Exploring the Concept of Scope to Provide Better Security for Internet Services

Mahdi Aiash, Glenford Mapp, Aboubaker Lasebae
School of Engineering and Information Science
Middlesex University
London, UK
Email:M.Aiash, G.Mapp, A.Lasebae@mdx.ac.uk

Raphael Phan
Electronic and Electrical Engineering
Loughborough University
Loughborough, UK
Email: R.Phan@lboro.ac.uk

***Abstract*—The Internet was originally designed to support universal reachability by allowing any host to communicate with any end server over the globe. Unfortunately, this feature has been abused by attackers to overload the servers with malicious traffic. In order to deal with this situation, many mechanisms such as Firewalls and Access Lists have been introduced to restrict servers' accessibility only to legitimate users. This paper discusses some of these mechanisms, highlights their pros and cons and then proposes a new mechanism that attempts to limit a server's reachability based on its operational scope.**

I. Introduction

Whenever a device accesses the Internet, it needs to register with some Internet servers such as the Domain Name System (DNS)[5] [6] and the Dynamic Host Configuration Protocol (DHCP)[7] [8] to uniquely identify itself and obtain network resources. This allows information to be sent and routed among hosts over the globe. The current Internet is characterised by its open and dynamic nature, these properties enable the Internet to provide universal reachability; any host could send (and receive) any volume/type of traffic to (and from) any other host. This traffic might contain unwanted, hidden software that installs itself on the destination device and acts maliciously.

This open nature of the Internet, makes it vulnerable to serious security threats which come in form of compromise and resource exhaustion attacks. While the first subverts the victim end host itself (client or server), the latter leaves the server intact but however overloads it with a huge volume of traffic and thus preventing it from serving legitimate clients. These two attacks target the availability of services and thus, are categorized as forms of Denial of Service (DoS) attacks.

An obvious solution to deal with these attacks is by controlling access to the victim through the implementation of primitive mechanisms such as Access Control Lists (ACls) [9] [10], Firewalls [11] and Network Address Translation (NAT) [1] [3]. However, as will be discussed later, these mechanisms are adds-on to the communication procedure rather than an integrated security solution, this increases the complexity of setting up the connection and breaks the desired end-to-end connectivity feature of the Internet. Therefore, the authors in [2] proposed a comprehensive way for restricting servers' accessibility known as "Off By Default". Unlike the current "On By Default", the servers in the " Off By Default" world could specify the source and the type of the traffic, they are willing to receive and thus, restricting the server accessibility. In spite of the significance of this approach, there are many implementation concerns in terms of the scalability and adaptability of this concept in the current Internet structure.

In order to address the shortages of "Off By Default" and to provide a systematic way to define and enforce servers' reachability, the authors in this paper introduce the scope concept which limits servers' visibility based on their functionality, and thus, four scopes have been proposed: Local, Local Area Network (LAN); Domain and Global scopes. Additionally, to show how these scopes could be enforced, the authors proposed novel models that describe the transactions between different components of the Internet. The paper is organised as follows: Section 2 analyses current, security mechanisms namely, the ACL, Firewall; NAT and "Off By Default" which control the server's accessibility. An enhanced model of the " Off by Default" by integrating the scopes concept is presented in Section 3. In Section 4, our proposed model is presented along with the recently introduced new addressing scheme. A potential application of the proposed model with 4G systems is described in Section 5. Further work and the conclusion are presented in Section 6.

II. Related Work

The proposed security applications to address the afore-explained situation are mainly based on access control mechanisms, these are as follows:

A. Access Control Lists and Firewalls

One of the earliest attempts to enforce access control was by configuring ACLs on the network's routers, ACLs provide basic packet filtering to protect the networks from the outside world [9]; they filter the traffic and based on pre-configured criteria such as the Source/destination IP address or ports numbers, they will forward or block packets on the interface routers. As stated in [9], configuring ACLs on the edge routers could mitigate many threats such as IP spoofing and DoS TCP SYN flooding. However, configuring ACLs is an error-prone procedure and for each traffic type a new rule has to be

added. Additionally, ACLs perform stateless packet inspection without considering the state of the whole session.

Firewalls address the shortages of basic ACLs, provide layered defence mechanisms; perform stateful packet inspection and have application awareness for a few transport protocols. This offers a higher level of protection than basic packet filtering. The firewalls also consider the state of the connection and thus, differentiate between packets belonging to different sessions. However, the problem with the Firewall is that, it breaks a single sessions into two connections and thus, it can have detrimental effects on end-to-end performance.

B. Network Address Translation

The idea of hiding the identity of the servers from external entities was initially proposed by the Network Address Translation (NAT) [1] where the NAT server acts as an IP converter that maps private IP addresses (the ones used in the internal network) to globally, registered addresses, in an attempt to allow hosts in private networks to transparently communicate with external hosts and visa versa.

However, the implementation of the NAT does not come without potential drawbacks. For instance, the connection between the hosts residing behind the NAT is broken on the first NAT-supporting router, this contradicts with the end-to-end concept which used to be the core principle of the current Internet [3]. Additionally, there are serious concerns about the operability of the NAT and Firewalls as well as the scalability of the NAT database.

C. Off By Default

To reduce the complexity and the overhead resulting from implementing the previous mechanisms, the authors in [2] proposed an integrated, access control-based approach through which, the host explicitly specifies the traffic it wants routed to it; thus defining its reachability. In this approach, the routers will not automatically route the packets unless explicitly directed to do so by the destination host.

This proposal however suffers from a number of drawbacks: Firstly, this approach requires the network to maintain accessibility information for each destination, this might place a burden on the network infrastructure. Secondly, the end host should be able to regulate its reachability for a wide spectrum of applications and protocols, update it in case of any modification, and then convey this information to the access router in a systematic way. Table I summarizes the pros and cons of the access control mechanisms.

TABLE I
A BRIEF DESCRIPTION OF THE RELATED APPROACHES

The Mechanism	Advantages	Disadvantages
ACLs	Mitigates IP spoofing and DoS TCP SYN flooding	Provides only stateless packet inspection
Firewalls	Support layered defence mechanism and stateful packet filtering	Break the end-to-end connection's property, adds-on security mechanism that is vulnerable to configuration error
NAT	Less administrative effort, was the first to hide the identity of the server rather than preventing packets from getting to it	Contradicts with the end-to-end concept, interoperability problems with the Firewalls and newer version of IP addresses
Off By Default	More integrated than the previous mechanisms	Place a burden on the network infrastructure, Not fully integrated

III. THE ENHANCED OFF BY DEFAULT

Although, the approach of "Off By Default" has addressed many drawbacks of the primitive access control mechanisms, it comes with problems of its own which might set challenges in front of any implementation attempt. Therefore, in this section, we introduce our approach to address the afore-mentioned security challenges. Our proposal is based on the "Off By Default" approach, however; it avoids most of its shortages.

In summary, our proposed approach tries to address the following drawbacks of the "Off By Default":

1) Currently, with the "Off By Default", the server could choose the hosts it wants to accept traffic from, this approach is not scalable nor applicable. To deal with this situation, it might be better for the server to set more general rules to determine its accessibility rather than specifying access rules per host.
2) Although, the "Off By Default" provided a certain degree of integration, the server still needs to explicitly specify its reachability to the gateway router which will propagate this to all routers via routing table update procedure. We agree that the gateway router must be aware of the server's accessibility, however, the process of conveying this information outside the network should be accomplished with a minimum involvement of the server. Additionally, we believe that only concerned entities should know the server's accessibility.

A. The Scope Concept

To address the problems of "Off By Default", we propose a novel, more efficient approach to convey the access control information to the relevant entities. In this approach the visibility of servers is defined by the scope of there functionality, thus, four main scopes have been introduced:

- The Local Scope: Local services could only be accessed from within the same machine; The existence and state of the services are not made known to any devices or applications outside the machine.
- The LAN Scope: the services are available for the clients at the Local Area Network (LAN).
- The DOMAIN Scope: the Server is accessible for all client within the Administrative domain. For instance only users of the www.XYZ.com could access the sever.

- The Global Scope: The service is available and accessible globally for all the clients over the Internet.

In contrast to the "Off by Default" approach where the host itself informs the gateway router about its desired reachability and the router then propagates this information via the routing update procedures, we believe it would be more efficient to launch the accessibility information on a global service such as the DNS thus, the sever needs to include its scope information in the initial DNS registration.

B. A Proposed Model

The proposed model discusses the case of a corresponding node (CN) trying to contact a remote server. As shown in Fig 1, the model comprises the following entities:

- The Corresponding Node is the host trying to contact the Sever.
- The Source Access Router (SrcAR) is the gateway router of the CN's network, it relays packets to and from the Internet.
- The Source DNS (SrcDNS) is the authoritative naming server of the source network.
- The Destination DNS (DesDNS) is the authoritative DNS of the Server's network.
- The Destination Access Router (DesAR) is the gateway router in the destination network.
- The Server is the node receiving the connection requests

The access router in the destination network is responsible for controlling Server's accessibility based on its scope. We presume that the Server has previously registered itself with its authoritative naming service (DesDNS).

As shown in Fig 1, the transactions, needed for initiating a connection between the CN and the Server are as follows:

1) Msg 1: The CN, using the Server's name, asks its authoritative DNS (SrcDNS) for the Server's address. Since this is the first transaction between the CN and the Server, the SrcDNS does not hold any records for the Server and thus, it probes the Server's authoritative DNS (DesDNS).
2) Msg 2: Once the SrcDNS gets the Server's information- including the scope- from the DesDNS, it returns the Sever's IP address.
3) Msg 3: Now since the CN knows the Server's address, it sends a connection request packet with the Server's address in the destination address field.
4) Msg 4: When the request gets to the SrcAR, it checks with the SrcDNS for the server's scope. If the the scope indicates that it is accessible by the CN, the SrcAR passes the connection request to the DesAR, otherwise, the packet is dropped.
5) Msg 5: The DesAR checks the packet's destination address once again and verifies that it's allowed to go through to the server.

Since the server needs to reveal its scope to the authoritative DNS only at the initial registration, the server's intervention is kept to a minimum. Additionally, unlike "Off By Default", the scope information is provided only to the requesting hosts via explicit DNS request. In "Off By Default", scope information is propagated -via router update- to the neighbour routers, many of which might not be ever involved in setting up a connection to the server, also when the server is globally accessible, the scope information should be available at a global level and this support the argument of using a global service such as the DNS to propagate the scope information. Moreover, in case of modifying the server's scope, there might be a time delay before all the relevant routers are updated via the routing table updates.

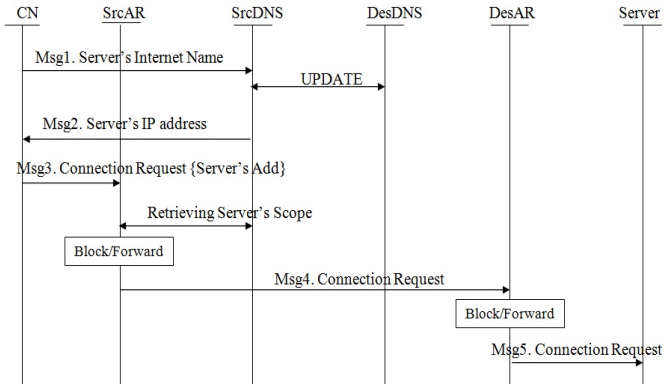

Fig. 1. The Connection Model

However, one major drawback of the proposed model is in transferring the scope information to the access router; for each connection request, the access router (SrcAR) has to explicitly approach the DNS to get the scope information. This is an extra work for the router and it breaks the flow of the communication procedure. Therefore, a more integrated approach to reduce the complexity of this model and eliminate the extra work will be investigated in the following section.

IV. An Integrated Security Model

As was highlighted in the previous section, there is a need to launch the scopes in the access routers via an integrated approach. One potential solution might be by dynamically launching the scope information in the router without explicitly referring to the DNS. This could be achieved if we include the server's scope within its address format. In this case, the router will recognize the server's scope by checking its address without consulting the DNS sever. The authors in [4] have proposed a novel addressing scheme which includes a Scope Field (SF) that determines the host accessibility.

A. The New Addressing Scheme

As shown in Fig 2, the new address comprises 128 bits divided into three portions: a 56-bit Location ID which corresponds to the network address of the IP, it defines the address of the access network to which the MN is attached. The Node ID is a 64 bits long and it uniquely defines the device regardless of the number of the Network Interface Cards (NICs) it might have. an 8 bits long field called NetAdmin

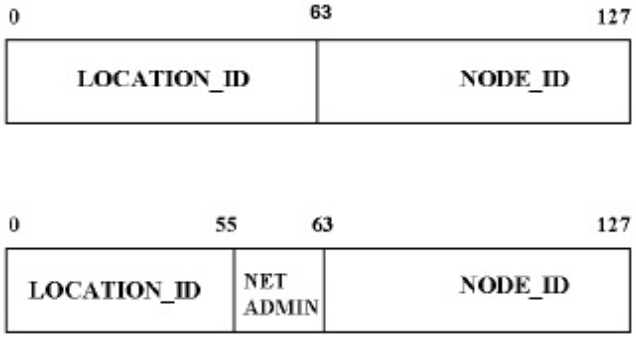

Fig. 2. The New Addressing Scheme

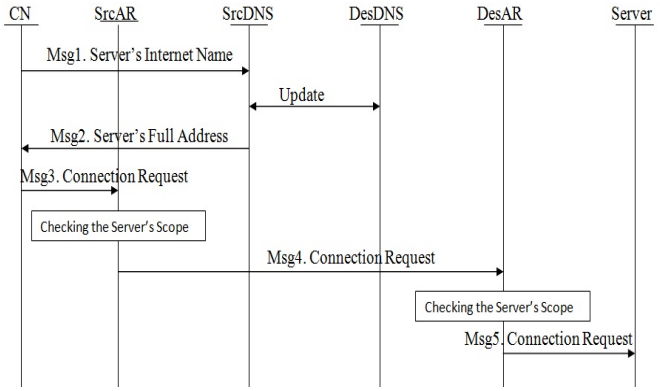

Fig. 3. The Integrated Connection Model

and it is responsible for the following network administering tasks:

- *The Scope Field (SF):* is a 2-bit field, responsible for defining nodes' accessibility. So The value 00 represents a local service which could be accessed only from within the same machine, so remote devices will not even know about these services. The value 01, indicates LAN scope in which the node is only accessible by other devices on the same LAN. The value 10 signals that only machines on the same site are allowed to access the server. The value of 11 denotes that the device can be globally accessed.
- *The Static (S) field:* this 1-bit long field indicates that the node is static or mobile.
- *The Multicast (M) field:* when set, this bit indicates that the address represents a multicast group rather than a unicast address.
- *The Interface Number Field (INF):* is a 4-bit field used to address up to 16 virtual or physical network interfaces. Where the address 0 defines any-cast address, 0xF is a broadcast address and 0x1 is the primary interface.

B. The Proposed Integrated Model

As shown in Fig 3, the system comprises the same entities explained in Section III-B, the only difference is that the IP address will be replaced by the new addressing scheme. Also, similar to the previous model, we presume that the server has already registered itself with the authoritative DNS server thus, the DNS knows the server's address which includes the Scope Field (SF). Also, similar to the " Off By default", we presume that the DesAR is aware of the Server's address, however, this is not propagated to other routers.

When the corresponding node (CN) wants to communicate with the server, the connection procedure goes as follows: The CN knows the server's Internet Name (DNS name) so it approaches the DNS to get the server's address. Once the CN receives the full address (Node and Location IDs), it composes a connection request which has the server's address in the destination address field. When this request gets to the router (SrcAR), it checks the SF of the destination address. If the SF indicates that the server is accessible to the CN, the SrcAR passes the connection request, otherwise, it's dropped by the router. When the request gets to the DesAR, it compares the request's destination address with the Server's address and checks the SF. This procedure mitigates address spoofing attacks; for instance if the CN has changed the scope defined in the SF, the SrcAR will not be able to discover this. However, it will be discovered when the DesAR compares the destination with the server address thus, the request will be dropped on the DesAR.

V. Integration with 4G Systems

Since 4G is an IP-Based environment, it will suffer from most of the IP-specific security vulnerabilities found in the Internet. Therefore, it is possible for the proposed security mechanism to be used to protect the server in 4G systems such as the Y-Comm framework [12] [13].

A. The Y-Comm Framework

Y-Comm is a 4G, communication architecture to support vertical handover for multi-homed nodes in heterogeneous environment. The architecture has two frameworks:

- The Peripheral framework deals with operation on the mobile terminal.
- The Core framework deals with functions in the core network to support different peripheral networks.

As shown in Fig 4, the two frameworks share a common base subsystem consisting of the hardware platform and network abstraction layers. Both frameworks diverge in terms of functionality but the corresponding layers interact to provide support for heterogeneous environments.

To support multi-homed nodes, the Network Abstraction Layer (NAL) contains the drivers of different networks and thus provides a common interface that supports different networking technologies. Additionally, issues such as network operability and overlapping are addressed by this layer.

B. Security in Y-Comm

The Y-Comm's security approach approach is based on the concepts of an Integrated Security Module (ISM) to protect data and Targeted Security Models (TSMs) which are needed

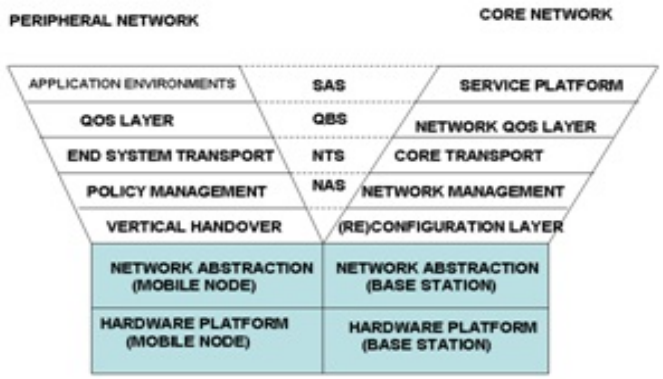

Fig. 4. The Complete Structure of Y-Comm

to protect entities, such as users and servers that are using the open infrastructure [14] [15]. As shown in Fig 4, the four-layer security model comprises the following layers:

- Service and Application Security (SAS): provide security at the application level.
- QoS-Based Security (QBS): concerned with QoS issues and the changes of QoS as the Mobile device moves around.
- Network Transport Security (NTS): is used to set up secure connections through the core network.
- Network Architecture Security (NAS): addresses security issues in the peripheral access network.

Y-Comm proposes three targeted security models (TSMs), these are as follow:

- The connection security model: protecting the connection between users and thus it is mainly related to security of the connection initiation process.
- The handover security model: facilitates secure vertical handover and attempts to prevent network resources from being abused and overloaded.
- The Ring-Based security model: is concerned with restricting access to servers by using the concept of scope; so servers are only accessible by the users in the same scope. There are four scopes: Local, LAN, domain and global.

We believe that, the proposed model in this paper along with the new addressing scheme could facilitate the Ring-Based security model.

VI. Conclusions

This paper investigated current mechanisms to secure servers over the Internet. The result showed that, many of the current mechanisms suffer from major drawbacks mainly related to the scalability and lack of integration. Therefore, we propose a new model based on the previously introduced " Off By Default" concept. The proposed model introduces the scope concept where server's visibility is determined by its range of functionality. The work on a testbed, composed of Linux routers has started at Middlesex University, this will be used to implement the proposed model along with the new addressing scheme.

References

[1] P. Srisuresh and M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*. RFC 2663, August 1999.

[2] H. Ballani, Y. Cathwathe, S. Ratnasamy, T. Roscoe and S. Shenker, *Off by Default*.Proc.the 4th Workshop on Hot Topics in Networking (HotNets-II). 2005

[3] R. Bush and D. Meyer, *Some Internet Architectural Guidelines and Philosophy*. RFC 3439, December 2002.

[4] G. Mapp, M. Aiash, H. C.Guardia and J. Crowcroft, *Exploring Multi-homing Issues in Heterogeneous Environments*,Proc. 1st International Workshop on Protocols and Applications with Multi-Homing Support (PAMS'11). Singapore.2011.

[5] P. Mockapetris, *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*. RFC 1035, November 1987.

[6] P. Mockapetris, *DOMAIN NAMES - CONCEPTS AND FACILITIES*. RFC 1034 , November 1987.

[7] R. Droms, *Dynamic Host Configuration Protocol*. RFC 1541, March 1997.

[8] B. Aboba, S. Cheshire, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*. RFC 3397, November 2002.

[9] C. Paquet, *Authorized Self-Study Guide Implementing Cisco IOS Network Security (IINS)*Indianapolis, USA: Cisco Press, 2009.

[10] A. Melnikov, *IMAP4 Access Control List (ACL) Extension*. RFC 4314, December 2005.

[11] N. Freed, *Behavior of and Requirements for Internet Firewalls*. RFC 2979, October 2000.

[12] J. Crowcroft, D. Cottingham, G. Mapp and F. Shaikh, *Y-Comm: A Global Architecture for Heterogeneous Networking*,Proc. 3rd Annual International Wireless Internet Conference (WICON 2007).October 2007.

[13] G. Mapp, F. Shaikh, M. Aiash, R. P.Vanni, M. Augusto and E. Moreira, *Exploring Efficient Imperative Handover Mechanisms for Heterogeneous Wireless Networks*,Proc. International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS-09) August 2009.

[14] M. Aiash, G. Mapp, A. Lasebae, R. Phan,*Providing Security in 4G Systems: Unveiling the Challenges*,Proc. The Sixth Advanced International Conference on Telecommunications (AICT'10),Barcelona, Spain 2010.

[15] G. Mapp, M. Aiash, A. Lasebae, R. Phan,*Security Models for Heterogeneous Networking*,Proc. the International Conference on Security and Cryptography (SECRYPT'10), Athens Greece, July 2010.