**A link of introducing MTD:**

https://blog.cryptomove.com/moving-target-defense-recent-trends-253ce784a680

MTD methods: adaptive address space layout randomization,adaptive data structure layout randomization, dynamic platforms and software diversity.

**Conception of MTD**:

--Instead of defending unchanging infrastructure by detecting, preventing,monitoring,tracking,

Or remediating threats, moving target defence makes the attack surface dynamic.

--The idea of moving target defense(MTD) is to impose the same asymmetric disadvantage on attackers by making system dynamic and therefore harder to explore and predict.

--The ultimate goal of MTD is to increase the attacker’s workload so as to level the cybersecurity playing field for both defenders and attackers

A set of papers that relating to MTD:

# **U-TRI: Unlinkability Through Random Identifier for SDN Network**

U-TRI employs a randomly changing identifier to replace the original static data link layer address. By obfuscating the identifiers of in network and transport layer to defend traffic analysis.

# **WebMTD: Defeating Web Code Injection Attacks using Web Element Attribute Mutation**

WebMTD randomizes certain attributes of Web elements to differentiate the application code from injected code and disallow its execution. This is done without requiring Web developer involvement and browser code modification.

# **Mixr: Flexible Runtime Rerandomization for Binaries**

Mixr is an improvement on ASLR system. It gives the security architect the flexibility to specify **the randomization points and granularity** and does not require access to the target program/library’s information.

ASLR system: it is a computer security technique to prevent memory corruption vulnerabilities. In order to randomly prevent the attacker to reliably jumping to a particular function in the memory, ASLR arranges the address space of a process,including the base of the executable and positions of the stack,heap and libraries.

**Mutated Policies: Towards Proactive Attribute-based Defenses for Access Control**

It collects the attributes from the entities involved in the access request process,then carefully select the attributes that uniquely identify the entities,and randomly mutate the original access policies over time by adding additional policy rules constructed from the newly-identified attributes.

# **Detecting Stealthy Botnets in a Resource-Constrained Environment using Reinforcement Learning**

It optimally and dynamically deploy a limited number of defensive mechanisms, honeypots and network-based detectors,within the largest network. The goal is to reduce the lifetime of stealthy botnets by maximizing the number of bots identified and taken down through a sequential decision-making process.

**Multi-Stage Attack Graph Security Games: Heuristic Strategies, with Empirical Game-Theoretic Analysis**

It formulated the administrator and cybercriminals as a security game. they propose parameterized heuristic strategies for both players. The heuristics exploit the topological structure of the attack graphs and employ different sampling methodologies to overcome the computational complexity in determining player’s actions.

**Online Algorithms for Adaptive Cyber Defense on Bayesian Attack Graph**

MTD: the defender dynamically and proactively reconfigure developed defense so as to increase uncertainly and complexity for attackers.

Given previous actions, induced utility values and observations,the defender forms a belief about the current state of the system and takes the empirical average of utility values to estimate of the utility functions.

# **Path Hopping: an MTD Strategy for Quantum-safe Communication**

It use MTD strategies as a cryptographic mechanism for providing secure communication. This paper propose a cryptographic system that uses an MTD strategy that achieves long-term quantum-safe security.

# Path Hopping: an MTD Strategy for Quantum-safe Communication

Moving target defense (MTD) strategies have been widely studied for securing computer communication systems. We consider using MTD strategies as a cryptographic mechanism for providing secure communication when the adversary has access to a quantum computer and security is required over a long period of time. We assume Alice and Bob are connected by multiple disjoint paths, not all of which can be eavesdropped by the attacker at the same time. We propose a cryptographic system that uses an MTD strategy that achieves long-term quantum-safe security. We model the system as a Markov chain, and propose two security measures that correspond to two types of adversaries, called risk-taking and risk-averse. Our numerical simulations shows dependencies between system parameters, and leads to new insights, such as quantifying the cost of being a risk-averse adversary.

# If You Can't Measure It, You Can't Improve It: Moving Target Defense Metrics

We propose new metrics drawing inspiration from the optimization domain that can be used to characterize the effectiveness of moving target defenses better. Besides that, we propose a Network Neighborhood Partitioning algorithm that can help to measure the influence of MTDs more precisely. The techniques proposed here are generic and could be combined with existing metrics. The obtained results demonstrate how additional information about the effectiveness of defenses can be obtained as well as how network neighborhood partitioning helps to improve the granularity of metrics.