Università degli Studi di Salerno

Dottorato di Ricerca in Informatica e Ingegneria dell'Informazione
Ciclo 33 – a.a 2019/2020

ABSTRACT

TESI DI DOTTORATO / PH.D. THESIS

Statistical Techniques for Mitigation and Prevention of Distributed Attacks over Communication Networks

MARCO TAMBASCO

SUPERVISOR: **PROF. VINCENZO MATTA**

PHD PROGRAM DIRECTOR: **PROF. PASQUALE CHIACCHIO**

Dipartimento di Ingegneria dell'Informazione ed Elettrica
e Matematica Applicata
Dipartimento di Informatica

Abstract (English)

The thesis is focused on statistical methods to characterize, mitigate, and counteract distributed network attacks. When coping with distributed network attacks such as Distributed Denial of Service (DDoS) attacks, two main stages/issues emerge manifestly. The first issue pertains to the design of suitable strategies aimed at revealing and tracking the distributed threats that typically act sneakily to compromise the resources of a network target. The second issue concerns the precautionary countermeasures that a network manager can put in field to mitigate the damages that a distributed threat can provoke. Accordingly, the contributions offered in this thesis move along the two aforementioned lines as detailed in the following.

The first contribution pertains to *a novel class of application-layer (a.k.a. L7) DDoS attacks*. In a Distributed Denial of Service (DDoS) attack, a network (*botnet*) of dispersed agents (*bots*) send requests to a website to saturate its resources. Since the requests are sent by automata, the typical way to detect them is to look for some repetition pattern or commonalities between requests of the same user or from different users. For this reason, recent DDoS variants exploit communication layers that offer broader possibility in terms of admissible request patterns, such as, e.g., the application layer. In this case, the malicious agents can pick legitimate (thus, not suspicious) messages from an *emulation dictionary* that a botmaster learns steadily by gleaning patterns of legitimate activity performed by normal users. Then, each individual malicious agent sends a relatively low number of admissible requests, so as to make its activity non suspicious in terms of request rate. This problem has been recently addressed under the assumption that all members of the botnet use the same emulation dictionary. This situation is an idealization of what occurs in practice, since different clusters of agents are typically sharing only part of a global emulation dictionary. As a novel contribution, we therefore address the relevant decentralized setting where the emulation dictionary is disseminated across the botnet, and the *diversity* among the emulation dictionaries across different clusters introduces significant complexity in the botnet identification challenge. In this thesis work we tackle this issue and provide the following main contributions. First, we provide an analytical characterization of the pairwise interaction between bot clusters, in terms of message innovation rate. Exploiting this result, we design a botnet identification algorithm (*BotClusterBuster*) equipped with a *cluster expurgation rule*, which, under appropriate technical conditions, is shown to provide exact classification of bots and normal users as the observation window size increases. Distinguishing the clusters of bots from normal users is in fact critical in view of the attack mitigation purpose: banning the former while not denying the service to the latter. An experimental campaign over two datasets containing real-world traffic has been carried out to assess the validity of the theoretical analysis, as well as to examine the effect of a number of non-ideal effects that are unavoidably observed in practical scenarios, showing the resilience of the proposed methodology w.r.t. the operational conditions.

The second contribution pertains to the formalization of network availability and performability problems along with the design of suitable prevention strategies. Specifically, the focus is on the so-called virtualized networks, where two architectural peculiarities emerge: *i)* each network node can be logically split in different nested parts (such as software, hypervisor, hardware) and, hence, *common-mode failures* must be taken into account; *ii)* nodes are interconnected so as to form a service chain, implying that *single points of failure* can arise from this particular arrangement. In order to tackle the availability issues arising from the virtualized service chains, we considered the Stochastic Reward Network (SRN) and the Reliability Block Diagram (RBD) frameworks. The SRN formalism allows to model each virtualized node in terms of a state-space system, and to examine it by considering randomly distributed failure and repair events. The RBD formalism is useful to capture high-level interconnections among nodes resulting in different series (chain) and parallel (redundancy) configurations. The availability assessment is complemented with a sensitivity

analysis, useful to evaluate the robustness of service chains when critical parameters (e.g. failure/repair rates) deviate from their nominal values. The consequent prevention strategy is then recast as an optimization problem, whose solution leads to the optimal trade-off between redundancy and costs. In particular, an algorithm nicknamed *OptChains+* has been devised to: *i)* evaluate SRN/RBD models associated to particular service chains, and *ii)* pinpoint the chains yielding minimum cost and high availability under specific performance criteria.

Abstract (Italiano)

La tesi è incentrata su metodi statistici per caratterizzare, mitigare e contrastare attacchi di rete distribuiti. Quando si considerano attacchi di rete distribuiti come gli attacchi Distributed Denial of Service (DDoS), emergono chiaramente due principali fasi/problemi. La prima fase riguarda la progettazione di adeguate strategie utili a rivelare e tracciare le minacce distribuite che tipicamente agiscono in modo subdolo per compromettere le risorse di un target di rete. La seconda fase riguarda le contromisure precauzionali che un *network manager* può mettere in campo per mitigare i danni che una minaccia distribuita può provocare. Di conseguenza, i contributi offerti in questa tesi seguono le due linee sopra menzionate come dettagliato di seguito.

Il primo contributo riguarda una nuova classe di attacchi DDoS a livello applicazione (L7). In un attacco DDoS (Distributed Denial of Service), una rete (botnet) di agenti distribuiti (bot) invia richieste ad un sito Web per saturarne le risorse. Poiché le richieste vengono inviate da agenti automatici, una tipica procedura per rivelarle consiste nel cercare dei *pattern* ripetitivi, o delle caratteristiche comuni tra le richieste dello stesso utente o di utenti diversi. Per questo motivo, alcune varianti DDoS recenti sfruttano quei livelli di comunicazione che offrono maggiore flessibilità nella costruzione di messaggi ammissibili, come, ad esempio, il livello applicazione. In questo caso, gli agenti malevoli possono selezionare messaggi legittimi (quindi non sospetti) da un dizionario di emulazione che un botmaster apprende costantemente attraverso la selezione di messaggi legittimi provenienti da utenti normali. Ogni singolo agente malintenzionato invia quindi un numero relativamente basso di richieste ammissibili, in modo da rendere la propria attività non sospetta in termini di tasso di richiesta. Questo problema è stato affrontato di recente partendo dal presupposto che tutti i membri della botnet utilizzino lo stesso dizionario di emulazione. Questa situazione rappresenta un'idealizzazione di ciò che accade nella pratica, poiché diversi cluster di agenti malevoli condividono in genere solo una parte di un dizionario di emulazione globale. Come contributo innovativo si considera quindi una configurazione decentralizzata in cui il dizionario di emulazione è disseminato attraverso la botnet e la *diversità* fra i dizionari di emulazione dei diversi cluster introduce una complessità significativa nella sfida dell'identificazione della botnet. In questo lavoro di tesi si affronta questo tipo di problema e si forniscono i seguenti principali contributi. Innanzitutto, si fornisce una caratterizzazione analitica dell'interazione a coppie tra cluster di bot, in termini di tasso di innovazione dei messaggi. Sfruttando questo risultato, è stato progettato un algoritmo di identificazione della botnet (*BotClusterBuster*) dotato di una regola di *cluster expurgation*, che, sotto determinate condizioni, consente di discriminare in maniera esatta i bot dagli utenti normali all'aumentare della dimensione della finestra di osservazione. Distinguere i cluster di bot dagli utenti normali è infatti fondamentale nell'ambito della mitigazione degli attacchi: bandire i primi senza negare il servizio ai secondi. È stata condotta una campagna sperimentale su due dataset contenenti traffico reale per valutare la validità dell'analisi teorica, nonché per esaminare l'effetto di una serie di non idealità che sono inevitabilmente osservate in scenari pratici, mostrando la resilienza della metodologia proposta rispetto alle condizioni operative.

Il secondo contributo riguarda la formalizzazione dei problemi di disponibilità e *performability* della rete, e la progettazione di adeguate strategie di prevenzione. Nello specifico, il focus è sulle cosiddette reti virtualizzate, dove emergono due peculiarità architetturali: *i)* ogni nodo di rete può essere logicamente suddiviso in diverse parti innestate (come software, hypervisor, hardware) e, quindi, i guasti di modo comune devono essere presi in considerazione; *ii)* i nodi sono interconnessi in modo da formare una *service chain*, il che implica che singoli punti di guasto (*single points of failure*) possono derivare da questa particolare disposizione. Per modellare i problemi di disponibilità associati ad infrastrutture di tipo *service chain*, si sono presi in considerazione due formalismi: le Stochastic Reward Network (SRN) ed i Reliability Block Diagram (RBD). Il formalismo SRN consente di modellare ogni nodo virtualizzato in termini di una macchina a stati e di esaminarlo considerando gli eventi di guasto e di ripristino modellati come variabili aleatorie. Il formalismo RBD è utile per catturare interconnessioni di alto livello tra i nodi che possono dar

luogo a configurazioni di tipo serie (*chain*) e/o parallelo (ridondanza). La valutazione della disponibilità è completata da un'analisi di sensitività, utile per valutare la robustezza delle *service chain* quando i parametri critici (es. tassi di guasto/riparazione) si discostano dai loro valori nominali. La conseguente strategia di prevenzione viene quindi riformulata come un problema di ottimizzazione, la cui soluzione porta al compromesso ottimale tra ridondanza e costi. In particolare, è stato ideato un algoritmo soprannominato *OptChains+* per: *i)* valutare modelli SRN / RBD associati a particolari *service chain*, e *ii)* individuare le configurazioni aventi, allo stesso tempo, un costo minimo ed un'elevata disponibilità considerando specifici criteri di prestazione.