Computer and Information Science; Vol. 13, No. 4; 2020
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Securing and Improving the Internet Architecture

Austin Liu[1]

[1] Los Altos High School, Los Altos, California, United States of America

Correspondence: Austin Liu, Los Altos High School, Los Altos, California, United States of America.

Received: October 5, 2020 Accepted: October 26, 2020 Online Published: October 27, 2020

doi:10.5539/cis.v13n4p42 URL: https://doi.org/10.5539/cis.v13n4p42

Abstract

The information transfer protocol that supports the modern Internet with its hundreds of thousands of petabytes per month to billions of Internet users across the world was designed in 1981, and it lacks the capacity to properly ensure the security and stability of the Internet today. Features such as the prevention of network attacks, a large address space for the increasing number of devices, verification of the source of an Internet request, and so on are all absent from the current architecture. This paper seeks to review, summarize, and compare six proposals submitted to address the issues IP faces: the Accountable Internet Protocol, the Expressive Internet Architecture, MobilityFirst, Passport, StopIt, and the Traffic Validation Architecture. Finally, the paper details a protocol design that not only is feasible to adopt with the present infrastructure/computing power but also addresses some of the pressing issues of IP, with particular focus on the address space, mitigation of network attacks, and source verification.

Keywords: address, architecture, DDoS, DoS, internet, network, protocol, verification

1. Introduction

The information transfer protocol that supports the modern Internet with its hundreds of thousands of petabytes per month to billions of Internet users across the world was designed in 1981 for limited use by the ARPANET connecting American universities (RFC 791 - Internet Protocol, 1981). As the Internet has scaled exponentially, the weaknesses of the Internet Protocol have become glaringly obvious: modern web services and applications are under increasing attack by malicious individuals, and the market for network security continues to grow larger and larger. The number of Internet Protocol (IP) addresses available for private use has been exhausted and can only be acquired through a change of ownership. The original use case permitting only trusted universities has expanded to enable the proliferation of IP address spoofing, as packets can specify any IP as the source IP.

Numerous proposals have been submitted to address these issues to limited adoption by the Internet as a whole. The IETF's IPv6 revision to the most widely used version of the Internet Protocol, IPv4, has been available for over two decades as a standard and is still not used by the majority of Internet connected devices. Many other proposals have also been suggested both as requests for comments (RFCs) to the IETF and as papers; the most notable project was the National Science Foundation Future Internet Architecture Project supporting five proposals, one of which (Expressive Internet Architecture) is included in this survey. The content of this paper aims to describe the various proposals to improve IP, which can be sorted into a few major categories based on the level of change to the overall IP architecture. The proposals range from offering additional functionality to IP that Internet providers can choose to add, to a complete overhaul of the structure of the Internet. From there, papers also differ on the issues they choose to target. The solutions proposed in this survey paper commonly address DoS attacks and the integrity of a source header. The content of the papers is summarized and compared both in detail in Section 3 and as an overall categorized comparison in Section 3.4.

Finally, the paper proposes an architecture resolving some of the issues of IP after the comparison of the strengths and weaknesses of existing approaches. The architecture, detailed in Section 4, combines the existing proposals of the Accountable Internet Protocol and Traffic Validation Architecture and addresses the concerns and changes to IP of each, unifying them into a single proposal. The paper additionally describes the estimated performance of the architecture, changes to the existing IP infrastructure, examples of usage, cases of improvements over IP, and plans for the deployment of the architecture.

2. Background

The Internet Protocol establishes the Internet by defining the communication of packets of information from a source host to a destination host based on an IP address. The first major version of IP, IPv4, still remains in primary use today. IP provides a best effort, end-to-end packet delivery - that is to say, IP will deliver the packet from beginning to end, but does not guarantee the packet will not be lost during transmission, reordered, or arrive in a timely manner. IP delivers packets by connecting routers across the Internet; a router will receive a packet, read the information in the packet header according to the IP standard, and forward the packet accordingly to the next appropriate location, whether it is another router or the destination host. Each destination on the Internet has an IP address, a series of numbers identifying the location a packet must be sent to. Routers employ routing tables to look up the destination of a packet and then forward the packet to the location to be connected to in its routing table. The path a packet travels is formed as each router forwards the packet to the next router (Kurose & Ross, 2013). In the IPv4 standard, IP addresses were 32 bits typically expressed as four decimal numbers separated by full stops (RFC 791 - Internet Protocol, 1981). The number of possible addresses is 2 to the power of 32, or roughly ~4 billion, which has already been completely exhausted with the current number of Internet connected devices. IP addresses are structured hierarchically; every autonomous system (AS) is assigned a block of IP addresses routed to them according to their assigned network bits of the IP addresses, which is then forwarded to the end hosts within their network with the host bits of the IP address (RFC 1930 - Guidelines for Creation, Selection, and Registration of an Autonomous System (AS), 1996). The Internet Assigned Numbers Authority administers the assignment of IP addresses to regional Internet registries, who then allocate IP addresses to networks.

The design of IP presents a few fundamental problems introduced in Section 1, mainly regarding security. The design of IP permits any host to send any packet to any destination, whether or not the destination desires the traffic or can handle the traffic or not. Such denial of service (DoS) attacks overwhelm the servers of the destination host, preventing normal traffic from accessing the service of the destination host. There is also no intrinsic verification of the headers of an IP packet; as such, a host can specify the source of the packet as any IP. Denial of service attacks take advantage of this, sending requests from multiple locations to normal servers and then directing the responses to the target destination host, multiplying the magnitude of the attack. Some Internet service providers solve this by limiting the range of source IP addresses permitted to leave the network through packet egress filtering, although this has limited adoption (Kurose & Ross, 2013).

These issues present in the IP architecture lead to the various proposals to replace or add to the functionality of IP in Section 3.

3. Related Work/Existing Solutions

As stated in Section 1, the existing proposals to amend the IP standard can be categorized into three main categories: improvements to the existing IP architecture, replacements for the IP architecture, and replacements for the entire Internet infrastructure. The paper compares six different proposals to amend IP: the Accountable Internet Protocol (AIP), the eXpressive Internet Architecture (XIA), MobilityFirst, Passport, StopIt, and the Traffic Validation Architecture. The proposals can be further divided into the issues of IP they tackle; the proposals in this paper mainly focus on either the validation of the source IP or DDoS mitigation, but many other proposals introduce features to IP, such as content-based networking and mobility, represented by XIA and MobilityFirst in this paper.

3.1 Improvements to IP

Three of the proposals implement changes on top of the existing IP architecture: Passport, StopIt, and the Traffic Validation Architecture. These proposals also vary in the degree of changes to the architecture, ranging from modular attachable functionality to Internet routers to changes in the structure of the IP packet.

The first of the improvements is Passport. The sole aim of Passport is to verify the source of a packet with fast performance. Passport works exclusively at the AS level and only verifies an IP has not been spoofed by another autonomous system; as such, packets will only be verified on the border between ASes and will not be verified within the network. Outbound packets from the origin AS will be stamped with a generated hash computed from the information contained within the packet, as well as a secret key shared between the source AS and autonomous systems along the path. An AS receiving a packet from an external interface to another AS will verify the source of the packet by looking up the corresponding AS from the source address listed in the packet, recomputing the generated hash with the AS’s copy of the secret key, then comparing the result. Passport has been implemented and tested with performance nearly identical to IP (Liu, Li, Yang, & Wetherall, 2008).

StopIt builds off of Passport with the addition of DoS mitigation functionality. Autonomous systems can choose to implement StopIt with the addition of a StopIt server(s) to their network, which on the verified request of a host will filter malicious requests from within their network. When a destination host is under attack, it can request to send a StopIt request to the StopIt server via their access router within their intranet to block the source IP of the attack for a certain amount of time. The destination host's StopIt server verifies the request with the source IP's StopIt server and then forwards the destination's StopIt request to the source's StopIt server. The source StopIt server then locates the access router of the attacking host and sends a request to the router, which then installs a filter and sends a StopIt request to the host. StopIt has been implemented and tested with performance nearly identical to IP (Liu, Yang, & Lu, 2008).

Traffic Validation Architecture is similar to StopIt in that the main focus is to mitigate DoS attacks, but the approaches to solve the issues are completely different. TVA accomplishes its aims with an approach that requires hosts to first obtain permission, or a capability, to send data to a destination host. A host will initially send a request packet with no capability in its header to the destination host, which will then either respond with a capability, usually along with the response packet, or a packet with no capability to reject the request, usually along with a packet that closes the connection. Capabilities contain a timestamp in addition to a keyed hash to permit the host to send information for a certain amount of time. Routers along the path will then permit the packets to be sent if the capability is valid and will also cache the path of the packet to permit further packets without extensive verification (Yang, Wetherall, & Anderson, 2008).

3.2 Replacements to IP

Proposals can also fundamentally replace IP with designs mandating redesigned addresses, forwarding behavior, and packet structures. Two of the proposals present replacements to IP: the Accountable Internet Protocol and the eXpressive Internet Architecture, addressing source verification and content types of the Internet, respectively.

AIP maintains much of the same structure as IP but emphasizes the design of the addresses, forwarding around self-certifying addresses, and verification of the source. Independent administered networks are each assigned one or more unique accountability domains (ADs) and each host is assigned a globally unique endpoint identifier (EID). As such, an AIP address follows the format of AD:EID, with the last eight bits of the EID identifying the interface the host is connected to the AD with. This is to help identify when a host connects to an AD multiple times. The removal of the hierarchical structure of IP permits the AD and EID to be self-certifying; the AD is the hash of the public key of the administrative domain, and the EID is the hash of the public key of the host. The self-certifying component of the addresses extends the length of an AIP address to 160 bits. Routers forward an AIP packet to the AD listed in the header until the packet reaches the destination AD, at which point the AD forwards the packet to the appropriate EID. Routers in the network can verify the source of a packet with its cryptographically generated address by sending a verification packet to the source. The verification packet contains the source and destination AIP addresses, the hash of the packet, and an encoded representation of the interface on which the packet arrived and is also cryptographically signed by the router with a rotating secret key. The sender is able to prove they have identity EID by signing the verification packet with the private key of the EID (Andersen et al., 2008).

XIA also implements self-certifying addresses, but with a much different structure as a result of the different aims of proposals. The design goal of XIA is to support different content types, or principals, on the Internet. The basis for XIA is formed with unique eXpressive identifiers (XIDs) for principals, which can represent hosts, administrative domains, services, or content. Principals must specify the semantics for communicating with the content type, a unique XID to specify the principal, a method for allocating, routing, and communicating with XIDs of the principal, and any security properties for communication. XIDs are cryptographically signed to verify the source of the content. XIA addresses are structured as directed acyclic graphs connecting nodes of XIDs: routing begins at the untyped entry node with no XID and ends at the last node (Naylor et al., 2014).

3.3 Replacements to the Internet Infrastructure

MobilityFirst fundamentally replaces the host/server model of the Internet that has persisted to this day. MobilityFirst aims to permit devices to identify themselves, rather than with tethered hosts identifying themselves with addresses. Network-attached objects, whether they be hosts, a group of hosts, or content, are each assigned a globally unique identifier (GUID) by an independent name certification service derived from the cryptographic hash of the public key. GUIDs are separate from the network addresses of the objects they identify. GUIDs are looked up in a request to a global name resolution service and correspond to a set of network addresses (Raychaudhuri, Nagaraja, & Venkatramani, 2012).

3.4 Summary

Table 1. Comparison of Proposals

Internet Architecture	IP Replacement	Support for DDoS Protection	Performance	Source Verification	Upgradable	Mobility	Deployable
Accountable Internet Protocol	Yes	Prevents reflection attacks	Reasonable performance	Verifies the host	Version header	None	Changes to the host and router level
Expressive Internet Architecture	Yes	Prevents reflection attacks	Reasonable performance	Verifies the host	Version header	Addresses can be generated and linked to a specific device	Changes to the host and router level
Passport	No	Prevents reflection attacks	Nearly identical to IP	Verifies the AS origin	Version header	None	Changes to the router level
Traffic Validation Architecture	No, but changes the behavior of the host, router, and endhost	Prevents reflection attacks + capabilities	Nearly identical to IP	No	Version header	None	Changes to the host and router level
StopIt	No	Prevents reflection attacks + allows the endhost to prevent hosts from sending to an endhost	Nearly identical to IP	Verifies the AS origin	N/A	None	Changes to the router level
MobilityFirst	Yes	Prevents reflection attacks + capabilities	Performance statistics not available	Verifies the host	N/A	Addresses can be linked to a specific device	Requires complete restructuring and significant change to the Internet

Table 1 contains the overall findings and comparison of the proposals.

4. Protocol Design

A comparison of the papers in the previous section allows us to address the most salient issues and concerns. Proposals involving a restructured Internet or addressing system present too large of a change to replace IP, requiring significant modifications to services or equipment. Thus, the most feasible issues to resolve are those that prevent the effective usage of the existing IP system, without influencing the primary structure of the Internet: those listed above are the length of the IP address, DoS mitigation, and the verification of the origin of a packet. A proposal addressing these concerns would require changes to both the hosts and the routers; a synthesis of the Accountable Internet Protocol and the Traffic Validation Architecture is presented.

The two proposals can easily fit together; the Accountable Internet Protocol modifies the IP architecture without changing the underlying behavior or abstract design and thus a deployment would be mostly logistical. The Traffic Validation Architecture only modifies the headers of a packet and the behavior at the router level and can be easily integrated with the AIP proposal.

The unification of the two approaches solves issues that no one architecture alone cannot address; AIP cannot effectively prevent DDoS attacks without additional hardware changes, and TVA alone cannot verify the source of attacking packets effectively.

The behavior at the routers forwarding the packets occurs one after the other; first the source of the packet is verified according to AIP, then the packet continues to its destination or is deferred according to the verification of the capability by TVA.

The domain name system associating human-readable domains to addresses works similarly as in IP. For a hostname, one or more AIP addresses are listed and can be connected to. As stated, this is one of the primary aims of the synthesis of AIP and TVA; the underlying infrastructure can remain similar and only logistical changes regarding the adoption of AIP behavior and addresses at routers/in the DNS are necessary.

Furthermore, the proposal presents benefits over the other proposals compared in the table. The addition of separate servers or other hardware level changes is not necessary (as in StopIt), and in benchmarks for high-bandwidth links, TVA has also been shown to be more effective than StopIt in successful data transfer during an attack. AIP also provides additional benefits over Passport because of its comprehensive verification down all the way to the host, rather than to simply the AS.

Both TVA and AIP have performance very similar to IP by themselves due to fast cryptographic verification, and the two cryptographic processes together would not result in a significant performance decrease compared to IP.

The basic process for a host connecting to a destination host is as follows:

1. The host sends an AIP packet/TVA request packet containing an empty capability to the first-hop router or switch.
2. The router checks if the host’s address has been recently verified, and if not, the router sends a verification packet to the host and drops the unverified packet.
3. The host signs the verification packet and resends the original packet.
4. The router forwards the packet in the allocated request packet bandwidth.
5. On borders between ASes, the edge router of the AS may also choose to reverify the host if the origin AS is not trusted to verify.
6. If the destination host chooses to permit traffic, the host sends back the response packet along with capabilities. If the host does not choose to permit traffic, the host will send back a packet with an empty capability.
7. If the source host receives a capability, it initially sends its next several packets with the capabilities to permit routers to cache the capability.
8. Routers check the capability cryptographically and forward the packet.

5. Conclusion

The current IP standard presents several pressing issues directly impacting its usability, and various proposals have been drafted to address them. The proposals differ greatly in both the issues they confront and the methods they address them with. Another proposal is presented in the paper synthesizing two existing proposals compared in the paper which does not exhibit challenges in its adoption and has several benefits over existing proposals in terms of the security of IP. The discussion, comparison, and proposal presented in this paper concludes that a more secure and reliable Internet is possible, and I hope that the discussion, development, and plans for adoption will continue in the future.

Acknowledgments

Thank you to Dr. Fahad Dogar at Tufts University for inspiring and providing guidance on the research throughout the entire process, as well as Cameron Taylor at Georgia Institute of Technology and Arron Liu at Duke University for the guidance provided on the preparation of the manuscript of this paper.

References

Andersen, D. G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D., & Shenker, S. (2008). Accountable internet protocol (AIP). Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication, 339-350. https://doi.org/10.1145/1402958.1402997

Kurose, J. F., & Ross, K. W. (2013). Computer networking: A top-down approach (6th ed.). Pearson.

Liu, X., Yang, X., & Lu, Y. (2008). To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication,* 195-206. https://doi.org/10.1145/1402958.1402981

Naylor, D., Mukerjee, M. K., Agyapong, P., Grandl, R., Kang, R., Machado, M., … Steenkiste, P. (2014). *XIA: Architecting a more trustworthy and evolvable internet.* Association for Computing Machinery. https://doi.org/10.1145/2656877.2656885

Raychaudhuri, D., Nagaraja, K., & Venkataramani, A. (2012). *MobilityFirst: A robust and trustworthy mobility-centric architecture for the future internet.* Association for Computing Machinery. https://doi.org/10.1145/2412096.2412098

RFC 1930—Guidelines for creation, selection, and registration of an Autonomous System (AS). (1996, March). Retrieved from https://tools.ietf.org/html/rfc1930

RFC 791—Internet Protocol. (1981, September). Retrieved from https://tools.ietf.org/html/rfc791

Xin, L., Ang, L., Yang, X. W., & David, W. (2008). Passport: Secure and Adoptable Source Authentication. *5th USENIX Symposium on Networked Systems Design and Implementation.*

Yang, X., Wetherall, D., & Anderson, T. (2008). *TVA: A DoS-limiting network architecture. IEEE Press.* https://doi.org/10.1109/TNET.2007.914506

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).