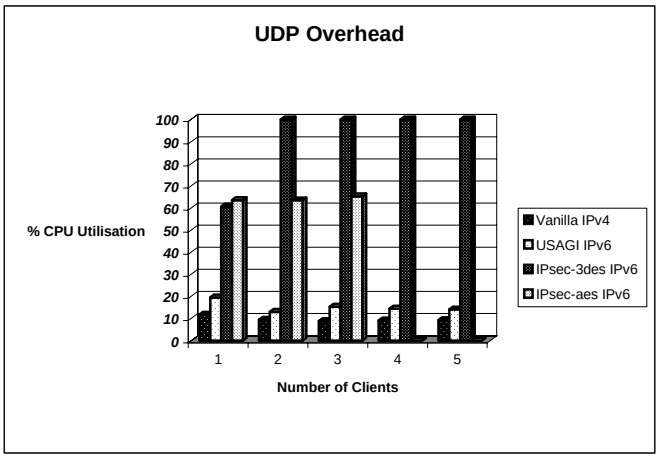



Figure 6 – UDP Overhead

Firstly, before analysing the results, it should be noted that results could not be obtained for 4 and 5 client connections using UDP. These tests were attempted several times and their failure is currently being investigated.

Looking at Figure 3 it can be seen that enciphering the link with AES and using HMAC-MD5 for authentication does not reduce the throughput of the clients appreciably. AES is markedly superior to DES in this case.

Looking at Figure 4 it can be seen that the load induced by the AES algorithm seems to maintain a relatively constant level of 60%, except in the case of a single client. This would seem to indicate that the bottleneck, in this case, is the network card and not the processor.

The results are similar for AES with UDP traffic, but it can be seen from Figure 5 (at least up to and including 3 clients) that DES throughput falls dramatically once more than one client is involved, which indicates that the server is being overworked. This is borne out by Figure 6, which shows the DES CPU utilisation approaching 100% when more than one client is involved.

## 7. Conclusion

After applying the above tests the conclusions can be drawn that the AES algorithm performs more efficiently than its predecessor, DES, on similar hardware. Hence, IPsec could be deployed as an encryption and authentication service in the TORRENT architecture, without hitting any significant performance bottlenecks, if the algorithms deployed are AES for encryption and HMAC-MD5 for authentication.

## References

[1] The Linux Kernel Archives, Available: http://www.kernel.org
[2] USAGI UniverSAl PlayGround for Ipv6) Kernel, Linux IPv6 Development Project. Available: http://www.ipv6.org
[3] E. Scharf, P. Hamer, K. Smparounis, W. Payer, J. Ronan, M. Crotty, “An Intelligent Integrated Approach to Multi-service Residential Access Networks”, Journal of the Communications Network, July-September 2002
[4] TORRENT (Technology for a Realistic End User Access Network Test-bed), IST-2000-25187. http://www.torrent-innovations.org
[5] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” Internet Engineering Task Force, RFC 2401, November 1998.
[6] S. Kent and R. Atkinson, “IP Authentication Header,” Internet Engineering Task Force, RFC 2402, November 1998.
[7] S. Kent and R. Atkinson, “IP Encapsulation Security Payload,” Internet Engineering Task Force, RFC 2406, November 1998.
[8] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", Internet Engineering Task Force, RFC 2408, November 1998.
[9] H. Orman, "The OAKLEY Key Determination Protocol", Internet Engineering Task Force, RFC 2412, November 1998.
[10] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", Internet Engineering Task Force, RFC 2407, November 1998.
[11] D. Harkins, and D. Carrel, "The Internet Key Exchange (IKE)", Internet Engineering Task Force, RFC 2409, November 1998.
[12] C. Madson and N. Doraswamy, “The ESP DES-CBC Cipher Algorithm with Explicit IV”, Internet Engineering Task Force, RFC 2405, November 1998.
[13] S. Frankel, S. Kelly and R. Glenn, “The AES Cipher Algorithm and Its Use With IPsec”, Internet Engineering Task Force, Internet draft, December 2002.
[14] C. Madson and R Glenn, “The Use of HMAC-MD5 within ESP and AH”, Internet Engineering Task Force, RFC 2403, November 1998.
[15] SuSE, Linux Distribution, http://www.suse.com
[16] Netperf, A Network Performance Benchmark, Available: ftp://ftp.cup.hp.com/dist/networking/benchmarks/netperf/netperf-2.2pl2.tar.gz
[17] The KAME Project, http://www.kame.net/
[18] USAGI IPv6 IPsec AES enhancement patch, Available: http://www002.upp.so-net.ne.jp/h-yamamo/ipv6/usagi/ipsec.html
[19] J. Postel, “User Datagram Protocol”, Internet Engineering Task Force, RFC 768, August 1980
[20] Defence Advanced Research Projects Agency, “Transmission Control Protocol”, Internet Engineering Task Force, RFC 793, September 1981.

# Suitability of IPsec for securing the Access Network in TORRENT

John Ronan, Steven Davy & Jerry horgan
Telecommunications Software & Systems Group (TSSG),
Waterford Institute of Technology, Cork Road, Waterford, Ireland
{jronan,jhorgan,sdavy}@tssg.org

February 12, 2004

**Abstract**

This paper evaluates the performance of IPsec between the Residential Gateway (RG) and the Local Access Point (LAP) as a network level security mechanism for the purposes of securing media streams from unauthorised interception. Concerning the applications, this paper discusses the use of the netperf performance monitoring tool, with the associated KAME IPv6 patches.

**Keywords:** Encryption, Residential Gateway

# Contents

# 1 Introduction

IPv6 is integrated in TORRENT as a transport protocol and the IP Security Protocol (IPsec) is used as a service for securing the data between the Residential Gateway (RG) and the Local Access Point (LAP). Investigations of various authentication and key agreement schemes have been carried out in the IPsec performance trials, as documented in [6].

Since that work was carried out, there have been enhancements made to the Linux kernel that improve the performance and also have better IPv6, and in particular IPsec support. Here, we extend the work done previously, and thoroughly examine if the latest Linux kernels are now suitable for the task.

# 2 Experiments Carried out

The tests consisted of NetPerf being scripted to run 10 times, one hour at a time. The purpose of each test run was to send as much data as possible in a defined length of time between the client and server. NetPerf allows for testing over IPv4 and IPv6, while calculating overall throughput as well as monitoring the processor overhead on both client and server.

The initial tests were done on a LAP in WIT-TSSG in order to test the maximum performance for the system. Following from this, we then migrated our testing to the tesbed in UST Suttgart. Here we performed testing on the IPv6 protocol only.

The following set of tests were performed in WIT-TSSG:

- IPv4
  - TCP
  - UDP
- IPv6
  - TCP
  - UDP

All tests were run in Transport[**?**] mode. The set of tests that were run were:

- Authentication header[**?**]

  - Secure Hash Algorithm No 1. (SHA-1)
  - Keyed Message Digest No 5 (MD-5)
- Encrypted Security Payload header (ESP)
  - Triple DES (3DES)
  - Advanced Encryption Standard - Rijndael (AES)
- AH & ESP together
  - SHA-1 & 3DES
  - SHA-1 & AES
  - MD-5 & 3DES
  - MD-5 & AES
- ESP with optional Authentication
  - SHA-1 & 3DES
  - SHA-1 & AES
  - MD-5 & 3DES
  - MD-5 & AES

# 3 TSSG Testbed

The TSSG Testbed consists of a Flextel WebVision 4012 with 4 blades. Two of the blades were used to conduct the following performance tests.

## 3.1 IPv4

We began by testing all algorithms using Linux kernel version 2.6.0, we also did the tests on the USAGI snapshot and linux-2.6-test10 kernel. There was no difference in the IPv4 test results between the three different kernels . Figures 1 and 2 shows the throughput achieved and the overhead incurred.

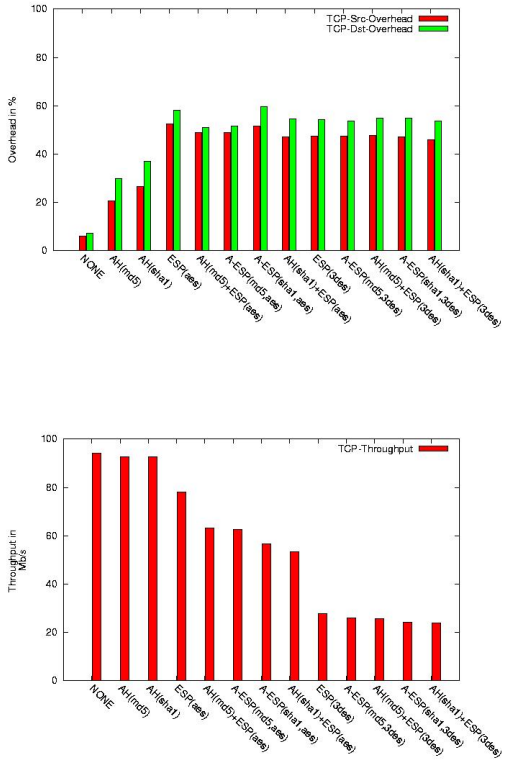



Figure 1: TCP Transport Mode Overhead & Throughput

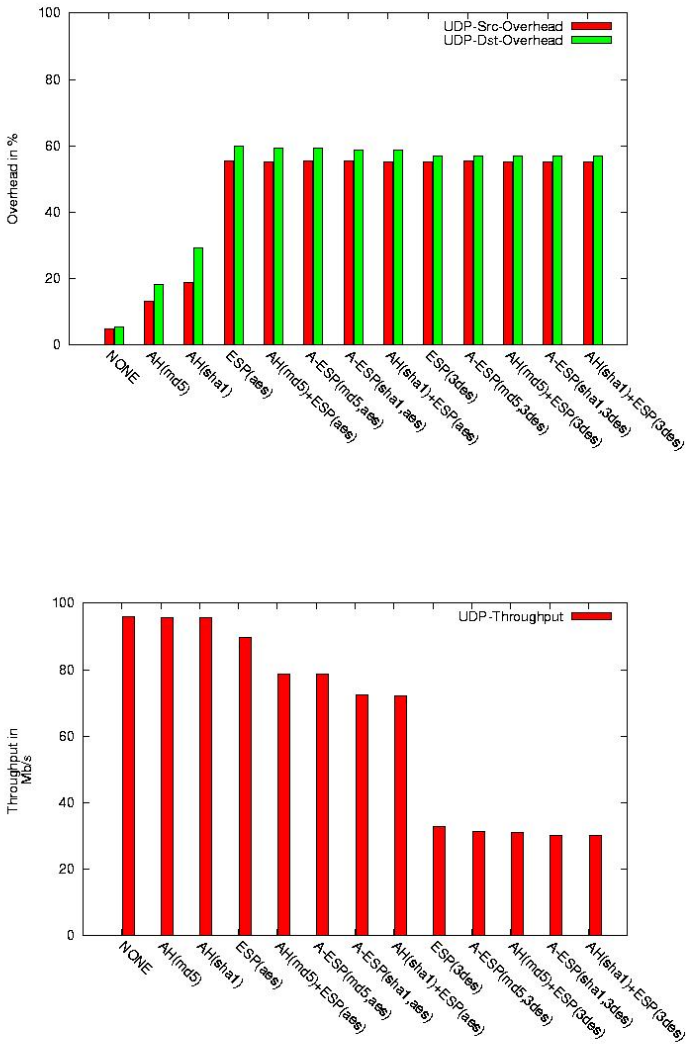



Figure 2: UDP Transport Mode Overhead & Throughput

### 3.1.1 IPv4 Summary

In figure 3 it can be seen that the AES encryption algorithm coupled with the MD5 authentication is the most efficient combination.

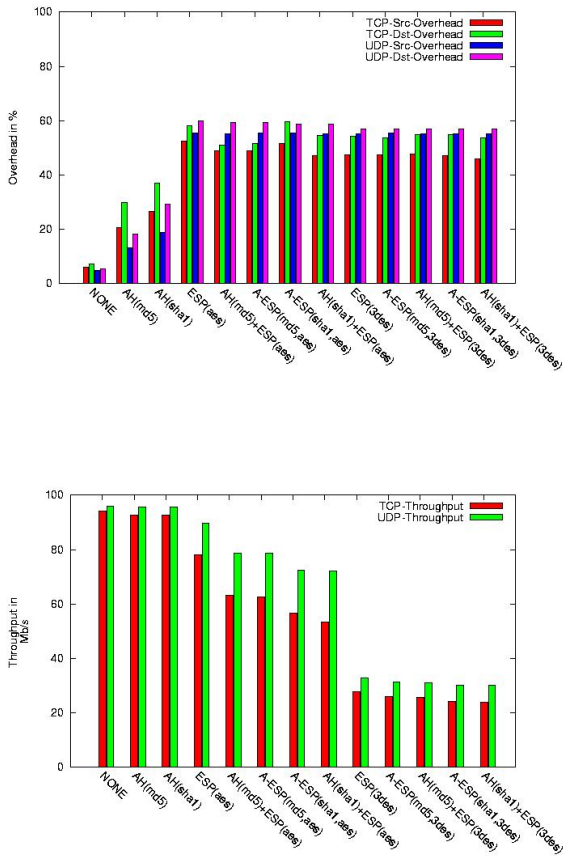



Figure 3: Transport Mode Overhead & Throughput

### 3.2 IPv6

For this section, we changed our configuration scripts to use IPv6 addresses instead of IPv4 addresses, no other changes were made to the configuration.

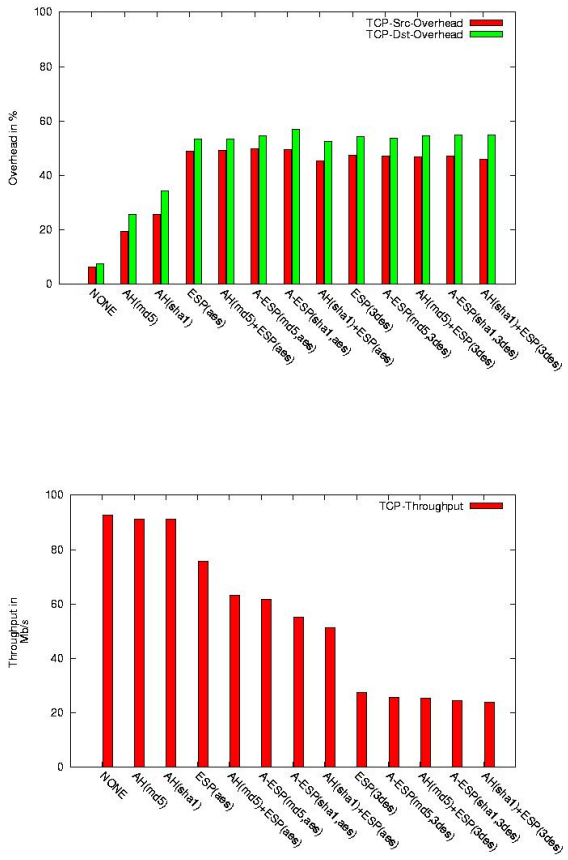



Figure 4: TCP Transport Mode Overhead & Throughput

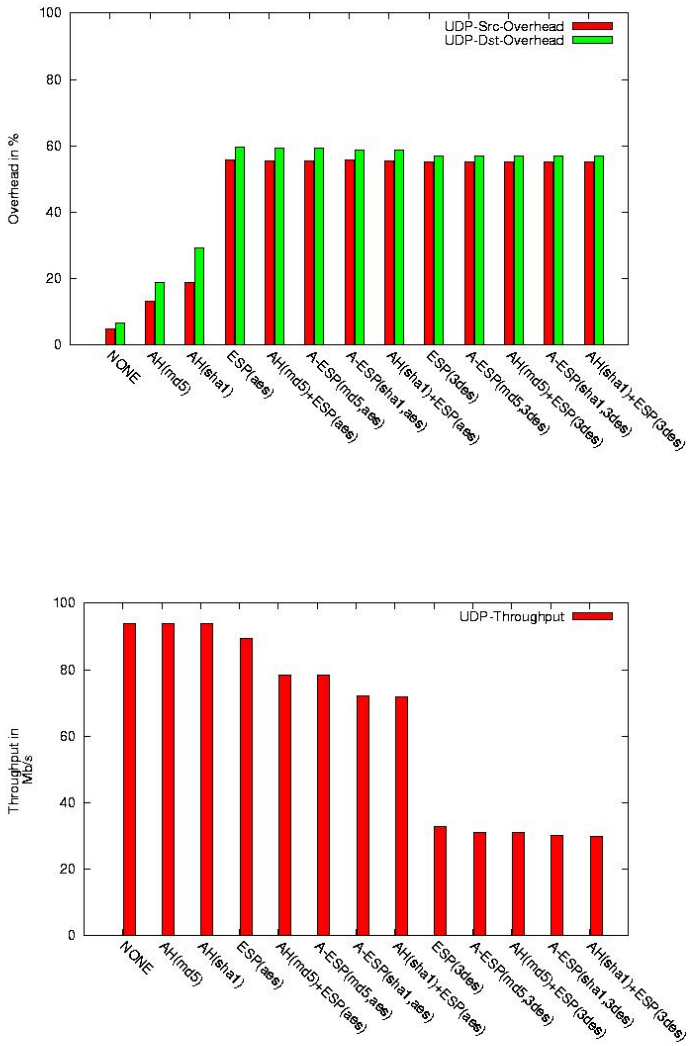



Figure 5: UDP Transport Mode Overhead & Throughput

### 3.2.1 IPv6 Summary

As expected, the figures are much like the figures obtained for IPv4.

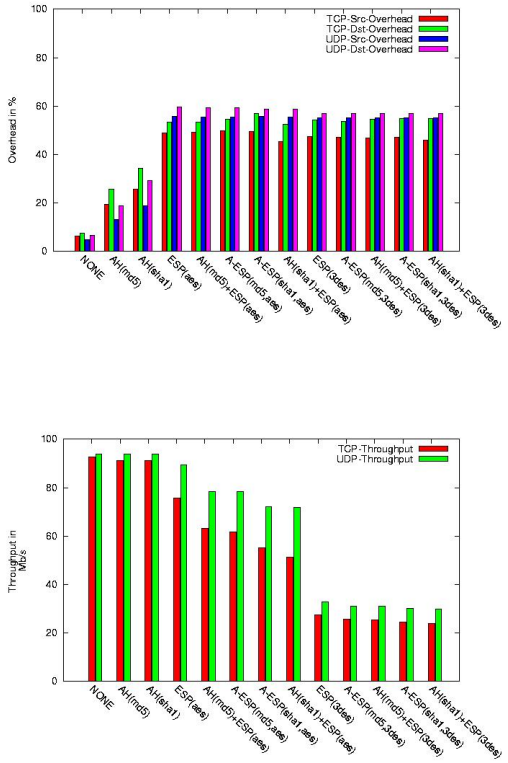



Figure 6: IPv6 Overhead & Throughput

### 3.3 IPv4 vs IPv6 Comparison

Here we compare IPv4 directly with IPv6, figure 9 is the most interesting as it shows IPv4 has a slight advantage over IPv6 in terms of throughput in virtually every case. This is consistent with the extra overhead incurred by the longer IPv6 headers. And there doesn't seem to be any other performance issues with the IP stacks.

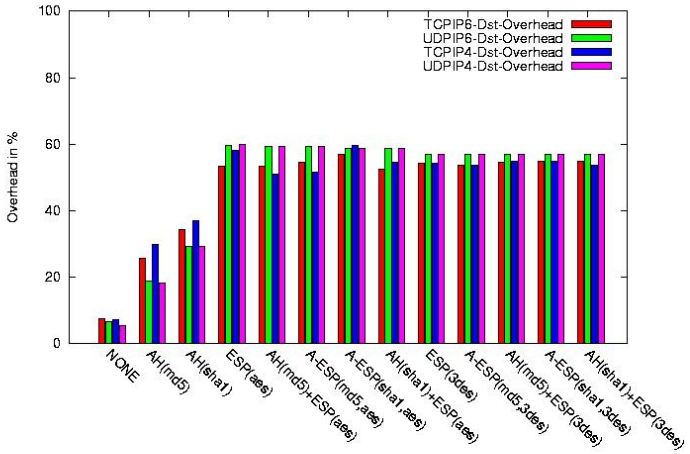



Figure 7: IPv4 vs IPv6 Destination Overhead

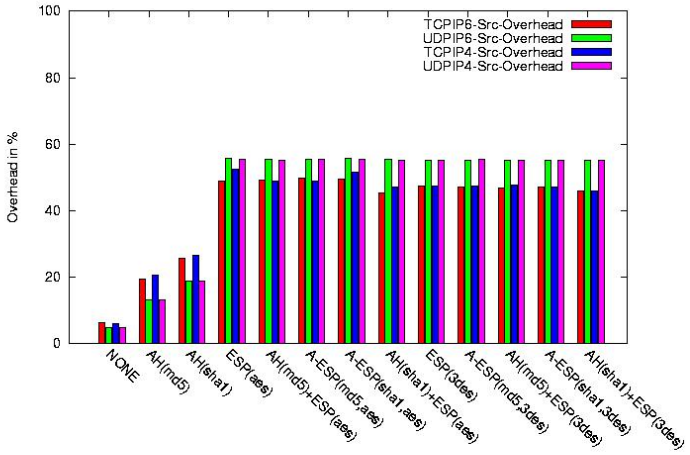



Figure 8: IPv4 vs IPv6 Source Overhead

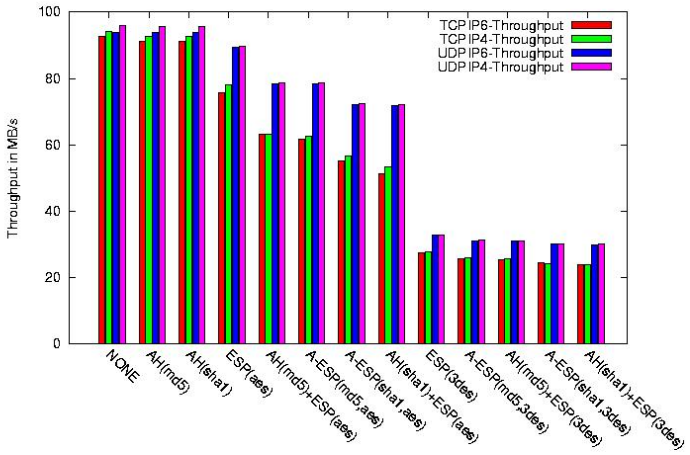



Figure 9: IPv4 vs IPv6 Througput

# 4 UST Testbed

In this case, we were only interested in the IPv6 protocol so we restricted our tests to IPv6. At this stage it was apparent that AES and MD5 are the most efficient algorithms, so we further restricted our tests to these algorithms. There are two things to note before interpreting the graphs. Firstly, the Flextel Blade in Stuttgart was single processor, secondly the link between the LAP and the RG was only a 10Mbit connection. Interestingly, as can be seen from Figure 10, once any extra load is put on the processor due to cryptographic computations, the throughput immediately suffers. Looking at Figure 11, the RG's processor is almost immediately overwhelmed with the amount of processing required.

## 4.1 IPv6

### 4.1.1 Transport Mode - TCP

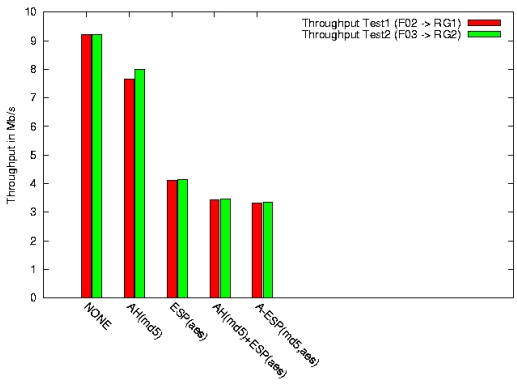



Figure 10: IPv6 Throughput between RG and LAP

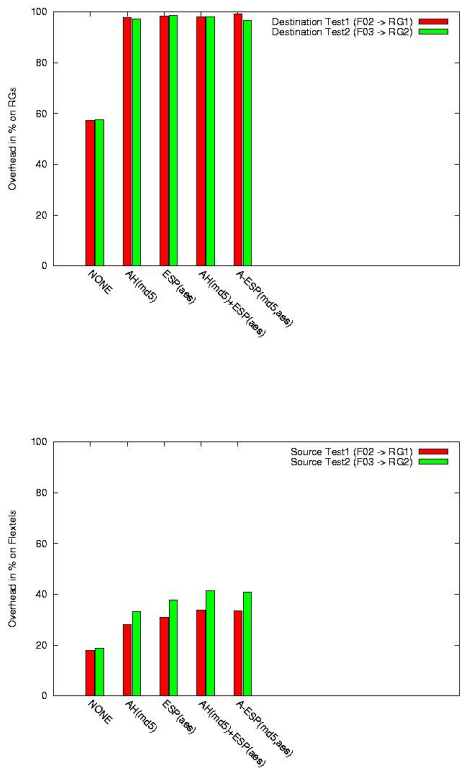



Figure 11: Residential Gateway & Local Access Point Overhead

# 5 Conclusion

With planning, IPsec can be deployed, today, as a security service. For TORRENT, it would be possible to deploy IPsec services on an access network serviced by a single Flextel blade, up to a cumulative bandwidth of about 60Mbits per second (assuming external xDSL/Cable termination devices). This figure could, most likely, be improved upon with the addition of hardware accelerator devices.

Looking at the RG figures. With the current hardware, TORRENT would be unable to offer any IPsec services at bandwidths over 3Mbits.

### 5.1 Future Work

As TORRENT is finishing, we hope to continue this work as part of the SEINIT project and test IPsec accelerator cards in the Flextel WebVision we have at our disposal. We intend to compare the various vendors solutions solutions, both hardware and software deployed in a realistic environment.

## References


[1] The Linux Kernel Archives, available http://www.kernel.org

[2] USAGI Project, available http://www.linux-ipv6.org

[3] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Internet Engineering Task Force, RFC 2401, November 1998.

[4] S. Kent and R. Atkinson, *IP Authentication Header*, Internet Engineering Task Force, RFC 2402, November 1998.

[5] S. Kent and R. Atkinson, *IP Encapsulation Security Payload*, Internet Engineering Task Force, RFC 2406, November 1998.

[6] Ronan J, Malone P, Ó Foghlú M, *Overhead Issues for Local Access Points in IPsec enabled VPNs*, IPS Workshop, Salzburg, February 2003. Retreived: 3. April, 2003 from `http://www.ist-intermon.org/workshop/papers/09_01_vpn-overhead.pdf`

[7] TORRENT (Technology for a Realistic End User Access Network Testbed), IST-2000-25187. `http://www.torrent-innovations.org`