Project Number :	IST-2002-002154
Project Title :	Distributed Adaptive Security by Programmable Firewall

DIADEM Firewall

D13 – Plan for exploitation of results

Deliverable Type :	Document
Dissemination:	Public
Contractual date :	September 2006

Editor :	Yannick Carlinet (FT)
File Name	
Contributors :	See list of authors
Version :	1.0
Version Date :	September 2006
Deliverable Status:	

The DIADEM Firewall consists of:

	Partner	Short name	Country
1	France Telecom	FT	France
2	University of Tübingen	TU	Germany
3	IBM Research GmbH Zurich Research Laboratory	IBM ZRL	Switzerland
4	Imperial College London	ICL	United Kingdom
5	Jozef Stefan Institute	JSI	Slovenia
6	Groupe des Ecoles des Télécommunications	GET	France
7	Polish Telecom	TP	Poland

Project Management:

Yannick Carlinet (FT)
Phone +33 2.96.05.03.25
Fax: +33 2 96 05 37 84
E-mail yannick.carlinet@francetelecom.com
France Telecom CORE/M2I
2 ave. Pierre Marzin,
22307 Lannion, France

List of authors:

Gerhard Muenz, TU
Patricia Sagmeister, IBM ZRL
Jan Van Lunteren, IBM ZRL
Morris Sloman, ICL
Paweł Tobiś, TP
Olivier Paul, GET
Dušan Gabrijelčič, JSI
Yannick Carlinet, FT

Executive summary

This document describes the plan for exploitation of the results of the Diadem Firewall project. It presents the different strategies put in place, for exploitation in collaborative projects, academic projects, operators' internal projects, partnerships with industrials, and in standardization bodies.

Acronyms

ANSI	American National Standards Institute
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
DDoS	Distributed Deny of Service
DPI	Deep Packet Inspection
DSL	Digital Subscriber Lines
E&TS	Engineering & Technology Services
ETSI	European Telecommunications Standards Institute
FPGA	Field-programmable gate array
HARTES	Holistic Approach to Reconfigurable Real Time Embedded Systems
HISTORY	High Speed Network Monitoring and Analysis
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Intellectual Property
IPFIX	IP Flow Information Export
IPS	Intrusion Prevention System
ITU	International Telecommunication Union
MUSE	Multi Service Access Everywhere
NSTT	Non-Spoofed Traffic Transmitter
OSCAR	Overlay Network Security: Characterization, Analysis and Recovery
OSI	Open Systems Interconnection
PSAMP	Packet Sampling
QoS	Quality of Service
RFC	Request For Comment
RNRT	Réseau National de Recherche en Télécommunications
SHERIFF	Security Handler for Evaluation & Reaction against Intrusions, Frauds, Floods
SpoVNet	Spontaneous Virtual Networks
VERMONT	Versatile Monitoring Toolkit
WG	Working Group
XML	Extensible Markup Language

Table of Contents

1. Introduction

This document describes the plan for exploitation of the results of the Diadem Firewall project. Our strategy for exploiting the Diadem Firewall results is fourfold: first we will use the code, architecture and concepts developed in the project in other collaborative and academic projects. This is possible because of the very innovative nature of some of the results. For commercial exploitation we will follow two leads: partnerships with industrial and operators' internal projects which aims at deploying new services and equipment in the network. Partnerships with industrials will allow for the implementation in hardware of the functions for which operators have a need. Operators' internal projects are also a good way to adapt and refine the technical innovations developed in Diadem Firewall according to the requirements of the business units. Finally we will present the relevant results to standardization bodies, so that these results can be used by manufacturers who wish to have their products inter-operable with others.

Section 2 will describe all the opportunities to re-use the innovative project results in collaborative/academic projects. Section 3 explains the advantages of partnerships with manufacturers and presents the contacts we have for this purpose. Section 4 explains our strategy towards standardization bodies. Finally a table of the exploitable knowledge produced in the project is given.

2. Collaborative projects

2.1. History project

The University of Tuebingen is going to exploit the results of Diadem Firewall for future research on network monitoring and traffic analysis. Software components like the Monitoring Element Vermont and the Violation Detection Framework are flexible and extensible tools that will be used and further developed in the context of other research activities. A current project that is directly related to Diadem Firewall is called History (High-Speed Network Monitoring and Analysis, cf. [12] and [16]), which is a research cooperation between the Universities of Erlangen-Nuremberg and Tuebingen.

Another national project with participation of the University of Tuebingen is called SpoVNet (Spontaneous Virtual Networks) and is starting right now in September 2006. In the scope of this project, the monitoring techniques developed in Diadem Firewall will be extended for usage in overlay networks.

Proposals for new research project on advanced methods for traffic analysis are in an advanced preparation status, e.g. for submission to the Deutsche Forschungsgemeinschaft (German Research Foundation).

2.2. Imperial College collaboration with US Army Labs

The policy-based approach developed in the Diadem Firewall project will be used in an international follow-on project related to security in Defence systems funded by UK Ministry of Defence and US Army Research Laboratory [17]. IBM Research is leading the International Technology Alliance, as a consortium of 24 institutions from industry and academia in both the UK and the US.

We will be working on security across systems of systems focusing on security issues that are unique to dynamic military environments such as automated negotiation of security policies across coalitions, developing energy-efficient security protocols, and managing trust and risk dynamically, instead of as a design time activity, by including operational context. Adaptive policy security is an important aspect of this system. This is a 10 year research project focussing on long term research issues.

2.3. Hartes

An EU IST project HARTES (Holistic Approach to Reconfigurable Real Time Embedded Systems, cf. [13]) will reuse some of the work on the in-line FPGA processor for next-generation communication and entertainment facilities.

2.4. Oscar

Oscar (for Overlay Network Security: Characterization, Analysis and Recovery) is a collaborative project funded by RNRT (French governmental institution). It aims at developing a prototype for detecting attacks in overlay networks, and protecting both the overlay and the underlying networks. We will use the Diadem Firewall response system to deal with the attacks identified in Oscar. The Oscar project is interesting because it is classified as a pre-competitive project, which means it will develop a working prototype that will be tested in an operational network environment.

2.5. IST-MUSE

MUSE [14] is an IST-funded project into the research and development of a future, low cost, multi-service access network. The access network should provide secure connectivity between end-user terminals and edge nodes in a multi-provider environment. It should also be suited for the ubiquitous delivery of broadband services to every European citizen. MUSE aims at a consensus view of the future access and edge network achieved by the co-operative research of almost all major players in Europe in the area of Broadband Access. The project addresses the network architecture, techno-economics, access nodes, solutions for the first mile, and inter-operating with the home network. Solutions will be evaluated in end-to-end lab trials and promoted in standardisation.

France Telecom and Polish Telecom are already contributors to MUSE and they will propose the architecture and security functions developed in the Diadem Firewall project to the Task Force 1 (Access architecture and platforms). This will greatly benefit the MUSE project and it will also be an important asset in the standardization of said architecture and security network functions.

2.6. Collaboration with industrials in Slovenia

Jozef Stefan Institute will exploit the results of the project in future research into response actions in the scope of flexible and manageable firewall elements. JSI is planning to do additional development in the field with further enhancements of the software developed in the project. Currently we are seeking the funding for this development through national funding for applicative research. We are negotiating possible collaboration in such project with a local service provider (http://www.t-2.net/) and system integrator in the area (http://www.smartcom.si). If the project proposal is successful the result of the project will be an industrial product used/sold by target project partner. In the short term we are also working on new research topics and issues that we will seek to address in the next EU research framework programme.

The results of the Diadem Firewall project will be also exploited through scientific publications and educational process (Faculty of Criminal Justice and Security**,** http://www.fpvv.uni-mb.si/defaultEng.aspx).

2.7. GET future projects

GET contribution to the Diadem Firewall project will be reused in several manners. The extensions to the Ipfilter filtering module will be advertised to Ipfilter users. In order to ease the use of these extensions our current exporter is currently merged with the existing Ipfilter monitoring software.
We are pursuing the research in traffic analysis using the models and software that were developed during the Diadem Firewall project. Our current focus is on the adaptation of our inference models to speed up well-known pattern matching traffic analysis techniques. We are currently working on proposals for new research projects that could take advantage of such adaptations.

2.8. SHERIFF

It is a project internal to France Telecom and Polish Telecom.The aim of the SHERIFF project (Security Handler for Evaluation & Reaction against Intrusions, Frauds & Floods) is to create a platform which could deal with security incidences such as intrusions, DoS attacks, viruses, spam, etc.
The algorithm implemented in Diadem Firewall which detects TCP SYN flood attacks will be used to improve detection method for DoS type attacks in the SHERIFF project. The TCP SYN flood detection method is based on difference between SYN packets sent to destination IP address and SYN/ACK packets sent form source IP address. This algorithm will be used in filtration module which is part of a system preventing network attacks (traffic cleaning centre).

Testing scenarios and work on firewalls will be used for testing solutions created during the SHERIFF project, in particular for DoS attacks, TCP SYN flood attacks, and HTTP performance tests. Tests that generate SYN flood traffic will be used in functional testing of NSTT module (Non-Spoofed Traffic Transmitter) which is equipped with SYN Cookie mechanism. For DoS attacks there are two main use cases: SYN flood use-case and WWW server stress test use-case. In those two tests two main measurements are made: TCP connection time and average HTTP transfer time.

3. Dissemination

Dissemination of the results of the project is an important part of the exploitation strategy. The more widespread the results are, the more beneficial the architecture and the innovative ideas will be.

First of all, we will have articles about the project in the specialized press. This will enable key players in the security area (manufacturers, operators, researchers) to know about the project. We already had three press releases in [18], [19], [20], and one pending in a Swiss newspaper.

Secondly, the project will be presented internally by each organization and particularly by the two operators to their Business units. We will also write an article about the results obtained (detailed in deliverable D14 [1]) in a conference related to network security or network management (ongoing work).

Finally, we have organized a two-day workshop in Tuebingen (28-29 September) with a quite large attendance expected (28 submissions were received after the call for papers). The workshop is entitled "Monitoring, Attack Detection and Mitigation", see [21] for more details.

4. Commercial exploitation

4.1. Partnerships with industrials

Some functions developed in the Diadem Firewall project will only be commercially exploited if they yield sufficient performance, for instance in the case of components such as the reaction functions, the Firewall Devices, and the Monitoring Elements. The results of our experiments, described in Deliverable D14 [1], demonstrate that the approach is feasible if some components are implemented in hardware. This is why establishing a partnership with manufacturers is strategically important.

Consequently we will mainly aim to establish partnerships with manufacturers. Such partnerships will benefit the manufacturer as well for the following reasons:

- It is a cost-efficient way for them to improve their technology, both in terms of the technology they use and of implementing the functions needed by the operators (i.e. their clients). They can better anticipate the evolution of the protocols used in the network and understand the requirements of the operators on the equipment they will use in their network.
- It is a cost-efficient way to develop their Intellectual Property, by sharing the costs of the research and developments with their partner.
- It is a good way for manufacturers to gain leverage for standardization of their technologies, protocols and patents.
- They can benefit from the academic knowledge of a collaborative project such as Diadem Firewall. In this way they can improve their algorithms and methods with cutting-edge techniques.
- They can also benefit from funding from operators, in exchange for exclusive use for the operator of specific functions during a limited amount of time.
- They will sell more of their products if they better match the requirements and needs of their clients.

The benefits for France Telecom and Polish Telecom include:

- Pieces of equipments that match their requirements, allowing for a more cost-effective and faster integration in their operational network.
- Exclusive rights on specific technologies or functions, allowing them to provide more advanced services to their customers than their competitors.

We currently have contacts with manufacturers, including IDS/IPS, routers and DPI (Deep Packet Inspection) devices vendors that are interested in having a partnership with France Telecom or Polish Telecom.

IDS/IPS manufacturers we are in contact with are interested mainly by the Detection Modules, the Reaction Functions and the APIs defined and implemented in Diadem Firewall. We are currently in discussion with Arbor Networks and EADS.

We are also aiming at a partnership with router vendors, since the routers can implement security functions, in particular regarding the monitoring functions, but also the reaction functions (traffic shaping, flow blocking) as shown in the Diadem Firewall project. Therefore we are discussing with two router manufacturers: Mitsubishi Electrics and Cisco.

Finally we are in contact with a number of DPI devices vendors. Deep Packet Inspection (DPI) is a form of computer network packet filtering that examines the data part of a through-passing packet, searching for non-protocol compliance or predefined criteria to decide if the packet can pass. This is in contrast to shallow packet inspection (usually called just packet inspection) which just checks the header portion of a packet. DPI devices have the ability to look at Layer 2 through Layer 7 of the OSI model. This includes headers and data protocol structures. The DPI will identify and classify the traffic based on a signature database and will allow the user to perform various actions. A classified packet can be redirected, marked/tagged (for QoS services), blocked, rate limited, and so on.

There are many benefits to be expected from collaborating with a DPI vendor. Firstly the DPI devices decode the application-layer protocol, which is a useful complementary functionality to the monitoring approach we have in Diadem Firewall. Indeed a lot a DDoS attacks require analysis of the layer 7 protocols if they are to be detected and mitigated. Secondly most DPI devices are designed to run in the access and the core network, which means that they can deal with traffic in the order of tens of gigabits. The approaches of DPI devices and Diadem Firewall have many similarities therefore it makes sense to collaborate with each other. For example, some monitoring functions of the Monitoring Elements can be adopted for DPI and implemented in hardware for better performance. The Firewall API can be adopted for DPI device configuration to provide interoperability with other devices, and to increase flexibility with respects to the range of possible responses to attacks.

We are currently in contact with the following DPI manufacturers: Allot [3], Ellacoya [4], L7-Networks [11], Niksun [5], Qosmos [2], Netintact [6], Packeteer [7], Radware [8], Sandvine [9], and Narus [10].

4.2. Exploitation for network operation and management

The Diadem Firewall prototype is intended to be the proof-of-concept illustration of an architecture that (among others) allows the policy-based management of several commercial pieces of equipment with different proprietary control interfaces. The system could therefore be used as a generic framework for dynamic network management and configuration tasks, provided that the modules to control the different pieces of equipment of the network are developed.

This presents many interesting opportunities, so the Diadem Firewall system will be presented to the operational branch and the business units of France Telecom and Polish Telecom.

4.3. IBM exploitation

IBM ZRL plans to disseminate the results of the project through IBM Engineering & Technology Services (E&TS). This is a service organisation which combines IBM technology with our intellectual property to offer customized solutions for our clients. There are two parts which can be offered as service:

- Intellectual property rights
- Hardware prototype including the proprietary software API

In the case of intellectual property (IP) rights our clients can licence the according IP for the classification algorithm and can either implement this filtering mechanisms on their own. Or it is possible that E&TS provides this solution as a customized system solution according to the requirements of the client.

In the second case it is also possible that IBM provides the prototype for the high-speed classifier engine, developed within the Diadem Firewall project, including the proprietary software part as it is. This would be put in an asset data base of E&TS, which could be used by any IBM consultant to shape the system solution for a specific client.

5. Standardization

5.1. DSL Forum

The DSL Forum [15] is a consortium of approximately 200 leading industry players covering telecommunications, equipment, computing, networking and service provider companies. Each member company contributes to the work of the Forum through the development of the technology and its effective delivery. They participate in technical and marketing working groups, sharing their knowledge, experience and expertise to create common, agreed protocols, processes and best practice recommendations for use by the industry and for standards and other related industry bodies. The Forum contributes to global industry standards by developing Technical Reports and through formal liaisons with global standards bodies such as ANSI, ETSI, ATIS and ITU. Completed DSL Forum Technical Reports cover the technology itself, network operations and management, interoperability and integration of DSL technology into existing infrastructures. Two partners of the Diadem Firewall consortium are members of the DSL Forum: France Telecom and Polish Telecom.

The partner France Telecom plans to contribute to the DSL Forum in 2006. We intend to participate in the "Architecture and transport" and "Operations and network management" working groups.

Our goal is to contribute to technical reports related to security architectures and the security functions required in broadband operational networks. We will also contribute on the topic of integration of such architecture and functions in the network. In order to achieve this objective we will present the results of the Diadem Firewall project to the Task Force 1 of the IST-MUSE project, in which France Telecom and Polish Telecom are already contributors.

5.2. IETF

The University of Tuebingen is going to continue its active participation in the IPFIX/PSAMP standardization process in the IETF, using the ideas and technology developed within the Diadem Firewall project. Recently, a new -00 draft on XML-based configuration of IPFIX/PSAMP devices has been submitted, generating considerable interest within the IPFIX community. This draft contains the specification of an enhanced and generalized version of the Monitoring API used in Diadem Firewall. This work is ongoing in the IPFIX working group at the IETF.

6. Exploitable knowledge and its use

All software developed in the project will be made available on the Diadem Web site.

The following table lists the exploitable knowledge produced in the project.

Overview table

Exploitable Knowledge (description)	**Exploitable product(s) or measure(s)**	**Sector(s)** of application	Timetable for commercial use	Patents or other IPR protection	**Owner** & Other Partner(s) involved
1. Detection and response to DDoS attacks in distributed security architecture	Improvement of other similar research projects in security area - collaboration with FT	Research and Development			Diadem Firewall Consortium (Owner) TP
2. Tests scenarios and other aspects in firewalls testing area	Part of firewalls testing methodology & procedures for TP security laboratory accreditation	Firewall vendors, Measurement quality & standardization	Second half 2006.		TP
3. Monitoring Elements	Open Source Monitoring Element	1. IETF 2. router vendors 3. operators	2005 2006 2008		TU
4. Monitoring API	Configuration of Monitoring Elements using the Netconf protocol	1. IETF 2. router vendors 2. operators	2007 2008		TU
5. Framework for Violation Detection	Framework for real-time violation detection	1. operators 2. Research community	2008 2006		TU
6. Integration of commercial firewall	Prototype for adaptation of the Firewall API to the CiscoPIX firewall	Firewall vendors			TU
7. Counter-measure to TCP SYN flood DDoS attack	Prototype used for proof-of-concept and performance testing	1. ISP 2. operators	2007	patent	FT
8. Service API	API definition for dynamic deployment of counter-measures	Research and Development			FT
9. Firewall Element	Prototype of a firewall element that implements the Firewall API, and that controls a CiscoPIX firewall	Firewall & router vendors	2007		JSI
10. High speed classifier	Implementation of a high-speed classification algorithm on a FPGA board	Firewall & router vendors	2007		IBM ZRL
11. Web Server Violation Detection	Prototype for proof-of-concept and performance evaluation	Research and Development			GET

Exploitable Knowledge (description)	**Exploitable product(s) or measure(s)**	**Sector(s)** of application	Timetable for commercial use	Patents or other IPR protecti on	**Owner** & Other Partner(s) involved
Module					
12. Policy Management Agent	Prototype	Research and Development			Imperial
13. D^{3}ADAMS	Distributed DDOS Attack and Mitigation Scheme	operators	2007		Imperial

Detection and response to DDoS attacks in distributed security architecture. The knowledge gained in the Diadem Firewall project can be used to improve other research projects into network security, which are/will be realized in collaborations between FT and TP. Detection and response to DDoS attacks in distributed security architecture is an important topic for operators.

Tests scenarios and other aspects in firewalls testing area. Test scenarios and other aspects related to firewall testing are part of the testing methodology and procedures, which will be used by Polish Telecom R&D for future testing of such devices. The main goals of this process are: performing the tests faster according to approved steps; avoiding situations where tests results are argued, especially by external companies.

Monitoring Elements. The Monitoring Element implementation realizes packet sampling and flow accounting functionality as well as the export of monitoring data using the IPFIX protocol, as specified by the IETF IPFIX and PSAMP working groups. University of Tuebingen participated with the Monitoring Element implementation in an interoperability testing workshop before the 63rd IETF meeting in Paris (August 2005). The implementation of the University of Tuebingen was tested with different implementations from different participants in the workshop: Cisco, FOKUS, IBM, and NEC. The interoperability workshop was helpful for the participants to get a feedback from each other and to clarify some issues in the protocol specification and some common implementation mistakes. The interoperability workshop was a major achievement for the IETF IPFIX and PSAMP WGs. Four working group items in the IPFIX WG will be submitted in September to the IESG for publication as an RFC. The Monitoring Element implementation of the University of Tuebingen includes also flow aggregation functionality which is also currently proposed at the IETF for standardization. The Monitoring Element implementation has been released in an open source project called VERMONT (VERsatile MONitoring Toolkit).

Monitoring API. The configuration of Monitoring Elements using the Netconf protocol is unique. The IPFIX and PSAMP working groups are currently working on a MIB module for IPFIX/PSAMP devices which could be used for configuration using SNMP. In comparison, Netconf enables more flexible configuration than SNMP. Both the IPFIX and the PSAMP WGs showed interest in the configuration of IPFIX/PSAMP devices with Netconf. The Monitoring API implementation can be improved and re-used for other network monitors.

Framework for Violation Detection. The framework for violation detection can be used by network operators in their networks in order to receive and evaluate monitoring data in real-time. Due to its flexibility, the framework can be extended with new pluggable detection modules. Three modules for attack detection and traceback have been already developed in the Diadem Firewall project.

Integration of commercial firewall. The integration of the CiscoPIX firewall proved that, on the one hand, commercial firewalls can be integrated within the Diadem Firewall architecture, but on the other hand, that some features in the Firewall API can not be supported by the CiscoPIX firewall and that configuration is only possible by communicating to the firewall via CLI interface. There is a need in the market for more support for flexible dynamic configuration of firewalls.

Counter-measure to TCP SYN flood DDoS attack. This result is a counter-measure to a specific DDoS attack. The TCP SYN flood attack is one of the most commonly seen attack on TCP based servers. This result is protected by a patent owned by FT.

Service API. This dynamic deployment mechanism enables great flexibility of the system since it allows designing and deploying counter-measures to specific attacks.

Firewall Element. Prototype of a Firewall Element that implements the Firewall API and that is able to controls CiscoPIX firewalls, Linux Firewalls, and an inline FPGA-based firewall. The Firewall API is an abstraction layer for the underlying firewall or router device. Upon the call of one of the function offered in the API, the Firewall Element sends the appropriate device-dependant commands to the device to which it is attached.

High speed classifier. Implementation of a high-speed classification algorithm on an FPGA board. The algorithm is implemented into a Classification Engine which is a piece of hardware integrated with Linux.

Web Server Violation Detection Module. Prototype for proof-of-concept and performance evaluation. This detection module detects HTTP requests flooding attacks on web servers. It extracts measurements data from the Monitoring Element and infers the application-level operations. Then it checks if these operations conform to a normal behaviour, if not then a flooding attack might be in progress.

Policy Management Agent prototype. It is a policy interpreter. Each policy is associated with a specific PMA. This allows a policy to be loaded/unloaded, enabled/disabled, receive notifications of events and perform actions depending on the notification event received. The PMA is implemented as a Java RMI application.

D3ADAMS (Distributed DDoS Attack and Mitigation Scheme)

Public Project Web Site
http://www.diadem-firewall.org

7. Conclusion

Thanks to the many innovative results of the Diadem Firewall project, there are many leads that can be pursued so as to make the results of the project very beneficial to the European research community, to the industrial partners, and to European technology.

8. References

[1] Deliverable D14 – "Results of Evaluation" - http://www.diadem-firewall.org/documents/index.php
[2] Qosmos - http://www.qosmos.com

[3] Allot - http://www.allot.com
[4] Ellacoya - http://www.ellacoya.com
[5] Niksun - http://www.niksun.com
[6] Netintact - http://www.netintact.com
[7] Packeteer - http://www.packeteer.com
[8] Radware - http://www.radware.com
[9] Sandvine - http://www.sandvine.com
[10] Narus – http://www.narus.com
[11] L7 Networks - http://www.l7.com.tw
[12] F. Dressler and G. Carle, "History - high speed network monitoring and analysis," in 24th IEEE Conference on Computer Communications (IEEE INFOCOM 2005).
[13] IST HARTES project - http://cordis.europa.eu/fetch?CALLER=PROJ_IST&ACTION=D&RCN=79337&DOC=11&CAT=PROJ&QUERY=1154018641387
[14] IST MUSE - http://www.ist-muse.org
[15] The DSL Forum - http://www.dslforum.org/index.shtml
[16] The HISTORY project - http://www.history-project.net
[17] http://www.research.ibm.com/titans
[18] "Super firewall aims to stop DDOS" by Jeremy Kirk in InfoWorld, 13 July 2006 - http://www.diadem-firewall.org/press/infoworld.pdf
[19] "Seeking to tighten the Net against attack", IST Results, 10 July 2006 - http://www.diadem-firewall.org/press/ISTResults.pdf
[20] "Saboteure und Spione im Visier", Article in attempto! (Magazine by the University of Tuebingen), October 2004 - http://www.diadem-firewall.org/press/attempto.pdf
[21] IEEE/IST Workshop on "Monitoring, Attack Detection and Mitigation" - http://www.diadem-firewall.org/workshop06/index.php