[14] Gary Kunis. A note on boeing internet security, October 1988.

[15] Paul Mockapetris. Domain names—concepts and facilities. *RFC 1034*, November 1987. Available via anonymous ftp from nic.ddn.mil.

[16] Paul Mockapetris. Domain names—implementation and specification. *RFC 1035*, November 1987. Available via anonymous ftp from nic.ddn.mil.

[17] John Moy. The ospf specification version 2. *RFC 1247*, August 1990. Available via anonymous ftp from nic.ddn.mil.

[18] Executive guide to the protection of information resources. NIST Special Publication 500-169.

[19] Management guide to the protection of information resources. NIST Special Publication 500-170.

[20] Computer user's guide to the protection of information resources. NIST Special Publication 500-171.

[21] OARnet technical committee. OARnet security policy, 1992. Available via anonymous ftp from ftp.oar.net.

[22] Richard D Pethia and Kenneth R van Wyk. *Computer Emergency Response—An International Problem.* CERT/CC, Software Engineering Institute, Carnegie Mellon University, 4500, Fifth Avenue, Pittsburgh, PA 15213-3890.

[23] Proteon, Inc., 2, Technology Drive, Westborough, MA 01581. *Proteon Models p4100/p4200 Software Options Manual.*

[24] Deborah Russell and G T Gangemi Sr. *Computer Security Basics.* O'Reilly & Associates, not known.

[25] John P Wack and Lisa J Carnahan. Computer viruses and related threats. Technical Report Special Publication 500-166, NIST, not known.

7 Author's Address

Kannan Varadhan
Network Engineer, OARnet,
1224, Kinnear Road,
Columbus, OH 43212.

Phone: +1 614 292 4137
Email: kannan@oar.net

References

[1] Steven M Bellovin. Security problems in the tcp/ip protocol suite. *ACM Computer COmmunications Review*, April 1989.

[2] Bob Braden. Requirements for internet hosts—application and support. *RFC 1123*, October 1989. Available via anonymous ftp from nic.ddn.mil.

[3] Bob Braden. Requirements for internet hosts—communication layers. *RFC 1122*, October 1989. Available via anonymous ftp from nic.ddn.mil.

[4] Russell L Brand. Coping with the threat of computer security incidents—a primer from prevention through recovery. *Internet document*, June 1990. Available via anonymous ftp from cert.sei.cmu.edu.

[5] Bill Cheswick. The design of a secure internet gateway. In *Proceedings of the Usenix Summer '90 Conference*, pages 233–237, Anahiem, California, 1990.

[6] cisco Systems, 1525, O'Brien Drive, Menlo Park, CA 94025. *Cisco Gateway System Manual, Software Release 8.2.*

[7] David A Curry. Improving the security of your unix system. Technical Report ITSTD-721-FR-90-21, Information and Telecommunication Sciences and Technology Division, SRI International, 333, Ravenswood Avenue, Menlo Park, CA 94025, April 1990.

[8] Department of defence trusted computer system evaluation criteria. Also known as the *Orange Book.*, August 1983. Available via anonymous ftp from ftp.oar.net.

[9] Sun-Nets email discussion. Summary of a discussion on firewalls, June 1991. Available via anonymous ftp from ftp.oar.net.

[10] Dan Farmer and Gene Spafford. The cops security checker system. In *Proceedings of the Usenix Summer '90 Conference*, pages 165–170, Anahiem, California, 1990.

[11] Simson Garfinkel and Gene Spafford. *Practical UNIX Security.* O'Reilly & Associates, not known.

[12] Charles Hedrick. Routing information protocol. *RFC 1058*, July 1991. Available via anonymous ftp from nic.ddn.mil.

[13] Paul Holboork and Joyce Reynolds. Site security handbook. *RFC 1244*, July 1991. Available via anonymous ftp from nic.ddn.mil.

4.3 Mailing lists

There are a variety of lists where security related announcements are made.

- CERT puts out advisories from time to time on the list, `cert@cert.sei.cmu.edu.` To join, please send a note to `cert-request@cert.sei.cmu.edu.`
- There is a UNIX security mailing list, `security@cpd.com.` To join, send a note asking for information from `security-request@cpd.com.`
- The `VIRUS-L` list is a group for the discussion of viruses. To join, send a note to `listserv@lehiibm1.bitnet,`with a line of the form *SUB VIRUS-L your full name.*
- The discussion group `alt.security` on USENET is an open forum for discussing security related issues. Likewise, there is a moderated forum, `comp.security.announce.`
- Other miscellaneous lists are the tcp/ip list, `tcp-ip@nic.ddn.mil, sun-spots@rice.edu, sun-nets@uunet.uu.net, sun-managers@eecs.nwu.edu,` and `sysadm@sysadmin.com.` To join any of these lists, please send a note to the corresponding request address. The first two lists are also available on USENET as `comp.protocols.tcp-ip` and `comp.sys.sun` newsgroups.

5 Summary

This document discusses a variety of possible measures to enhance network security for an organization intending to connect to a regional network. These are just general principles for building firewalls and security. Absolute solutions are possible only when exact configurations are available, and are outside the scope of this document.

OARnet engineers have been working with Proteon and cisco routers, and are very familiar with the design of firewalls for a variety of purposes. OARnet engineers will also assist customers who desire special help in setting up various network related services. The OARnet technical committee has setup a subcommittee to deal with security issues on OARnet[21]. Please contact oartech-chair@oar.net for details.

6 Acknowledgements

I would like to thank the networking group, Joel Replogle, Henry Clark, John Wieronski and Dan Wintringham for their ideas, comments and helping me in writing this document.

I would also like to thank Steve Romig (OSU) and Dan Farmer (Sun Microsystems) for their comments on earlier versions of this document.

kinds of things it detects are weak passwords, misconfigured directories, such as world writable ftp repositories, strange and new setuid programs, world writable system directories etc.[10].

The latest version of COPS is available via anonymous ftp from cert.sei.cmu.edu:/pub/cops.

4.2 Literature Survey

4.2.1 "Improving the Security of your UNIX System", by David A Curry

[7] comprehensively lists a variety of potential things to check for in setting up your system. This paper is a "must-read" for any security conscious sysadmin (and otherwise). It has a variety of check lists that COPS does not check for, or cannot, and also has pointers to other literature.

4.2.2 "Coping with the Threat of Computer Security Incidents" by Russell L Brand

[4] has some hints similar to the previous paper. It has a list of common accounts on VMS and CMS systems that are obvious holes, and have been used in the past by one or miscreants in time. It also has hints on dealing with incidents as they occur, including tips opn whom to contact in the event of trouble, and tips on handling the press etc.

4.2.3 "Site Security Handbook" RFC 1244 by J. Paul Holbrook

This document, [13], was worked on the security working group of the Internet Engineering Task Force (or IETF for short). It lists possible short comings on various systems, and suggests policies that an organization should adopt.

4.2.4 "Security Problems in the TCP/IP Protocol Suite" by S.M.Bellovin

This paper, [1], discusses problems in the TCP/IP protocol suite, and the potential for spoofing hosts etc. Most of the problems discussed herein are highly esoteric, and are far beyond the capabilities of the average cracker.

4.2.5 Miscellaneous publications

- The National Institute of Standards and Technology has a few publications[25, 18, 19, 20] that discuss general management issues with regard to computer security.
- The Host Requirements RFCs, [3, 2] defines the standards for host configurations for all hosts on the Internet, while the orange book[8] is the classification of all hosts on the basis of their security.
- O'Reilly and Associates has recently published two new books on security. These are "Computer Security Basics" by Deborah Russell and G.T.Gangemi Sr.[24] and "Practical UNIX Security" by Simson Garfinkel and Gene Spafford[11].

```
                        604800  ;expiration period
                        86400   ;minimum TTL
                        )
frobozz.com.        in      ns      Ins.frobozz.com.
                    in      ns      Ins1.frobozz.com.
                    in      ns      Ins2.frobozz.com.
$ORIGIN frobozz.com.
Ins                  in      a       10.0.0.53
Ins1                 in      a       10.0.53.0
Ins2                 in      a       10.53.0.0
$ORIGIN .
*      in      mx      mail-relay.frobozz.com.
```

The internal zones files for frobozz.com. then look as specified in the RFCs, or your local vendor.

The DNS is a dynamic, distributed database with very free flow of information between the various servers. Care should be taken that all details concerning the internal DNS is never leaked to the outside world. Potential disasters follow when such leakage occurs.

Notice that the mail-relay machine should therefore know to look at the internal DNS resolving all hostnames internal to frobozz.com, and the external root servers for all other data. This can be done with a proper cache file. None of the externally accessible machines should contain copies of the internal zone.

4 Host security

An important component of reinforcing network security is enhancing internal host security. There are a variety of tools, guidelines, recommendations etc. that are freely available and help the lay system administrator with security related administration.

OARnet encourages the use of such tools. OARnet also encourages individual administrators to keep abreast of the various security advisories put out by organizations such as the Computer Emergency Response Team (CERT) [22] and the sundry measures that vendors distribute from time to time.

> *OARnet strongly discourages the principle of organizations permitting anonymous unauthenticated access to the Internet via terminal servers, guest logins etc.*

The following subsections discuss various tools and references that are available.

4.1 COPS

The COPS (Computerised Oracle and Password System) Security Checker System was written by Dan Farmer. It is currently at version 1.02, and 1.03 is now in beta test. This package does a complete audit of the system it is run on, and flags possible violations. Some examples of the

It may be advantageous for an organization to run parallel DNSs. The external DNS has enough information to satisfy the primary requirements of the DNS, and a more complete internal DNS for the use and convenience of network users within the organization.

3.1 Configuring the external DNS

The DNS made available to the external world must have pointers to at least one machine, which is to exchange mail between the organization and outside entities. The primary and secondary DNS servers and the mail relay machine should exist on a network reachable from the outside world. A miminal external DNS zone file for a sample organization, Frobozz Widgets, Inc. looks as:

```
frobozz.com.    in      soa     ns.frobozz.com. hostmaster.frobozz.com. (
                          9209115           ; serial
                          86400             ; refresh
                          21600             ; retry
                          3600000           ; expire
                          86400 )           ; minimum
                          in      ns      ns.frobozz.com.
                          in      ns      ns.oar.net.
                          in      a       192.9.200.1
net-frobozz               in      a       192.9.200.0
                          in      hinfo   Frobozz net-address
ns.frobozz.com.           in      a       192.9.200.53
                          in      hinfo   "sun4/110" "unix"
mail-relay.frobozz.com.   in      a       192.9.200.25
                          in      hinfo   "mail-gate" "header mangler"
ftp.frobozz.com.          in      a       192.9.200.21
                          in      hinfo   "PC clone" "Gigabit File Server"
broadcast-frobozz         in      a       192.9.200.255
                          in      hinfo   Frobozz broadcast
localhost.                in      a       127.0.0.1
localhost                 in      cname   localhost.
```

3.2 Configuring the internal DNS

Assuming that the inside network is totally isolated from the external world, the internal DNS should be configured with root servers, and primary and secondary name servers. The root zone will have delegations for frobozz.com. pointing to the primary and secondary servers, and have MXs for everything else, pointing to mail-relay.frobozz.com.

The root zone thus looks as shown below.

```
.        in      soa     ns1.frobozz.com. hostmaster.frobozz.com. (
                        920910  ;serial (version)
                        10800   ;refresh period
                        900     ;retry refresh this often
```

2.4 Hazards of Source Routing

IP source routing is a technique for indirect delivery of a packet to a remote destination.

With an ingenous mix of packet spoofing[1], and IP source routing, one can subvert the set of access filters on a gateway. Routers have options to disable forwarding packets with source routing options enabled in them. We encourage people following these procedures to use this feature, and turn off forwarding of source routed packets through the gateway.

2.5 Route management

Route management is the principle of controlling route exchange between the organization's network and the service provider. This is done with a view to enhancing routing security, and is achieved by using routing filters. Such routing information is never compromised or subverted either by design or by accident.

The mechanism for achieving this is to place filters for both inbound routing information, and outbound route advertisement on every interface capable of receiving routes or having the potential to do so. The filters should validate the sender of the routing information, and then verify each individual route information, and only accept valid and permissible routes configured in its access lists. The gateway should ignore and not propogate all other routes.

The OARnet routing architecture is configured to permit routes for all OARnet sites to be available on all the OARnet routers. The preferred Interior Gateway Protocol (IGP for short), on OARnet is OSPF, with RIP as a second choice. OSPF stands for "Open Shortest Path First[17]" and RIP stands for "Routing Information Protocol[12]." The OARnet backbone itself is running OSPF.

For explicit routing control and route security, OARnet requires running a distance vector based routing protocol to exchange routes with the organization. Typical routing techniques are either using static routes, or a routing protocol such as RIP[12].

OARnet routers at the regional network boundaries are configured to generate a floating default based on the presence of routes to the NSFNet backbone. This default route is propagated throught the routing domains on OARnet, to handle outbound traffic.

OARnet will announce all networks that a customer specifies as required to be reachable from the outside to the NSFNet backbone via the AS boundary routers. Filtering the customer routes is done on both the customer's router, and the OARnet backbone to ensure that routes are propogated correctly.

3 The Domain Name System

The Domain Name System (or DNS, for short) is a distributed database primarily for mapping hostnames and internet addresses, and for providing pointers to mail exchangers for an organization on the Internet[15, 16].

A router can also apply selective criteria when deciding to accept or ignore routing information that arrives on any of its interfaces. These criteria are called routing filters.

2.3.1 Packet filters on a cisco gateway

```
ip address 192.9.200.254 255.255.255.0
ip broadcast-address 255.255.255.255
ip access-group 102
!
! The first list drops ICMP_ECHO_REQUESTS.  This disallows ping from the
! outside world.  The next list allows everything else to go through.
! Some sites may even wish to drop the port and net unreachables that
! an internal host may generate, if, say, someone from the outside world
! attempted connecting to a bizarre socket on the internal hosts.
!
access-list 102 deny   icmp 0.0.0.0 255.255.255.255 192.9.0.0 0.0.255.255 eq 8
access-list 102 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
! Disallow all UDP traffic except domain and ntp queries inbound.
! Permit only domain and ntp queries to specific machines inbound.
! Permit everything outbound.
!
access-list 102 deny   udp  0.0.0.0 255.255.255.255 192.9.0.0 0.0.255.255 lt 1024
access-list 102 permit udp  0.0.0.0 255.255.255.255 192.9.200.53 0.0.0.0 eq 53
access-list 102 permit udp  0.0.0.0 255.255.255.255 192.9.200.123 0.0.0.0 eq 123
access-list 102 permit udp  192.9.0.0 0.0.255.255 0.0.0.0 255.255.255.255
!
! Disallow all TCP traffic except smtp, domain and nntp connections inbound.
! Permit connections to smtp, domain and nntp ports on specific machines only.
! Permit everything outbound.
!
access-list 102 deny   tcp  0.0.0.0 255.255.255.255 192.9.0.0 0.0.255.255 lt 1024
access-list 102 permit tcp  0.0.0.0 255.255.255.255 192.9.200.25 0.0.0.0 eq 25
access-list 102 permit tcp  0.0.0.0 255.255.255.255 192.9.200.53 0.0.0.0 eq 53
access-list 102 permit tcp  0.0.0.0 255.255.255.255 192.9.200.119 0.0.0.0 eq 119
access-list 102 permit tcp  192.9.0.0 0.0.255.255 0.0.0.0 255.255.255.255
```

For more details on configuring a cisco gateway, see also [6].

2.3.2 Packet filters on a proteon gateway

Proteons do not have adequate facilities for building such a filtration facility. At most, one would build a `((source address, source mask), (destination address, destination mask))` set of ordered pairs to absolutely filter out traffic from one host to the other.

For more details on configuring a proteon gateway, see also [23].

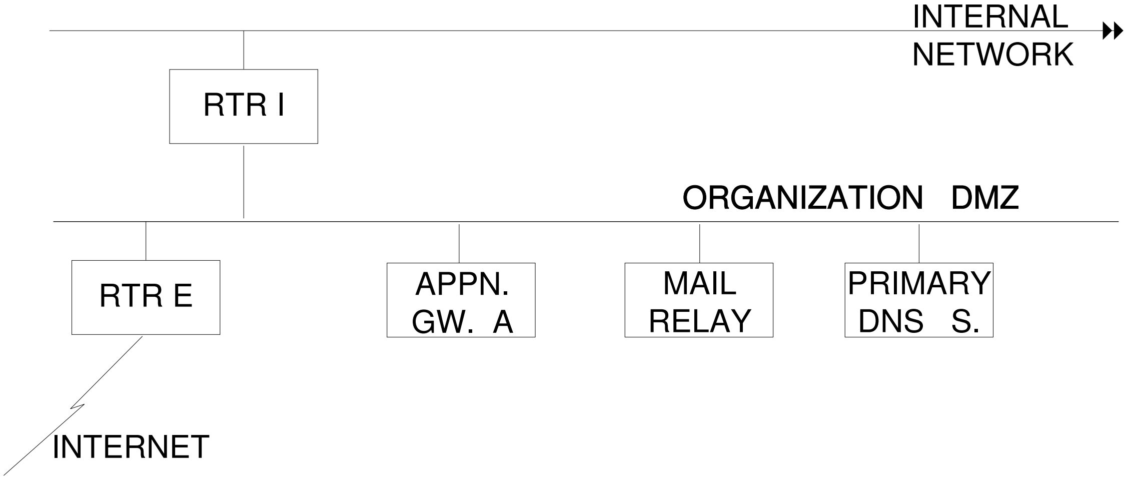

Figure 3: Firewalling with Application Gateways

2.2.3 Designing an isolate network, with application gateways

To be totally confident of network security, we need to maintain a carefully structured, and well monitored application gateway.

In this scenario, shown in figure 3, the internal network is not advertised to the outside world, and is not directly reachable, except via the application gateway, 'APP GW. A'. The organization DMZ is the only entity directly reachable from the outside world. The interior gateway, 'RTR I', will not accept any packets directly from the external router, 'RTR E'. 'RTR E' only has knowledge of the DMZ, and can only pass packets to the application gateways, the mail relay and the primary DNS server. The mail relay and the primary Domain Name System (or DNS) server are placed on the DMZ.

If this scheme is implemented, it might also be advantageous to run two parallel DNSs, one external and one internal, with a view to minimizing the information provided to the outside world. For more details on this, see the section 3.

2.2.4 Additional Sources

For more discussions and details on firewalls, see also [5, 14, 9].

2.3 Implementing packet filters

A router can be configured to actively look at every packet that arrives on any of its interfaces, and pass through or discard the packet based on a set of criteria configured into it. These criteria are called access lists or packet filters.

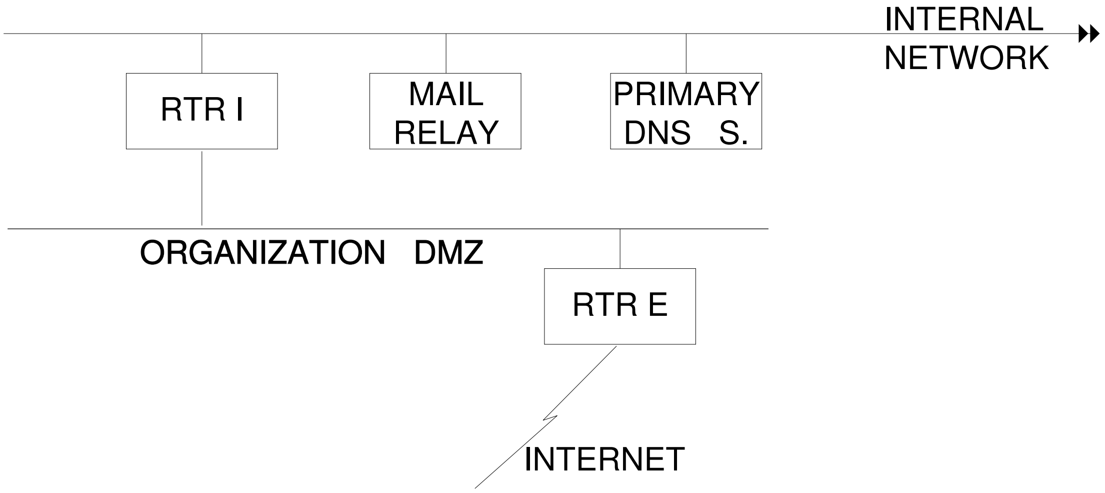

Figure 2: Firewalls with at least two routers

2. Not all well known services have ports less than 1024. Notorious examples are NFS, YP and related RPC based services, X windowing systems.

   Additionally, newer protocols and services pick up arbitrary port numbers not necessarily less than 1024. These protocols and services present unknown threats and dangers.

2.2.2 A more complex firewall system

To overcome the first disadvantage, we use multiple routers connected by an isolation network, or the organization DMZ, as shown in figure 2.

The DMZ is a class C network, that is not advertised to the outside world, and not directly reachable from any place. The only entities on this network are 'RTR I', the trusted interior gateway, and the network service provider's gateway, 'RTR E'.

The trusted interior gateway is configured as in the one router case; and can only be reached from within the organization network. Both routers, 'RTR E' and 'RTR I', are configured to reject telnet and snmp requests from non-trusted hosts or networks. The two gateways only have static routes to pass traffic between the trusted interior network, and the outside world.

This prevents direct subversion of this gateway from the outside. Subverting the exterior router, 'RTR E' does not damage the organization's internal network integrity.

This scheme still does not address the second problem with the earlier solution, which cannot control all well known and other ports[1].

---

[1] If the mail relay and the primary DNS server in figure 2 were moved to the organization DMZ, RTR I could be configured to deny any and all connections from the outside except on an exception basis. This overcomes the second disadvantage, albiet at a greater cost

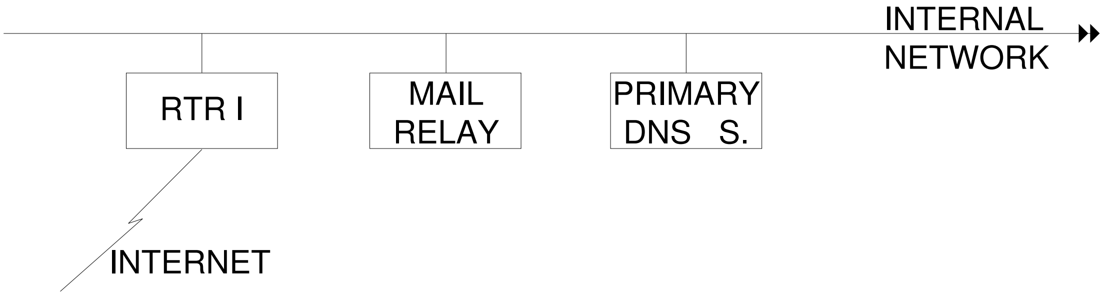

Figure 1: Firewalls with a single router

- exclude unwanted traffic generated on an unknown external network from entering a trusted, internal network.
- prevent information about the trusted internal network from being learned by the outside world.

2.2.1 Firewalls with single routers

Consider the process of setting up a single router, RTR I, as a firewall, as in figure 1. In this system, we would define a series of access-lists, such that all unwanted inbound traffic is excluded. Such an access control list would have the following characteristics:

- *Inbound ICMP traffic*
  All inbound ICMP traffic is permitted. It is conceivable that one may wish to disallow pings from the outside world. This can be done by dropping echo requests from the outside world.
- *Inbound UDP traffic*
  Packets destined for ports less than 1024 and not bound for the domain service port or the ntp port are prohibited. Domain and ntp chiming packets are only permitted to specific machines as are advertised as name or time servers.
- *Inbound TCP traffic*
  Packets destined for ports less than 1024 and not bound for the smtp, nntp or domain service port are prohibited. smtp, nntp or domain packets are only permitted to hosts as are advertised by the organization for such purposes.
- *Outbound traffic*
  There is no restriction on outbound traffic.

The router itself is configured to reject telnet or snmp requests from all other than specific machines or networks which are part of the internal network and the service provider's backbone.

This scheme has two disadvantages.

1. The primary disadvantage is that the router is a single point of failure, or attack.

This paper discusses some aspects of computer security in a networked environment, and ways and means of protecting systems. In the following sections, we class protection mechanisms into network security and host security.

Under network security, we discuss firewalls, packet filters, means of implementing the various options, techniques of information hiding of network related data like routing updates, internal network details etc. The section on host security is mostly a pointer to various tools, papers, techniques and tips on system security for administrators.

2 Network Security

2.1 A Trust model for Connecting to the Internet

We view the network as a series of concentric circles of trust, with each outer circle being less trusted than the inner one. We then define the interactions at the perimeter very rigidly. This section defines the various levels.

- The internal network is completely under the control of the organization, and is by definition, trusted and secure.
- The network service provider runs the backbone WAN, and offers connectivity to the Internet.
- The organization and the Internet service provider interconnect on a special purpose LAN, called the “DMZ.” The organization’s router on the DMZ is called RTR I (for the internal router), and the router connecting to the service provider is called RTR E (or external router).
- 'RTR I' is only accessible by the organization’s own networking authority, and is the outer perimeter of absolute trust.
- The service provider’s Network Operations Center, and the Network Engineering group access to 'RTR E' for purposes of configuring, network management and trouble shooting in the event of network problems. RTR E and the service provider are partially trusted.
- Other networks and hosts external to the organization and the backbone of the network service provider are not trusted.

It is possible, in the simplest case, that the entities, 'RTR I', 'RTR E', and the organizational DMZ may be collapsed into one entity, as we shall see when we configure a firewall with a single router, in section 2.2.1. In this case, the Network Operations Center and the Network Engineering Group of the service provider access the combined entity’s external interface for the purposes of management and trouble shooting, and the organization’s internal network connects directly to the combined entity’s internal interface.

2.2 Firewalls

A firewall enforces restrictions on the flow of traffic through it. These restrictions are usually asymetric, and provide the functionality to

2.3.1 Packet filters on a cisco gateway 7
2.3.2 Packet filters on a proteon gateway 7
2.4 Hazards of Source Routing 8
2.5 Route management 8
3 The Domain Name System **8**
3.1 Configuring the external DNS 9
3.2 Configuring the internal DNS 9
4 Host security **10**
4.1 COPS 10
4.2 Literature Survey 11
4.2.1 "Improving the Security of your UNIX System", by David A Curry 11
4.2.2 "Coping with the Threat of Computer Security Incidents" by Russell L Brand 11
4.2.3 "Site Security Handbook" RFC 1244 by J. Paul Holbrook 11
4.2.4 "Security Problems in the TCP/IP Protocol Suite" by S.M.Bellovin 11
4.2.5 Miscellaneous publications 11
4.3 Mailing lists 12
5 Summary **12**
6 Acknowledgements **12**
7 Author's Address **13**

1 Introduction

Computer security is the means of defending oneself against unwanted external influence. With the advent of computer networks, the face of security has been altered dramatically. Networking computers has become a form of Damocles sword for system administrators and users.

OARnet engineering group
OARnet

Kannan Varadhan
OARnet
September 15, 1992

OARnet Security Procedures

Status of this document

This document is produced by the combined efforts of the OARnet engineering group. It discusses various alternatives of enhancing the network security of an organization that is connected to OARnet. It does not specify a standard. Distribution of this document is unlimited.

Abstract

Computer Security is the means of defending oneself against unwanted external influence. With the advent of computer networks, the face of security has been altered dramatically. Networking computers has become a form of Damocles sword for system administrators and users. This paper discusses some aspects of computer security in a networked environment, and ways and means of protecting systems.

Contents

1 Introduction **2**

2 Network Security **3**

2.1 A Trust model for Connecting to the Internet 3

2.2 Firewalls 3

2.2.1 Firewalls with single routers 4

2.2.2 A more complex firewall system 5

2.2.3 Designing an isolate network, with application gateways 6

2.2.4 Additional Sources 6

2.3 Implementing packet filters 6