A Decision Support System for Placement of Intrusion Detection and Prevention Devices in Large-Scale Networks

RAMI PUZIS, MEYTAL TUBI, and YUVAL ELOVICI, Ben-Gurion University
CHANAN GLEZER, Ben-Gurion University and Ariel University Center of Samaria
SHLOMI DOLEV, Ben-Gurion University

This article describes an innovative Decision Support System (DSS) for Placement of Intrusion Detection and Prevention Systems (PIDPS) in large-scale communication networks. PIDPS is intended to support network security personnel in optimizing the placement and configuration of malware filtering and monitoring devices within Network Service Providers' (NSP) infrastructure, and enterprise communication networks. PIDPS meshes innovative and state-of-the-art mechanisms borrowed from the domains of graph theory, epidemic modeling, and network simulation. Scalable network exploitation models enable to define the communication patterns induced by network users (thereby establishing a virtual overlay network), and parallel attack models enable a PIDPS user to define various interdependent network attacks such as: Internet worms, Trojans horses, Denial of Service (DoS) attacks, and others. PIDPS incorporates a set of deployment strategies (employing graph-theoretic centrality measures) in order to facilitate intelligent placement of filtering and monitoring devices; as well as a dedicated network simulator in order to evaluate the various deployments. Experiments with PIDPS indicate that incorporating knowledge on the overlay network (network exploitation patterns) into the placement and configuration of malware filtering and monitoring devices substantially improves the effectiveness of intrusion detection and prevention systems in NSP and enterprise networks.

Categories and Subject Descriptors: G.2.2 [**Discrete Mathematics**]: Graph Theory—*Graph algorithms; Network problems*; G.3 [**Probability and Statistics**]: *Stochastic processes; Experimental design*; K.6.2 [**Management of Computing and Information Systems**]: Installation Management—*Benchmarks; Computing equipment management; Performance and usage measurement; Pricing and resource allocation*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Invasive software (e.g., viruses, worms, Trojan horses)*

General Terms: Design, Experimentation, Security

Additional Key Words and Phrases: Overlay networks, intrusion detection, decision support systems

ACM Reference Format:
Puzis, R., Tubi, M., Elovici, Y., Glezer, C., and Dolev, S. 2011. A decision support system for placement of intrusion detection and prevention devices in large-scale networks. ACM Trans. Model. Comput. Simul. 22, 1, Article 5 (December 2011), 26 pages.
DOI = 10.1145/2043635.2043640 http://doi.acm.org/10.1145/2043635.2043640

1. INTRODUCTION

Malware such as computer viruses and worms, spying programs, Trojans, and distributed denial of service attack (DDoS) pose a severe risk to the Internet's

This work is supported by Deutsche Telekom AG.
Authors' addresses: R. Puzis, M. Tubi, and Y. Elovici, Deutsche Telekom Laboratories and the Department of Information Systems Engineering at Ben-Gurion University of the Negev, Israel; C. Glezer, Ben-Gurion University and Ariel University Center of Samaria; S. Dolev, Department of Computer Science, Ben-Gurion University of the Negev, Israel; email: {puzis, tubim, elovici, chanan, dolev}@bgu.ac.il.

DOI 10.1145/2043635.2043640 http://doi.acm.org/10.1145/2043635.2043640