Moving Target Defenses and Their Applications in the Internet of Things

Dilli P. Sharma
Ph. D. Student
Cybersecurity Lab, University of Canterbury
Christchurch, New Zealand

August 9, 2019
Outline

• Introduction
• System Models
  • Network Model
  • Attacker Model
• Our defense approaches
  • Flexible Random Host Multiplexing Technique
  • Random Host and Service Multiplexing Technique
• Dynamic security metrics for MTDs
• MTD Approaches to IoT
• Summary of work
What is Moving Target Defense (MTD)?

- **Motivation**: static configurations of the computing systems make:
  - Easy to operate and manage
  - But, always give advantages to attacker:
    - An attacker can have sufficient time to study and collect information of a target system
    - Information asymmetry between attacker and defending system

- **Why MTD?**
  - Confuse attackers and increase the attack effort of attacker

- **How?**
  - Continuously and dynamically changing/shifting the *attack surface*
  - *Attack surface* is a set of system properties that can be used for attack (e.g., exploitable vulnerabilities)

- **MTD Elements**:
  - Space to Move/What to move
  - Mechanism to Move/How to Move
  - When to move/adaptation

- **Moving Elements (What to Move)**:
  - MAC address, IP address, port#, route, topology, protocols
  - Memory address layout, Instruction set, VM, VMM
  - Operating systems, Application programs, API, Data etc.

- **Mechanism/techniques (How to Move)**:
  - Randomization/shuffling
  - Artificial diversity/Diversity
  - Redundancy

- **MTD Strategy (When to Move)**:
  - Time-based (fixed/variable time interval)
  - Event/alert based (IDS/IPS-based)
  - Hybrid/Combined (both)
System Model

- **Software-Defined Networking (SDN)**
  - Why SDN-based MTDs?
  - Conventional network consists of heterogeneous elements (e.g., switch, router, firewall) with their own software and proprietary protocols
  - SDN is a promising technology that can provide **flexibility, robustness, and programmability**
  - The programmable interfaces afforded by SDN can be comforted to achieve a dynamic and adaptable defensive strategy based security including MTD
Attacker model: Scanning/reconnaissance attacks

- Attacker located outside the network and performs scanning
- Scanning attack is used for gathering the information before the actual attack is launched.
- An attacker usually use customized set of software tools (*e.g.*, *Nmap*, *Nessus etc.*) to scan the target network and system to find and the information:
  - OS types, IP addresses, port numbers, running services, protocols, topology and exploitable vulnerabilities.
- Common scanning methods used to discover host and services are:
  - ICMP echo request (ICMP Ping)
  - UDP Port Scanning
  - TCP Port Scanning
    - TCP Connect (Full)
    - TCP SYN (Half)
Related Work

• **IP/Port shuffling-based MTDs:**
  
  • MTD technologies are emerging proactive/reactive defense mechanisms
  
  • IP-shuffling (e.g., [1], [2]) and Port-shuffling/hopping (e.g., [3], [4]) based MTD techniques have been researched
  
  • These techniques map an actual IP/port of each host/service to a random, short-lived IP/port address called-virtual IP/port; and the mapped *IP and/or port* is changed frequently and dynamically
  
  • These approaches have some limitations:
    
    • IP/port mapping is *1-to-1* manner (e.g., a virtual IP/Port mapped to a real IP/port)
    
    • *1-to-1* mapping requires more *virtual IP/ports* to satisfy the mutation/shuffling rate constraints and unpredictability (e.g., required more *virtual IP* for high shuffling frequency)
    
    • Lacks the scalability due to the limited address space (range allocation constraints- each host requires address space range which is limited in size)

---


Our Approach

- We proposed a novel SDN-based MTD technique called Flexible Random Virtual IP Multiplexing (FRVM) [5]:
  - It enables a host to have multiple, random, time-varying virtual IP addresses (vIPs)
  - The vIPs are changed randomly and dynamically in order to invalidate the target system’s information collected by attacker
  - It creates an extremely diversity environment and makes difficult for an attacker to identify the entire network and reduces the attack success probability

FRVM Architecture

FRVM system’s elements:

- A set of server-hosts
- An SDN controller
- A DNS Server
- A set of Open-Flow/SDN switches
- End-users
Implementation & Evaluation

• **Implementation:**
  • FRVM controller was developed
    • It is a customized SDN controller that implements FRVM address mapping
    • It has been deployed using *Mininet*.

• **Evaluation models:**
  • Comparative analysis with a baseline model (i.e., a typical static SDN controller Vs. FRVM controller)
  • Probabilistic analytical models derived for random scanning strategy:
    • Hypergeometric distributions for a static network w/o FRVM
    • Binomial distribution for a network w/ FRVM
  • Experimental evaluation via simulations:
    • We collected data such as scan duration, delay, TCP file transfer duration, etc.
    • Comparatively analyzed the security and performance overhead using:
      • **Security metrics** (e.g., Attack success probability, Deterrence and Effectiveness)
      • **Performance metrics** (e.g., End-to-end delay, Throughput overhead etc.)
Results & Analysis

Fig.: Security analysis w/ FRVM and w/o FRVM (a) Analytical ; and (b) Simulation Results
Results & Analysis (Contd.)

Fig.: Performance overhead analysis: (a) Delay; and (b) Throughput
Other our similar work

• **Random Host and Service Multiplexing (RHSM)** [6]:
  - RHSM de/multiplexes both virtual IPs (i.e., hosts) and virtual ports (i.e., services)
  - It adapts FRVM concept to multiplex/de-multiplex addresses
  - Results show that our RHSM reduces attack success probability
  - The effect of service multiplexing is more pronounced under a smaller number of vulnerable services (i.e., $v \leq 5$)

Moving Target Defenses and Their Applications in the Internet of Things

Other our similar work (Contd.)

• Dynamic security metrics for SDN-based MTD:
  • Our dynamic metrics capture dynamic changing of the network due to the shuffling event of the MTDs.

Dynamic MTD Metrics

- Attack Stage-based
- Attack Path-based
- Network/Host Address-based
Work on going

• Game-theoretic approach for optimizing shuffling strategy of moving target defense in software-defined networks:
  • In time-based shuffling MTD, the determination of the optimal shuffling interval time or shuffling frequency is critical (i.e., *When to Move*)
  • Why game-theory?
    • To determine an optimal shuffling frequency
    • Security Game = Game + Optimization
MTD Approaches to IoT

• IP-shuffling based MTD for IoT:
  • Micro-Moving Target IPv6 defense (μMT6D) for the IoT [7]:
    • How?: Shuffling of IP address (IPv6) of the IoT device
    • Its goal to limit time of an attacker for conducting reconnaissance

• Code Diversification for IoT:
  • MTD for IoT Using Context Aware Code Partitioning and Code [8]:
    • How?: When context dictates, the IoT devices request code and download it from a secure source (e.g., Cloud)

---


MTD Approaches to IoT (Contd.)

- Constraints on nodes:
  - Energy, CPU, Flash, RAM etc.
  - Nodes are easily accessible (i.e., physically accessible)
- Constraint on network:
  - Low bandwidth, high packet-loss
  - Fixed network configurations
- These constraints of the IoT makes **difficult to adopt dynamic and adaptable security mechanisms**
- **Software-defined IoT (SDIoT)** can make feasible for adopting the dynamic and adaptable security mechanisms including MTD
  - MAC address/ IP address/ virtual IP address shuffling (e.g., FRVM, μMT6D etc.)
  - Network topology shuffling/network reconfigurations/route mutations etc.
  - Virtual CAN-ID shuffling for SD-vehicular network
  - Etc.
Summary of work

• We proposed a novel SDN-based Moving target defense techniques (e.g., FRVM, RHSM) to deal with the network reconnaissance and scanning attacks
  • We validated the performance of the proposed approaches against a typical static network counter-part in terms of attacker success probability and overhead introduced by the MTDs
  • The experimental results proved that our approaches can effectively thwart scanning attacks increasing the attacker’s work effort with acceptable operational overhead

• We have designed a suite of dynamic security metrics for assessing the effectiveness of the MTDs

• We can apply MTD mechanisms to the SDIoT by:
  • Adapting the current MTD mechanisms or defining new MTD techniques leveraging the SDN technology
Thank you for your attention!

Please email me if you have any questions
Email: dps72@uclive.ac.nz