論 文 の 内 容 の 要 旨

論文題目　End-to-End Encryption Enabled Overlay-based Mitigation of HTTP and HTTPS DDoS Attacks: Design and Proof of Concept Implementation
(エンド・ツー・エンド暗号化に対応したオーバーレイに基づくHTTPおよびHTTPS DDoS攻撃緩和手法：設計と概念実証実装)

氏　名　　モハマド　サミル　アビデラヒマン エイド
Mohamad Samir AbdelRahman Eid

To date, DDoS attacks against web servers remain among the most common types of cyber-attacks for their simple yet effective nature. Unlike volumetric attacks that utilize the transport or network layer protocols (low-level), high-level DDoS attacks based on HTTP are smaller in volume and harder to detect. Although mitigation at server's premise (locally-based) can be effective against certain attack categories, coping only locally with the increase in attack volumes and sophistication would require large spending that may only be affordable by large-sized enterprises. Conversely, SMEs require affordable, scalable, and practical remotely-based mitigation (i.e., third-party-managed overlay-based).

As overlay-based mitigation of low-level DDoS became well established, recently more frequent attacks are reported that are based on HTTP and its SSL encrypted version (HTTP(S)-DDoS) attacks. Current overlay-based mitigation systems can mitigate HTTP(S)-DDoS attacks, yet they either suffer from traffic decryption, limited identification, or both. Limited identification at the overlay-nodes necessitates traffic decryption to mitigate complex HTTP(S)-DDoS, while true end-to-end encryption limits the behavior identification attributes.

Practicality is a key for wide acceptance of the system by organizations and users. So, in order to effectively mitigate HTTP(S)-DDoS while complying with the encryption requirement, practical enhancement of overlay-based identification of clients is investigated in this dissertation. Focusing particularly on the complex versions of HTTP(S)-DDoS, namely: single-request per-connection,

sub-detection-thresholds, slow-requesting HTTP-DDoS, and multi-vector attacks.

To enable the desired enhanced identification, firstly a new overlay-based system is designed which practically introduces a third level of client identification (per-session) in addition to the conventional two-level identification (per-IP and per-connection). Web servers are unmodified and managed locally by their administrators (called Secret Servers or SS), while the third-party-managed overlay-based mitigation system consists of distributed special purpose overlay-nodes of two kinds; Access Nodes (AN) through which alone the client-server communication takes place, and Public Servers (PS) which act as initial preparation points. The new system also assumes no client-side modification or special downloads.

Then, a novel taxonomy of HTTP(S)-DDoS attacks is introduced organizing possible source behavior strategies from the AN's and PS's perspectives. In addition, enabled by the introduced enhanced identification, a unique reputation and penalty system based on three levels of behavior attributes records is designed. The novel reputation system requires no traffic decryption at the overlay nodes or special software at the client or server. While the PS and AN can be equipped with several degrees of countermeasures (CM) against attacks, each component in the proposed system is equipped with two degrees of mitigation measures. For the PS and AN, a practical client probing (slow-responding) mechanism is introduced to counter certain defense-unaware attacks. In addition, the AN's second degree CM analyzes the enhanced behavior records for only the per-session identification level to detect complex defense-aware attacks. Further, the PS's second degree CM aims to block PS-targeted attacks two steps away from the SS.

Furthermore, a proof of concept prototype of the proposed system is implemented, with non-optimally configured parameters to demonstrate the concept's soundness, and deployed on the DeterLab cyber-security testbed for experimental evaluation. At first, to examine the system's practicality and its transparency to both clients and servers, the prototype system is qualitatively tested for usability with actual commercial websites. Then, considering the goal of DDoS attacks, four metrics are defined for comprehensively measuring the mitigation effectiveness, namely; mitigation factor, cost, time, and collateral damage. Among the experiments conducted with simple and complex HTTP(S)-DDoS attack assumptions

that are absent from related works and conventionally hard to detect, the results of seven experiments are presented and discussed, including; brute-force, below detection thresholds, single-request per-connection, slow-requesting HTTP-DDoS, multi-behavior per-shared-IP, and multi-vector attack conditions. For attack traffic, attack tools popular among attackers are utilized (i.e., LOIC and Slowloris) for experiments with limited number of sources (10 to 20 sources), and similarly built custom tools for highly distributed centrally controlled automated attacks (1,000 to 10,000 sources).

The results suggest that utilizing the introduced practical enhanced identification can eliminate the necessity for traffic decryption by overlay-nodes and for inspection of client-server traffic content. With the enabled reputation and penalty system, we can accomplish high mitigation factors of conventionally hard to detect HTTP(S)-DDoS attack categories in relatively short mitigation times, in contrast to conventional overlay-based methods. Especially considering complex attack conditions that are missing in related research such as single-request per-connection sub-detection-threshold HTTPS-DDoS. It suggests that less complex attack categories can be equally mitigated. In addition, results suggest that enhanced identification can achieve low collateral damage in terms of the chance of receiving service and service time for non-attacking clients that share an attack IP. However, the unoptimized implementation of the prototype system shows a cost in service time even without attack. Also, it shows a temporarily decrease in mitigation factor and rise in cost during mitigation time. Experimentally demonstrating the concept's soundness based on the introduced per-session identification alone opens the way for investigating the inclusion of the three identification levels within various machine learning techniques for adaptive system parameters' tuning and for analyzing the enhanced behavior record patterns.