Survey of Cyber Moving Targets Second Edition

Authors: B.C. Ward S.R. Gomez R.W. Skowyra D. Bigelow J.N. Martin J.W. Landry H. Okhravi

Presenter: Jinghui Liao

Outline

- Cyber Kill Chain
- Attack technique
- Moving-targets technique
- Weakness

Cyber Kill Chain

- Reconnaissance
- Access
- Exploit Development
- Attack Launch
- Persistence

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
  - Leakage of cryptographic keys from memory(WannaCry)
  - Side-channel attacks(spectre meltdown)

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
  - Exhaust or manipulate shared resources
  - Denial-of-service using CPU saturation

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
    - buffer overflow
    - script injection
    - SQL injection

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
    - Timing
    - Ordering
    - Arguments
    - Return-oriented programming (ROP)

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
  - Fake identity
  - Man-in-the-middle
  - Phishing

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
  - Compromise authentication process
  - Cross-site scripting

ATTACK TECHNIQUES

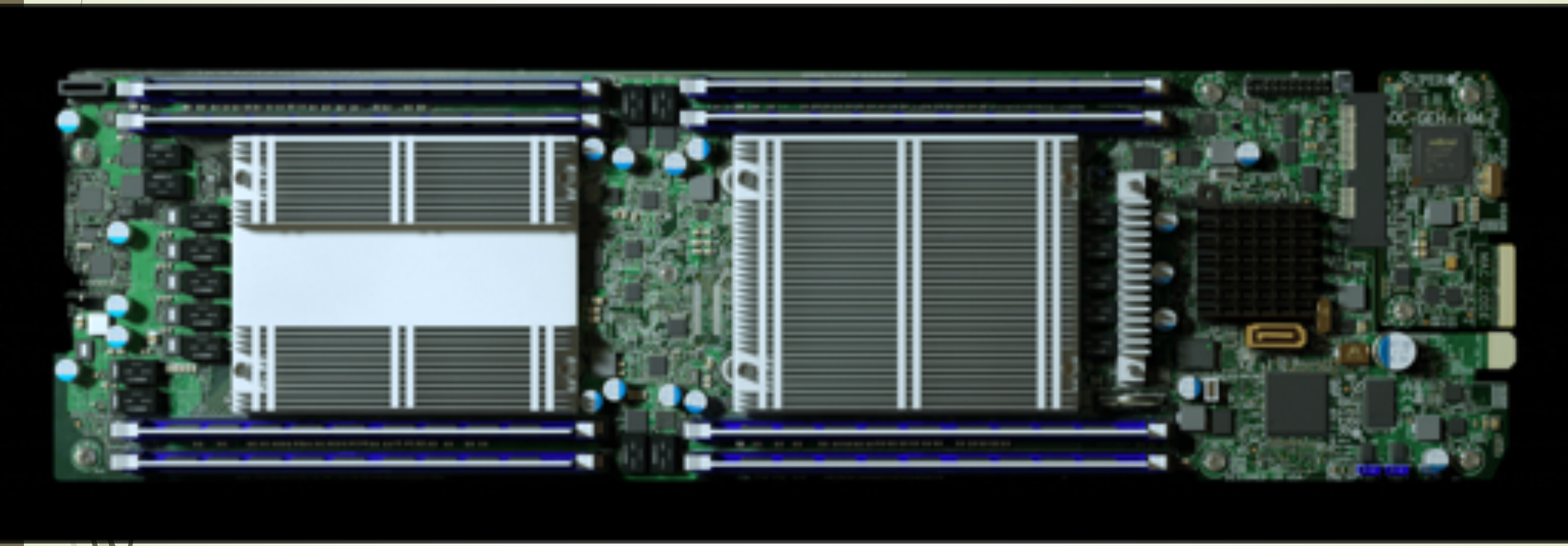
- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks

ATTACK TECHNIQUES

- Data Leakage Attacks
- Resource Attacks
- Injection
  - Code Injection
  - Control Injection
- Spoofing
- Exploitation of Authentication
- Exploitation of Privilege/Trust
- Scanning
- Supply Chain/Physical Attacks



https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

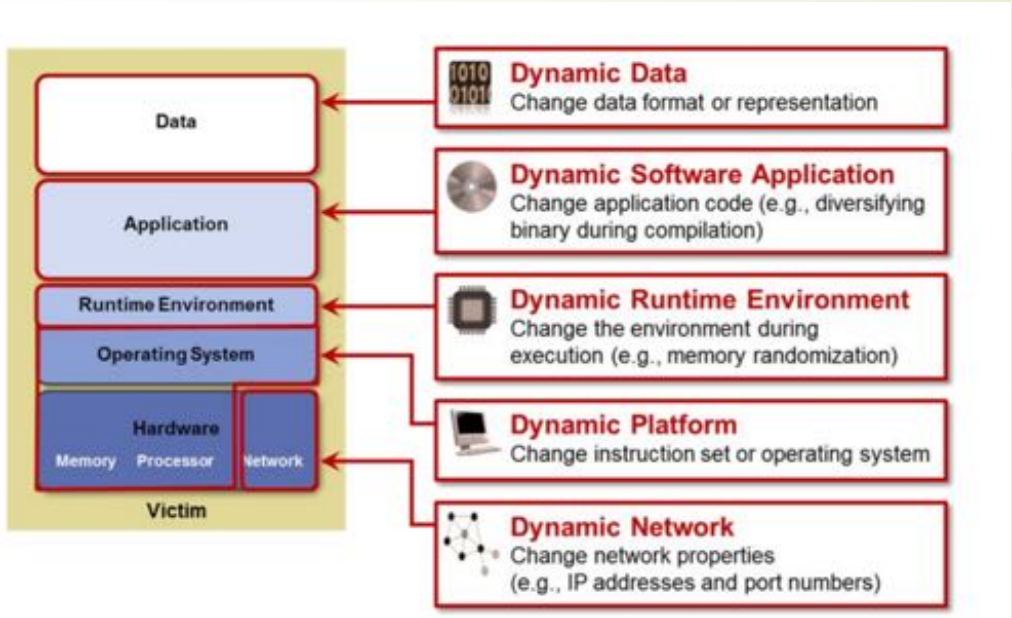


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
  - Format
  - Syntax
  - Encoding
  - Encryption
  - Representation

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

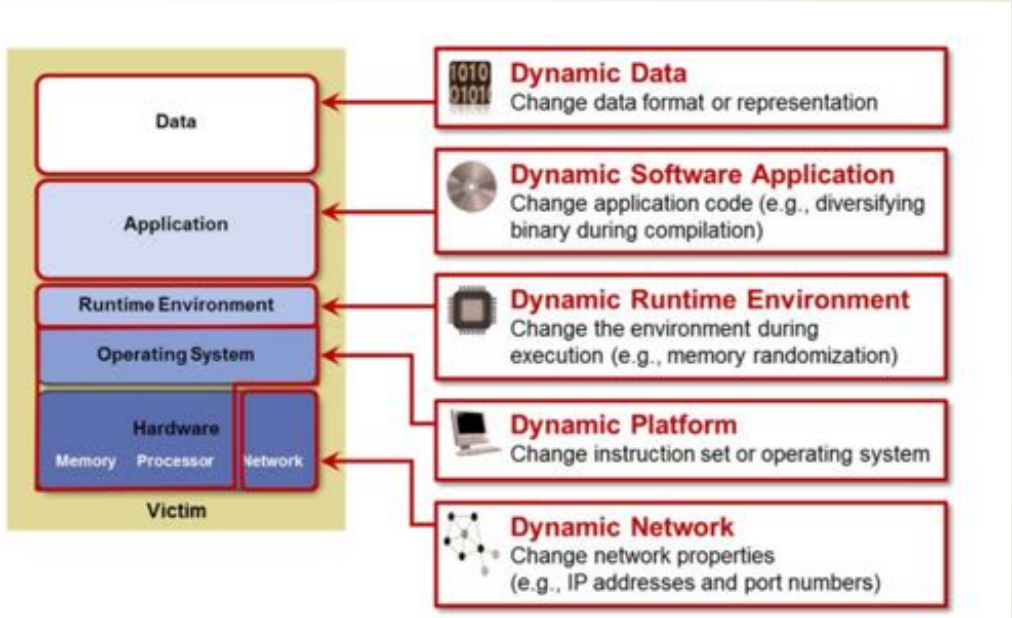


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
  - Instructions
  - Order
  - Grouping
  - Format

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

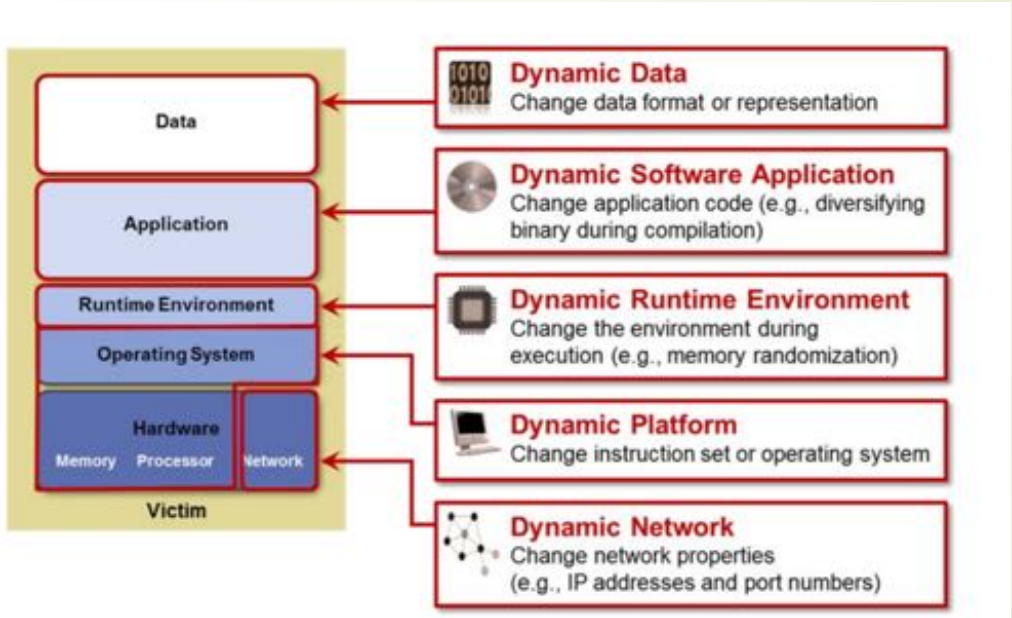


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

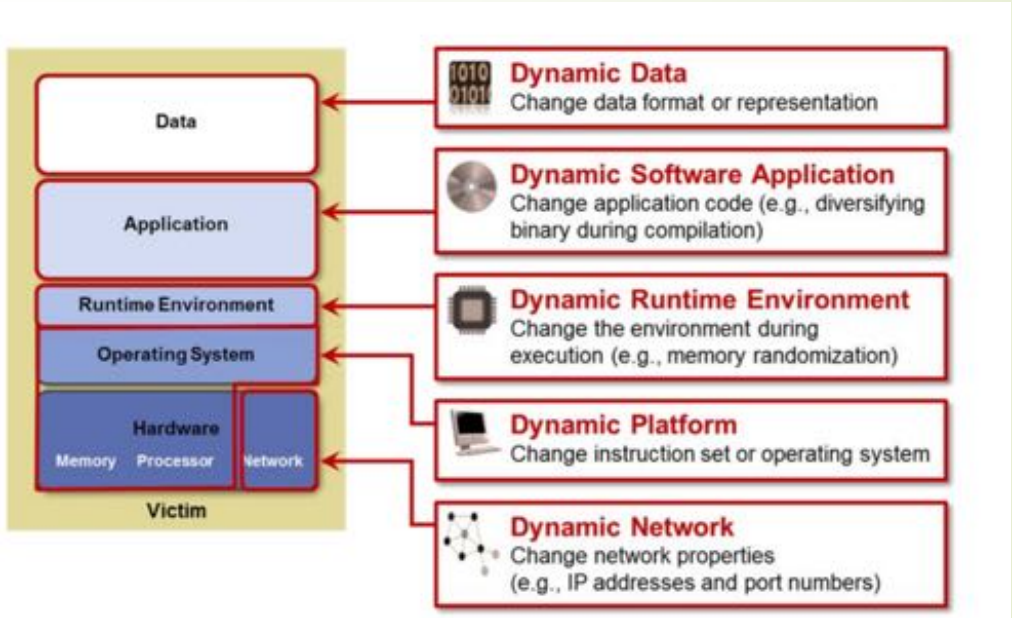


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
    - Code
    - Libraries
    - Stack/heap
    - Functions

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

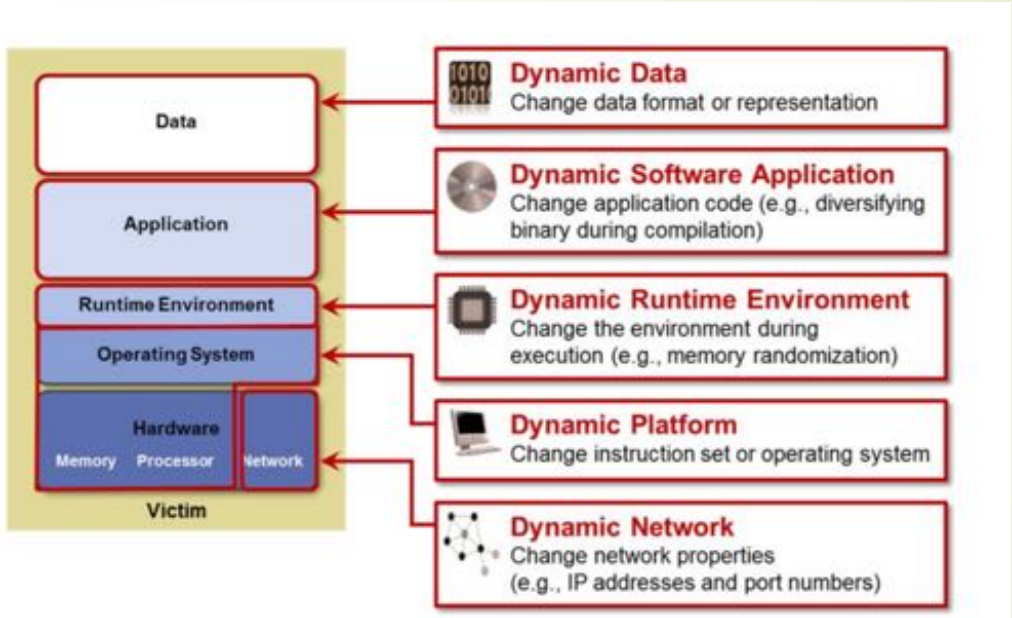


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
    - Interface presented by the operating system

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

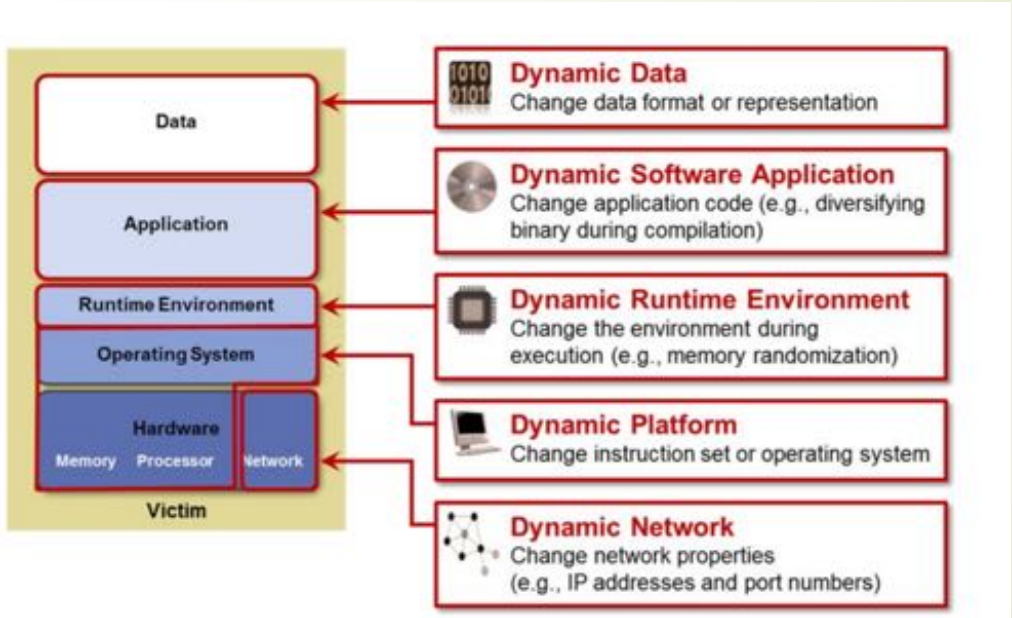


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
  - OS version
  - CPU architecture
  - OS instance
  - Platform data format

Moving-Targets

- Any technique that attempts to defend a system and increase the complexity of cyber attacks by making the system less homogeneous, static, or deterministic
- Dynamic Data
- Dynamic Software
- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks

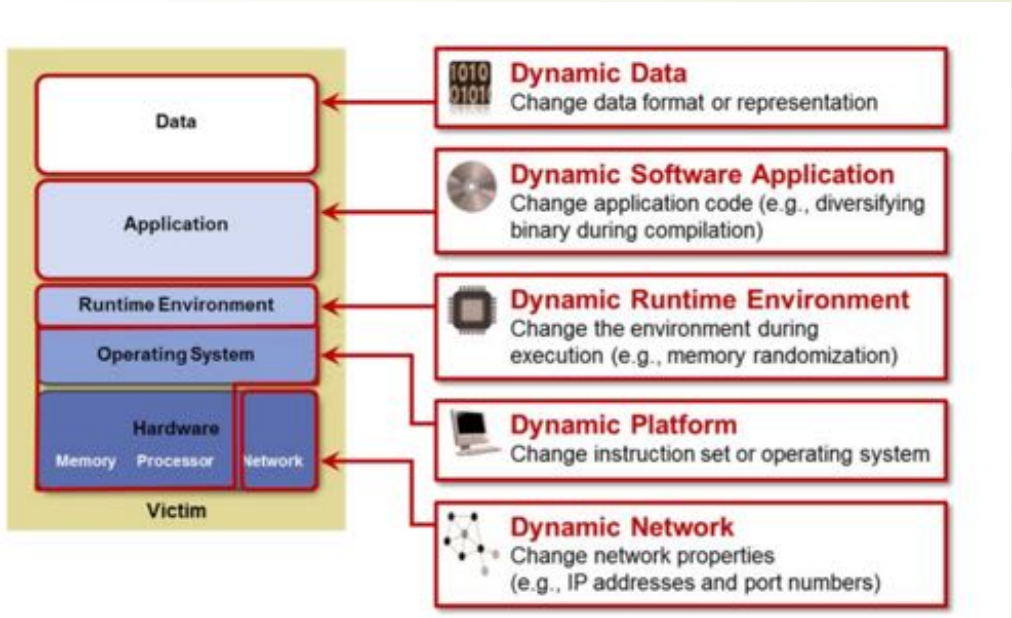


Figure 1. Different categories of moving target techniques.

Moving-Targets

- Dynamic Runtime Environment
  - Address Space Randomization
  - Instruction Set Randomization
- Dynamic Platforms
- Dynamic Networks
  - Protocols
  - Addresses

WEAKNESSES

- Overcome Movement
- Predict Movement
- Limit Movement
- Disable Movement

Thank you!