

# Random Host Mutation for Moving Target Defense

Ehab Al-Shaer, Qi Duan, Jafar Haadi Jafarian

University of North Carolina at Charlotte, Charlotte, NC, USA

{ealshaer, qduan, jjafaria}@uncc.edu

**Abstract**—IP mutation, or IP hopping, has been proposed as a proactive cyber defense against scanning attacks. However, proposed techniques have significant practical limitations because they are either too inefficient to counter adversary due limited mutation space and speed, or operationally too expensive as they require end-host changes and session interruption. In this poster, we propose a novel transparent IP mutation technique, called RHM, which provides high-speed and unpredictable IP mutation while maintaining active session integrity and low overhead.

## I. INTRODUCTION

Static assignment of IP addresses gives adversaries significant advantage to remotely scan networks and identify their targets accurately and quickly. IP mutation, or IP hopping, approach has been proposed by some researchers as a proactive countermeasure against reconnaissance, including APOD [1], DyNAT [2], and NASR [3]. However, none of the previous techniques provide a deployable transparent mechanism for IP mutation that can defend against external and internal scanning attacks without changing the configuration of the end-hosts.

In this poster, we introduce a moving target technique called *Random Host Mutation* (RHM) which combines the most important features of IP mutation, including (1) transparency to end-hosts, (2) unpredictability in IP mutation to complicate host discovery for attackers, (3) fast mutation rate to quickly invalidate collected information, and (4) preserving end-to-end reachability. We show that the IP mutation is an NP-hard optimization problem, formulate it as a constraint satisfaction problem, and solve it using Satisfiability Modulo Theories [4] (SMT) solvers.

## II. APPROACH

The main objective of RHM is to mutate IP addresses of end-hosts randomly and transparently. To provide transparency, RHM keeps the actual or real IP addresses of hosts (called *rIP*) unchanged, but associates each host with random short-lived virtual IP addresses (called *vIP*) at regular intervals which are translated to *rIP*s right before the host. Normal users will reach named hosts via querying their *vIP*s from DNS, while authorized administrators can still reach all hosts using their *rIP*s.

To perform IP mutation with high unpredictability and speed, the mutant *vIP*s are selected randomly from the entire unused address space in the network. Each host must be associated with an unused range for mutation. However, if the mutation range is fixed the unpredictability is severely reduced. To this aim, RHM uses two levels of random mutation granularity: *Low Frequency mutation (LFM)* and *High Frequency mutation (HFM)*. Low frequency mutation is used for selecting a random address range for the hosts, and high frequency mutation is used to select a random *vIP* within range assigned during last LFM. The two levels of mutation are introduced to further increase the distance between two consecutive assignments of the same *vIP* to any or a specific *rIP*, and therefore to enhance the unpredictability of mutation.

Selection of a range for a host is performed by a central entity called *Moving Target Controller (MTC)*. At each LFM interval, MTC selects a new range for each host while satisfying various constraints such as mutation requirements of the host, unpredictability of mutation, routing update convergence, as well as minimizing routing table size. We show that this problem is an NP-hard optimization problem, formulate it as a constraint satisfaction problem and solve it using Satisfiability Modulo Theories [4] (SMT) solvers.

After selection, new designated ranges are announced to distributed entities, called *Moving Target Gateway (MTGs)*, which are boxes deployed at the boundary of subnets (between subnet switch and the core). MTG is also responsible for translation of source *rIP* to *vIP* for outbound, and destination *vIP* to *rIP* for inbound packets. It also provides session tracking for active connections.

## III. DEPLOYMENT AND EFFECTIVENESS

To study and demonstrate the feasibility of RHM, we implemented a proof-of-concept for RHM in a designated class C subnet in our university campus network. The MTG and MTC components are implemented on Linux-based (Ubuntu) boxes and interact with RIP-2 based routers and local firewalls.

RHM is a proactive defense strategy against internal and external reconnaissance. RHM can prevent hitlist attacks (e.g. hitlist worms) effectively, since the IP addresses in the hitlist will be soon out-of-date. Due to high mutation speed, and unpredictability of *vIP* assignments, our solution will be the *optimal* solution for defense against hitlist worms. RHM also slows down worm propagation in networks. It is specially effective for non-repeat random worms and cooperative worms (e.g. divide-and-conquer worms), where the probability that an IP is scanned more than once is low. Strengthened with intelligent mutation to already-scanned IPs, RHM can save up to 90% of network hosts from infection.

## REFERENCES

- [1] M. Atighetchi, P. Pal, F. Webber, and C. Jones. Adaptive use of network-centric mechanisms in cyber-defense. In *ISORC '03*, page 183. IEEE Computer Society, 2003.
- [2] D. Kewley, R. Fink, J. Lowry, and M. Dean. Dynamic approaches to thwart adversary intelligence gathering. In *DARPA Information Survivability Conference Exposition II, 2001. DISCEX '01. Proceedings*, volume 1, pages 176–185 vol.1, 2001.
- [3] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis. Defending against hitlist worms using network address space randomization. *Comput. Netw.*, 51(12):3471–3490, 2007.
- [4] N. Björner and L. de Moura.  $z3^{10}$ : Applications, enablers, challenges and directions. In *CFV '09*, 2009.