

Counter Attacks as Self-Defense

Vanamala Sairam

Prof. Mahendra Kumar B

Dept. of M.C.A
Dayananda sagar College of Engineering
Bangalore, India

Abstract - The poor state of security on the Internet calls for more effective ways to protect networked systems from attacks. One solution is to be able to counter attack with offensive capabilities. With attacker information available, companies find themselves in a dilemma - counter attack for immediate self-defense, retaliate for future deterrence, inform the appropriate law enforcement authorities, or do nothing. We examine justification for the hack back SPY-defense and deterrence arguments in the context of current technology and legal framework. This paper extends discussion of issues surrounding using offensive capabilities for defensive purposes to the civilian/commercial Internet context beyond information warfare.

Keywords- Virtual anywhere, Antihack products, Traceback

I. INTRODUCTION

Computer systems today are under an unprecedented threat from Internet attacks from “hackers”. Attacks can be launched from virtually anywhere in the world and the impact level of attacks are larger. This situation calls for effective ways to protect networked systems from attacks. One example is the number of recent Denial-of-Service (DOS) attacks against high profile E commerce companies such as Yahoo and E-bay. These attacks are characterized by large amounts of traffic which overload a victim site and can be coordinated from multiple sources (distributed DOS or DDoS). Tracing a DDoS attack can be extremely difficult as a result of the nature of the attack. The attacks are launched from systems across the Internet unified in their efforts or by compromised systems remotely controlled by servers, all of which provides attack anonymity. The compromise of innocent systems occurs through the means of a hacker releasing a seemingly benign program. An unknowing user installs a program that infects higher computer and provides a backdoor to their computer for the future use of the hacker.

While Internet attacks are using more sophisticated tools, system administrators: (1) are overwhelmed trying to keep up with patches to known vulnerabilities; (2) are too busy or unable to recognize if their systems are compromised; and (3) barely able to understand the complexity of their systems [2]. Automated scripts are now identifying and compromising vulnerable systems and covering their tracks all in a matter of seconds per system. At the same time, DDoS networks of thousands of compromised systems (zombies) can target a particular system or network and disable it for a couple of hours to a couple of days. One solution is the ability to counterattack with offensive capabilities. There are clear indications that Internet security is shifting beyond passive firewall protection to a more active defense [9].

About two-thirds of one vendor’s customers are looking for ways to gain leverage over attackers including tracing, trapping, and counterattacking; “I’m not sure about fighting back in terms of counterattacking, but in terms of defending yourself we’re just beginning to scrape the surface of defensive measures and tools.” Ruth Lestina, Predictive Systems [8] The timing of the decision to hack back is crucial with the mobility of the attacker and economic losses mounting. In addition, since September 11 2001, an Internet attack may actually be considered a terrorist act or an act of war. The Pentagon’s current passive policy of prohibiting the US.

Military from mounting a counterattack was criticized by a 1999 report issued by the National Research Council (NRC) stating it may result in “severe consequences for US military capabilities” [6,14]. Under this policy, the US military can only track Internet attacks and when the attacker is identified must transfer the responsibility of prosecution to law enforcement officials. Both [21,22] show how maintaining a credible ability to use force on the Internet is lawful and a fundamentally important aspect of deterrence. There have been two documented accounts of hack back incidents.

The first documented hack back occurred in September 1998 when the Pentagon reacted to a browser-based denial-of-service attack by the Electronic Disruption Theater (hactivist organization) by using offensive applets to shut down the attacking browsers [13] However, this offensive strike against hackers was against a military prime directive which, forbids the military from taking unilateral actions within the U.S. and against U.S. citizens and was unapproved by Pentagon lawyers since the net effect is that both attacker (original DOS) and victim (back-hacking) broke the law. The second documented hack back happened during the World Trade Organization (WTO) summit in January

2000. The WTO server hosted by Conxion Inc. (of San Jose CA. USA) was hit by a denial-of-service attack launched by the self-proclaimed Electro hippies (E-hippies), a U.K.-based online activist group. Conxion traced the IP trail directly back to the E-hippies server and read postings encouraging E-hippies to mail-bomb the W O . Instead of filtering these incoming packets at the router in a typical defensive firewall tactic to stop denial-of-service attacks, Conxion redirected the mail bomb packets back to the E-hippies server disabling it for several hours. Conxion was so proud of its defensive tactics that it issued a press release [18]. A typical counterattack would be to cut off the attack as close to the source as possible by contacting relevant Internet Service Providers to filter specific packets once these packets are identified.

A counterattack designed especially for deterrence may consist of the following: sending a “message” to the identified attackers that you detect an attack, you do not welcome the attack, you know the identity and virtual Vphysical locations of the attackers, and if you attack us again you will be prosecuted. The remainder of this paper examines the use of back-hacking in more depth and is organized as follows: Section 2 describes the state-of-the-art in technology that determines available hack back options. Section 3 outlines the major problems with a hack hack option. Section 4 speculates on social ramifications of legitimizing hack back. Lastly we close with a summary and conclusions in Section 5.

II. TECHNOLOGY

1. Traceback

While in the past companies may have taken weeks or even months to trace an attacker, recent. Technological trace back capabilities seek to identify the course of an Internet attack within seconds. It is generally too late if an attack is already impacting a system or has stopped. Systems in this position have no recourse but to filter attack packets and try to reconfigure their system in real-time. Without effective intrusion source tracing, no effective countermeasures such as containment, redirection, or back-hacking can be implemented. The attacker can log-in through a series of hosts (chained. connections) before attacking the eventual victim, making it extremely difficult to trace back the real source. Therefore, the reason for lack of active back-hacking at present is the lack of source tracing but this is changing rapidly. The fundamental problem is that most Internet attacks are very short which leaves very little time for trace back. Manual intrusion source tracing in Internet is extremely difficult, if not impossible yet most current intrusion detection systems have left trace back untouched and primarily a manual effort. Most computer emergency response teams (CERTs) make little or no effort to traceback an attack to the source once an

intrusion has been reported to them (usually they trace back one hop to identify zombies used in the attack). The remainder of this section summarizes current trace back research. Firewalls or intrusion detection systems have the capability to capture all incoming IP addresses (in a revolving storage) that can be used to start a trace. The problem is that most Internet attacks are not direct but instead come indirectly from other compromised computers owned by innocent and unaware participants. Thus tools are needed to untangle an attack path back to the ultimate IP packet source given indirect, spoofed, and encapsulated packets coming from compromised computers. If all Internet Service Providers (ISPs) were to coordinate mechanisms for preventing IP source spoofing (which is technically possible) then IP trace back or source identification would be solved but unfortunately this is not the case and may never be the case. While there has been work focused on detecting DOS attacks and mitigating their effects upon the victim, these approaches do not eliminate the problem or deter potential attackers. However, there have recently been a number of technical papers attempting to solve the problem of tracing the physical source of a DOS attack.

Knowledge of the source of a DOS attack via a trace back capability has the possibility to both deter and eliminate DOS attacks altogether with prosecution and/or counter-attack. ISPs typically manage and monitor their networks from a centralized network management system. DOS attacks would manifest themselves as unexpected increases in traffic based on long-term trend analysis. [5] Proposes an SNMP mib variable he created so standard network management tools could track DOS attacks. ISP UUNET proposes an IP tunnel overlay network for logging “interesting datagram’s” directly to a mesh network of special hacking routers [17]. This solution, referred to as Center Track, may be feasible for a single provider’s backbone network but has high storage and processing overhead. The MCI Security Team uses a program to detect DOS attacks that starts on border router and propagates to neighboring routers until the source of a DOS attack or the bordering ISP is identified [5].

While network routers can be used to reconstruct a packet’s path through the network if detailed logging is enabled (and the logs themselves are not attacked and erased), packet marking is viewed as a form of “stateless logging” greatly reducing the amount of overhead necessary to trace back. Deterministic packet marking puts source information permanently within each outgoing IP packet. The significant drawback of this approach is the increasing packet header size requirement that grows linearly with hop count [7]. In probabilistic packet marking [12] and router stamping [3], each router probabilistically inscribes partial path information onto traversing packets during packet forwarding. This

corresponds to probabilistically “sampling” the attack path using a constant packet header, independent of hop

count. [7] shows that probabilistic packet marking can localize possible attackers to between 2-5 sites given single source attacks but under distributed DOS attacks. [20] proposes an active intrusion response technique called “sleepy watermark tracing” which becomes active upon detection of an attack signature to inject watermark into a backward connection with collaborating routers along the attack path to trace back to the source using correlation. The Internet Engineering Task Force (IETF) ICMP Traceback working group (itrace) created in March 2000 and chaired by Steve Bellovin is considering a proposal for routers to generate authenticated trace back messages (with low probability) to be sent along to the destination [1]. With enough traceback messages from enough routers along the path the ultimate IP source and packet path can be reconstructed.

There is the possibility that some or all traceback messages could follow a different path from the attack path and be blocked by a firewall or other policy routing device. There remains the possibility that if a router is compromised, it can forge markings from other uncompromised routers and hence subvert the destination machine’s path reconstruction. Even worse, the destination machine will not be able to tell if a router is compromised just from the information in the packet it receives. [16] addresses this problem with a computationally efficient authenticated marking scheme that preserves traceback integrity such that even a compromised router cannot forge or tamper markings from other uncompromised routers.

2. Current “Anti-Hack” Products

First note when marketing products with counterattack capabilities, the term “anti-hack” is used as opposed to “back-hack” for liability reasons. While security vendors would not publicly recommend a counterstrike using their product, privately they boast that their product has significant retaliation capabilities that, if used correctly, can have devastating impact. Some Linux products, as well as FreeBSD, ship tools that can be used to counterattack such as Trojan horses (hidden executable programs) and port scanners. However these tools can also be very dangerous if mis configured or directed at an innocent party. Future vision of Sante Fe New Mexico has unveiled a security system it calls Blitzkrieg that is designed to retaliate against an attacker [11,19]. Blitzkrieg is installed on a central server from where it places small “daughter” programs on machines that are part of the network it is meant to protect. There are separate business and military versions of Blitzkrieg: the business version hacks back with a DOS designed to overload the attacker’s machine; the military version

goes one step further by also launching a virus counterattack in an attempt to destroy data on the attackers computer. Laurence Wood, Chief Scientist of Network Waffen Und Munitions fabriken (Network Weapons Munitions Factories subsidiary of Futurevision) and Blitzkrieg’s inventor states, “Out internal system exercises show that a collective Blitzkrieg server offensive is similar to an attack of a biological killer virus with an overall collective objective and agenda” [11]. Two startup companies, Mazu Networks in Boston and Asta Networks in Seattle, have proprietary auto detection software that stops a DOS attack at the ISP level. The M a d A s t a approach is to detect and contain a DOS attack before its leaves an ISP and impacts a destination victim (Ecommerce server) [15]. Since ISPs can withstand DOS attacks due to large capacity backbones (with some degradation of service), then an There is, however, a fine line between reactive forward-looking self-defense and aggressive backward-looking countermeasures.

Back-hacking combines both elements. Backward-looking retributions are popularly associated with revenge and vengeance and strictly illegal. Forward-looking retributions are popularly associated with self-defense and prevention. But the goal of prevention also raises the practical question: What means may be employed to prevent (an Internet attack)? We can imagine stopping Internet attacks in a degree of violence that would be excessive and reprehensible. “By any means necessary” is not an adequate answer. “If ... functioning solely within their own system to take preventative action during an attack, there should be no problem. Rejecting mail is a normal system administration function. ... Returning ‘mail to sender’ does not constitute a crime. ... Now if they were inserting their own mail and sending that back to the site, you may have a problem.”

Chris Malinowski, the retired lieutenant commander of the New York Police Department’s Computer Crime Squad [8,10], attack can be stopped before it creates a problem. The Mazu/Asta approach has two drawbacks: (1) it requires ISPs to purchase their auto detection software at an edge or point-of-presence (POP) router - an extra cost that ISPs may not feel is justified and (2) identifying the distinction between attacks and normal traffic based on packet characteristics. One classic example of a DOS attack signature is numerous packets simultaneously heading to one server but there are legitimate packet streams that also have these characteristics - website contests, streaming media, E-Trade after an unexpected business announcement. Bind view sells a tool called Zombie Zapper to respond to DOS attacks. Instead of returning the DOS attack back to the closest zombie, it impersonates the “master”

of the zombie and sends an order to those slaves to stop sending DOS packets [IO]. Of course an order could also be given to send DOS packets back at the source. RSA Laboratories is developing a protocol that can be classified as both defensive and offensive in response to a well-known class of DOS attack called the "TCP SYN flood connection depletion attack" [4].

A connection depletion attack is one in which the attacker seeks to initiate and leave unresolved a large number of connection requests to a server, exhausting its resources and rendering it incapable of servicing legitimate requests. The "client puzzle" protocol under development does nothing under normal circumstances but when under attack the server sends each client wishing to make a connection a unique client puzzle based upon time, server secret, and client request information [4]. In order to have server resources allocated to it for a connection, the client must submit to the server a correct solution to the puzzle within a time-out period [4]. Thus while legitimate clients will experience only a small degradation in response time, attacking clients loaded with puzzles are most likely disrupted. Cryptographic puzzle challenge-response protection has also been proposed for defending against junk mail.

III. PROBLEMS WITH BACK-HACKING

There have traditionally been two different justifications for retaliation - one is backward-looking approach and one is forward-looking approach. The backward-looking approach justifies retaliation purely in terms of meting out punishment. The idea is that one who does harm deserves to suffer appropriate punishment in order to "right the wrong" and restore the moral balance. The forward-looking approach justifies retaliation as a means of bringing good consequences such as preventing or deterring further violence or (in some cases) reforming and/or rehabilitating the wrongdoer. For both approaches there is also a requirement to punish only the guilty and to do so in proportion to the crime.

1. Incorrect Identification

A main concern is accidentally slamming innocent sites through which hackers have routed their attacks to conceal their identity [XI]. This is a problem that will not disappear with advances in technology since it is an escalating game between an attacker and the pursuer. 'My fear is that US. Government agencies [involved in information warfare] will build in react capabilities. smart hacker will launch a [denial-of-service] attack using those agencies IP addresses and they all start attacking each other. The worst case is Amazon shoots eBay who shoots the IRS who shoots

Cisco who shoots. "-John Pacatore. Gormer Group Analyst [8]

2. Liability

Most company executives with fiduciary responsibilities to their stockholders, government regulators, and anomeys would never expose themselves to civil and criminal charges by allowing counterattacks. In general if it is illegal for someone to attack you, it is also illegal for you to attack them. Just because a victim hack backs an attacker does not make it any less of a crime in the eyes of the law. "Launching a counterattack is very difficult because of all the liability issues that come up. ... what if the attack comes from a boundary outside the United States and I act against it?" - Pete van de Gohm, Director of Information Asset Protection at ENon Energy Services Inc.

[SI "Don't hack back. If you do anything that can be perceived as intrusion or denial-of-service and you contact the police, you've just made it really easy for the police to arrest you." -Ira Winkler, President of Internet Security Advisors Group[B] Following an IP address across the Internet means passing through every server the attacker has compromised. Since each of these servers is privately owned you need permission or else you are trespassing. In his book, Tangled Web, Richard Power asserts that as far back as 1994 when the US. Air Force Research Laboratory in Rome New York was under attack, agents grappled with tracking attackers through a maze of private servers. Anti-hack vendors have considered trespassing when designing their tools but the effectiveness of their tools is questionable. In order to traceback and identify the attacker, traces must occur during a live connection. The solution for Recourse Technologies ManHunt product is to pass a digitally signed Email message upstream to predestinated points-of-contact which requests the recipient to read the mail and respond. Of course this response and time constraints limit the value of this approach. If, however, the upstream service provider were running ManHunt software already, traces could occur in real-time.

Lastly, the compromised machines or zombies are in a unique position: they are both victims and culprits. The question is - Are they victims that could have protected themselves? No one appears yet to have sued a third-party site for being used to perpetrate an Internet attack. Because most hackers are presumed to be judgment-proof, there is a consensus that it is only a matter of time before companies that suffer damage from attacks start to "move up the food chain" [IS]. The issue in such a suit would be whether the computer owner had a duty of care to the ultimate victim(s). There have as yet been no test cases. "Whether there's a duty depends on whether the courts think there should be. As the damage to others increases, I think courts will have less and less patience

for the argument] that there's no du ty.... People hacked into these computers using known holes in most cases. If you maintain security against known hacker attacks, then it's much more difficult to plant the code that allows your server to be turned into a zombie." Stewart Baker, Partner in the Law Firm Steptoe and Johnson LLP and former General Counsel for the NSA [15]

3. Law Enforcement Option

Typically, the website owner calls in a security expert after an attack and this expert starts following the electronic trail by examining packets. This can range in time from several hours to 48 hours. Every hour the security expert spends trying to find the attacker and cutoff the attack is another hour the victim is off the Internet accumulating huge losses along with a stigma attached to company stability reliability. The result is often the identification of a zombie used by the attacker but the not the source attacker.

If you do report the crime to the police, be prepared to show law enforcement that the cost of the crime meets the investigative threshold that varies depending on the law enforcement involved. For this reason, despite the difficulty you must quantify your loss in monetary terms. Unless your company is a large organization - multibillion-dollar company that is publicly traded and frequently in the media - whatever help is forthcoming from agencies like the FBI will take a relatively long time especially in "Internet time". Acting as your own forensic security analyst can accomplish more in less time if qualified staff is available.

IV. FUTURE SCENARIOS

The effects of legitimizing hack back as self defense can be categorized into two extremes: protected E-commerce and public access to information versus a chaotic Wild West scenario. In the optimistic scenario, legal hack back provides deterrence and remedy for Internet attacks. Attacks are not initiated since retaliation is severe and certain. Prevention of attacks will rely more on protecting innocent systems from being used remotely as zombies than protecting target systems. Legal remedies will exist but will not be frequently used because everything is handled at the time of attack.

Part of this scenario is already happening. In the pessimistic scenario, legal hack back encourages vigilante action over legal remedies in an analogy to the Wild West. Companies protect themselves using hired gunslingers (Wells Fargo private security) to hack back at attackers since the law is too slow and not much of deterrence. Innocent bystanders (zombie computers) are treated as accomplices worthy of retribution if their security allows an attack to be directed through their machine. The biggest gunslinger may well be a sanctioned ethical hacker (Wyatt Earp) but there are too

few to monitor the entire territory (Internet). A small number of traveling judges on horseback (virtual organization) may hear cases that are prosecuted but this is not a high percentage of cases. In most cases (those businesses that cannot hire a gunslinger and the public-at-large) victims pool their resources to form a posse to track down the attackers and provide justice themselves. Other Wild West market-based solutions include insuring assets in terms of armored cars (hardened sites) and "hacking insurance". Part of this scenario is already happening. One window may be a popular game called Hack. Back "The City is in danger. .. An evil hacker is on the loose .. . You are the only one who can stop him!".

V. CONCLUSIONS

So what is the solution to Internet attacks? This paper posits that one solution is to build an offensive posture. If legalized, industry will design a set of hack back tools that will stop Internet attacks. Is it not self-defense to protect your assets under attack even if it means striking your attacker? But is this the right direction? Future Internet scenarios from the widespread use of back hacking vary from peace to chaos. If not legalized, hack back tools will continue to evolve and be used covertly since legal remedies against attackers do not yet exist on "Internet time".

We have identified several significant technical problems (trace back) with back-hacking that make it impractical at present but technology is advancing rapidly and these problems may disappear. The more challenging problems are social identification, legal liability, and law enforcement. There are certainly some cases when hack back is permissible - when life is threatened (maybe the "life" of a shut down Ecommerce dot.com), however, the worse case scenario beyond the Wild West analogy is self destruction. With hack back tools legalized and attacks/counterattacks rampant, the integrity of the Internet may be undermined. Current attacks on websites may turn to infrastructure attacks on entire business sectors. Applying common law to the Internet to distinguish an illegal counter attack from a valid self defense is needed

REFERENCES

- [1]. S. Bellovin, "ICMF" Traceback Messages," IETF Internet Drdr, March 2000. draft-bellovin-itrace-OO.txt
- [2]. D. Dittrich, "Fighting the Rising Tide," excerpted from annicle appearing in Information Security, November 2000.
- [3]. T. W. Doepfner, P. N. Klein, and A. Koyfman, "Using Router Stamping to Identify the Source of IP Packets," The ACM Conference on Computer and Communications Security (CCS), Athens Greece, 2000, pp. 184-189.

- [4]. A. Iuets and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," Network and Distributed System Security Symposium (NDSS). Internet Society Press, 1999, pp. 151-165.
- [5]. K. Moria, "DDoS Incident Handling: Management Information Base to Trace Incidents - Revision I," IETF Internet Draft. March 2000. draft-moria-ndss-ddos-mib00.txt
- [6]. National Research Council, Computer Science and Telecommunications Board, Realizing the Potential of Fundamental Challenges, National Academy Press, 1999.
- [7]. K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Trace back under Denial of Service Attack," IEEE Info com, 2001. (an earlier version is Purdue University, Network Systems Lab and CERIAS, Dept. of Computer Sciences, Technical Report CSD-TR-00-013, June 2000.)
- [8]. D. Radcliff, "Should You Strike Back?" Computer World, Nov. 13, 2000. 191 D. Radcliff, "Can You Hack Back?" Network World, June 1, 2000. [IO] D. Radcliff, "Hack Back" Network World, May 29, 2000.
- [9]. C. Robinson Jr., "Make My Day Server Throws Gauntlet to Network Hackers," Signal Magazine, May 1998.
- [10]. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Support for IP Traceback," ACM SIGCOMM, Stockholm Sweden, 2000, pp. 295-306. (an earlier version exists as Dept of Computer Science and Engineering, University of Washington, Technical Report UW-CSE-2000-02-01)
- [11]. W. Schwartau, "Honeypots Wreak Sweet Revenge Against Cyber Intruders," Network World, Dec. 4, 2000, p. 63.
- [12]. W. Schwamu, "Can You Counter-Attack Hackers?" Network World, April 7, 2000.
- [13]. R. Shepherd, "Getting Hacked Could Lead to Getting Sued," American Lawyer Media News Service, March 2, 2000.
- [14]. D. X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback." IEEE Info com, 2001. (an earlier version is Computer Science Division (EECS), University of California at Berkeley, Report No. UCB/CSD-00-1107, June 2000)
- [15]. R. Stone, "Center Track: An IP Overlay Network for Tracking DOS Floods," USENIX Security Symposium.
- [16]. R. Tadjer, "Detect, Deflect, Destroy," Internet Week, Nov. 13, 2000.
- [17]. M. Ward, "Don't Hack Back," New Scientist, May 30, 1998.
- [18]. X. Wang, "Survivability Through Active Intrusion Response," IEEWSEI/CERT 3d Information Survivability Workshop. October 2000, pp. 173-176.