Intel
Research
and
Development

Elimination of Distributed Denial of Service Attacks using Programmable Network Processors

Version 1.0

June 2002

David Durham[+], Priya Govindarajan, Dylan Larson[#], Priya Rajagopal, Ravi Sahita

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

[+] Email: David.Durham@intel.com

[#] Email: Dylan.Larson@intel.com

Elimination of DDoS Attacks using Programmable Network Processors

June 2002

Introduction:

Denial of Service attacks represent an ever increasing, ever changing threat to productivity and profitability on the Internet. The scope and severity of these attacks is only limited by the imagination of their creators. To cope with these threats, a highly distributed and flexible solution must be deployed. Processing power and programmable silicon in the network represents the foundation for deploying such a solution.

The Internet has become highly vulnerable to a number of different types of attacks. Using backscatter analysis, scientists from CAIDA and UCSD have observed "12,805 attacks on over 5000 distinct Internet hosts belonging to more than 2000 distinct organizations during a 3 week period". The most common type of attack is the Denial of Service (DoS). In Denial of Service attacks, the attacker exhausts resources (like CPU, network bandwidth, available ports etc) of the victim by sending illegitimate traffic thereby denying service to legitimate users.

According to the SANS institute [SANS], "Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000. According to bookseller Amazon.com, its widely publicized attack resulted in a loss of $600,000 during the 10 hours it was down. During their DoS attacks, Buy.com went from 100% availability to 9.4%, while CNN.com's users went down to below 5% of normal volume and Zdnet.com and E*Trade.com were virtually unreachable." Yankee group analysts estimate that the total impact of Denial of Service attacks in 2000 topped $1.7 billion.

A key problem in detecting denial of service attacks is that the source address of the packets is spoofed. This ensures that the compromised machines remain undetected and thereby can be used for other attacks. Even when ISPs properly employ egress and ingress filtering, an attacker can still spoof addresses within their domain. This type of filtering is expensive to deploy and is not commonly implemented. Such filtering also limits mobility and tunneling capabilities for customers.

If the source of the attack is kept constant (even if it is spoofed), it is possible to block that particular address and recover from the attack. However, the attack now takes a new form by being distributed (DDoS). In this form, a number of compromised systems all over the world are used in a synchronized manner to attack a particular server. By distributing the attack, the intensity near the source is lessened and is therefore not detected there. Meanwhile, the concentrated effect at the victim is sufficient to overload networks and systems and thus deny service.

Different types of Attacks

The following are a few of the types of attacks that have readily occurred on the Internet:

- **Ping of Death:** In this attack the attacker sends fragmented IP packets with overlapping offsets that cause some machines to hang.
- **SYN Flood:** TCP connection establishment is dependent on a three-way handshake. In this attack, the attacker does not complete the third part of the three-way handshake for TCP thereby causing the attacked server's TCP stack to set aside resources that don't get freed. Thus, the server runs out of resources for valid connections and service is denied to legitimate clients
- **LAND Flood:** Similar to SYN flood but the attacker sets the source IP address to that of the target's IP address. So the System becomes unavailable while it is trying to reply to itself.
- **SMURF Attack:** Attacker uses an amplifier network and sends a directed broadcast Ping to the network. [ICMP] The attacker sets the Source IP address as that of the intended victim. If the network is not configured correctly, all the machines in the network will respond and the replies will be directed to the target causing a flood of traffic on the network bringing the victim off-line.

The above is only a tiny snapshot of possible attacks and their variations. More information on Denial of Service attacks can be found at [SANS] and [CERT]. The type of attack keeps changing as solutions for the old attacks are found (e.g. Worm-initiated DDoS attacks such as Code Red have recently wreaked havoc in the Internet). Attacks can also target operating systems, protocol stacks, and applications as well as the network infrastructure. It is necessary, therefore, to have a solution that is programmable and intrinsically adaptable to the ever-changing threats to a network environment.

Programmability in the Network

The Internet is a set of interconnected heterogeneous computer networks. In order for these networks to communicate deterministically, communication protocols are standardized in standards bodies like the [IETF]. These protocols are a set of published rules that specify the structure of the information on the wire and their associated semantics. Like any design, protocol specifications have bugs or weaknesses. Protocols are sometimes used in ways they were not intended which results in invalid behavior of the end systems. Errors in protocol implementations sometimes introduce weak points in an otherwise sound specification. These errors can cause failure of the services using the underlying protocols. A malicious client, server or peer node in the network can misuse various facets of the protocol. With the Internet usage becoming more and more mission critical, a large number of miscreants can launch coordinated attacks on the protocol implementations and eventually on the businesses relying on the Internet. Many of these attacks, as explained in the previous section, take the form of Denial of Service attacks, which try to deplete the prime resources of e-businesses, including its servers and communication infrastructure, like routers. These attacks are coordinated and distributed in nature and thus take advantage of the ever-increasing speed of the compromised nodes and the increasing bandwidth available.

To take counter-measures against such attacks, the capability is needed in network devices to monitor and collect statistics for the new protocols used in a network. This data is used to baseline a network's *normal* behavior and to thus be able to flag *deviant* behavior as would be seen during an attack/misuse. The requirements for such a flexible framework are that it should be able to keep up with wire speed in order to not impact network performance and, at the same time, the system should be highly configurable since new attacks are constantly being developed and old attacks are updated to work around the fixes. These requirements are met by Network Processors used to build smart devices in the network, which can be programmed to adapt to new attacks and apply new heuristics while not sacrificing performance. A programmable framework can also analyze network usage in ways appropriate to other network resource utilization applications—for example, load balancing, bandwidth on demand, and traffic engineering. This adaptable functionality is in addition to the common tasks of routing, switching, and so on.

Intel® Internet Exchange Architecture is a packet processing architecture focused on network processors. These network processors give a high performance gain due to a set of programmable, hardware multi-threaded microengines. The microengine clusters provide the processing power to perform tasks traditionally reserved for high-speed ASICs, with the added advantage of flexible programmability. The instruction set for the microengines is specifically designed to forward data efficiently in networking and communications applications. The parallel processing of the microengines enables network application designers to divide the tasks into high performance functional building blocks. With software-based dispatch loops that tie together blocks, programmers achieve reuse of functional blocks across various network applications. Newer blocks can also be added to an existing microengine-based application at runtime. The microengines give the programmer the capabilities of full programmability, scalability and wire-speed performance to design applications for intrusion detection, automated traffic engineering, and stateful firewalling.

A Distributed Feedback and Programmable Network Control Solution

In the previous sections, we discussed several well-known forms of DDoS Attacks and the serious threats that they pose to today's computing environment. In this section, we discuss an adaptable distributed framework that can be used to automatically detect and counter such attacks. This distributed solution has been developed by Intel Research and Development and is shown in Figure 1.

The system consists of the following components:

- Smart-Links (SL) are programmable network devices based on Intel network processors and other networking silicon capable of actively and passively monitoring the network and collecting statistical information. The SLs periodically report the locally analyzed and summarized information, to a Network Health Control Center (NHCC). By using Intel's network processors, Smart-Links can maintain programmable flexibility without sacrificing performance. In this framework, the SLs are distributed across the network—typically at the edges of the network.
- The Network Health Control Center (NHCC) is the central management server responsible for configuring, controlling and receiving feedback from the SLs using the IETF's Common Open Policy Service (COPS) protocol. The COPS standard and its features are described in the IETF RFCs 2748, 3084 and 3159. See also [COPS-NC] for more information on COPS.
- NHCCs communicate using the Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML). This allows simplified peering relationships across domains for reporting and tracing attacks through the Internet. See [SOAPSPEC] and [XML] for more information.

The SLs work together with the NHCC to form a distributed, fully-programmable, closed-loop network control system that can be used to automatically detect, trace and eliminate a DDoS attack.

To deal with DDoS attacks, Intel Lab's solution comprises the following steps:

1. **Detection of anomalous traffic patterns by the SLs (Figure 1: A, B, C and D)**:
   The SLs are capable of constantly monitoring the network traffic and are appropriately programmed to detect anomalous traffic patterns—for example, incoming ICMP broadcast packets and sudden surges in unacknowledged TCP SYN/ACK packets to specific servers. Such anomalous conditions constitute the signature of the attack and are reported to the NHCC.
2. **Identifying the Attack Signature at the NHCC**:
   The NHCC is then responsible for correlating and analyzing the statistical information collected at each of the SLs in its domain that have reported anomalous traffic conditions. The result of the analysis would be information that constitutes the attack instance data. The NHCC is itself programmable and can quickly be adapted to detect and deal with emerging threats.
3. **Automatic Trace Back of the Attack to the origin (Figure 1: E):**
   The NHCC correlates the statistics seen at the various SL's to re-trace the path of the attack through its domain. The NHCC is also responsible for communicating the attack signature and attack instance data with peer NHCCs in different domains through a SOAP/XML interface. These peer NHCCs use this data to recursively trace an attack through the Internet—even after the attack has already finished.
4. **Thwarting of the attack at its source (Figure 1: F):**
   Once the local NHCC identifies the source of the attack, it is responsible for appropriately configuring the SLs close to the source to stop or throttle back traffic that contains the attack signature. The attackers are isolated from legitimate customers, the attacking traffic is shutdown, and the network resumes normal operations.

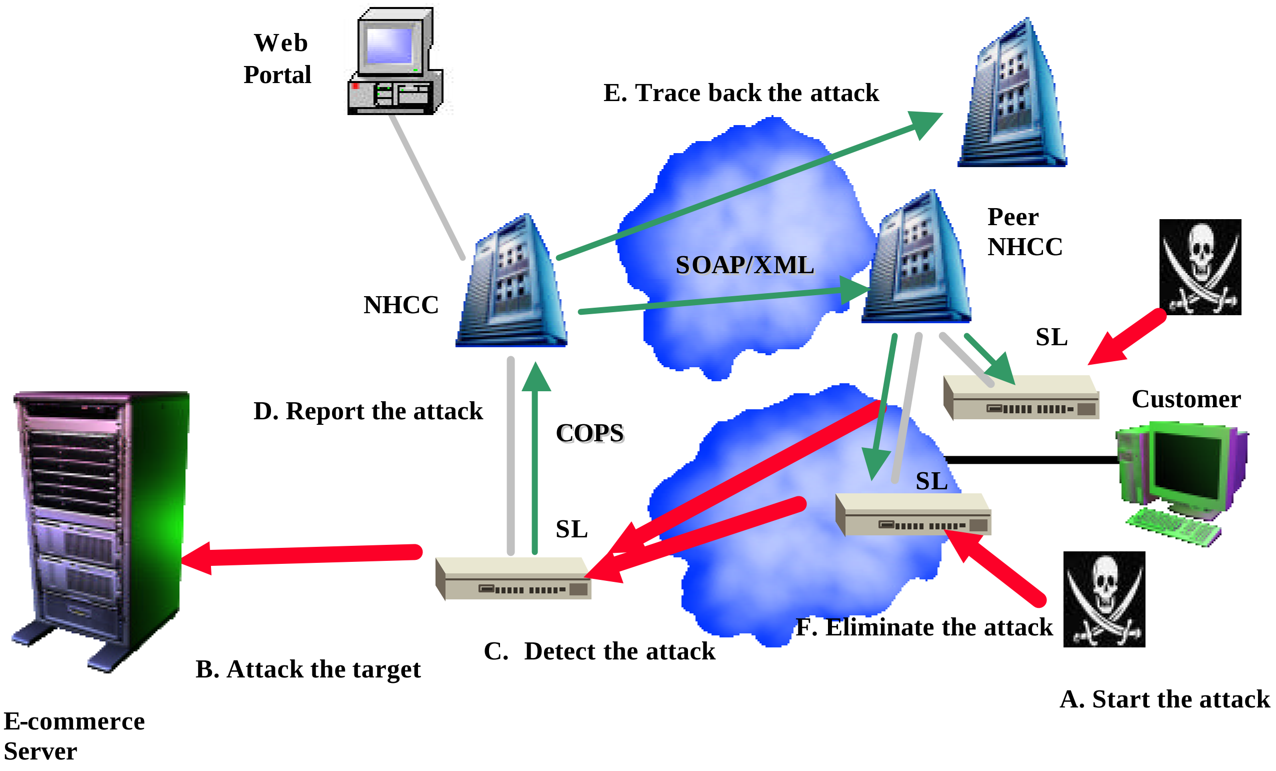

Figure 1: Distributed & Programmable Solution to Automatically Detect and Thwart DDoS Attacks

The advantages of the above solution are multifold:

- The distributed system provides a global view of the entire network domain and hence can detect and thwart Denial of Service attacks that are distributed in nature.
- The Programmable Network Control System uses the network processor microengines that provide the flexibility for expanding the system to counter newer forms of attacks. SLs are easily programmed both to detect various forms of attacks through Intel's network and general-purpose processors and to preserve maximum network performance. Likewise, the NHCC is programmable to adapt to new threats at the system level.
- A portable and extendable software solution allows for easy deployment into existing networks. The portability of SL software means that it can run on switches, routers, servers or network appliances. SL control-plane software is easily ported across Intel processing platforms including IA-32, Intel® Internet Exchange Architecture [IXA], and Intel® XScale™ microarchitecture to fit the custom processing needs of virtually any network device.
- Eliminating the attack close to the source quickly diminishes the attack while allowing legitimate customer traffic to continue. Using this solution, the attack is traced and stopped at the domains that are the actual source of the attack rather than the spoofed source domains. In comparison, a centralized solution blocks spoofed domains, in the process blocking legitimate customer traffic from those domains, which effectively achieves the goals of the attacks.
- A programmatic web-based interface to the entire system is provided through SOAP/XML. This interface allows for both integrated administrative control of the system as well as automated peer-to-peer interactions.

Summary

DDoS Attacks pose a serious threat to networks, and the distributed and ever-changing nature of these attacks makes them difficult to detect and suppress. This paper describes a flexible, programmable distributed network control system, developed by Intel Research and Development, which uses a new approach to detect, trace back and eliminate distributed attacks automatically. To address the constantly changing face of the threat, this solution uses software that is re-configurable at system and device/data-plane levels. Adding full programmability to the network infrastructure devices ensures that the network is capable of dealing with any threat—past, present or future.

Defending the Defender

Many network security solutions are deployed with the intent of protecting a network from attacks only to end up being the target of the attacks themselves. Therefore, it is critical to ensure that the system protecting a network is itself secure and immune to attack. The system described herein protects itself at a number of levels:

1. Built-in Message Level Integrity & Encryption techniques built into the COPS protocol.

2. Persistent TCP connections between the SLs and the NHCC make it less susceptible to SYN Flood attacks.

3. Pre-Configured keys ensure that only trusted systems can communicate.

4. COPS data model validation assures all received data is verified before it is used.

5. XML Digital Signatures can be used for authentication between NHCCs.

References

1. [SOAPSPEC] - http://www.w3.org/TR/SOAP
2. [XML] - http://www.w3c.org/xml
3. [COPS] - http://www.ietf.org/rfc/rfc2748.txt
4. [SANS] - http://rr.sans.org/threats/DDoS.php
5. [CERT] - http://www.cert.org
6. [ICMP] -http://rr.sans.org/threats/ICMP_attacks.php
7. [IXA] - http://www.intel.com/design/network/ixa.htm
8. [COPS-NC] - http://www.intel.com/update/departments/netcomm/nc11011.pdf
9. [IETF] - http://www.ietf.org