論文の内容の要旨

論文題目

DEFENDING AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS

（分散サービス停止攻撃の対策方式）

氏　　名　　チェン　エリック　イファ

（本文）Distributed denial of service (DDoS) attack is one of the most alarming threats on the Internet. DDoS attacks attempt to disrupt the target server by exhausting its critical resources in order to deny its service to legitimate clients. The attacker plants attack software on a large number of remote computers. These compromised computers, commonly known as "zombies", become the launch pads for DDoS attacks at the attacker's command. There are two types of DDoS attacks - those that target on server resources and those that target on network bandwidth. We can defend against the former by deploying a conventional firewall with an intrusion detection system near the exterior router to block offending packets in front of servers. However, such methods are ineffective in defending against the latter since the bandwidth upstream of that router will remain blocked. It takes coordination with the upstream nodes to effectively block the attack traffic.

This thesis presents an effective defense system for detecting and mitigating DDoS attacks. We first comprehensively survey all known attacks and look for characteristics that can help us recognize these attacks when they occur. We then propose a forecast mechanism that finds a time series model of normal traffic for each server. Using this model, we can detect anomalies in the ongoing traffic. A significant anomaly would trigger our detection engine to perform further in-depth analysis that looks for specific attack characteristics and create signatures that can identify the attack flows. These signatures are forwarded to multiple upstream nodes, which then mitigate attack flows near the attacking sources. In order to minimize collateral damage, the system also adaptively segregates legitimate traffic that happens to match the attack signatures. This system effectively prevents attack traffic from penetrating the victim's network while protecting access from legitimate users.

We have implemented this defense system in two forms: as a dedicated hardware that utilize network processing units (NPU) to achieve wire-speed, and as a general software that runs on Linux platform. We also conduct experiments using simulations to assess the effectiveness of our defense system. Finally, we propose a practical framework that may be standardized by service providers to deploy our system across different autonomous networks.

（和訳）

分散サービス停止(DDoS: Distributed Denial of Service)は、インターネットでのセキュリティ脅威として注目されている。DDoS攻撃とは、不正なプログラムを多数の端末に侵入させ、それらのプログラムが同時に標的ホストへ大量のパケットを送信し、サービスを停止させる攻撃である。現在知られているDDoS攻撃手法を大別すると、「ホスト資源消費型」と「ネットワーク帯域消費型」の二つのタイプに分けられる。このうち前者の場合は、侵入検知システムと連動したファイアウォールを標的サイトに設置する“点”での防御により、ある程度の効果が得られる。しかし、後者の場合、サーバを守るだけではネットワークが輻輳し、サービス停止を防ぐことができない。従来のサーバが設置されたサイトだけでの防御システム、つまり、“点”での防御だけでは、攻撃を防ぐことも、攻撃中に正規ユーザにサービスを継続することも困難である。

そこで、本論文ではDDoS攻撃を検出および対策する防御システムを提案する。まず、既知の攻撃手段を徹底的に調査し、検出手法の検討に向けて攻撃の特徴をまとめる。また、時列系分析により普段の正常トラヒック量の時間遷移をモデル化し、トラヒックの異常検出を実現する。異常性の高いトラヒックを発見した場合、より詳細な特徴分析を行い、攻撃トラヒックを特定するためのシグネチャを作成する。次に、このシグネチャを攻撃端末に近い上流ノードへ転送する。ネットワークに流れる攻撃パケットの帯域をネットワーク全体の“面”で制限することにより攻撃被害を局所化し、サービスの停止もしくは低下というDDoS攻撃の被害を最小化する。正規ユーザは、DDoS攻撃が発生しているときでも、攻撃の影響を受けずにネットワークを利用することが出来るようになる。

本防御システムは専用装置および汎用ソフトウェアの二つの形で実装されている。前者は、ネットワーク・プロセシング・ユニット(NPU)を用いてワイヤースピードを実現する。後者は、標準Linux上で動作する。また、仮想シミュレーションにより本防御システムの効果を検証する。最後に、本防御システムの汎用性を向上させるため、複数サービスプロバイダを連携させ、異なった自律ネットワーク間の導入法も提案する。