Intelligent Programmatic Peering Summary Report

Alliance for Telecommunications Industry Solutions
December 2016

ATIS-I-0000054

Abstract

The TOPS Council's Intelligent Programmatic Peering Landscape Team (IPLT) completed an assessment of several possible near-term mechanisms that would enable automated service provider coordination across peering interfaces to quickly mitigate the impact of Distributed Denial of Service (DDoS) attacks. Possible operational limitations were discussed, and potential protocol work identified.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

Problem Statement

Existing Distributed Denial of Service (DDoS) mitigation techniques do not take advantage of real-time information exchange between service providers. When a service provider identifies the source (or sources) of a DDoS attack, manual coordination (for example, via phone calls) is required between the service providers to assess the extent of the attack, determine the appropriate response, and coordinate actions. This can take hours, or in extreme cases, even days.

Overview

The Intelligent Programmatic Peering Landscape Team (IPLT) surveyed available protocols and management techniques to identify mechanisms that could potentially leverage service-provider-to-service-provider communications to offer better mitigation of DDoS attacks. This assessment identified mechanisms that could potentially be used to shut down DDoS attacks and then conducted an analysis to:

- Assess how each mechanism could be applied in network configurations.
- Identify potential weaknesses and limitations.
- Determine what information would need to be exchanged between service providers.
- Identify network resource implications for network elements.

Based on this assessment, BGP Flowspec was selected for further consideration. An architectural model was proposed to illustrate how this would be applied in a multi service provider environment, clearly distinguishing between the *intra*-provider domain and the *inter*-provider domain. Finally, the IPLT identified where further protocol work is required, and highlighted the groups doing this work.

Value Proposition Assessment

Automated DDoS mitigation between service providers inherently introduces complexity and risk. Therefore, it is important to clearly understand the value proposition to ensure it is worth taking any techniques further. The IPLT analysis recognized that a “DDoS Cleaner” could be provided almost anywhere in the network, but showed there is usually little value to the user when it is applied near the DDoS target. As mitigation is applied further upstream, the value to both the user and the service provider increases. The maximum value is realized when the DDoS Cleaner is invoked at the source of the DDoS attack, thus preventing the DDoS traffic from entering the network at all. Since most DDoS attacks originate on a number of networks, applying mitigation near the source requires communication and coordination between the service provider of the DDoS target and the service providers where the DDoS traffic originates. The conclusion of this analysis was that automated DDoS mitigation between service providers would, in fact, provide significant value, and that it was worth further investigation of potential mechanisms.

Inter-Provider Model

The IPLT developed a model to show how "intelligent peering" could be used to mitigate DDoS attacks. This model includes six steps:

1. The terminating service provider detects and qualifies the attack to determine the appropriate response.
2. The terminating service provider signals to the upstream service provider that the attack is underway and suggests actions that should be taken to stop the attack. This model clearly specifies that the downstream service provider never specifies what the upstream service provider should do – it only recommends actions and requests that the recommendations be implemented. A key assumption is that each service provider has ultimate authority over its internal network and will only follow recommendations if it believes these are the appropriate actions.
3. The upstream service provider validates the information received from the first service provider before even considering acting on this information. A secure protocol and communication path is critical here to ensure that the DDoS mitigation mechanism does not become a target that can be exploited for DDoS attacks in its own right.
4. The upstream service provider will then deploy an appropriate countermeasure. This may, or may not, be the action suggested by the terminating service provider. The decision on what action to take within a service provider network rests solely with the service provider.
5. The service provider monitors the effectiveness of the countermeasure and confirms the end of the attack. If the initial countermeasure is not effective, it may be necessary to deploy additional countermeasures and monitor until it is confirmed that the attack has ended.
6. The upstream service provider then signals to the downstream (terminating) service provider what countermeasures were taken and confirms that the attack has ended.

This model covers the interaction between the terminating service provider and the upstream service provider, but if the DDoS traffic traverses multiple networks, this can be repeated as often as necessary until reaching the source(s) of the attack.

The model developed by the IPLT covers the end-to-end response to a DDoS attack, but the focus of the IPLT work is on the "negotiation" between service providers – steps 2, 3, and 6 in the model. Specifically, it identifies what information needs to be exchanged and suggests the following as the appropriate place to begin:

- **Information that signals details about the attack and the proposed actions**. It should be noted that the IPLT did not conduct an analysis of protocols to signal the attack, but did identify existing protocols, and protocols under development, that could be useful in this regard:
    - Structured Thread Information Expression (STIX): STIX is a language to provide a standardized representation of cyber threat information. The STIX language can be used by a number of protocols to share information that characterizes threats.
    - Trusted Automated Exchange of Indicator Information (TAXII): TAXII is a set of specifications for exchanging cyber threat information. STIX and TAXII are not pieces of software, but they do provide standards that a range of software developments can use.

    - IETF DDoS Open Threat Signaling (DOTS): DOTS is an IETF working group developing a protocol that can be used by an enterprise to signal details of an ongoing DDoS attack to a service provider. This will give the service provider a clear indication of the threat, and allow them to respond accordingly. The scope of DOTS is not exactly the same as the IPLT scope; IPLT is concerned with service-provider-to-service-provider signaling, while DOTS is concerned with enterprise-to-service-provider signaling. However, it is expected that the type of information that needs to be signaled will be very similar in both cases, and DOTS may be equally valuable for service providers. The DOTS protocol is still under development, and it is not clear when it will be available.
- **Information that reports details on the mitigation techniques applied and the status of the attack.**

Assessment of Potential Mitigation Techniques

The IPLT considered a number of existing techniques that can be used to scrub DDoS attacks and assessed the strengths and weaknesses of each when applied in an inter-provider context. The key techniques considered were:

- Remotely Triggered Black Hole (RTBH): Could be used to effectively block DDoS traffic, but unfortunately could have the effect of blocking all traffic, both good and bad. As a result this was not deemed to be a good approach.
- Policy Based Routing: Would allow DDoS traffic to be identified based on a specification of factors such as source address, destination address, protocol, and packet size. A range of actions could also be specified, including discarding packets, logging, rate-limiting, or redirection (for example, to a DDoS scrubber). Unfortunately this would require contacting the service provider and requesting it run the specified filter on each of its backbone and edge routers. In practice this seems unlikely to happen, and therefore this approach was also discarded.
- BGP Flowspec: Allows static policy-based routing to become a dynamic solution, enabling the rules to propagate throughout the network by using the existing Multiprotocol Border Gateway Protocol (MP-BGP) infrastructure. This approach is interesting, but in reality there are a number of practical issues and risks that need to be addressed first. For example, if the rules are too general, it would be possible to drop more traffic than was intended. Well-defined Best Practices could be one way to address this issue, by defining rules that would ensure that BGP Flowspec was “safe”.

Summary

The IPLT identified clear value in coordinating DDoS mitigation between service providers in order to scrub DDoS traffic as close to the source as possible. Several potential DDoS mitigation techniques were ruled out because they had the potential to disrupt all traffic. BGP Flowspec was identified as an interesting technique for further consideration, but best practices would help to ensure that it was applied consistently across all service provider networks. Without suitable best practices, BGP Flowspec also has the potential to negatively impact other network traffic and is unlikely to be widely

used. The development of such best practices could be a useful future activity.

Using Intelligent Peering to mitigate DDoS attacks also requires exchange of DDoS information between carriers. Several encouraging initiatives were identified, but in each case, additional ongoing work is still required. Specifically:

- STIX/TAXII defines a cyber threat language and framework for exchanging information, but still needs to be implemented in code to share information between service providers.
- IETF DOTS is defining a protocol that would allow enterprises to inform a service provider of a DDoS attack and request specific mitigation actions. Although DOTS does not directly address communication between service providers, it could potentially be extended to cover this case. Work in IETF DOTS is incomplete, but it could be relevant when it is available.

The IPLT concluded that automated inter-provider DDoS mitigation could have value, and that key enablers are being developed. However, the required protocols and techniques are not sufficiently mature to implement at the current time.