A Stealth Migration Approach to Enhancing the Security of Moving Target Defense (MTD)

Saikat Das, Sajjan Shiva

Game Theory and Cyber Security Lab, Department of Computer Science, The University of Memphis

Introduction

✓In cyber security, Moving Target Defense (MTD) is the counter deception way of constantly changing the target surface from the attackers.

✓Live migration is the technique that uses MTD to move the Virtual Machine across the cloud network.

✓MTD is the most commonly used technique in cyber security.

✓The security of MTD is well established, but still not adequate to defeat the attackers who can trace route the moving path even when data and path are encrypted.

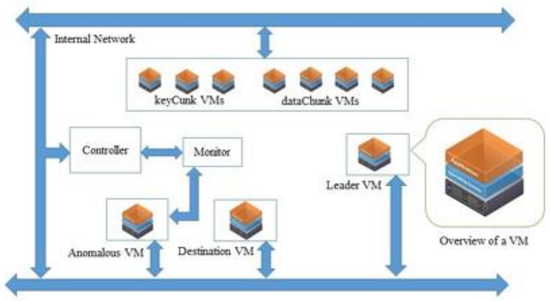
✓A compromised cloud system employing MTD can facilitate untrusted access to the moving VM.

✓A stealthy way of migrating the VM is required to hide the VM live migration information from the attacker.

Methods

Components:

- ✓ Monitor: That monitors corresponding VM.
- ✓ Controller: Controller of the VM Manager (VMM).
- ✓ $VM_{anlomaous}$: VM that identified as affected by monitor.
- ✓ $VM_{available}$: Intermediate VMs that accept data/ key chunks
- ✓ VM_{leader}: VM that leads all intermediate VMs
- ✓ $VM_{destination}$: Final destination of anomalous VM data.

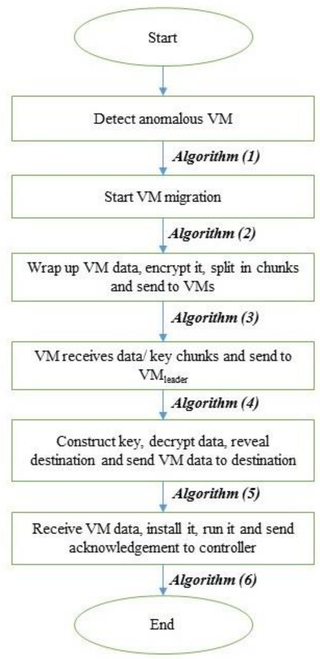


Top-level view of Stealth Migration Protocol

Split and Construction

✓Secret Key Split and Construction:
- ✓ Shamir's Secret Sharing Encoding Scheme

✓Data Split and Construction:
- ✓ OS default file splitting using buffer size



Work Flow of Stealth Migration Approach

Step by Step Approach

✓Detection of Anomalous VM by Monitor

✓Encryption of VM data and destination VM address

✓Split encryption key by Secret Sharing

✓Split data into adjustable chunk size

✓Transfer chunks to intermediate VMs

✓Construct key and data in leader VM

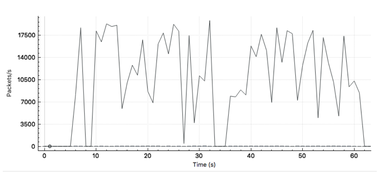
✓Decrypt data and destination address in leader VM

✓Transfer data to destination address

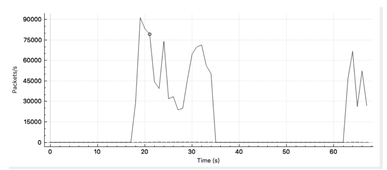
Algorithmic Approach

- ✓ ***Algorithm (1):*** *Detecting anomalous activity of VMs*
- ✓ ***Algorithm (2):*** *Maintain the connectivity among VMs and control all VMs to operate the VM migration.*
- ✓ ***Algorithm (3):*** *Data wrap up, encryption, split data and key, send.*
- ✓ ***Algorithm (4):*** *Receive datachunk, mark it as data segment and send it to the VM_{leader} address.*
- ✓ ***Algorithm (5):*** *Construct secret key, reveal destination VM address after decrypting the data and send it to the destination VM.*
- ✓ ***Algorithm (6):*** *Receives data, install it, notify controller after successful running.*

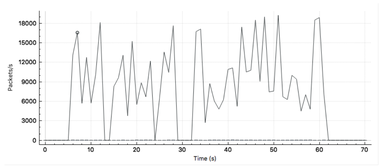
Results



Normal Traffic



Migration Traffic (Without Stealth Migration)



Migration Traffic (With Stealth Migration)

Traffic Definition

- ✓ Normal Traffic:
  - ✓ Application running on VMs
- ✓ Migration Traffic:
  - ✓ VM dirty pages
  - ✓ VM states

Discussion and Future Work

✓Enhance MTD security by

- ✓ Obfuscating the VM migration from intruder
- ✓ Encrypting VM data
- ✓ Splitting secret key using Shamir's Secret Sharing
- ✓ Using multiple intermediate VMs way to destination
- ✓ Hiding destination address

✓Traffic Maintenance

- ✓ Adjustable chunk size by measuring normal traffic

✓Future Work

- ✓ Machine learning to
  - ✓ Detect the anomalous VM
  - ✓ Detect the abnormal migration process
- ✓ Reducing false positive alarm during migration

References

1.Achleitner, Stefan, et al. "Stealth migration: Hiding virtual machines on the network." INFOCOM 2017-IEEE Conference on Computer Communications, 2017.

2.https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing