THE PROVISION OF DEFENSES AGAINST INTERNET-BASED ATTACKS

Li-Chiou Chen, Thomas A. Longstaff, and Kathleen M. Carley

INTRODUCTION

Internet-based attacks have become an important concern to the government and business since more systems are reliant upon the Internet to exchange information. Without a secure Internet infrastructure, neither E-commerce such as online purchasing nor E-democracy services such as online voting can be conducted successfully. For business, both Internet worms and distributed denial of service attacks were listed among top ten security concerns of more than 1,230 organizations globally (Ernst &Young 2004). For government, preventing Internet-based attacks has been an important issue in national plans to secure critical infrastructure (WH 2003).

Among various Internet-based attacks, distributed denial-of-service (DDOS) attacks have emerged as a prevalent way to compromise the availability of online services. These attacks have imposed financial losses for e-commerce businesses. For example, in February 2000, over a period of three days, a sixteen year-old hacker launched DDOS attacks against several high-profile e-commerce web sites including Yahoo, eBay, and Amazon.com (Tran 2000; Verton 2001). The Yankee Group estimates that the financial losses imposed by the attacks on these companies total more than $1billion (Yankee 2000). The CSI/FBI survey (Gordon, Martin et al.) shows that 17% of respondents in the last 12-months period have detected DDOS attacks and the financial loses are estimated as more than $26 million.

DDOS attacks are usually sent from wide spread sources. Since most attack tools are now designed to scan and exploit vulnerabilities automatically, the spread of attack tools is faster and easier. For example, Code-Red worm attacks in August 2001 highlight the potential risk of large-scale DDOS attacks launched from wide spread sources. Moreover, in order to generate attacks from distributed sources, these attack tools usually form a network of attack bots by exploiting vulnerable computers over the Internet. An Internet Security survey from Symantec reveals that the number of computers infected with attack bots increases from under 2,000 to more than 30,000 among their customers in the first six months of 2004 (Symantec 2004).

We investigated the technological factors and economical factors in providing defenses against DDOS attacks. We asked how Internet Service Providers (ISPs) can provide DDOS defenses to their subscribers. Many defenses that mitigate the effect of ongoing DDOS attacks have been proposed but none of them have been widely deployed on the Internet infrastructure at this point because of a lack of understanding in the tradeoffs inherent in the complex system consisted of attacks and defenses. The problem is not just technical but is a management and policy problem as well, involving the setting of policies and meeting the needs of diverse subscribers with different priorities (WH 2003; McCurdy 2004). Security services, such as Virtual Private Networks or firewalls, have been provided by ISPs as optional network services to deal with the secrecy of data transportation. In this case, the services that provide DDOS defenses ensure the availability of online services.

We will provide recommendations for subscribers, ISPs and policy makers in making decisions about deploying DDOS defenses. The effectiveness of DDOS defenses depends on many factors such that the nature of the network's topology, the specific attack scenario, and the settings of the network routers because the attacks are distributed in nature and the scale of the attacks can vary. Understanding the nature and severity of these tradeoffs will assist attack victims, network providers and public policy makers in making security policy decisions while they are assessing potential defenses against these attacks. This paper aims to increase our understanding of these tradeoffs and to derive insights that will enable a more secure infrastructure.

BACKGROUND

Distributed Denial of Service Attacks

Distributed denial-of-service (DDOS) attacks are an Internet-based attack that aims at compromising the availability of computers or network resource. A denial-of-service (DOS) attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious actions taken by another user. These attacks do not necessarily damage data directly, or permanently, but they intentionally compromise the availability of the resource (Howard 1997).

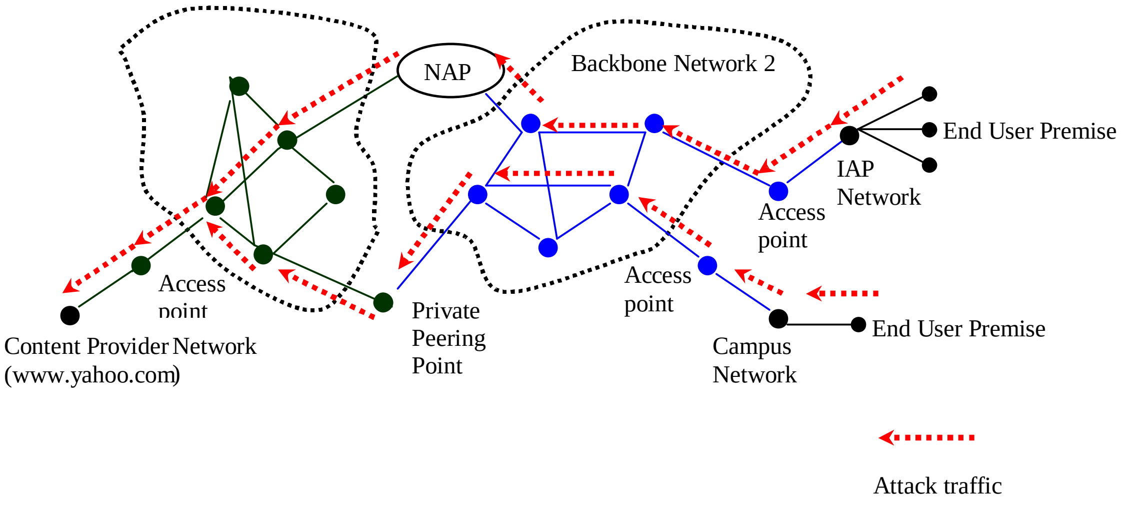

Figure1: An illustration of a DDOS attack

In a DDOS attack, an attacker could trigger tens of thousands of concurrent attacks on either one or a set of targets by using unprotected Internet nodes around the world to coordinate these attacks (CERT/CC 1999). A DDOS attack can unfold in the following way. Referring to Figure 1, suppose that DDOS attacks are launched against Yahoo's web servers from both the computers connected to the DSL line provided by the Internet Access Provider's (IAP's) network and from the computers inside the campus network in the backbone network 1. Theses computers are attack sources and the IAP network is the source network while Yahoo's web servers are attack victims and Yahoo's network is the victim network. In this example, to maintain the availability of Yahoo's web servers during such an attack, the mitigation strategy is to detect and filter out the attack traffic at some points of the routing path from the IAP network to Yahoo's network.

Several reasons have made tracing and filtering DDOS attacks difficult. First, IP spoofing conceals the true origins of attacks. IP spoofing means attackers use false source IP addresses in attack packets to conceal their origins. The source addresses of IP packets are not required for IP routing since the routers need only the destination addresses in order to forward the IP packets. Senders of IP packets can forge the source addresses in order to hide their true identities. The forged source addresses make it difficult to trace and to determine the true origins of DDOS attack traffic within the current IP routing environment. Secondly, tracing and filtering attacks is not only a technical problem but also a policy and economic problem since attack sources can be distributed across multiple administrative domains. Since vulnerability-scanning tools have been automated as mentioned earlier, attackers can exploit the vulnerable computers across the Internet and utilizes them as attack sources. As a result, attack sources can be distributed across multiple administrative domains. In this case, the attack tracing and blocking is more difficult since it involves the cooperation of multiple network providers and subscribers. Under this circumstance, the attack tracing and filtering is a policy and economic problem among various network providers. Thirdly, filtering attack traffic has a side effect on legitimate traffic because attack tools utilize various vulnerabilities in IP protocols that make it harder to distinguish attack traffic from legitimate traffic. Many tools have been used to launch DDOS attacks (Dietrich, Long et al. 2000; Dittrich 2001) and several characteristics in these attack tools make it hard to distinguish attack traffic from legitimate traffic (Houle and Weaver 2001).

Defenses against Distributed Denial of Service Attacks

In responding to ongoing DDOS attacks, a variety of defenses have been proposed. This section will provide an overview of the current solutions to DDOS attacks. A detail characterization of automatic responses against DDOS attacks is in (Chen, Longstaff and Carley 2003).

Reaction points: network-based vs. host-based

Reaction points refer to where the responses against attacks take place. Reaction points could be network-based such as those on network routers or host-based such as those on servers that the attack targets. Host-based defenses refer to the defenses that are deployed on the machines that are potential targets of attacks, and defenses are used to increase the tolerance of the targets to the attacks. The methods proposed in (Spatscheck and Peterson 1998; Yan, Early et al. 2000) are in this category. These methods can only mitigate the impact of attacks on the services that the attack targets provide but not block attacks. When attack traffic is large enough to deplete the resources used for mitigating the attacks, additional methods for blocking attacks are needed. Network-based methods are deployed on the points where packets route through the network connections to the targets, such as routers or proxy servers (Ferguson and Senie 1998; Bellovin 2000; Burch and Cheswick 2000; Savage, Wetherall et al. 2000; Stone 2000; Mahajan, Bellovin et al. 2001; Park and Lee 2001b; Ioannidis and Bellovin 2002). These methods are used to either trace or block attack traffic. Our analysis later will focus on network-based defenses.

Type of response: active vs. passive

A few defenses are designed to actively respond to the attack traffic while the majority is designed to passively trace/log attack traffic. Tracing back to the real sources of attacks has been an established part of DDOS defense studies (Bellovin 2000; Burch and Cheswick 2000; Savage, Wetherall et al. 2000; Park and Lee 2001a; Snoeren, Partridge et al. 2001; Song and Perrig 2001). These methods could facilitate future liability assignments if source IP addresses of attack packets are forged. These methods are for identifying the sources of attacks, not for stopping ongoing attack traffic. In contrast, other defenses are designed to actively reduce the amount of ongoing attack traffic (Ferguson and Senie 1998; Mahajan, Bellovin et al. 2001; Park and Lee 2001b; Ioannidis and Bellovin 2002; Sung and Xu 2002; Yaar, Perrig et al. 2003). However, even with these responses, an ISP can only trace and respond against attack traffic within the boundary of its own network. Technically, an ISP needs the assistance of upstream or downstream ISPs to stop attack traffic at another network. Legally, an ISP can only trace the suspicious attack traffic within its own network under the US Wiretap Act[1]. Our analysis later will focus on the responses that actively reduce ongoing attack traffic within the boundary of an ISP's network.

Attack traffic sampling: probabilistic sampling vs. check-everything

Since examining every packet that goes through a router may impose an enormous storage or computational power requirement, some defenses sample network packets probabilistically to reduce the number of packets to be examined and logged (Huang and Pullen 2001). Our analysis later will focus on the defenses that check everything once they are triggered.

[1] 18 U.S.C. §2510; 18 U.S.C. §2511.

Reaction timing: constant vs. event-triggered

Some defenses needed to be active all the time in order to detect suspicious packets. Egress (SANS 2000) and ingress filtering (Ferguson and Senie 1998) are deployed at local edge routers to examine all incoming and outgoing packets. However, if a defense can be automatically turned on whenever an attack is launched, the overhead could be limited to a certain time period. However, it is difficult to determine the exact timing to trigger a defensive response. A few defenses are triggered based on the congestion level of network links (Huang and Pullen 2001; Mahajan, Bellovin et al. 2001; Xiong, Liu et al. 2001; Ioannidis and Bellovin 2002). Our analysis later will model both constant- and event-triggered responses.

Detection criteria: attack signatures, congestion pattern, protocols, or source IP addresses

It is hard to distinguish attack packets from legitimate packets especially when both types are sent to the same destination. Many different criteria have been examined. Each criterion has a tradeoff in terms of the number of false positives[2] and false negatives associated with the outcome. Moreover, some criteria are only effective at identifying certain types of attack packets. For example, most intrusion detection systems detect attacks based on anomaly pattern matching or statistical measures of attack signatures (Debar, Dacier et al. 1999). The pushback method treats traffic aggregates as attack flows (Mahajan, Bellovin et al. 2001; Ioannidis and Bellovin 2002). A revised TCP state machine has been used to identify TCP SYN packet flood (Schuba, Krsul et al. 1997). A route-based method detects attack packets with spoofed source IP addresses based on the knowledge of the network's topology on core routers (Park and Lee 2001b).

[2] False positive here means the rate of mistakenly regarding normal packets as attack packets.

Deployment location: a single point, attack path, or distributed points

Deployment location refers to where a defense is placed and triggered. If a defense is placed at the firewall or the proxy server in a subscriber's network (Schuba, Krsul et al. 1997), it will help the subscriber to discover attacks but will not be effective when the bandwidth of the subscriber's network is saturated. The pushback method triggers filters along the path that traffic aggregates travel (Mahajan, Bellovin et al. 2001; Ioannidis and Bellovin 2002) if the routers on this path have deployed such a defense in advance. A defense can be gradually deployed at distributed locations across a network (Schnackenberg and Djahandari 2000; Park and Lee 2001b; Ioannidis and Bellovin 2002). To prevent the attack detection from slowing down the backbone network, CenterTrack routs suspicious traffic to an additional overlay network (Stone 2000). Our analysis later will distinguish them as source filtering (filtering at the upstream of the attack sources) and destination filtering (filtering at the upstream of the victim's networks).

THE PROVISION OF DDOS DEFENSES

A Simulation Model of DDOS Attacks and Defenses

The provision of DDOS defenses involves both technological and economical factors. Technically, the effectiveness of DDOS defenses depends on the false positives of the detection algorithms, the type of network topology, the type of attacks and whether all ISPs are compliant in establishing defenses. Economically, once an ISP decides to deploy the defenses on its network, the provision of the service is influenced by the cost of the provision, the willingness to pay of the subscribers and the cooperation of interconnected ISPs. Since little is known about the interactions among these factors, the service provision model for deploying the defenses is still unclear.

To study these problems, we built a simulation model for simulating DDOS attacks given a network topology. Figure 2 is an overview of the components in this model. This simulation tool consists of four sets of input parameters, including parameters that quantify the network scenario, the attack scenario, the attack detection, and the attack response. The network scenario parameters model how network traffic is transported on a network. Attack scenario parameters decide the number of victim networks and attack source networks for a scenario. The attack detection parameters and attack response parameters describe a given defense mechanism.

Three sets of output parameters are generated from this tool, which includes performance measures, cost measures, and topology measures. Performance measures are for the analysis on the performance impact of the defenses. Cost measures are for the analysis on the economic cost of operating the service. Topology measures are for the analysis on the correlation between network topology and other output measures.

The tool has three sets of algorithms. During a simulation, the attack generation algorithm sets the packet rate of attack traffic, selects attack sources networks, legitimate source networks and victim networks. After simulated attacks are determined, the routing path construction algorithm calculates the routing path between attack source networks, legitimate source networks and victim networks. At the end, for each attack scenario and each defense, the output measure calculation algorithm calculates performance measures and cost measures for the further analyses.

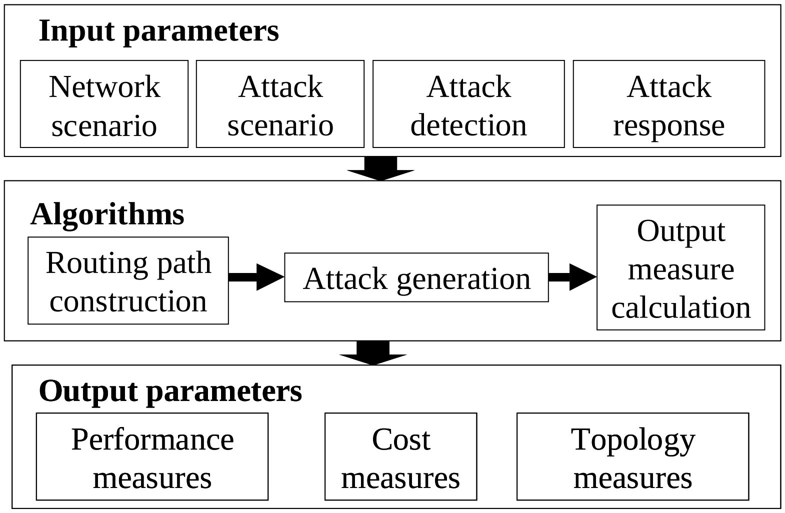

Figure 2: The Simulation Model of DDOS Attacks and Defenses

Assumptions

Using this tool, we studied three issues for providing DDOS defenses: 1) the service models for dealing with the technological uncertainty in defenses, 2) the economic incentives for providing the services, and 3) the incentives for cooperation with other ISPs. The assumptions for our analyses are as follows.

- The DDOS attacks saturate the network connections of subscribers to their backbone networks or take down servers inside the network of the subscribers.

- Network subscribers would pay based on the utility received from the defense. The utility that a subscriber derives from DDOS defenses is the expected value of losses that would be incurred from DDOS attacks.

- Providers would like to provide DDOS defenses to their subscribers if the operational benefit is larger than the operational cost.

- Statistical data about DDOS attacks to subscribers of ISPs are hard to obtain due to confidentiality and technical difficulty of data collection. The DDOS data and the Code-Red data (Moore, Voelker et al. 2001; Moore 2001) used in this study are the closest approximation to the probability of attacks using publicly available data. However, using their proprietary data, ISPs can adopt our model to estimate their benefit and cost of providing defense services. The network topology data is that of ISPs listed in (BW 2001), which is a simplified version of each ISP's actual network topology.

We analyzed the benefits and the costs of the stakeholders in the provisioning of DDOS defenses. The stakeholders include the subscribers that originate attacks (attack sources), the ISPs of the attacks sources (upstream ISPs), the subscribers that are victims of attacks (victims), and the ISPs of the victims (downstream ISPs). We provide a list of recommendations for these stakeholders as well as public policy makers based on the evidence found in our study (Chen 2003).

Recommendations to Subscribers

Several recommendations are provided for network subscribers when considering the DDOS defenses.

1) Subscribers need to recognize the attack tolerance of their online servers in order to estimate the availability of their servers during attacks. Since none of the current defenses can filter out attack traffic without posing an impact on legitimate traffic, network providers would be able to tune the defenses based on the availability of the servers to meet the needs of the subscribers. In particular, when the subscriber has a capacity that is larger

than the packet rate of the attack traffic, maintaining a certain tolerance to attacks can minimize any additional dropping of the legitimate traffic.

2) Subscribers should provide online services that are closer to where their clients are located when DDOS defenses are implemented in order to maintain the availability of the online service to legitimate clients. For example, distributed content storage systems can provide online content closer to legitimate clients.

3) Subscribers should implement defenses on the outbound traffic of an access network. The defenses will ensure the accessibility of legitimate clients to other online services, which is better than having the victim network filter out legitimate traffic.

Recommendations to Providers

To provide the defenses, ISPs need to consider the service models for dealing with the technological uncertainty in defenses, the economic incentives for providing the services, and incentives for cooperation with other ISPs. These issues are explained as follows.

Technological uncertainty

To provide DDOS defenses, ISPs should consider the following recommendations regarding technological uncertainty:

1) Network providers should design services that focus on adjusting the filtering rate of the attack traffic to meet the needs of different subscribers when providing defenses which are congestion-based and are dynamically enforced. The filter location and the filtering rate of attack traffic are the most sensitive variables for such defenses.

2) Network providers should design services that focus on the false positive rate of attack detection when providing defenses that are anomaly-based and are statically enforced. The false positive rate of attack detection is the most sensitive variable for such defenses.

3) In order to improve the quality of the defenses when attacks are distributed, network providers should cooperate with highly influential network providers. For attack detection, they should cooperate with administrative domains that have largest reachable source IP addresses. For attack filtering, they should cooperate with the ones that originate the most attacks. Possible incentives for cooperation include the increase in the quality of the defense service, the increase in reputation because conducting the best practice, and economic incentives for providing the services.

Economic incentives

To introduce the new service for their subscribers, network providers need to ensure that the operational profit in the long term would justify their capital investment. We has found several reasons to expect that the operational benefits will be higher than the operational costs of the service. Here is a sequence of actions for a provider to implement the services of DDOS defenses.

First, at the initial stage when few providers are able to deploy the service (monopoly market assumption), the provider should implement a differential pricing scheme. By doing this, the provider can benefit from the different levels of expected loss experienced by subscribers, from the different levels of the attack frequency, and the different quality of defenses demanded.

Secondly, when more and more providers are able to provide the service (competitive market assumption), no single provider can benefit from differential pricing since subscribers have more choices and can switch to another provider. In this case, the providers should consider the following:

1) Providers should set the filter location closer to the attack source since it is more beneficial for both the subscribers and the providers. This result is more significant when the network of the provider is capacity constrained.

2) Providers should provide the destination filtering service for free if the fixed cost per subscribers can be recovered from the additional income from additional subscribers to network transport services in a competitive market.

3) Providers should provide source filtering when attacks are launched at high packet rates and when subscribers that originate attacks suffer losses, such as losses due to liability assignment. Offering source filtering is more beneficial than offering destination filtering since the probability of originating attacks is higher than the probability of being attacked. This result is true even when the loss to originating networks is only 1% of the expected loss of attack victims. Source filtering is also more beneficial when the network of the provider is less connected and has a long average path length.

Recommendations to Policy Makers

The market mechanism is enough to sustain the provision of DDOS defenses. To facilitate cooperation among ISPs to reach a critical mass for providing the DDOS defense service, several recommendations are made for policy makers:

1) Policy makers should set up a program helping the industry to acquire the technologies that can detect and react against attack traffic at sources. The technologies for conducting

source filtering at subscribers' network are still underdeveloped. Even though ISPs would like to provide the services to their subscribers, the technologies are not ready at this moment. For example, Ingress filtering may not be feasible in several situations (Ferguson and Senie 1998; CISCO 2003).

2) Policy makers should provide capital incentives for highly influential ISPs to deploy the defenses once new DDOS defenses are available. Capital incentives are necessary to initiate the service provision for DDOS defenses although ISPs have an economic incentive to continue to operate the services. The initiation of the services becomes important for an overall service deployment. It is in the ISPs' interest to cooperate on the provision of the services once a critical mass is created for deploying the defenses.

3) Policy makers should consider laws that assign liability to the attack sources because liability assignment creates an incentive for subscribers to reduce the attacks originating from their networks. In this case, subscribers who subscribe to source filtering should be exempted from liability, since they have conducted the best practice[3]. To whom the liability of Internet-based attacks should be assigned is an on-going debate in both academia and public policy making. In the future, if the liability is assigned to the software companies for buggy programs and if the liability assignment manages to improve the quality of software, the benefit of deploying DDOS defenses would be reduced because the risk of Internet-based attacks would be lower. However, assigning liability to software companies may not necessarily improve the quality of software. Before the debate is resolved, we propose to

[3] Several technical issues about conducting the best practice to prevent DDOS have been documented in IETF RFC2013 (Killalea 2000) and in (Greene, Morrow, et al. 2002).

assign the liability to the sources of attacks since the liability assignment is an incentive for cooperation in providing DDOS defenses.

FUTURE TRENDS

In the future, changes in both technology and legislation would inevitably alter the assumptions upon which the conclusions are drawn in this paper. For example, adaptive attackers would result in more dynamic scenarios of attacks. Our model does not consider the situation where attackers change attack sources dynamically during an attack in order to avoid filtering. The proposed model would have to be revised to capture the dynamic strategy of defending attacks that avoid filtering or prevent routers from detecting and filtering attacks.

Several future research areas can be conducted based on our study. First, attacks to network routers or attacks that cause the instability of global routing (Cowie, Ogielski et al. 2001) are another threat to network providers. In this case, the providers are attack victims themselves. The deployment of defenses will bring more obvious performance benefits to network providers in addition to the economic benefits mentioned in this paper. Secondly, liability assignment on the attack sources should be considered as a future research issue for cyber laws. Third, calibrating the probability of attacks using security incident records is important for pricing security services. Finally, the assessment of the utility function of subscribers is important for determining the price of DDOS defenses.

CONCLUSIONS

We described our study on the technological and economical factors in the provision of defenses against distributed denial of service attacks. Recommendations are provided for subscribers, Internet service providers and public policy makers.

There are a large number of possible benefits of the tool that we developed. First, the proposed service provision framework for DDOS defenses will help ISPs and subscribers to consider the benefits of providing DDOS defenses and to recognize the tradeoffs in DDOS defenses. Secondly, the simulation model provides a systematic framework for thinking through the tradeoffs in defense strategies in the complex attack-defense system. Thus, this work has direct bearing on security policy decisions at the router level for a critical infrastructure. Thirdly, our research framework provides a new method to evaluate the costs imposed by various attack scenarios and defenses since it is neither cost effective nor ethical to conduct real world experiments of DDOS attacks on a large network. Finally, this approach provides a theoretical basis for evaluating the provision of security service, DDOS defenses in this case.

Our study has several limitations. First, the quantitative analysis in our study provides an order of magnitude benefit and cost comparison among defenses. However, the real dollar value of the cost will depend on the implementation of these defenses. Secondly, our cost model is based on the router overhead and the bandwidth consumption costs by either attack traffic or defenses. Other implementation costs are not examined since we focus on examining the operational benefit and the operational cost caused by defenses. Finally, our simulation model is intended to provide decision support for tradeoffs in DDOS defenses only. This model would need further revision to analyze defenses for other types of Internet-based attacks.

REFERENCES

[1] Bellovin, S. M. "ICMP Traceback Message." Internet Draft: draft-bellovin-itrace-00.txt, 2000.

[2] Burch, H., and B. Cheswick. "Tracing Anonymous Packets to Their Approximate Source." Paper presented at the LINUX System Administration Conference, New Orleans, LA, December 2000.

[3] BW. "Directory of Internet Service Providers." The Board Watch Magazine, Spring 2001.

[4] CERT/CC. "Distributed Denial of Service Tools." Pittsburgh, PA: CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 1999.

[5] Chen, Li-Chiou, Thomas. A. Longstaff, and Kathleen M. Carley. "Characterization of DDOS Defense Mechanisms." Computers & Security, to appear (2003).

[6] Chen, Li-Chiou. "Computational Models for Defenses against Internet-Based Attacks." Carnegie Mellon University, 2003.

[7] CISCO. "The IP Source Tracker." CISCO systems, 2003.

[8] Cowie, J., A. Ogielski, B. J. Premore, and Y. Yuan. "Global Routing Instabilities Triggered by Code Red Ii and Nimda Worm Attacks." Renesys Corporation, 2001.

[9] Debar, Herve, Marc Dacier, and Andreas Wespi. "Towards a Taxonomy of Intrusion Detection Systems." Computer Networks 31, no. 8 (1999).

[10] Dietrich, S., N. Long, and D. Dittrich. "Analyzing Distributed Denial of Service Tools: The Shaft Case." Paper presented at the USENIX Systems Administration Conference, New Orleans, LA, Dec. 3-8 2000.

[11] Dittrich, David. “Distributed Denial of Service Tools.” Available from http://staff.washington.edu/dittrich/misc/ddos/.

[12] Ernst&Young. "Global Information Security Survey." Ernst& Young, 2004.

[13] Ferguson, P., and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ Ip Source Address Spoofing." IETF RFC2267, 1998.

[14] Garber, Lee. "Denial-of-Service Attacks Rip the Internet." IEEE Computer 33, no. 4 (2000): 12-17.

[15] Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. "CSI/FBI Computer Crime and Security Survey." Computer Security Institute, 2004.

[16] Greene, Barry Raveendran, Christopher L. Morrow, and Brian W. Gemberling. "ISP Security - Real World Techniques." The North American Network Operators' Group, 2002.

[17] Houle, Kevin J., and George M. Weaver. "Trends in Denial of Service Attack Technology." Pittsburgh: CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 2001.

[18] Howard, John D. "An Analysis of Security Incidents on the Internet." PhD Dissertation, Carnegie Mellon University, 1997.

[19] Huang, Yih, and J. Mark Pullen. "Countering Denial-of-Service Attacks Using Congestion Triggered Packet Sampling and Filtering." Paper presented at the 10th International

Conference on Computer Communications and Networks 2001.

[20] Ioannidis, J., and S.M. Bellovin. "Implementing Pushback: Router Defense against DDOS Attacks." Paper presented at the Network and Distributed System Security Symposium, 6-8 Feb. 2002.

[21] Killalea, T. "Recommended Internet Service Provider Security Services and Procedures." IETF RFC2013, 2000.

[22] Mahajan, R., S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. "Controlling High Bandwidth Aggregate in the Network." Computer Communications Review (2001).

[23] McCurdy, Dave. "The DHS Infrastructure Protection Division: Public-Private Partnerships to Secure Critical Infrastructures." ISAlliance, 2004.

[24] Moore, David. The Spread of the Code-Red Worm (Crv2) 2001. Available from www.caida.org/analysis/security/code-red/.

[25] Moore, David, Geoffrey M. Voelker, and Stefan Savage. "Inferring Internet Denial-of-Service Activity." Paper presented at the USENIX Security Symposium, Washington DC, August 2001.

[26] Park, Kihong, and Heejo Lee (a). "On the Effectiveness of Probabilistic Packet Marking for Ip Traceback under Denial of Service Attack." Paper presented at the Proceedings of IEEE INFOCOM 2001.

[27] ——— (b). "On the Effectiveness of Route-Based Packet Filtering for Distributed Dos Attack Prevention in Power-Law Internet." Paper presented at the ACM SIGCOMM'01, San Diego, CA, Dcember 3 2001.

[28] SANS. "Egress Filtering V 0.2." SANS Institute, 2000.

[29] Savage, Stefan, David Wetherall, Anna Karlin, and Tom Anderson. "Practical Network Support for Ip Traceback." ACM/IEEE Transactions on Networking 9, no. 3 (2001): 226-37.

[30] Schnackenberg, Dan, and Kelly Djahandari. "Infrastructure for Intrusion Detection and Response." Paper presented at the DARPA Information Survivability Conference and Exposition (DISCEX), January 25-27 2000.

[31] Schuba, C. L., I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni. "Analysis of a Denial of Service Attack on TCP." Paper presented at the IEEE Symposium on Security and Privacy 1997.

[32] Snoeren, Alex C., Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer. "Hash-Based IP Traceback." Paper presented at the ACM SIGCOMM 2001.

[33] Song, Dawn X., and Adrian Perrig. "Advanced and Authenticated Marking Schemes for IP

Traceback." Paper presented at the IEEE Inforcom 2001.

[34] Spatscheck, Oliver, and Larry L. Peterson. "Defending against Denial of Service in Scout." Operating Systems Review, no. Winter (1998).

[35] Stone, Robert. "Centertrack: An Ip Overlay Network for Tracking Dos." Paper presented at the USENIX Security Symposium, Denver, CO, July 2000.

[36] Sung, Minho, and Jun Xu. "Ip Traceback-Based Intelligent Packet Filtering: A Novel Technique for Detecting against Internet DDOS Attacks." Paper presented at the IEEE International Conference on Network Protocols, November 2002.

[37] Symantec. "Symantec Internet Security Threat Report." Symantec, 2004.

[38] Tran, Khanh T L. "Yahoo! Portal Is Shutdown by Web Attack." Wall Street Journal, February 8 2000, 6.

[39] Verton, Dan. "Teen Hacker 'Mafiaboy' Pleads Guilty to 55 Charges." Computer World Magazine, January 18th, 2001.

[40] WH. "The National Strategy to Secure Cyberspace." The White House, 2003.

[41] Xiong, Yong, Steve Liu, and Peter Sun. "On the Defense of the Distributed Denial of Service Attacks: An on-Off Feedback Control Approach." IEEE Transaction on Systems, Man, and Cybernetics - Part A: Systems and Humans 31, no. 4 (2001): 282-93.

[42] Yaar, Abraham, Adrian Perrig, and Dawn Song. "Pi: A Path Identification Mechanism to Defend against DDOS Attack." Paper presented at the IEEE conference on security and privacy 2003.

[43] Yan, Jianxin, Stephen Early, and Ross Anderson. "The Xenoservice - a Distributed Defeat for Distributed Denial of Service." Paper presented at the Information Survivability Workshop 2000.

[44] Yankee. "$1.2 Billion Impact Seen as a Result of Recent Attacks Launched by Internet Hackers." The Yankee Group, 2000.

ABOUT THE AUTHORS

Dr. Li-Chiou Chen (lchen@pace.edu) received her Ph.D. from Carnegie Mellon University in Engineering and Public Policy. She is an assistant professor at the Department of Information Systems in the School of Computer Science and Information Systems, Pace University. Her dissertation entitled “Computational Models for Defenses against Internet-based Attacks,” utilizes a network-based simulation tool to analyze the policy and economic issues in the provision of defenses against Distributed Denial of Service attacks. Her current research interests are focused on combining artificial intelligence and agent-based modeling to conduct technological and policy analysis in the area of information security.

Dr. Thomas A. Longstaff (tal@cert.org) received his PhD in 1991 at the University of California, Davis in software environments. He is a senior member of the technical staff in the Network Situational Awareness Program at the Software Engineering Institute (SEI), Carnegie Mellon University. He is currently managing research and development in network infrastructure security for the program. His publication areas include information survivability, insider threat, intruder modeling, and intrusion detection.

Dr. Kathleen M. Carley (kathleen.carley@cmu.edu) received her Ph.D. from Harvard. She is a professor at the Institute for Software Research International, Carnegie Mellon University. Her research combines cognitive science, social networks and computer science. Specific research areas are dynamic network analysis, computational social and organization theory, adaptation and evolution, computational text analysis, and the impact of telecommunication technologies and policy on behavior and disease contagion within and among groups. Her models meld multi-agent technology with network dynamics and empirical data. Illustrative large-scale multi-agent network models she and the CASOS team have developed are: BioWar -- city, scale model of weaponized biological attacks; OrgAhead -- a strategic and natural organizational adaptation model; and DyNet -- a change in covert networks model.

ACKNOWLEDGMENTS

This work was supported in part by the NSF/ITR 0218466 and the Pennsylvania Infrastructure Technology Alliance, a partnership of Carnegie Mellon, Lehigh University, and the Commonwealth of Pennsylvania's Department of Economic and Community Development. Additional support was provided by ICES (the Institute for Complex Engineered Systems) and CASOS – the Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University (http://www.casos.cs.cmu.edu). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the National Science Foundation, the Commonwealth of Pennsylvania or the U.S. government.