Gui-lin Cai, Bao-sheng Wang, Wei Hu, Tian-zuo Wang, 2016. Moving target defense: state of the art and characteristics. *Frontiers of Information Technology & Electronic Engineering*, **17**(11):1122-1153. http://dx.doi.org/10.1631/FITEE.1601321

Moving target defense: state of the art and characteristics

Front Inform Technol Electron Eng

Key words: Moving target defense, Security model, Function-and-movement model, Characteristics

Corresponding author: Gui-lin Cai
E-mail: cc_cai@163.com
ORCID: http://orcid.org/0000-0002-9322-2539

Motivation

- Moving target defense (MTD) has emerged as one of the game-changing themes to alter the asymmetric situation between attacks and defenses in cyber-security.
- Numerous related works involving several facets of MTD have been published.
- Comprehensive analyses and research on MTD are still absent.

Front Inform Technol Electron Eng

Main idea

1. Describing the changes in the traditional defense paradigm and security model caused by the introduction of MTD
   (1) A new security model is introduced to describe the changes
2. Presenting a systematic interpretation of published literature to describe the state of the art of three main areas in MTD field
   (1) A function-and-movement model is provided to give a panoramic overview for understanding the existing MTD research works
   (2) In the area of MTD theory: extracting the three elements of an MTD
   (3) In the area of MTD strategy: identifying the common characteristics
   (4) In the area of MTD evaluation: summarizing existing evaluation approaches

Front Inform Technol Electron Eng

Major results

1. The changes on the defense paradigm and process

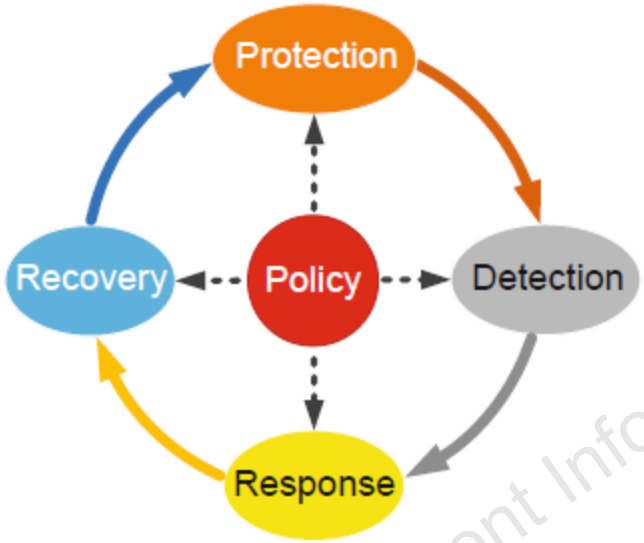

Fig. 1 The policy, protection, detection, response, and recovery (PPDRR) model

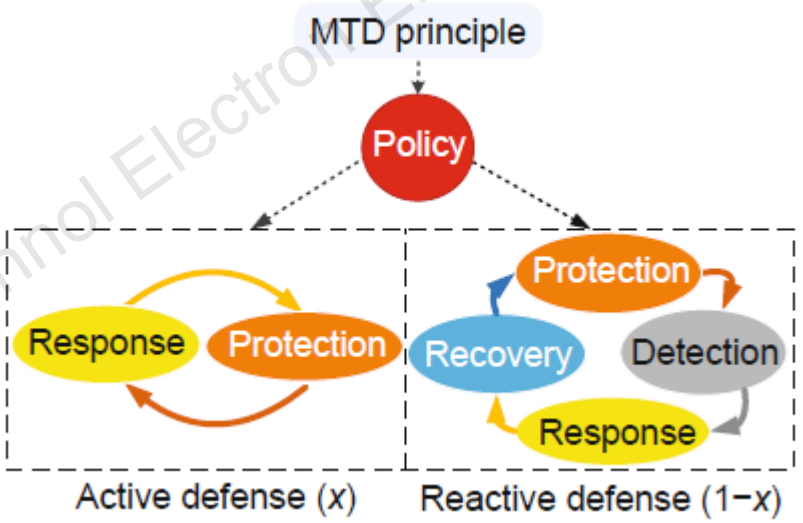

Fig. 2 New security model with moving target defense (MTD)

$0.5 < x \leq 1$, and the value of x is determined by the defender/administrator as a security-cost trade-off.

Front Inform Technol Electron Eng

Major results

2(1). A function-and-movement model

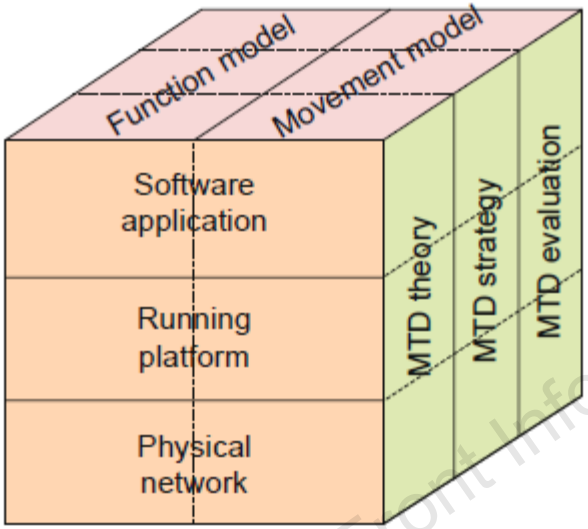

Fig. 3 Function-and-movement model

- Three areas in MTD field
  - MTD theory / MTD strategy / MTD evaluation
- A networking system:
  - Constitution: Software / running platform / physical network
  - Abilities: normal functionality / MTD
- MTD can implemented in one of the three layers or more
- The research of movement involves all the three areas

Front Inform Technol Electron Eng

Major results

2(2). The three elements of an MTD technique

- What to move
  - the moving parameter
    - software/application (the category of ST)
    - execution environment (the category of DPT)
      - running platform, or configuration
    - Network address (the category of NAS)
      - IP address, port number, or both of the two
- How to move
  - the way to move
    - Selection: choosing the next value of the moving parameter
    - Replacement: using the selected new value to replace the old one
- When to move
  - the frequency of moving

Front Inform Technol Electron Eng

Major results

2(3)-1. The common characteristics shared by MTD strategies

- The characteristics
  - Four main characteristics
    - multi-candidates / diversity / randomness / limited timeliness
  - A minor characteristic
    - attack surface reduction
- The types of MTD technique
  - HETE-type: to make the target less homogeneous
  - DYNA-type: to make the target less static and less deterministic
  - Mixed-type: to make the target less static, less deterministic, and less homogeneous

Front Inform Technol Electron Eng

Major results

2(3)-2. The necessary and sufficient conditions to create an MTD

- For each proper MTD, multi-candidates is the necessary condition for all the three types of MTD
- For an MTD strategy with HETE-type, multi-candidates and diversity are the two necessary and sufficient conditions
- For an MTD strategy with DYNA-type, multi-candidates, randomness, and limited timeliness are the three necessary and sufficient conditions
- For an MTD strategy with Mixed-type, multi-candidates, diversity, randomness, and limited timeliness are the four necessary and sufficient conditions
- Attack surface reduction is an assistant method, and it can only be used in the strategies falling in the categories of ST and DPT

Front Inform Technol Electron Eng

Major results

2(4). Summarizing the existing evaluation approaches

- Existing evaluation approaches can be divided into two groups according to their goals
  - One group aims to evaluate the effectiveness of one type of MTD strategies
  - The other group not only evaluates the effectiveness of one type of MTD strategies, but also identifies the parameters that can influence the defense effect of these MTD strategies
- The shortcomings for the existing evaluation approaches
  - lacking the evaluation of performance and efficiency
  - lacking the comparison among different MTD techniques

Front Inform Technol Electron Eng

Conclusions

There are still some directions that need to be researched in depth in this field

- Practicality
- Hybrid MTD design
- Network monitoring
- Application on existing approaches
- Evaluation
- Application of game theory and adversarial model
- Application of SDN architecture

Front Inform Technol Electron Eng