International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 1
ISSN: 2454-4248
180 – 186

Evasive Internet: Reducing Internet Vulnerability through Transient Destination

Mrs. M. Priya [1], Mrs. K. K. Kavitha M.C.A., Mphil, Set (Ph.D)[2],
Research Scholar, Dept. of Computer Science, **S**elvamm Arts & Science College (Autonomous), Tamilnadu, India[1]
HOD, Department of Computer Science, Selvamm Arts & Science College (Autonomous), Tamilnadu, India [2]

ABSTRACT: In the current Internet architecture, traffic is commonly routed to its destination using DNS names that are mapped to IP addresses, yet there are no inherent means for receivers to attribute sources of traffic to senders or for receivers to authorize senders. These deficiencies leave the Internet and its connected hosts vulnerable to a wide range of attacks including denial-of-service and misrepresentation (spoofing, phishing, etc.) which continue to cause material damage. In this mechanism to combat these vulnerabilities by introducing attribution and authorization into the network using a transient addressing scheme to establish attribution through DNS, establish authorization at the host, and enforce authorization and attribution in the network. In this work, I developed and characterized a system for effecting in-network enforcement at the router, and I demonstrate the enforcement is possible on current commodity hardware at sustained throughput rates Ill above common Internet connection rates. The current internet architecture allows hosts to send arbitrary IP packets across a network, which may not reflect valid source address information. IP spoofing and Denial of service attacks are ubiquitous. Filtering techniques are not sufficient enough to counter these attacks. Current Internet design calls for in-network authentication of addresses and attribution of traffic they generate. In this architecture the destination can only be reached through a valid capability. The aim of this dissertation is to implement Evasive Internet Protocol for the end hosts and measure the preliminary performance as compared to current internet protocols.

KEYWORD: *DNS, Spoofing, Evasive Internet Protocol.*

*****

1. INTRODUCTION

In the current Internet, traffic is commonly routed to its destination using human-readable. DNS names that are mapped to machine-routable IP addresses, yet the current architecture offers no reliable means to attribute traffic to senders or for receivers to authorize senders. These deficiencies leave the Internet and its connected hosts vulnerable to a wide range of attacks including denial-of-service and misrepresentation1 which continue to cause damage on the Internet today. Evasive Internet Protocol (EIP) to combat these vulnerabilities with new network properties: sender-attribution and receiver-authorization. To enable these properties, EIP employs a transient addressing scheme which establishes attribution through DNS, establishes authorization at the host, and enforces authorization and attribution in the network. In this work, we develop and characterize a system for effecting this in-network enforcement at the router. Our implementation and experiments demonstrate that EIP adds less than 1ms latency per router hop to connection setup time, and that enforcement of authorization and attribution is possible using current general purpose hardware at sustained throughput rates in excess of 50 Mbps – well above typical Internet broadband access rates.

Today the Internet is assaulted from multiple fronts. Spam has already changed the social norms of using email, reflecting new assumption that legitimate mail might never be read by the recipient due to being entangled in spam filters. Malware dogs peer-to-peer networks and open source software distribution. A fundamental challenge in designing a more secure Internet is to reconcile the security needs with preserving the openness of the Internet and privacy of its users. Indeed, preventing bad actors in an open environment seems to entail being able to hold actors accountable for their actions, which in turn suggests being able to attribute t180he actions to particular users, which undermines user privacy. Evasive Internet Architecture aims to address this challenge, and to do so not by selecting a particular tradeoff point in this tussle space but by providing the tools that would give users the flexibility to select their own tradeoffs between openness and security.

2. RELATED WORK

The approach relies on the general notion of capabilities. In EIP, a capability is the only mean to reach a destination. The capability itself, which is an authorization to communicate with a host, is valid only for a specific sender and for a limited amount of time and data. The capabilities are distributed by a name system (e.g., DNS) which makes the design very effective as it uses the current name system with some feasible modification; this avoids extra infrastructure cost and maintenance.

This particular approach leaves the root name servers exposed for attacks since they need to be always reachable and thus demands a fixed capability to reach them.

 ISSN: 2454-4248
180 – 186

Security and Feasibility

Given the tussle space between security, openness and privacy, the aim of EIP is to empower the internet end points to impose their own policies in this regards. Furthermore, the design strives for a minimal change in the current internet architecture that would allow this empowerment. The design itself is not a new overarching architecture for the internet; rather it

Although the architecture relies on capabilities to reach a host, the IP addresses would still be used by the existing routing protocols for forwarding table indexing and route computation. Thus routing protocols (example BGP) properties can still be retained and also the scalability properties related to topological information that is embedded in an IP address is also retained.

Although IP addresses are used for route computation and forwarding tables, the host IP address in EIP architecture cannot be used to communicate with the host. A compliant router will not forward a packet that has an invalid destination capability. This EIP address which in effect becomes a transient destination address is referred by the authors as T-address.

As far as privacy is concerned, EIP itself does not undermine it. Since EIP uses IP address to identify communicating parties, it can be said that the privacy of a user remains the same as it is in today's internet.

Some of the security benefits that can be obtained by introducing EIP

Currently anti-spoofing techniques rely mostly on ingress address filtering [6] but their effectiveness is reduced by concept like multi homing where a user can have an IP address from one ISP and uses another ISP connection to connect to the internet, in such case ingress filtering often drops packet since the source IP for the packet and the network from which it is originating differs. Spoofing-based attacks continue to occur and exert damage. These attacks included old SYN-flood attacks and other DDoS attacks. Although specific mechanism have been proposed to counter some of these attacks, but the root of all these attacks, i.e. IP-forging, still exists

The notion of capability enables recipients control over incoming flows because each host can implement fine-grained capability-issuing policies for particular external destinations. These policies can reflect various trade off decisions between security and openness. At the extreme, a host can only allow incoming traffic from a known set of destinations, and EIP will prevent other destinations from forging their IP addresses to bypass this policy. Short of this extreme, the recipient's control allows a recipient to dynamically adjust the validity constraints granted to various external destinations based on their prior behavior.

Domain

The interconnected computers to do the job are known as Networking. There is a considerable confusion in the literature between a computer network and a distributed system. The key distinction is that in a distributed system a collection of independent computers appears to its users a single coherent system.

Depending upon the physical setup and the configuration the networks can be classified into as follows:

Local Area Network

Metropolitan Area Network

Wide Area Network

Local Area Network

Local area network generally called LAN's is privately-owned Networks within a single building or campus of up to a few kilometers in size. They are widely used to connect PC's and workstations in company offices and factories to share resources and exchange information.

Metropolitan Area Network

A metropolitan area network or MAN covers a city the city the best known example of a MAN is the cable television network available in many cities this system grew from earlier community antenna system used in area with poor over-the-air-television reception.

Wide Area Network

A wide area network or WAN spans a large geographical area often a country of continent. It contains a collection of machines intended for running user (i.e., applications) programs. We will follow traditional usage and call this machine host. The host is connected by communication subnet or just subnet for short.

TYPES OF COMMUNICATION OVER INTERNET

Computers running on the Internet communicate to each other using either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), as this diagram.

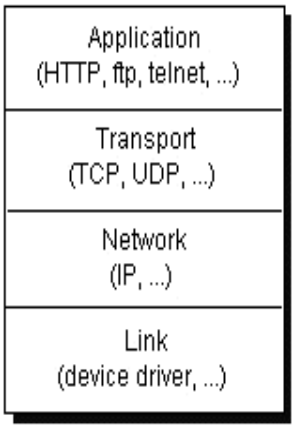


Fig: 2.1 OSI LAYERS

 ISSN: 2454-4248
180 – 186

TCP

When two applications want to communicate to each other reliably, they establish a connection and send data back and forth over that connection. This is analogous to making a telephone call. If you want to speak to Aunt Beatrice in Kentucky, a connection is established when you dial her phone number and she answers. You send data back and forth over the connection by speaking to one another over the phone lines. Like the phone company, TCP guarantees that data sent from one end of the connection actually gets to the other end and in the same order it was sent. Otherwise, an error is reported. TCP provides a point-to-point channel for applications that require reliable communications.

The Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Telnet are all examples of applications that require a reliable communication channel. The order in which the data is sent and received over the network is critical to the success of these applications. When HTTP is used to read from a URL, the data must be received in the order in which it was sent.

UDP

The UDP protocol provides for communication that is not guaranteed between two applications on the network. UDP is not connection-based like TCP. Rather, it sends independent packets of data, called datagram's, from one application to another. Sending datagram's is much like sending a letter through the postal service: The order of delivery is not important and is not guaranteed, and each message is independent of any other. For many applications, the guarantee of reliability is critical to the success of the transfer of information from one end of the connection to the other

PORTS

Generally speaking, a computer has a single physical connection to the network. All data destined for a particular computer arrives through that connection. However, the data may be intended for different applications running on the computer. So how does the computer know to which application to forward the data.

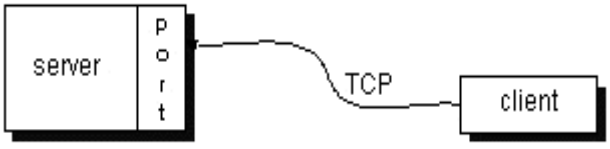


Fig: 2.2 TCP CONNECTON

In Port numbers range from 0 to 65,535 because ports are represented by 16-bit numbers. The port numbers ranging from 0 - 1023 are restricted; they are reserved for use by well-known services such as HTTP, FTP and other system services. These ports are called *well-known ports*. Your applications should not attempt to bind to them.

ROUTING

Routing is the act of moving information across an internet work from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. Only recently large-scale internetworking has become popular.

3. EXISTING SYSTEM

In the current Internet architecture, traffic is commonly routed to its destination using DNS names that are mapped to IP addresses, yet there are no inherent means for receivers to attribute sources of traffic to senders or for receivers to authorize senders. These deficiencies leave the Internet and its connected hosts vulnerable to a wide range of attacks including denial-of-service and misrepresentation (spoofing, phishing, etc.) which continue to cause material damage. In this mechanism to combat these vulnerabilities by introducing attribution and authorization into the network using a transient addressing scheme to establish attribution through DNS, establish authorization at the host, and enforce authorization and attribution in the network.

Drawbacks of Existing System

- Denial of service attacks against network infrastructures and Web sites have become routine. Computer break-ins and hijacking is wide-spread. Identity theft through phishing or break-ins is on the rise.
- Spam has already changed the social norms of using email, reflecting new assumption that legitimate mail might never be read by the recipient due to being entangled in spam filters.

4. PROPOSED SYSTEM

This paper presents our vision for Evasive Internet, where destinations are only reachable through capabilities, which serve as hosts' flat transient addresses. Just as today's host addresses, our capabilities are obtained from the DNS hierarchy, thus never exposing destinations themselves to unprotected traffic. Our design supports in-network authentication of transient addresses and attribution of traffic they generate; our design further gives hosts full control over incoming flows. We achieve these objectives without exposing hosts to unprotected capability request traffic and without distributed filtering infrastructure. we develop and characterize a system for effecting this in-network enforcement at the router.

 ISSN: 2454-4248
180 – 186

4.1Advantages of Proposed System

- Evasive Internet Protocol (EIP) to combat these vulnerabilities with new network properties: sender-attribution and receiver-authorization.
- To enable these properties, EIP employs a transient addressing scheme which establishes attribution through DNS, establishes authorization at the host, and enforces authorization and attribution in the network.

5. IMPLEMENTATION

ROUTING COMPONENTS

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internet work. In the context of the routing process, the latter of these is referred to as packet switching. Although packet switching is relatively straightforward, path determination can be very complex.

PATH DETERMINATION

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used. Routing algorithms fill routing tables with a variety of information..

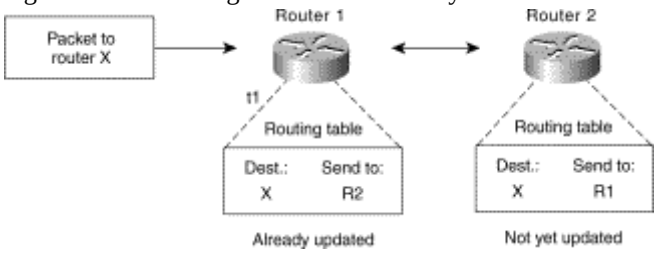


Fig: 5.1 Destination/Next Hop Associations Determine the Data's Optimal Path

Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

SWITCHING

Switching is defined as routing of each packet independently from all others and allocates transmission resources as needed. The principal goals of switching is to optimize utilization of available link capacity and to increase the robustness of communication. There are two types of Switching techniques available, they are:

- Circuit Switching
- Packet Switching

CIRCUIT SWITCHING

A type of communications in which a dedicated channel (or circuit) is established for the duration of a transmission. The most ubiquitous circuit-switching network is the telephone system, which links together wire segments to create a single unbroken line for each telephone call. The other common communications method is packet switching, which divides messages into packets and sends each packet individually. The Internet is based on a packet-switching protocol, TCP/IP.

PACKET SWITCHING

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies.

Sub domain

Network Security Refers to the proper safeguarding of everything associated with a network, including data, media, and equipment. It involves administrative functions, such as threat assessment, and technical tools and facilities such as cryptographic products, and network access control products such as firewalls.

PHYSICAL NETWORK

A network is defined as two or more computing devices connected together for sharing resources efficiently. Further, connecting two or more networks together is known as internetworking. Thus, the Internet is just an internetwork – a collection of interconnected networks. For setting up its internal network, an organization has various options.

WIRED AND WIRELESS NETWORKS

In a wired network, devices are connected to each other using cables. Typically, wired networks are based on Ethernet protocol where devices are connected using the Unshielded Twisted Pair (UTP) cables to the different switches. These switches are further connected to the network router for accessing the Internet. In wireless network, the device is connected to an access point through radio transmissions. The access points are further connected through cables to switch/router for external network access.

VULNERABILITIES & ATTACKS

The common vulnerability that exists in both wired and wireless networks is an “unauthorized access” to a

 ISSN: 2454-4248
180 – 186

network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection. After accessing, an attacker can exploit this vulnerability to launch attacks such as:

- Sniffing the packet data to steal valuable information.
- Denial of service to legitimate users on a network by flooding the network medium with spurious packets.
- Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a 'man-in-the-middle' attack.

NETWORK PROTOCOL

Network Protocol is a set of rules that govern communications between devices connected on a network. They include mechanisms for making connections, as well as formatting rules for data packaging for messages sent and received. Several computer network protocols have been developed each designed for specific purposes. The popular and widely used protocols are TCP/IP with associated higher- and lower-level protocol.

DNS PROTOCOL

Domain Name System (DNS) is used to resolve host domain names to IP addresses. Network users depend on DNS functionality mainly during browsing the Internet by typing a URL in the web browser. In an attack on DNS, an attacker's aim is to modify a legitimate DNS record so that it gets resolved to an incorrect IP address. It can direct all traffic for that IP to the wrong computer. An attacker can either exploit DNS protocol vulnerability or compromise the DNS server for materializing an attack.DNS cache poisoning is an attack exploiting a vulnerability found in the DNS protocol

ICMP PROTOCOL

Internet Control Management Protocol (ICMP) is a basic network management protocol of the TCP/IP networks. It is used to send error and control messages regarding the status of networked devices. ICMP is an integral part of the IP network implementation and thus is present in very network setup. ICMP has its own vulnerabilities and can be abused to launch an attack on a network.

The common attacks that can occur on a network due to ICMP vulnerabilities are:

- ICMP allows an attacker to carry out network reconnaissance to determine network topology and paths into the network. ICMP sweep involves discovering all host IP addresses which are alive in the entire target's network.
- Trace route is a popular ICMP utility that is used to map target networking by describing the path in real-time from the client to the remote host.

GOALS OF NETWORK SECURITY

As discussed in earlier sections, there exists large number of vulnerabilities in the network. Thus, during transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data, and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure.

- Confidentiality
- Integrity
- Availability

NETWORK SIMULATOR-2

After setting up the platform, software named ns2 was set up on it which was used for all the analysis and simulation work apart from other tools used. Ns2 is the de facto standard for network simulation. Its behavior is highly trusted within the networking community. It is developed at ISI, California, and is supported by the DARPA and NSF. Ns2 is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. This means that most of the simulation scripts are created in Tcl. If the components have to be developed for ns2, then both Tcl and C++ have to be used. Ns2 uses two languages because any network simulator, in general, has two different kinds of things it needs to do. On the one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets.

WIRED VS WIRELESS NETWORKS

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point.

WIRED NETWORKS

These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection.

 ISSN: 2454-4248
180 – 186

ADVANTAGES

- Physical, fixed wired connections are not pronet interference and fluctuations in available bandwidth, which can affects me wireless networking connections.

DISADVANTAGES

- Expensive to maintain the network due to many cables between computer systems and even if a failure in the cables occur then it will be very hard to replace that particular cable as it involved more and more costs.

WIRELESS NETWORKS

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs.

ADVANTAGES

- Mobile users are provided with access to real-time information even when they are away from their home or office.
- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.

DISADVANTAGES

- Interference due to weather, other radio frequency devices, or obstructions like walls.
- The total through put is affected when multiple connections exists.

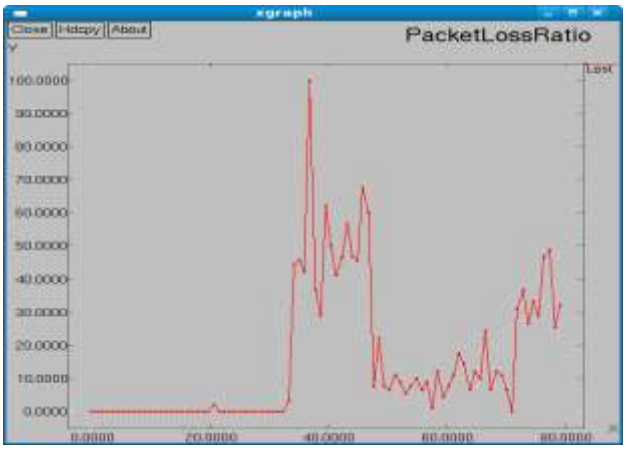
PROBLEMS IN WIRELESS COMMUNICATIONS

Some of the problems related to wireless communication are multipath propagation, path loss, interference, and limited frequency spectrum. Multipath Propagation is, when a signal travels from its source to destination, in between there are obstacles which make the signal propagate in paths beyond the direct line of sight due to reflections, refraction and diffraction and scattering. Path loss is the attenuation of the transmitted signal strength as it propagates away from the sender. Path loss can be determined as the ratio between the powers of the transmitted signal to the receiver signal.

6. PERFORMANCE AND EVALUATION

The speed of current off-the-shelf processors, especially with regard to cryptographic operations, has enabled research into schemes that require on-line cryptography. In Encrypting the Internet, researchers from Intel argue that advances in implementations of cryptographic algorithms allow general purpose processors to support ubiquitous use of transport-layer security (TLS). The Tcp crypt approach uses the observation regarding advances in cryptographic processing speeds to suggest a backward-compatible means for encrypting all TCP traffic at the end hosts. In Privacy-Preserving Network Forensics, the authors present a system called Clue which uses on-line group signatures to add device-level identification to outbound packets such that the packets can be identified later with the cooperation of the key-issuing entity

NS-2 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate “events handled at the same time” in real world, that is, events are handled one by one. Beyond the event scheduler, ns-2 implements a variety of network components and protocols. Notably, the wireless extension, derived from CMU Monarch Project, has 2 assumptions simplifying the physical world. This assumption holds only for mobile nodes of high-rate and low-speed.



Performance evaluation for Packet Loss Ratio

7. CONCLUSION

In this work, we have developed and characterized a system for effecting in-network enforcement of identity and authorization at the router using the Evasive Internet Protocol. Through the process of implementation we discovered and addressed the practical issues of

Prototyping EIP’s transient addressing scheme, most importantly describing the bounds on router state and how to overlay the protocol on the existing network stack. Our experiments demonstrate that enforcement of identity and authorization using transient addressing is possible using off-the-shelf hardware at sustained throughput rates in excess of 50 Mbps well above common Internet connection rates. We have shown that each EIP router hop in a connection path adds less than 1ms to round-trip connection setup time.

 ISSN: 2454-4248
180 – 186

It is required to fully prove the feasibility of EIP as an Internet-scale protocol. First, implementation of the DNS portion of the EIP architecture is needed to complete the characterization of the protocol. Second, a policy mechanism for control over issuing t-addresses and validity constraints is needed to enable hosts to articulate their desires to their local DNS.

REFERENCES

[1] A. Seehra and J. Naous and M. Walfish and D. Mazieres and A. Nicolosiand S. Shenker. A policy framework for the future Internet. In HotNets–VIII, 2009.

[2] D. Adkins, K. Lakshminarayanan, A. Perrig, and I. Stoica. Towards a more functional and secure network infrastructure. Technical Report UCB/CSD-03-1242, UC Berkeley, 2003.

[3] D. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker. Accountable Internet protocol (AIP). In SIGCOMM, 2008.

[4] T. Anderson, T. Roscoe, and D. Wetherall. Preventing Internet denial of service attacks with capabilities. In HotNets-II, 2003.

[5] K. Argyraki and D. Cheriton. Network capabilities: The good, the bad and the ugly. In HotNets-IV, 2005.

[6] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, and S. Shenker. Off by Default! In HotNets-IV, 2005.

[7] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh,N. McKeown, and S. Shenker. SANE: protection architecture for enterprise networks. In USENIX Security Symposium, 2006.

[8] A. C. Snoeren, T. Kohno, S. Savage, A. Vahdat, and G. M.Voelker. Privacy-preserving attribution and provenance. www.netsfind.net/Funded/Privacy.php.

[9] S. Guha and P. Francis. An end-middle-end approach to connection establishment. In SIGCOMM, 2007.

[10] A. Gurtov, D. Korzun, A. Lukyanenko, and P. Nikander. Hi3: An efficient and secure networking architecture for mobile hosts. ComputerCommunications, 31(10):2457 – 2467, 2008.

[11] Mark Handley and Adam Greenhalgh. Steps towards a DoS-resistantInternet architecture. In FDNA (ACM SIGCOMM Workshop), 2004.

[12] S. Hansell. Cablevision goes for U.S. broadband speed record. New YorkTimes, 04/28/2009. http://bits.blogs.nytimes.com/2009/04/28/cablevision-goes-for-us-broadband-speed-record/.

[13] D. Hartmann. Cisco QoS: Link fragmentationand interleaving. Network World, 03/04/2009.http://www.networkworld.com/community/node/39221.

[14] R. C. Hodgin. Gigabit broadband coming to Korea by 2012. TG Daily,02/03/2009. http://www.tgdaily.com/content/view/41292/103/.

[15] X. Liu, X. Yang, and Y. Lu. To filter or to authorize: Network-layer dos defense against multimillion-node bot nets. In SIGCOMM, 2008.

[16] J. Meisner. Comcast revs its engine in broadband-speed race. Linux Insider, 12/11/2008. http://www.linuxinsider.com/story/trends/65472.html?wlc=1256158928.

[17] R. Moskowitz and P. Nikander. Host identity protocol (HIP) architecture. Request for Comments 4423.

[18] R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. Communications of the ACM,21(12):993–999, December 1978.

[19] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y.-C. Hu.Portcullis: protecting connection setup from denial-of-capability attacks.In SIGCOMM, 2007.

[20] B. Quoitin, L. Iannone, C. de Launois, and O. Bonaventure. Evaluating the benefits of the locator/identifier separation. In MobiArch (ACMSIGCOMM Workshop), 2