

Distributed Security Appliances and their Configuration Methodology on the Basis of Information Access Policy

Vladimir Zaborovsky

St.Petersburg Polytechnical University, Russia
Infotelecom Center, vlad@rusnet.ru

Anton Titov

St.Petersburg Polytechnical University, Russia
Telematics Department, avt@npo-rtc.ru

ABSTRACT

Until recently one of the reasons that reduces efficiency and wide implantation of new security systems was absence of technologies of automation for adjustment and the analysis of security systems and their correspondences to corporate security policy requirements. Today absolutely clearly that without usage of the specialized solutions, that allow to provide effective functioning of security systems and their integration with other informational applications, perfection of secure corporate network infrastructure is impossible. In the paper this thesis is considered from the point of view of following aspects: a choice of the distributed architecture of the firewall and method to improve its performance; description of a security policy by means of Organization Based Access Control model; automation of process of adjustment of firewall rules based on requirements of specific corporate security policy.

Keywords

Access policy, security policy, distributed firewalls, Or-BAC model

1. INTRODUCTION

Information security infrastructure is necessary component of all modern computer networks and systems. In such systems the exchange of information is carried out in the form of the package traffic therefore key elements of security system are devices which control parameters and properties of transferred packages and forms of virtual transport connections. All solutions which are used for creation of information security systems are used common feature of modern computer technology – packet switching nature and recursive logic structure of virtual transport connection. Packets that form information traffic have two basic parts: header with the address and other protocol information, and packet payload with data which in turn can be other enclosed package. Therefore for reliable protection of the information flow on a network the security control system should have multilayer structure. Recursive feature extends both on headers of packages, and on a package payload, therefore affects a choice of the architecture of security appliances and network processors: firewalls, VPN gateways, IPS/IDS servers, etc. However a security requirement usually causes logical discrepancy with principles of functioning of OSI model. Therefore in practice some conciliatory proposals are used. For an estimation of these solutions various quantitative characteristics and criteria specified in formal and open source documentations. Used estimations considers such factors as: correspondence of firewall filtering rules to requirements of the corporate security policy, performance and reliability of security appliances, scalability of servers, decision and technologies, influence of protection appliances on a speed of information exchange, delays in transmission of packages and cost-complexity parameters of installation in corporate computer network. In this paper we propose new approach to design address invariant security appliances which basic functionality can be automatically configurable in accordance to formal specification of user access policy. Due to address invariant or "stealth" feature this security appliances have scalable architecture and as a result can be configured in such a manner that will correspond both to formal security and performance requirements. Proposed approach is based on integration of two factors raising efficiency of network security systems namely: scalable distributed pipeline-like architecture and specific model of user access to corporate information resources which is co-coordinated with requirements of a corporate informational security policy. Basic model has two subsystems that define: 1. data exchange environment, and 2. role-based access policy to network to information resources. First subsystem describes network as a set of nodes with addressable interfaces employed for data exchange via grid of links that forms topology and metric of the network nearness. In accordance to network practice the number of communication lines determines the distance between nodes. It is clear that the distance between the nodes without addresses is undefined. The source of information or application running on a node forms packet traffic that is delivered on the basis of the address specified in header of a packet. Within the standard network model all stages of information processing occurs in network nodes, and lines are used only for data transmission without

their processing. Thus, the basic functionality of network node is determined by two sequential processing stages of packets after their arrival from a communication line, namely, **store-and-forward**. Proposed model incorporate new functionality to grid of communication lines, namely add specific “stealth” nodes that are logically belong to lines grid because do not use addressable network interfaces but proved full cycle of packet processing. This “stealth” node does interfere with the existing routing policy and therefore does not change network address space supplement expensive routing equipment. Second subsystem describes access policy and used to configure “stealth” appliances in accordance to security and performance requirements. For this purpose a methodology will be suggested that considers a security policy as source while configuring the appliances. The methodology is based on Organization Based Access Control that makes the representation of access rules more similar to the security policy. The final firewall configuration is the result of the integration of network configuration and common access rules. The various benefits of the suggested methodology will be also considered.

2. DISTRIBUTED SECURITY APPLIANCE CONCEPT

As the data transfer rate over communication lines increases and the protocol spectrum broadens, we are witnessing a growth in demands on the performance of the NP employed in packet handling at network nodes. The architecture and specific features of operation of such processing engines has become a subject of a large number of studies [1--3]. Rather than drawing on a systematic analysis of the various specific requirements and design alternatives, however, most of these studies invoked the well-known results of application of multi-processor architectures to increasing the speed of data flow processing. The solutions proposed to improve the functionality of the router now include firewalls, network address translators, means for implementing quality-of-service (QoS) guarantees to different packets flows and other mechanisms. Such implementations are based on several primary operations with packets: parse, search, resolve, and modify (Figure 1). To implement all of these operations in real-time on a general purpose processor (GPP) often becomes unfeasible due to performance requirements. This issue motivates solutions where the packet-processing functionality of the NP is implemented in specific pooled and pipeline hardware. Such a decision has restricted flexibility. *Complex nature of packets operations favor software based implementations on GPP.* To address these conflicting issues and organizing the stages in packet processing, a recently new **store-process-and-forward** scenario has been proposed.

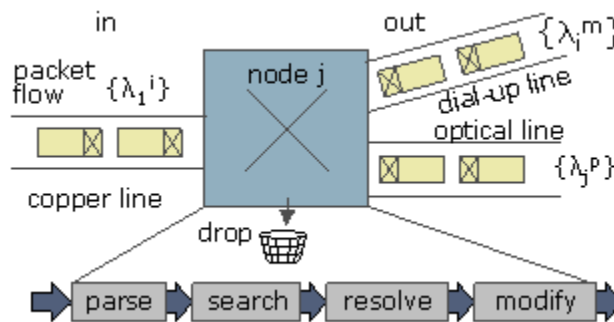


Figure 1. Basic packet processing scenario

In a general case, all solutions may be separated in two classes. Grouped in the first class are the solutions aimed at boosting the router's performance. The main parameters governing the such operation are the packet destination addresses, and, therefore, the solutions chosen are directed at accelerating data search in the router lookup tables. The second class of solutions involves implementation of various procedures without routing decisions: packet classification, data processing, providing the required QoS, bandwidth allocation, and so on. In principle, this separation of the handling processes permits one to break up the network appliance performance between several types of distributed nodes that belong to one virtual transport connection. So, if a packet operation among such nodes occurs without the use of a routing decision, they can be functionally assigned to communication lines. This approach modifies the basic network scenario from store-and-forward to process-store-and-forward concept. This concept offers a solution to providing necessary flexibility by keeping basic routing operation and adding new functionality without changing network topology and computation power (Fig 2)

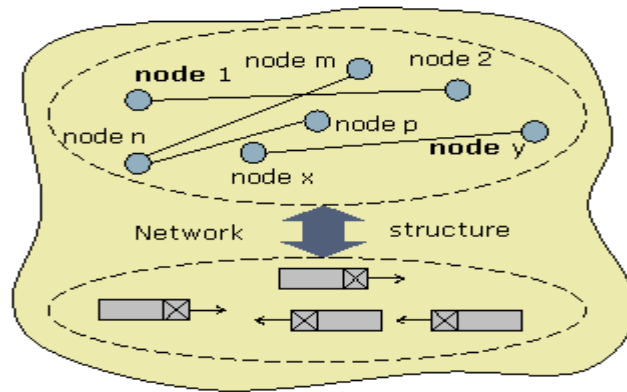


Figure 2. Network topology and structure

In practice, this concept actually uses the open-system interaction (OSI) model to provide several control layers. At each layer data structures are controlled by specific rules. The corresponding control rules can be broken down into the following stages: (1) collection of a data to be transmitted through the network; (2) configuring a structure to quantitatively determine the volume of the data to be transmitted; (3) attaching to the data a special header specifying the set of parameters to be used in handling the packet in network nodes; (4) formation of a frame meeting the requirements of the communication line hardware; and (5) frame transmission over the communication line connecting two network nodes. The above stages are prone to various malicious actions which are capable of interfering with the standard procedure of packet transmission or of substituting packets on the way from their generation. Protective mechanism can be implemented by several means, which divided into methods of packet filtration, and cryptographic processing. The first group of methods protects the network application by means of special firewall rules [3]. In common configurations firewall does not become an end point of packet transmission and has to be installed in the network segments crossed by packet flows. Routing policy does not invariant to the place where firewall has been placed but if network metrics does not changes by firewall due to filtering interfaces have no physical and network address the situation can be changed. The efficiency address less firewall processing is fully determined by the algorithmic features of used filtering engine and available processing power. In the case firewall systems the factors of particular significance are: the number of simultaneously processed virtual connections, QoS requirements, and admissible level of packets delays. Because the transmission of packets is executed in an asynchronous mode, i.e., it is initiated independently by each node, the number of logical connections passing through the node is a random quantity obeying a fractal distribution function [4]. In this case standard firewall architecture does not determine fully its performance, so that the optimum number of packet processing stages depends on the actual character of security requirements. New type of distributed firewall appliance can be based on the separation of packet processing into base and additional operations. Among the base operations is packet routing; other operations which do not demand routing of packages, define a set of additional processing options. Such option can be executed in nodes, whose network interfaces have no IP and MAC addresses. Application of this approach to firewall design implies that one part of packet processes is carried out in a parallel mode at network node and other part - in sequential pipeline mode in "stealth" network processor (NP) node that adjoining to addressable network node (Fig 3).

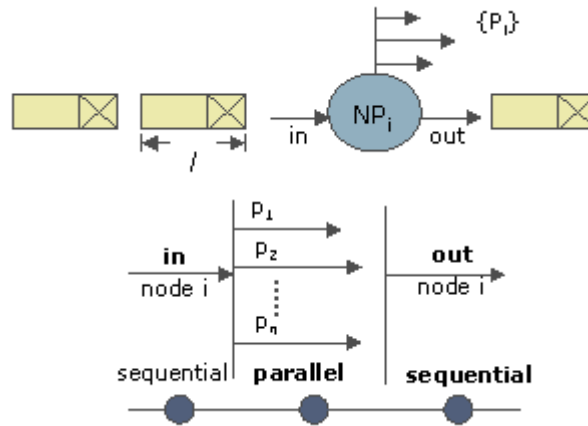


Figure 4. Firewall as a network processor (NP)

Development stealth mode to distributed firewall appliance becomes possible because such devices do not act in most of their operational regimes as sources or destinations of network packets. Therefore, the network interfaces of these devices may have no physical or logical addresses altogether and, hence, transmission of IP packets or MAC frames through them becomes similar in character to their passing through a hub or cable line segments used in packet exchange. To operate successfully, a firewall should work like a “sophisticated” parallel bundle of network cables or a transparent but secure logical channel between the network nodes. The next step of firewall decomposition based on sequential-parallel-sequential stages in packet-handling processes offers a possibility to cut packet delays in the packet reception and processing mode. Operation sequence in the second mode can be integrated into a specialized virtual pipeline cluster and spread out between “stealth” nodes (Figure 4). In this scheme, firewalls can either “bridge” or “route” traffic. In the first case, the firewall functions as a layer-2 network bridge with IP transparent or “stealth” interfaces. This means that each interface has a MAC address but the network or IP address space is the same on both sides of the firewall.

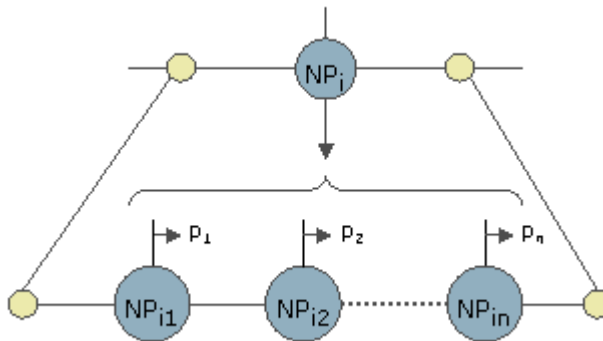


Figure 4. Virtual pipeline cluster

This method of concealing the network address of information protection devices, on one hand, provides conditions necessary for execution of the protection functions, while on the other, because of the packet processing device network interfaces having no addresses, no changes in the network connection topology and in the already accepted packet routing policy are required. Security devices based on “stealth” address technologies have a number of assets not only due to their concealed functioning but also from the standpoint of the scalability of performance and enhanced reliability of operation. The improved performance originates from the use of sequential/parallel character of the network traffic employed, where independent logical connections form through pipeline transmission of packets with definite addresses of message sources and receivers. Operation with network devices based on IEEE 802.3 Ethernet technologies in the stealth mode permits packet processing in the kernel of the built-in operating system without using the TCP/IP protocol stack. This method of processing reduces the packet buffering delay fluctuation level, which likewise improves concealment of the location of protection devices.

3. CONFIGURATION OF FIREWALL

Firewall is one among the large number of various devices that are employed for security policy support in organization. In modern networks a security officer must configure all of these devices in compliance with current security policy. Whereas he often doesn't have enough knowledge about the specificity of an informational security (IS) component (in particular, firewall) or he can't allow himself to waste time while considering all of its functionality details. As a result these details become unnecessary and even burdensome. To make the work of the security officer more effective it's necessary to have a model for each device that would represent a part of its functionality. This part must be complete enough to work with the device as an IS-component while all the unnecessary details must be hidden.

Consider the building of such a model for firewalls. There is a feature that is common for all firewalls: all of them execute an access control policy. Access control policy defines who (user) is allowed to access to a resource (network services). Common access rules are quite obviously represented, for example:

Mr. Black is disallowed to read www.youtube.com.

One can see that the rule above doesn't have a reference to how it could be executed. The description of "Mr. Black" and "www.youtube.com" are also unknown. However, someone (who is familiar with firewalls) may guess that this rule may be executed by some network traffic filter. In this case Mr. Black will correspond to some host in network.

The main function of access control device (ACD) is to decide whether a *subject* should be allowed to perform an *action* with an *object* (Fig. 5).

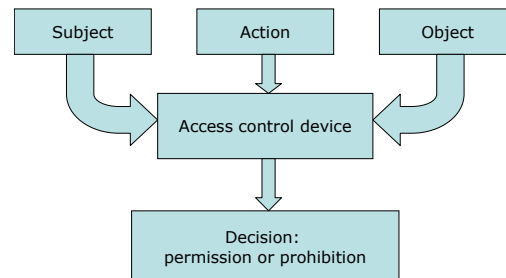


Figure 5. The principle of access control device operation

Corresponding to figure 5, in the above example Mr. Black is a subject, HTTP service on www.youtube.com is an object. The action that is performed by the subject is reading. So the configuration of ACD consists of common access rules which reference to subjects, actions and objects.

Although firewall is an ACD and must be configured with common access rules as source, each one uses its own specific configuration language. The language often reflects the features of firewall's internal architecture and traditionally is represented by the set of firewall rules. Each rule has references to hosts' addresses and other network configuration's parameters. The verbal description of a firewall rule can be like the following:

Host with IP address 10.0.0.10 is disallowed to establish TCP connections on HTTP port of host with IP address 208.65.153.238.

It's clear that just ACD may be a common representation of firewall as an IS-component. The main complexity of this approach is to know how firewall rules could be obtained from common access rules.

Each firewall vendor reasonably aims at increasing its sales appeal while suggesting various tools for convenient editing of firewall rules. However, by now the problem of obtaining firewall rules from common access rules is not resolved. Moreover, this problem has not been paid much attention. Consider it in more detail.

It is obvious that additional information is necessary except access rules in order to obtain firewall rules. This information is about the configuration of network services, the parameters of network protocols that are used for data exchange. Name all these parameters a *network configuration*. The network configuration can be mainly stored among the descriptions of subjects, actions and objects. Example:

Mr.Black:

host with IP-address = 10.0.0.10;

www.youtube.com:

**HTTP service on host
with IP-address = 208.65.153.238.**

Final firewall rules can be obtained via the addition of objects' description to access rules. It should be noted that even for small and especially for medium and large enterprises it's an actual necessity that the network configuration could be stored and managed separately from security policy. The suggested approach allows to achieve this goal: a security officer can edit access rules with references to real objects while a network administrator can edit the parameters of network objects.

It should be noted that there is no purpose to specify any fixed rules how network parameters could be associated with objects. HTTP port may be the parameter of object or it can be the parameter of action. A criterion is that the most natural representation of access policy must be achieved. A concrete decision may vary from one system to another [5].

Role Based Access Control and Or-BAC Model

The access rules which use the notions of subject, action and object are the basis of access control policy but they are not sufficient while working with complex policies. As a result, new approaches have been developed. One of them, *Role Based Access Control (RBAC)*, uses the notion of *role* - an abstract notion which is related to access control policy only. Role doesn't have fixed associations with the real objects of informational system. Role can replace subject in access rules. As an example, remember the roles of system administrator and unprivileged user that are commonly used while configuring various systems. It's obvious that role must be associated with some subjects as the only rules with subjects can be executed. Thus, during the realization of security policy the access rules for all the subjects must be specified. It must be done in two steps. At first, roles must be created and access rules must be specified with references to these roles. Then the roles must be associated with subjects. So role can be used in order to group subjects and for more clear access control policy representation.

Or-BAC model [4] expands the traditional model of Role Based Access Control. It brings in the new notions of activity and view. The notion of activity corresponds to action and its meaning is analogous to the meaning of role for subject. The notion of view corresponds to object. "Entertainment resources" can be an example of view and "read" or "write" can be an example of activity. Thus, the notions of role, activity and view form a new abstract level of access policy. Or-BAC allows of specifying access rules only on the abstract level using roles, activities and views. Therefore they are named abstract rules (Fig. 6).

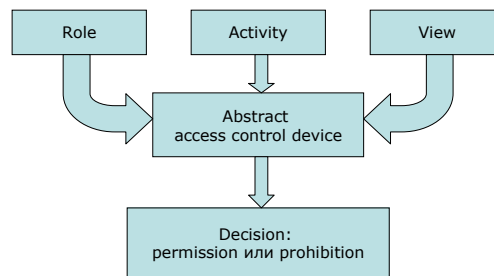


Figure 6. Abstract level of Or-BAC model

Rules with subjects, actions and objects are named concrete rules.

Consider the example of abstract rule:

User is disallowed to read entertainment resources

"User" – role, "read" – activity, "entertainment resources" – view. If Mr. Black is empowered in role "user" and www.youtube.com is considered as view "entertainment resources" then the previously considered common access rule (concrete rule) follows from the given abstract rule.

Configuration Methodology

The use of Or-BAC model for configuring a firewall makes it possible to divide the configuration process into several stages (Fig. 7).

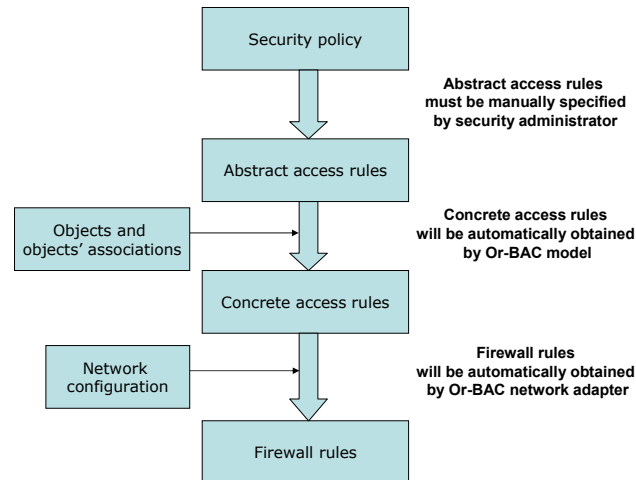


Figure 7. Obtaining firewall rules from security policy

Stage 1. A security officer must analyze all the requirements of security policy and write down all the abstract access rules which follow from the security policy. This stage is not so hard to implement since the formulations of abstract rules are similar to those ones used in official documents. Moreover, abstract access rules can be stored in some prepared template.

Stage 2. The only abstract rules are not sufficient. The model must be filled up by real objects along with their descriptions. These objects must be associated with roles, views and activities. So the security officer must classify and describe all the resources and users in own organization.

Stage 3. The information about network configuration must be available in order to get the final firewall rules. The network configuration may be specified manually by some expert (not the security officer necessarily).

Stage 4. The process of obtaining firewall rules for concrete firewall may be implemented automatically (the module called Or-BAC network adapter). There will be the abstract rules, objects' descriptions and the network configuration on the input of algorithm. The firewall rules will be on the output of algorithm. Some additions to the main algorithm may be required while working with various firewall models but if the models are similar then these additions will be small.

The Benefits of the Suggested Methodology

Decrease the Probability of Human Error

A feature of the suggested methodology is that the process of firewall configuration is divided into several stages. The most informal first stage is made quite simple for security officer due to suggestion of instinctively understandable notions to specify abstract access rules. Thus, the abstract rules can be easily specified, analyzed, edited and compared with an informally specified security policy. It will reduce the probability of the case that a firewall will not work in compliance with the security policy because of the security officer error.

Ready Access Policy

Most of abstract rules can be initially stored in prepared templates. For example, the abstract rule that a user can't read entertainment resources is quite common. It will be certainly employed by any security officer. So if he has a prepared template with such common rules then he must only describe the real objects and the network configuration of own organization in order to obtain firewall rules.

Reliable Configuring the System of ACDs

The suggested methodology uses the notion of abstract ACD which corresponds to a real ACD: some firewall or even not firewall but some other ACD (for example, the file access controller of operating system). The abstract ACD represents the only functionality of the real ACD that is related to informational security. Thus, very different real ACDs can be represented by similar abstract ACDs. This permits of more ease consideration of an informational system which employs many different ACDs. In such a system IS-components may interact with each other while pursuing the common goal: to execute security policy. As each ACD has its own configuration then it's possible that the configurations of different ACDs will not

correspond to each other: the case of conflict. If such conflicts occur and remain unnoticed then the behavior of the system may be unexpected with no accordance to the security policy. Unnoticed conflicts can be avoided if the configurations of all the ACDs have a single source. So the distributed system of ACDs must be considered. It will be difficult as ACDs may be very different. The use of abstract ACDs can provide the smart decision of this problem.

Dynamic Firewall Configuration

The network parameters of objects may change, for example, a user may log on any computer so its IP address changes during system work. However, the access rules for this user must be invariant. Thus, the configuration of firewall must be changed dynamically. The process of such a dynamic configuration requires the consideration of common access rules which are the source of firewall rules. As the suggested methodology initially considers common access rules so the evolution from static firewall configuration to dynamic one can be more easily developed.

Security Assessment

The suggested methodology also provides the means to IT security assessment. As the method is based on total resources, users and activities classification then this classification may not only be used for specifying access rules. Roles, views and activities can be supplied by special attributes which provide a numeric information about how much is a resource critical for informational system or about the reliability of an activity. Being based on these values it would be possible to estimate the total coefficient of security.

4. CONCLUSION

Application of network processors with a distributed architecture broadens substantially the range of use of information protection systems in telematic networks. The concealed character of operation of the protection devices offers a possibility of integrating additional packet processing procedures into the standard switching process while not changing in any way the routing policy. Application of the stealth technology cuts the costs of network upgrading, because its implementation permits redistribution of the required processing power among various network devices. The NP clusterization technology provides a possibility of scaling up the performance of network nodes and increases the overall system reliability. Each firewall is required to work in compliance with a corporate security policy. It cannot be considered separately from other security appliances. Thus, the methodology of proper firewall configuration was suggested that uses an informally specified security policy as source. The methodology also employs Or-BAC model that helps to translate high-level abstract access rules to low-level concrete access rules. A network configuration and common access rules must be available in order to obtain the final firewall configuration. The process can mainly be automated so a security officer must only specify high-level access rules. While using the suggested methodology the system of different access control devices (in particular, firewalls with stealth technology) can be more easily analyzed due to consideration of their abstract informational models instead of real devices.

5. REFERENCES

1. Intel Corp. Intel Second Generation Network Processor, <http://www.intel.com/design/network/products/npfamily/ixp2400.htm>
2. V.S. Zaborovsky «Multiscale Network Processes: Fractal and p-Adic analysis», Proceedings of 10-th International Conference on telecommunications ICT'2003, University of Haute Alsace, Colmar, France, 2003.
3. V.S. Zaborovsky, Y. A. Shemanin, Jim A. McCombs, A. Sigalov «Firewall Network Processors: Concept, Model and Platform», Proceedings of International Conference on Networking (ICN'04), Guadeloupe, 2004.
4. A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel et G. Trouessin, Organization Based Access Control. IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Como, Italy, June 4-6, 2003.
5. F. Cuppens, N. Cuppens-Boulahia, T. Sans and A. Miège, A formal approach to specify and deploy a network security policy. Second Workshop on Formal Aspects in Security and Trust (FAST). Toulouse, France. August, 2004.