Network Working Group
Request for Comments: 1675
Category: Informational

S. Bellovin
AT&T Bell Laboratories

August 1994

Security Concerns for IPng

Status of this Memo

Abstract

This document was submitted to the IETF IPng area in response to RFC 1550. Publication of this document does not imply acceptance by the IPng area of any ideas expressed within. Comments should be submitted to the big-internet@munnari.oz.au mailing list.

Overview and Rationale

A number of the candidates for IPng have some features that are somewhat worrisome from a security perspective. While it is not necessary that IPng be an improvement over IPv4, it is mandatory that it not make things worse. Below, I outline a number of areas of concern. In some cases, there are features that would have a negative impact on security if nothing else is done. It may be desirable to adopt the features anyway, but in that case, the corrective action is mandatory.

Firewalls

For better or worse, firewalls are very much a feature of today's Internet. They are not, primarily, a response to network protocol security problems per se. Rather, they are a means to compensate for failings in software engineering and system administration. As such, firewalls are not likely to go away any time soon; IPng will do nothing to make host programs any less buggy. Anything that makes firewalls harder to deploy will make IPng less acceptable in the market.

Firewalls impose a number of requirements. First, there must be a hierarchical address space. Many address-based filters use the structure of IPv4 addresses for access control decisions. Fortunately, this is a requirement for scalable routing as well.

Routers, though, only need access to the destination address of the packet. Network-level firewalls often need to check both the source and destination address. A structure that makes it harder to find the source address is a distinct negative.

There is also a need for access to the transport-level (i.e., the TCP or UDP) header. This may be for the port number field, or for access to various flag bits, notably the ACK bit in the TCP header. This latter field is used to distinguish between incoming and outgoing calls.

In a different vein, at least one of the possible transition plans uses network-level packet translators [1]. Organizations that use firewalls will need to deploy their own translators to aid in converting their own internal networks. They cannot rely on centrally-located translators intended to serve the entire Internet community. It is thus vital that translators be simple, portable to many common platforms, and cheap -- we do not want to impose too high a financial barrier for converts to IPng.

By the same token, it is desirable that such translation boxes not be usable for network-layer connection-laundering. It is difficult enough to trace back attacks today; we should not make it harder. (Some brands of terminal servers can be used for laundering. Most sites with such boxes have learned to configure them so that such activities are impossible.) Comprehensive logging is a possible alternative.

IPAE [1] does not have problems with its translation strategy, as address are (insofar as possible) preserved; it is necessary to avoid any alternative strategies, such as circuit-level translators, that might.

Encryption and Authentication

A number of people are starting to experiment with IP-level encryption and cryptographic authentication. This trend will (and should) continue. IPng should not make this harder, either intrinsically or by imposing a substantial perforance barrier.

Encryption can be done with various different granularities: host to host, host to gateway, and gateway to gateway. All of these have their uses; IPng must not rule out any of them. Encapsulation and tunneling strategies are somewhat problematic, as the packet may no longer carry the original source address when it reaches an encrypting gateway. (This may be seen more as a constraint on network topologies. So be it, but we should warn people of the limitation.)

Dual-stack approaches, such as in TUBA's transition plan [2], imply multiple addresses for each host. (IPAE has this feature, too.) The encryption and access control infrastructure needs to know about all addresses for a given host, belonging to whichever stack. It should not be possible to bypass authentication or encryption by asking for a different address for the same host.

Source Routing and Address-based Authentication

The dominant form of host authentication in today's Internet is address-based. That is, hosts often decide to trust other hosts based on their IP addresses. (Actually, it's worse than that; much authentication is name-based, which opens up new avenues of attack. But if an attacker can spoof an IP address, there's no need to attack the name service.) To the extent that it does work, address-based authentication relies on the implied accuracy of the return route. That is, though it is easy to inject packets with a false source address, replies will generally follow the usual routing patterns, and be sent to the real host with that address. This frustrates most, though not all, attempts at impersonation.

Problems can arise if source-routing is used. A source route, which must be reversed for reply packets, overrides the usual routing mechanism, and hence destroys the security of address-based authentication. For this reason, many organizations disable source-routing, at least at their border routers.

One candidate IPng -- SIPP -- includes source-routing as an important component. To the extent this is used, it is a breaks address-based authentication. This may not be bad; in fact, it is probably good. But it is vital that a more secure cryptographic authentication protocol be defined and deployed before any substantial cutover to source routing, if SIPP is adopted.

Accounting

An significant part of the world wishes to do usage-sensitive accounting. This may be for billing, or it may simply be to accomodate quality-of-service requests. Either way, definitive knowledge of the relevant address fields is needed. To accomodate this, IPng should have a non-intrusive packet authentication mechanism. By "non-intrusive", I mean that it should (a) present little or no load to intermediate hops that do not need to do authentication; (b) be deletable (if desired) by the border gateways, and (c) be ignorable by end-systems or billing systems to which it is not relevant.

References

[1] Gilligan, R., and E. Nordmark, "IPAE: The SIPP Interoperability and Transition Mechanism", Work in Progress, March 16, 1994.

[2] Piscitello, D., "Transition Plan for TUBA/CLNP", Work in Progress, March 4, 1994.

Security Consierations

This entire memo is about Security Considerations.

Author's Address

Steven M. Bellovin
Software Engineering Research Department
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, NJ 07974, USA

Phone: +1 908-582-5886
Fax: +1 908-582-3063
EMail: smb@research.att.com