Legal Perspectives on Distributed Denial of Service Attack Traceback: A Fresh Approach

Tim Goles
The University of Texas at San Antonio

Sandra G. Dykes
Southwest Research Institute

Abstract

Distributed Denial of Service (DDoS) attacks are a significant and growing problem that affects all users of the Internet. One way to mitigate DDoS attacks is to trace back the Internet Protocol (IP) packets used in the attack to their source. Knowing the source of the attack enables the victim to take immediate actions to alleviate the attack's impact, as well as uncovering information helpful in pursuing civil or criminal options. The purpose of this paper is to explore legal issues associated with IP traceback in response to DDoS attacks. The issues are illustrated in the context of a novel approach to IP traceback, based on the use of autonomous systems rather than individual routers. Stakeholders affected by DDoS attacks are interviewed to unearth their views. The results indicate that privacy and liability are the foremost issues, although it appears that the respondents' understanding of liability may not be complete. This demonstrates the need for policy decisions assigning responsibility and accountability for nefarious activities.

Keywords: Distributed Denial of Service, traceback, autonomous systems, legal issues, privacy, liability

Acknowledgement: This work was sponsored in part by the U.S. Department of Homeland Security under Contract NBCHC050093.

Introduction

A basic assumption underlying the current Internet infrastructure and its message delivery protocol is the goodwill of the user (Lee and Shields, 2002). Internet pioneers presumed that anyone sending a message would quite naturally want to provide the information necessary to receive a reply. Consequently, no safeguards were built into the Internet Protocol (IP) packet design to ensure the validity of the source address. Ultimately, this has opened the doors to a host of threats, not the least of which are Distributed Denial of Service (DDoS) attacks.
One way to mitigate DDoS attacks is to trace back the IP packets used in the attack to their true source. Knowing the source of the attack enables the victim to take immediate actions to alleviate the attack's impact, as well as uncovering information helpful in pursuing civil or criminal options. However, traceback raises a variety of technical, legal, and societal issues (Lee and Shields, 2002). The purpose of this paper is to propose a fresh technological approach to tracing back IP packets, and to explore the associated legal issues. To better explain the issues involved and our proposed solution, we begin with a brief discussion of DDoS attacks and the underlying structure of the Internet. This is followed by a review of prior traceback research, and an explanation of our approach. We then explore relevant legal issues, both from a conceptual perspective and in conjunction with interviews of assorted stakeholders affected by DDoS attacks.

**Distributed Denial of Service (DDoS) Attacks**

A distributed denial of service (DoS) attack is a deliberate action intended to prevent the legitimate use of an Internet-based activity or service. The basic idea behind a DDoS attack is to exhaust one or more resources necessary for the target to function, slowing or stopping the victim's ability to process valid requests. Although there are several different types of DDoS attacks, the basic premise is for the attacker to gain control of multiple subservient hosts and use them to send a high-volume stream of packets to a recipient. Faced with this onslaught of packets, either the victim's resources or its upstream link becomes overwhelmed, halting or severely restricting all traffic (Ianelli and Hackworth, 2005; Merkovic and Reiher, 2003).

DDoS attacks gained notoriety early in the 21st century via a series of high-profile disruptions of search engines, e-commerce sites, news bureaus (Krebs, 2003), credit card processing firms (Leyden, 2004), hosting firms (Kerner, 2004), and, most worrisome, DNS root servers that administer the domain names and IP addresses on the Web (Naraine, 2002).

According to recent surveys of tier-1 and tier-2 telecommunications carriers and IP network operators in North America, Europe and Asia, DDoS attacks remain their most significant cyber security concern. The majority of those surveyed spend more resources addressing DDoS today than any other security threat (Arbor, 2005; Arbor, 2006). This is exacerbated by the rapid growth in the use, size, and complexity of botnets.

The proliferation of readily available and increasingly sophisticated botnets has fueled the emergence of what has been termed the *miscreant economy*; an underground community that engages in cyber crime for financial reward (Cisco, 2006). This includes,

---

1 Botnets are often the focal point for launching DDoS attacks. A *bot*, short for *robot*, is an automated software program that asserts control over a remote computer and causes it to execute certain commands. A *botnet*, short for *robot network*, is an aggregation of computers compromised by bots that are controlled by the attacker. These compromised computers are often referred to as *zombies*, and botnets as *zombie armies* (CERT, 2005).

---
among other nefarious activities, stock price manipulation, attacks on competitors, and extortion demands predicated on threatened DDoS attacks (Cisco, 2005).

An underlying problem in reducing the frequency and extent of DDoS attacks is the lack of a consistently reliable mechanism for tracing an attack packet back to its original source. Without such a mechanism, instigators have virtual impunity from criminal and/or civil penalties. Furthermore, any involvement of carriers or service providers in traceback and attribution could entail some cost to them, and raise privacy and legal concerns.

**Internet Protocol and Autonomous Systems**

The Internet is an interconnection of independently owned and administered networks. These networks cooperate to deliver data packets from one source in a network to a destination in another. The path from source to destination may transit several intervening networks. Each network operates its own set of traffic routing devices (i.e., network packet switches, or routers) whose function is to select the next link in the path and forward packets toward their final destination. When a specific network is controlled and administered by an independent, autonomous entity it is termed an Autonomous System (AS). Autonomous systems may be private organizations, regional Internet Service Providers (ISPs), or large backbone providers such as AT&T or Sprint. For the purposes of this paper, the most important characteristic of an autonomous system is control and responsibility. If a DDoS attack could be traced back to the originating AS, then that organization would have the control and responsibility necessary for stopping the attack.

The Internet was designed with functionality in mind, not security. One consequence of this is that the source address field of IP packets is assumed to contain the true IP address of the machine that originated the packet. This address is generally not validated as the packet navigates the Internet (Mirkovic and Reiher, 2002). Thus the IP source address can be altered without authority or accountability, enabling a malicious user to gain anonymity by falsifying or "spoofing" the source address. This renders the IP address useless for identifying the true source. Conceptually, one way to identify the source of a spoofed packet is to trace its path in reverse (i.e., traceback), from destination to sender. Traceback is possible if monitors along the packet's path record IP header information (packet logging), or if routers add information to the packet header (packet marking) (Chang, 2002).

**Related Research in IP Traceback**

Prior traceback research has focused on a variety of packet logging and packet marking techniques. However, given current traffic volume, router processing speeds, and storage requirements, to this point none of these techniques have proven feasible for widespread deployment. Marking packet headers at each router would require a variable IP header format that substantially reduces the hardware efficiency and forwarding rate of the
router (Sanchez et al., 2001; Snoeren et al., 2002). Packet marking also requires changes to the Internet Protocol (Aljifri, 2003), something that is possible in theory, but a non-trivial undertaking in practice.

An alternative to packet marking is tasking routers to log information about the packets they process. Router links commonly used in backbone networks process up to 10 gigabits per second (Gbps), or approximately 1.25 million packets per second. At this rate, ten minutes of traffic would require 750 gigabytes of storage (Aljifri, 2003). Even taking Moore's law into account, it is clear that this is an inordinate requirement; the amount of additional storage required to retain the logged information for a meaningful period of time would be prohibitively expensive. Moreover, sorting and searching this amount of data would take large amounts of computing power and time. This drawback has led researchers to investigate the use of sampling techniques in an attempt to reduce the log size (Savage et al., 2001). Sampling works well against a denial of service attack from a single source, in which one host sends a large number of packets to the target. However, distributed denial of service attacks utilize many zombie hosts. It is unlikely that a sample would include all the zombies involved in the attack. Moreover, sampling cannot be used to trace back single packets that probe networks and systems prior to an attack. The ability to trace back single IP packets is critical for predicting and preventing attacks, and for identifying the attacker.

A recent development in packet logging is the use of Bloom filters to minimize storage requirements (Snoeren et al., 2002). In this approach, Bloom filters (Bloom, 1970) compute hash functions based on the packet header contents to set bits in a digest table, creating a packet signature. To institute a traceback, the target computer asks its upstream router to look up the packet signature in the router's digest table. If the signature is found, the upstream router in turn queries its predecessor routers. The query continues until reaching the first router in the path. Compared to packet logs, digest tables can reduce storage requirements by 2-3 orders of magnitude. However, there are two significant obstacles to this approach. First, hardware must be added to every router in the network. Given that the number of routers in the Internet core is over 100,000 (Govindan and Tangmunarunkit, 2000) this is patently impractical. Second, no single organization has full control over the Internet, making voluntary wide-spread deployment unlikely.

One outcome of prior research has been the identification of key requirements for IP traceback (Aljifri, 2003). In the following section we outline our proposed approach to IP traceback, and then evaluate it against the requirements.

---

2 Assuming an average packet size of 1000 bytes.

3 This section is, of necessity, somewhat abbreviated. For a fuller discussion of DDoS attacks and IP traceback see the following: Aljifri, 2003; Belenky and Ansari, 2003; Chang, 2002; Lee and Shields, 2002; Mirkovic and Reiher, 2002.
Autonomous System Traceback (AST)

We propose a design that conceptualizes autonomous systems (AS) as a single all-inclusive network, rather than an aggregation of smaller individual networks. We then trace packets through autonomous systems rather than through individual routers. An AS-based approach stems from two key observations. First, malicious spoofing of IP headers occurs at the source computer, not the individual routers. Second, the complete router path is irrelevant. We only need to know the path through the relevant autonomous systems. In other words, tracing a packet to its source does not require identifying every router or switch in its path. Figure 1 illustrates this concept.

Figure 1. Autonomous System Traceback (AST) Concept

Under this approach, monitoring hardware is placed at AS borders. The hardware is basically a passive monitor, similar in concept to a recording device on a voice phone line. The monitor uses an optical tap to collect packet data arriving at the AS border router. Using an optical tap guarantees that the monitor does not affect the network uptime or throughput. The monitor applies a one-way hashing algorithm\(^4\) to the packet header information. The final result of the hashing step is a set of Bloom filter digest tables. The monitor stores only these digest tables; all packet header and payload data are discarded. Bloom filters are well suited for high-speed monitoring because of their efficient data compression, minimizing storage requirements and facilitating rapid lookup operations (Fan et al., 2000).

\(^4\) Similar to one-way encryption, a one-way hashing algorithm is designed such that the resulting hash value cannot be deconstructed, or used to recreate the original header data. This is done for security and privacy reasons, as discussed later in this paper.
Each AS would also deploy a server that oversees the monitors, runs the traceback algorithm, and communicates with other AS servers. To determine if a packet traversed its network, the AST server queries each of its border monitors ("Have you seen this packet? If so, from where?"), which in turn search their local digest tables. If a monitor responds affirmatively, the AST server knows where the packet entered the AS, and therefore knows the preceding AS in the path. The process is repeated at the preceding autonomous systems until the originating AS is identified.

To illustrate this process, consider the following example (Figure 2). The victim $V$ is connected to three autonomous systems; $A$, $B$, and $C$. $V$ identifies an attack packet and sends traceback queries to $A$, $B$, and $C$. $A$ responds that it has seen the packet, and that it came from an upstream AS. The query is forwarded to that AS and the process repeated until the source is identified or until traceback halts due to insufficient deployment. The source is identified when it is known to be an edge or stub network; that is, a network that does not carry traffic from other networks. In no case is the source AS involved in the traceback. A successful traceback ends at the AS before the source AS.

Figure 2. Autonomous System Traceback (AST) Process

![Diagram of AST process]

Note that this approach also is effective even if AST is only partially deployed. To illustrate, consider the scenario where $A$ has not deployed AST. $V$ can skip over $A$ and query $A$'s upstream autonomous systems directly. This is possible because AS topology data is publicly available, since it is required for Border Gateway Protocol (BGP) routing. If the upstream ASs respond negatively, then $A$ is the source. If one of the upstream ASs respond affirmatively, then the process continues as previously described.

Simulation studies have corroborated the logic underlying the AST approach. The hardware has been designed and is undergoing validation testing. However, any proposed IP traceback method should be evaluated not only for technical feasibility, but also in light of pragmatic considerations faced by carriers and ISPs for deploying it. Prior research has identified a set of key requirements that must be satisfied for a traceback method to be effective (Aljifri, 2003). These requirements and the corresponding AST features are presented in Table 1.
Table 1. AST and Key Requirements for IP Traceback

<table>
<thead>
<tr>
<th>Key Requirements for IP Traceback (Aljifri, 2003)</th>
<th>AST Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility with existing network protocols, routers, and network infrastructure</td>
<td>AST requires no modifications to existing Internet routers, packets, or protocols.</td>
</tr>
<tr>
<td>Insignificant network traffic overhead</td>
<td>AST uses optical taps to collect packet data, ensuring that network uptime or throughput is not affected.</td>
</tr>
<tr>
<td>Support for incremental implementation</td>
<td>AST does not require full Internet deployment to be effective. Non-participating AS’s can be skipped over and traceback inquiries sent to their neighbors (see Figure 2). Furthermore, AST is scalable. On average, an Internet path contains 15-19 routers, but only 3-4 AS’s (Begtasevic and Van Mieghem, 2001; CAIDA, 2006).</td>
</tr>
<tr>
<td>Minimal overhead in terms of time and resources</td>
<td>Packet digests are collected only at the AS border routers, which directly connect one AS to its neighbor (see Figure 1). Because interior routers within the AS are not involved, deployment costs are minimized.</td>
</tr>
<tr>
<td>Effectiveness against DDoS attacks</td>
<td>In general, hash-based IP traceback is considered effective against massive DDoS attacks (Belenky and Ansari, 2003). More specifically, AST uses existing Intrusion Detection System (IDS) technology to identify DDoS probes and attacks. Traceback queries can be initiated either automatically by the IDS, or manually by an operator. Once the initial query is initiated, the process is fully automated, resulting in identification of the source AS in real-time.</td>
</tr>
</tbody>
</table>

The issues discussed in Table 1 are only the tip of the iceberg when considering any IP traceback method. There is a wide range of organizational, legal, political, and social issues that must be taken into account (Lee and Shields, 2002). In this paper we restrict ourselves to discussing the legal implications of IP trace back.
Legal Issues Associated with IP Traceback

This paper is an outgrowth of a traceback research project initiated by Southwest Research Institute (SwRI), a non-profit applied technology research institute. In the planning stages of the project, SwRI recognized that no traceback technology will be successful unless deployed by a critical mass of carriers and ISPs. Thus the project also addresses broad economic and legal issues. This paper focuses on the legal aspects of IP traceback. We illustrate the issues by examining them from the perspective of a specific approach to IP traceback – Autonomous System Traceback (AST) – highlighted by insights from interviews with affected stakeholders. The methodology used to gather data and arrive at the findings is as follows.

First, relevant legal issues were identified through a review of pertinent literature and informal discussions with practitioners, academicians, and attorneys. Second, a set of stakeholders was identified, and a series of interviews conducted. The interviews covered a wide range of technical, economic, political, and legal topics, including the previously identified legal issues. At the same time, arrangements were made with the Center for Terrorism Law (CTL), a legal research center housed in St. Mary’s University School of Law in San Antonio, Texas, for a review of the legal implications of the AST approach to traceback. The remainder of this section presents the results.

Cybercrime attackers and defenders move at Internet speed. Governments and legal systems move at a much slower pace. This results in 'cultural lag,' which occurs when technology advances more rapidly than its cultural support system, including legal and ethical standards (Ogburn, 1966). Thus there is little guidance from judicial case law applicable to IP traceback (CTL, 2006; Lichtman and Posner, 2006). Nevertheless, the significant legal issues can be grouped into three broad categories; privacy, liability, and countermeasures.

Before proceeding further, it must be made clear that DDoS attacks, and extortion based on threats of DDoS attacks, are internationally recognized as criminal activities. Thirty countries have signed the Council of Europe's Cybercrime Convention, including non-European countries such as the United States, Canada, South Africa, and Japan. This agreement defines offenses against the confidentiality, integrity, and availability of computer systems, their processing capacity, and their data. The Cybercrime Convention also addresses issues of jurisdiction, international cooperation, and extradition (Trachtman, 2006).

---

5 More information about SwRI can be found at www.swri.org.
6 The CTL specializes in legal issues associated with cyberspace and information assurance technologies. More information about the CTL may be found at http://www.stmarytx.edu/ctl/. It should be emphasized that this review is not a formal legal opinion, but rather an academic evaluation of AS traceback from a legal perspective.
Table 2. Interview Respondents

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier-1 and Tier-2 Telecomm. Firms</td>
<td>• Two senior managers, both of whom report to the Chief Security Officer</td>
</tr>
<tr>
<td>• 1 U.S. based Tier-1 firm</td>
<td>• Senior manager who reports to the Director of the network Business Unit</td>
</tr>
<tr>
<td>(multinational)</td>
<td></td>
</tr>
<tr>
<td>• 1 European based Tier-2 firm</td>
<td></td>
</tr>
<tr>
<td>(multinational)</td>
<td></td>
</tr>
<tr>
<td>Internet Service Providers</td>
<td>• Two upper level managers with responsibilities including network security</td>
</tr>
<tr>
<td>• 1 European ISP</td>
<td></td>
</tr>
<tr>
<td>Autonomous Systems Owners</td>
<td>• Director of Information Technology</td>
</tr>
<tr>
<td>• 1 U.S. based Autonomous System</td>
<td></td>
</tr>
<tr>
<td>Hosting and Content Delivery Firms</td>
<td>• Chief Network Engineer</td>
</tr>
<tr>
<td>• 1 U.S. based hosting firm</td>
<td></td>
</tr>
<tr>
<td>(multinational)</td>
<td></td>
</tr>
</tbody>
</table>

Specific to the U.S., there are several federal laws that protect the confidentiality, integrity, and availability of computer systems and data. The most significant is the Computer Fraud and Abuse Act (US Code, Title 18, section 1030). This act provides criminal penalties for several types of activities, including the creation of botnets and the instigation of DDoS attacks. It applies to any person or computer that affects interstate or foreign commerce or communication, regardless of whether or not that person or computer is located within U.S. boundaries (Schaffer, 2006).

Moving on now to the first category of legal issues, there is little doubt that many Internet users harbor significant concerns regarding the privacy of their communications and activities in the cyber world. Any traceback technology must take these concerns into account.

In the U.S., the Electronic Communications Privacy Act (ECPA) and the USA/PATRIOT Act dictate legal considerations for traceback. The ECPA generally protects the privacy of email contents. However, there is no expectation of privacy for 'transactional data' such as packet headers (Bellia, 2006; Lee and Shields, 2002). The USA/PATRIOT Act goes one step farther in explicitly stating that a "computer trespasser" (i.e., an unauthorized user of a computer) has no expectation of privacy. Internationally, the European Union's privacy laws stringently protect "natural persons" and their personally identifying information.

The AST approach abides by these standards in several ways. First, it only stores routing information gleaned from packet headers, not the packet's contents. Second, it applies a one-way (i.e., non-reversible) hashing algorithm to the header information, effectively masking any personally identifiable information. Finally, it is not designed to determine
the identity of a 'natural person,' but rather the autonomous system from which an attack originates. Thus the AST approach does not contravene U.S. or EU law in this area (CTL, 2006).

The interviewees generally were sensitive to concerns about disclosing packet contents and customer information. The tier-1 carrier went still farther, expressing reservations about even revealing that an individual customer was under attack. The fear was that such a revelation could trigger a drop in the customer's stock price, a concern that is supported by academic research (Campbell et al., 2003). The respondent was worried that his firm could be held liable for such a drop if the disclosure came from the carrier. Nevertheless, all respondents were comfortable with the notion of one-way hashing of header information, believing that it adequately protected customer privacy.

Another significant legal issue associated with DDoS attacks and traceback is liability. There is little that victims of DDoS attacks can do to protect themselves. Even the most secure systems are vulnerable. Techniques such as rate-limiting and filtering are of limited value during an overwhelming botnet onslaught (Chandler, 2004; Dittrich, 2005). Victims are likely to incur substantial losses; "...the kind of concentrated loss that would make litigation attractive" (Chandler, 2004, p. 234).

Pragmatically, it is difficult to identify the perpetrators, insulating themselves as they do behind several layers of zombies. Furthermore, they may be outside the legal jurisdiction of the victim. Targeting the intermediaries – the owners of the infected computers used as zombies in the attack – is likewise unrewarding because there are likely to be a large number of them, they are likely to be individuals or small firms with limited resources, and they may also be outside the legal jurisdiction of the victim. Thus the best option for a litigation-minded victim is "the first entity with deep pockets... a large Internet service provider" (Lee and Shields, 2002, p. 14).7

Conceptually, a compelling argument for assigning liability to ISPs is that assigning liability to the party that can best manage the risk is a fundamental economic principle (Anderson, 1994, 2001; Varian, 2000). ISPs are uniquely positioned to control the actions of their subscribers by enforcing security standards over large portions of the Internet (Alderson and Hoo, 2004; Lichtman and Posner, 2006). It may seem that holding one party liable for the injurious actions of another is inequitable, but this is a generally accepted legal response when it is impractical or ineffective to apply liability directly to the 'bad actors,' and there are related parties capable of controlling the bad actors. This is known as indirect liability (Lichtman and Posner, 2006).8

---

7 Parenthetically, we note that the distinction between Internet service providers and telecommunications backbone carriers is blurring. For example, AT&T offers points of entry to the Internet to individuals and organizations, making it an ISP. It also owns and operates a world-wide backbone network that services the Internet core, connecting to other backbone carriers. Thus for the remainder of this paper, when we use the term Internet service provider or ISP, we intend that to include telecommunications carriers as well.
8 This is also referred to variously as "vicarious," "secondary," third-party," and "downstream" liability (Lichtman and Posner, 2006).
Generally speaking, liability revolves around four linked concepts; duty, breach, causation, and damages. Duty is the prudent obligation to use reasonable care. Breach is a failure to perform duty. Causation exists when a breach causes damages. Damages occur when something is harmed (Zimmerman et al., 2002). In the case of DDoS attacks there can be little doubt that they cause damage, so the criteria of causation and damages are met. Less obvious is the standard of reasonable care underlying breach and duty. It has been argued that the failure of an ISP to provide "reasonable security" should be considered a breach of duty (Smedinghoff, 2003). Determining what is reasonable, however, can be problematic. For example, in one case a firm was found negligent for not taking reasonable care through failure to adopt a new technology, even though the firm met current industry standards without the new technology (CTL, 2006). Couple that finding with another legal precedent holding that network attacks have become so common they should be anticipated (Lee and Shields, 2001), and there is justification for arguing that even though the implementation of IP traceback technology is not an industry standard, the availability of such technology, such as AST, may be relevant in setting a new standard of reasonable care (CTL, 2006). In other words, it is incumbent on ISPs to become more proactive in protecting themselves and their customers from DDoS attacks.

Notwithstanding the above, our respondents expressed few apprehensions regarding the potential liability of their firms for DDoS attacks. The reason for this was summed up by one respondent who stated that his firm was not concerned about liability because of "carrier immunity." The notion of carrier immunity stems from legislative and judicial protection extended to telephone companies exempting them from responsibility for the content of voice communications carried over their wires. If a customer uses the phone service to plan or carry out a criminal act such as extortion, or to make threatening, harassing, or obscene calls, the phone company is immunized from liability.

In the U.S., the Communications Decency Act is the foundation on which ISP claims of carrier immunity are based (CTL, 2006; Lichtner and Posner, 2006). However, in the area of liability and immunity there is little that is black and white, but much that is grey. For example, one interpretation of the Communications Decency Act holds that in exchange for immunity the act encourages ISPs to take voluntary action to mitigate objectionable material (Lichtman and Posner, 2006). The Electronic Communications Privacy Act goes one step further, giving ISPs the right to exclude unlawful activity from their networks (Curran, 2006). Viewed in this light, if ISPs do not take steps to implement IP traceback, their claims to immunity may be weakened.

Another uncertainty relates to the blanket extension of immunity to all ISPs. The traditional tradeoff for carrier immunity is classification of telephone companies as "common carriers," which subjects them to regulation regarding services and rates (Alderson and Hoo, 2004). How this tradeoff applies to ISPs is unclear. No less an authority than the U.S. Supreme Court has found that when a cable company functions as an ISP it is not considered a common carrier, but when a telecommunications company functions as an ISP it is a common carrier (CTL, 2006). This has led to calls for clearly
defined responsibilities and liabilities among carriers, ISPs, and autonomous system owners (Alderson and Hoo, 2004; Baer, 2003; Lichtman and Posner, 2006). In fact, some commentators forcefully argue that immunity for ISPs "is difficult to defend on policy grounds and sharply inconsistent with conventional tort law principles … (and ISPs) should therefore bear some responsibility for not only stopping malicious code but also for helping to identify those individuals who originate it" (Lichtman and Posner, 2006, p. 221).

To summarize the preceding discussion of liability, our respondents are not concerned about being held liable for DDoS attacks. Their position is grounded in the notion of carrier immunity. However, there is a growing chorus of commentators arguing that ISPs have some indirect liability for all types of malicious activity, including DDoS attacks, and should take a more active role in helping to secure cyberspace.

There is another legal issue related to IP traceback. We would be remiss if we did not mention interest in the use of aggressive countermeasures against an identified attack source. We do not advocate what has been termed *hack back*, for several reasons. The primary one is the dubious legality of such an action. Generally speaking, if it is illegal for someone to attack an entity, it is also illegal for the entity to attack back (Jayaswal et al., 2002). There is also the problem of accurately identifying the true attacker. Intermediate hosts (i.e., zombies) are both victims and culprits. On one hand, they should have been more diligent about protecting themselves, making them at least partially responsible. On the other hand, they have been recruited without their knowledge, making them unwitting dupes. Any hack back that damages such intermediaries is morally and legally questionable, potentially subjecting the back hacker to civil and criminal penalties (Jayaswal et al., 2002; Schaffer, 2006). One response that seems to be acceptable from both a legal and ethical standpoint, however, is rejecting attack packets and returning them to their source. Returning rejected mail to its sender is a routine system administrative function, and does not appear to violate laws or Internet norms (Jayaswal et al., 2002). None of our respondents were in favor of unilateral action by their firms to counterattack DDoS instigators. However, several did mention the utility of a traceback method such as AST that provides forensic support for post-mortem investigation and possible prosecution. This leads to the next issue.

It is disturbing that only a small percentage of DDoS attacks are referred to authorities for investigation and prosecution (Arbor, 2005; CSI, 2006). One reason is the perception that resulting publicity would negatively impact the firm's stock price or public image (Campbell et al., 2003; CSI, 2006). Another is the lack of forensic tools and capabilities for gathering evidence, especially at the network edge (Arbor, 2005). While implementing AST will do little to assuage concerns over stock price and reputation, at least in the short term, it is designed to collect and store information that can be used post-attack to trace the path of the packets to their source AS. This capability complements calls for reporting cyber security incidents to the proper authorities (Schaeffer, 2006).
Conclusion

DDoS attacks are a significant and growing problem that affects all users of the Internet. In addition to those directly targeted, other users are impacted by degraded response time and the heightened consumption of bandwidth, imposing inconveniences and additional expenses on everyone. One approach to mitigating the effects of such attacks is IP traceback.

This paper has explored legal issues associated with IP traceback in response to DDoS attacks. A novel approach to combating such attacks – Autonomous System Traceback – was used to illustrate the issues. Perspectives on the legal issues were solicited from stakeholders affected by the attacks. Two of the more significant concerns relate to privacy and liability. Stakeholders felt that the privacy issues were adequately addressed through the one-way hashing of packet header information. There was also little trepidation about liability, based on the notion of carrier immunity. However, the applicability of carrier immunity to the broad set of ISPs is complex and far from clear. It may be that the respondents were not fully aware of all the nuances. The situation cries out for clearly defined responsibilities and accountability, and for the corresponding deployment of tools and techniques to mitigate nefarious activities.

References


