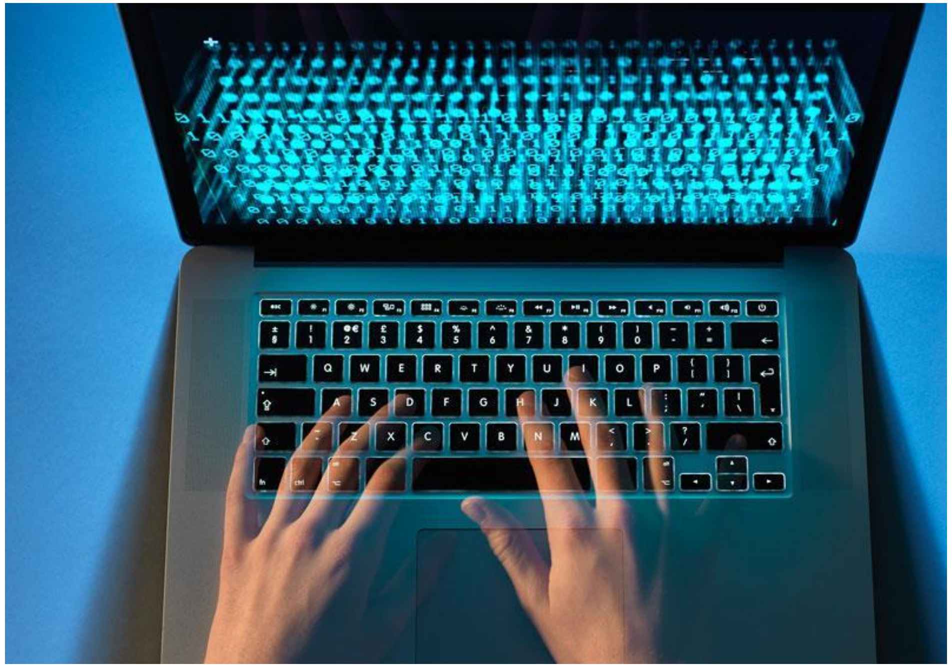
动态防御技术的实战应用与前沿发展

张长河

动态防御

动态防御技术 （Moving Target Defense）被誉为当今最具影响力的安全创新机会

技术目标



静态特性易于攻击难以防御

攻击者具有不对称优势

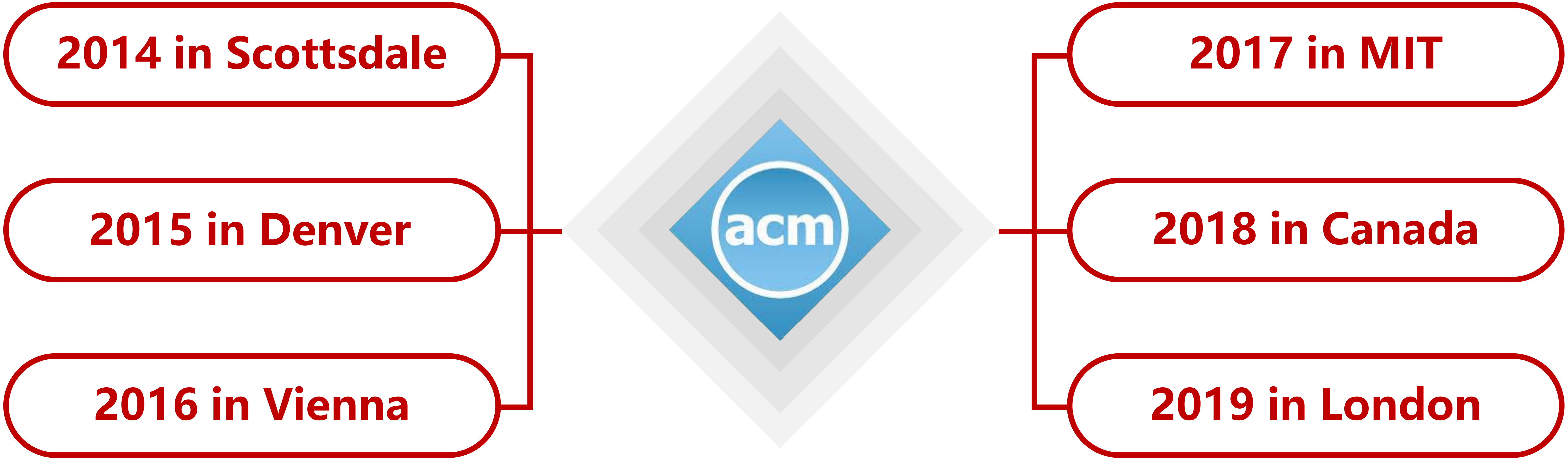
变化系统及其攻击面

迫使攻击者处理大量的不确定性

增加攻击者的工作量

防御者具有不对称优势

ACM 国际计算机学会



2014 in Scottsdale

2015 in Denver

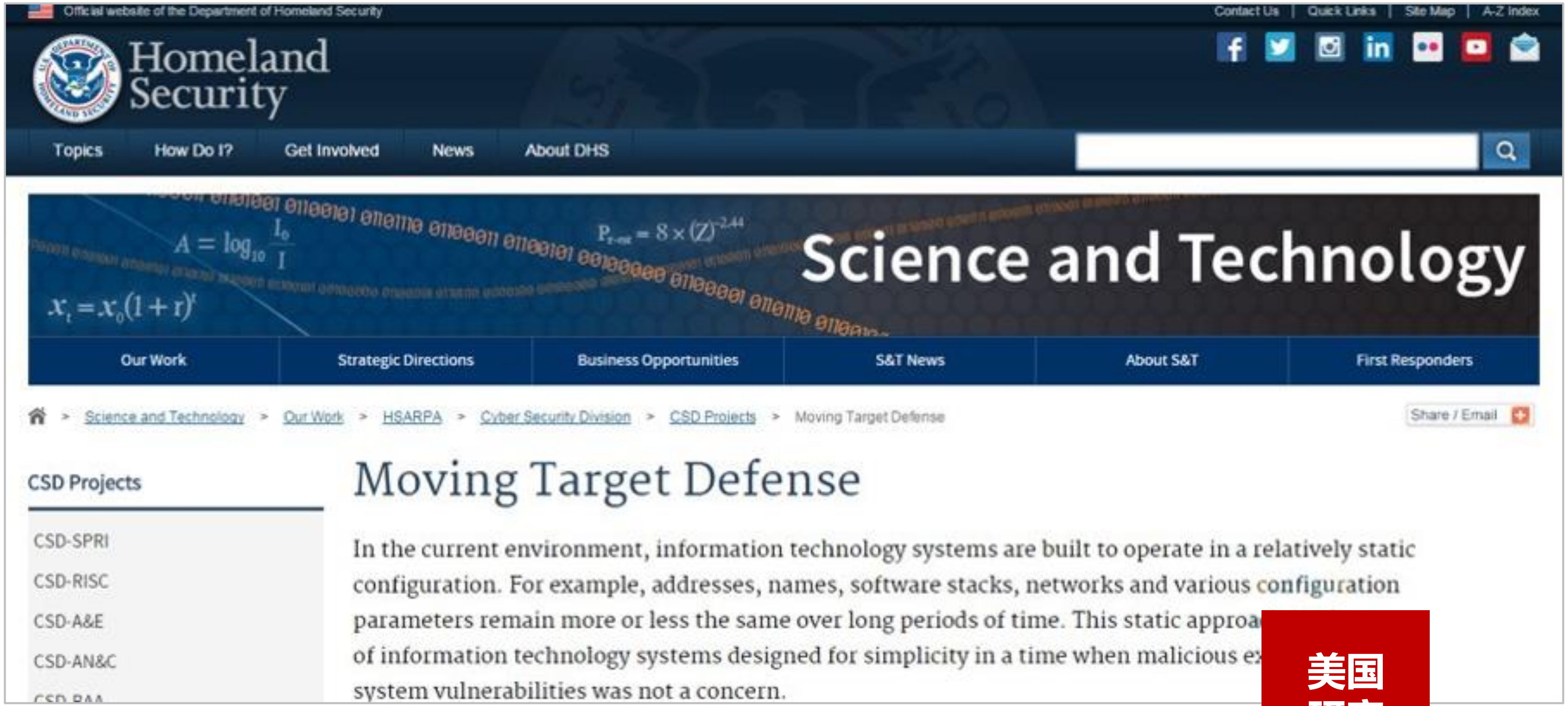
2016 in Vienna

2017 in MIT

2018 in Canada

2019 in London

业内行情


Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
$A = \log_{10}\frac{I_0}{I}$
$P_{f-ex} = 8 \times (Z)^{2.44}$
$x_t = x_0(1+r)^t$
Science and Technology
Our Work
Strategic Directions
Business Opportunities
S&T News
About S&T
First Responders
Science and Technology > Our Work > HSARPA > Cyber Security Division > CSD Projects > Moving Target Defense
Share / Email
CSD Projects
CSD-SPRI
CSD-RISC
CSD-A&E
CSD-AN&C
CSD-BAA

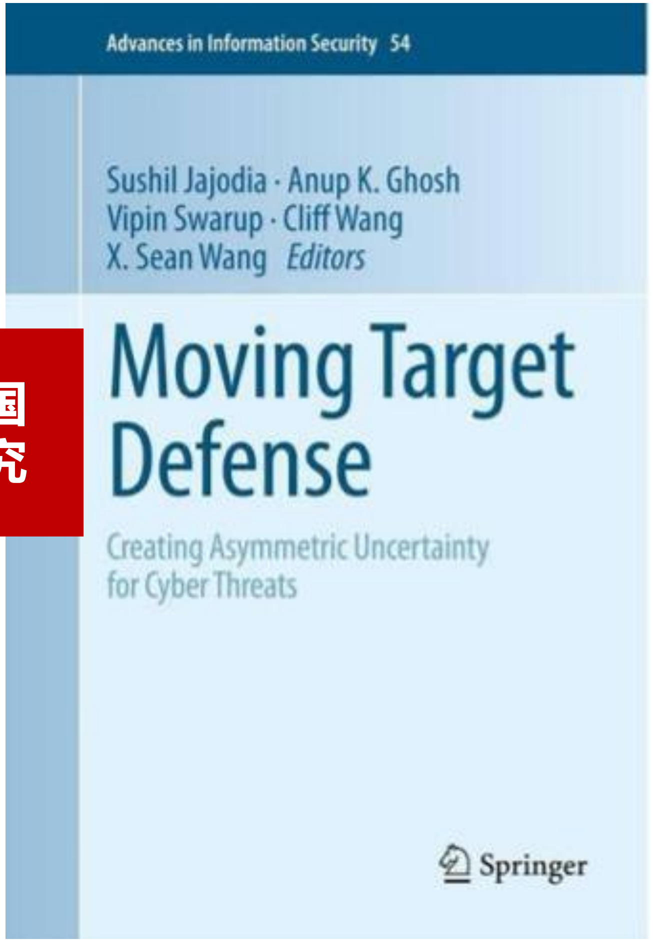
Moving Target Defense

In the current environment, information technology systems are built to operate in a relatively static configuration. For example, addresses, names, software stacks, networks and various configuration parameters remain more or less the same over long periods of time. This static approa of information technology systems designed for simplicity in a time when malicious ex system vulnerabilities was not a concern.

美国研究

业内行情

美国研究



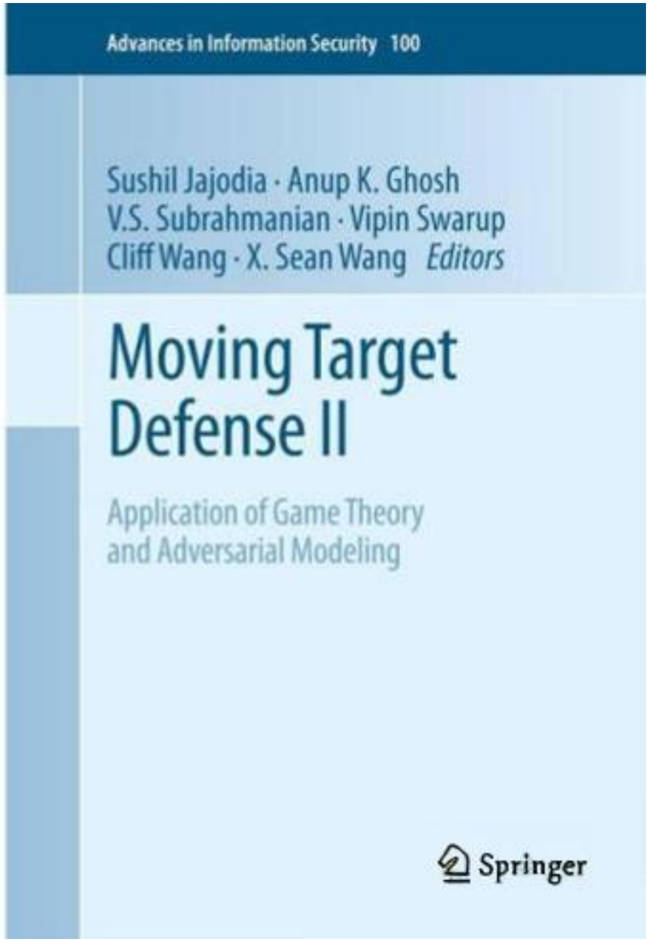
Advances in Information Security 54

Sushil Jajodia · Anup K. Ghosh
Vipin Swarup · Cliff Wang
X. Sean Wang *Editors*

Moving Target Defense

Creating Asymmetric Uncertainty for Cyber Threats

Springer



Advances in Information Security 100

Sushil Jajodia · Anup K. Ghosh
V.S. Subrahmanian · Vipin Swarup
Cliff Wang · X. Sean Wang *Editors*

Moving Target Defense II

Application of Game Theory and Adversarial Modeling

Springer

ACM2018

System randomization 系统随机化

Artificial diversity 人工多样性

Cyber maneuver and agility 网络机动和敏捷

Software diversity 软件多样性

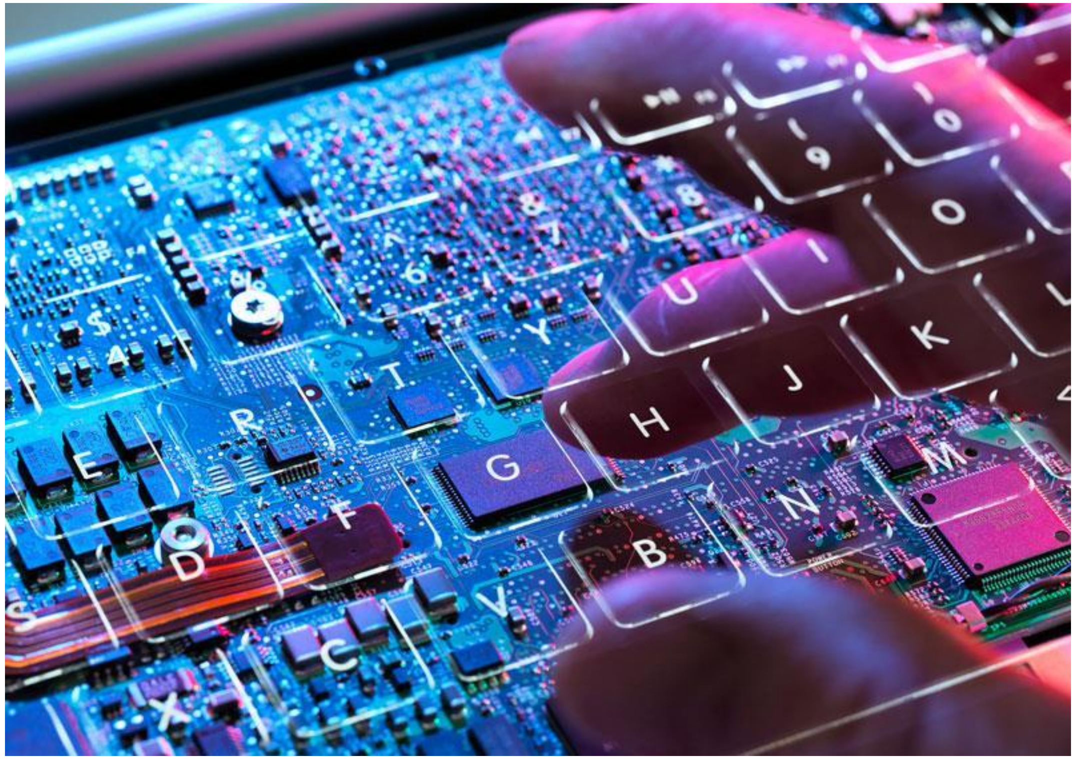
Dynamic network configuration 动态网络配置

Moving target in the cloud 云中移动目标

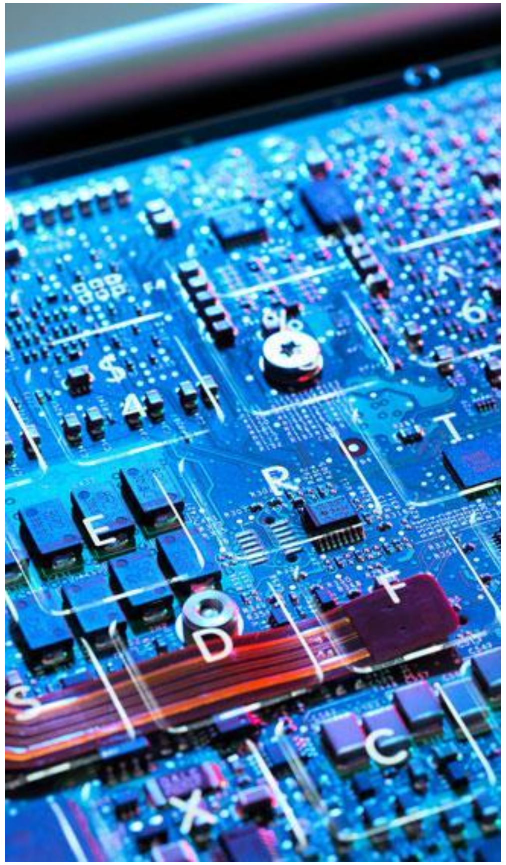
System diversification techniques 系统多样化技术

Dynamic compilation techniques 动态编译技术

Adaptive defenses 适应性防御



ACM2018



Intelligent countermeasure selection 智能对策选择

MTD strategies and planning MTD策略和计划

Deep learning for MTD 深入学习MTD

MTD quantification methods and models MTD量化方法和模型

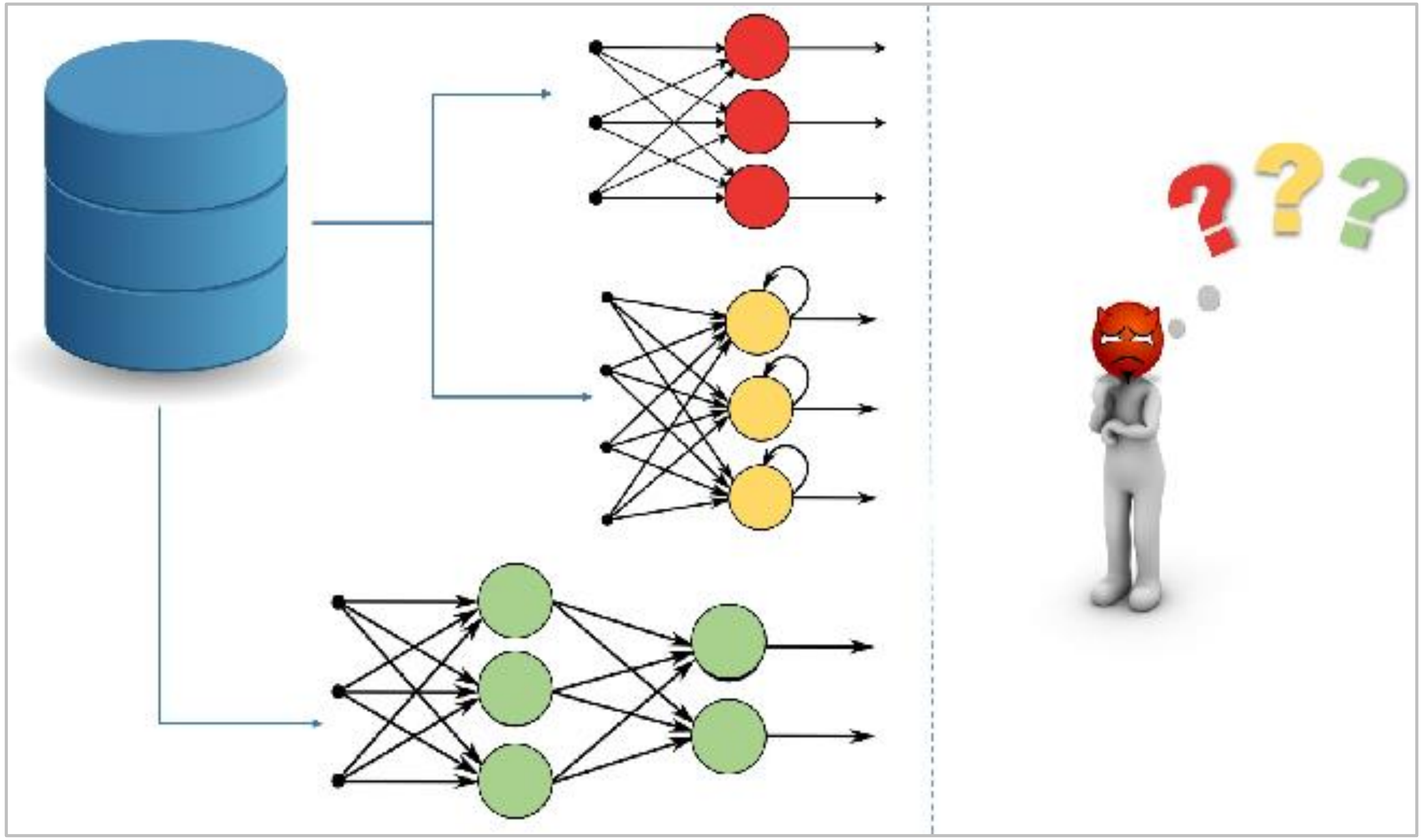
MTD evaluation and assessment frameworks MTD评估和评估框架

Large-scale MTD (using multiple techniques) 大规模MTD（使用多种技术）

Moving target in software coding, application API virtualization 在软件编码中移动目标，应用程序API虚拟化

Autonomous technologies for MTD MTD的自主技术

改变游戏规则



2015 in Denver,

改变游戏规则的

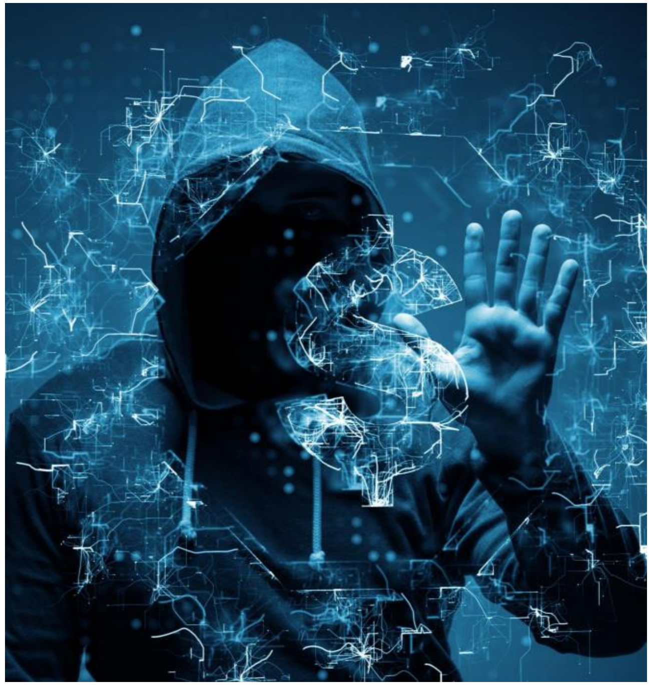
防御技术

增益效果

MTD的网络安全增益有多大？

HUGE!

增益效果



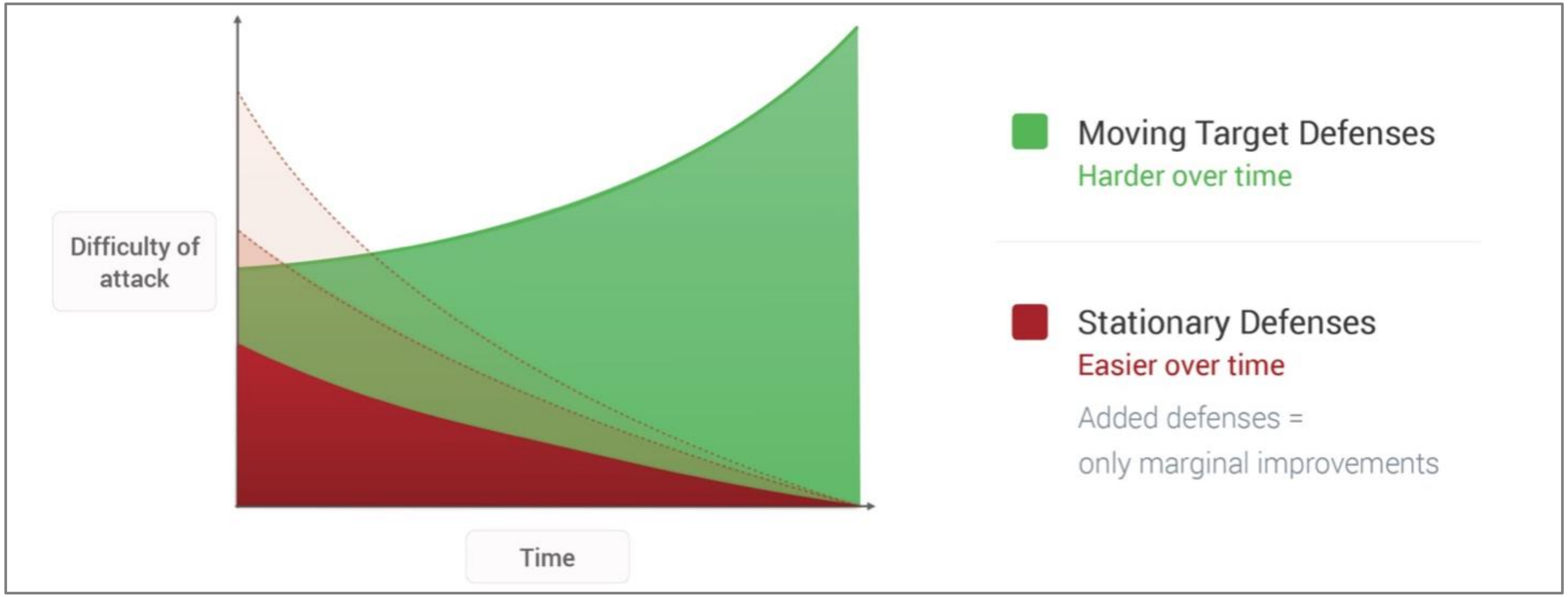
动态防御是一种颠覆性的防御理念，而不是优化目前的防御方式

今天的安全模型优先考虑监控，检测，预防和修复

安全团队以静态的基础架构为基础，防御千变万化的攻击方法，严重不对称

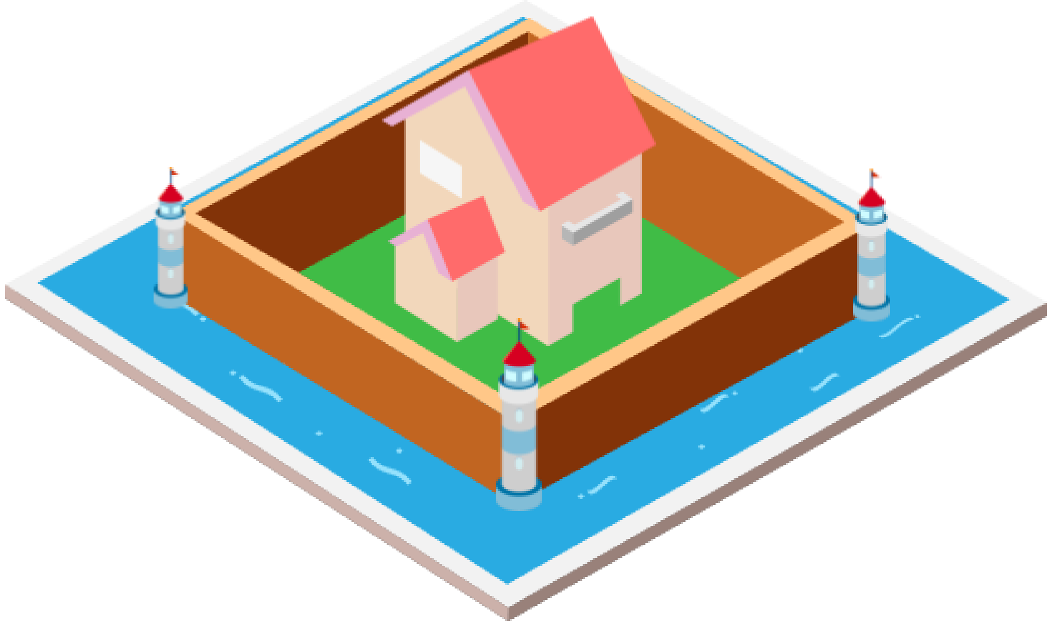
现在的安全创新都是想，怎么找到 更多的漏洞、找到更多的特征、提高检测效率，即使用了新的工具，防御者背负着巨大的压力，攻击者却有足够的时间研究静态基础设施和静态的防御技术。

增益效果



动态防御通过动态变化攻击面，让攻击者随着攻击时间难度不但不会降低，还会增加，大大增加了攻击者攻击成本，扭转了攻防不对称的局面。

传统防御方法



存在问题

被动的

静态的

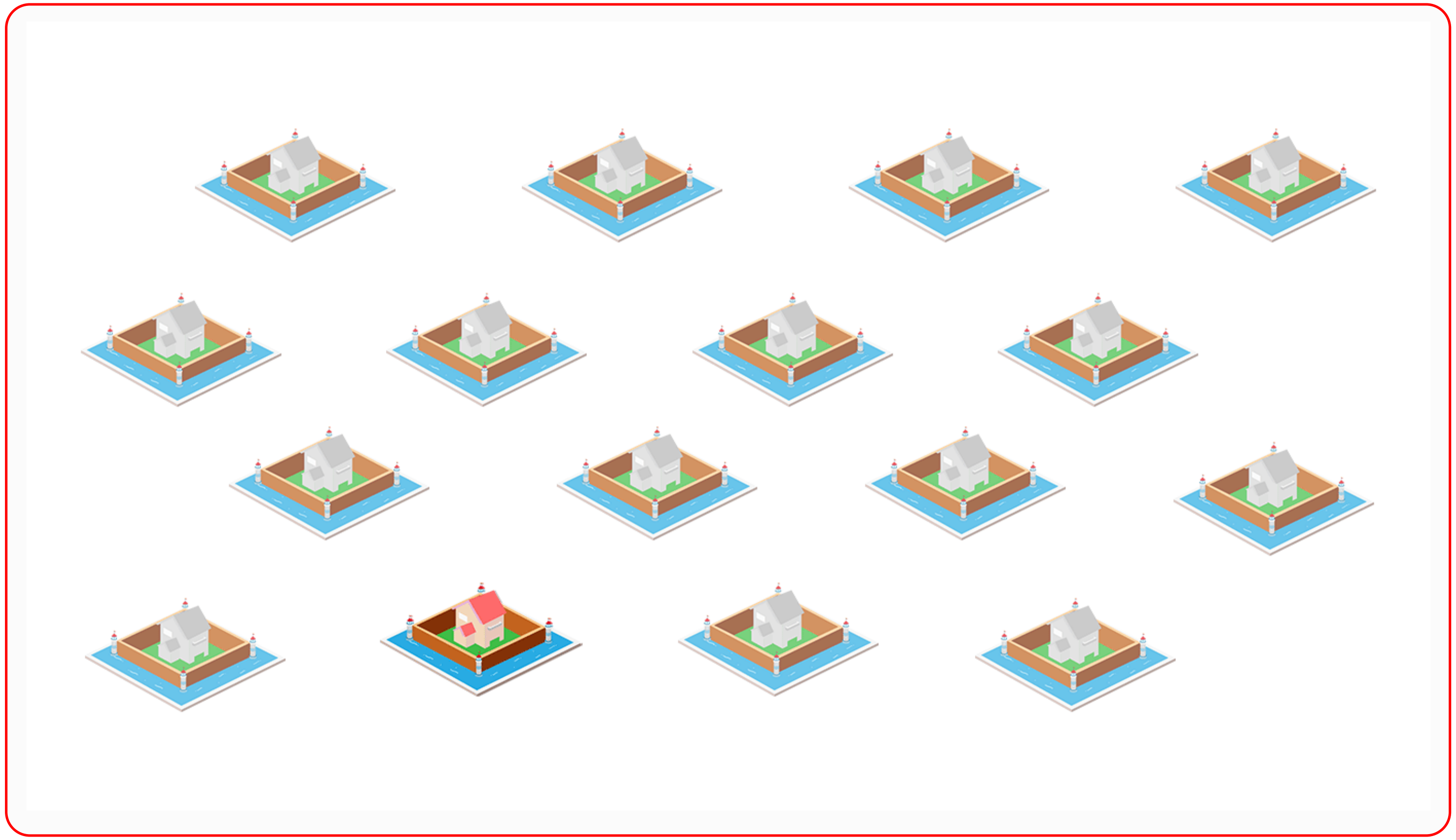
攻击者优势

效果差

动态防御优势

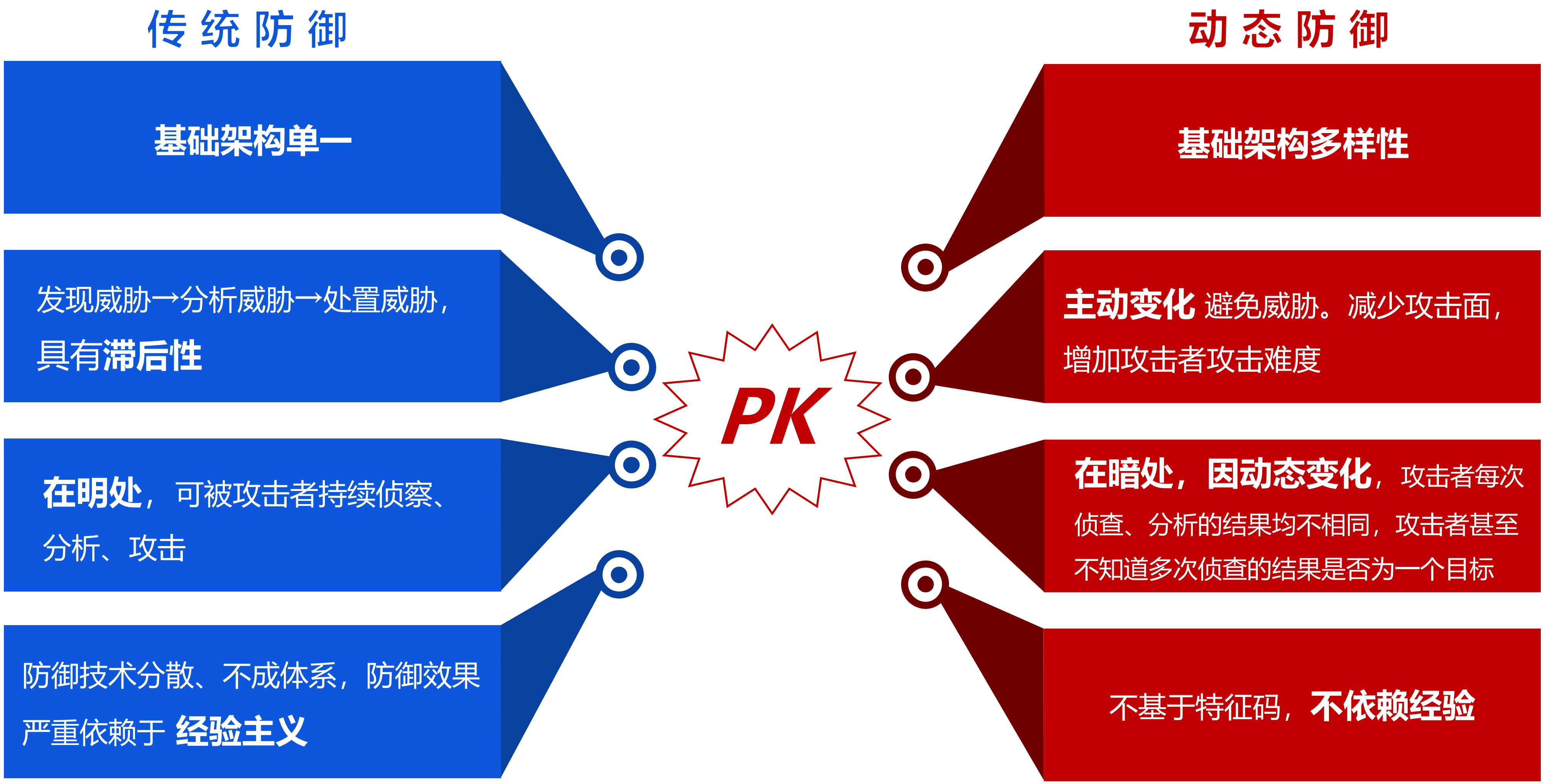
$$\left(\frac{1}{2^{48}}\right)^n$$

$$\left(\frac{1}{2^{128}}\right)^n$$



极大降低攻击成功概率

智能动态防御特点分析



传统防御

基础架构单一

发现威胁→分析威胁→处置威胁，具有**滞后性**

在明处，可被攻击者持续侦察、分析、攻击

防御技术分散、不成体系，防御效果严重依赖于 **经验主义**

PK

动态防御

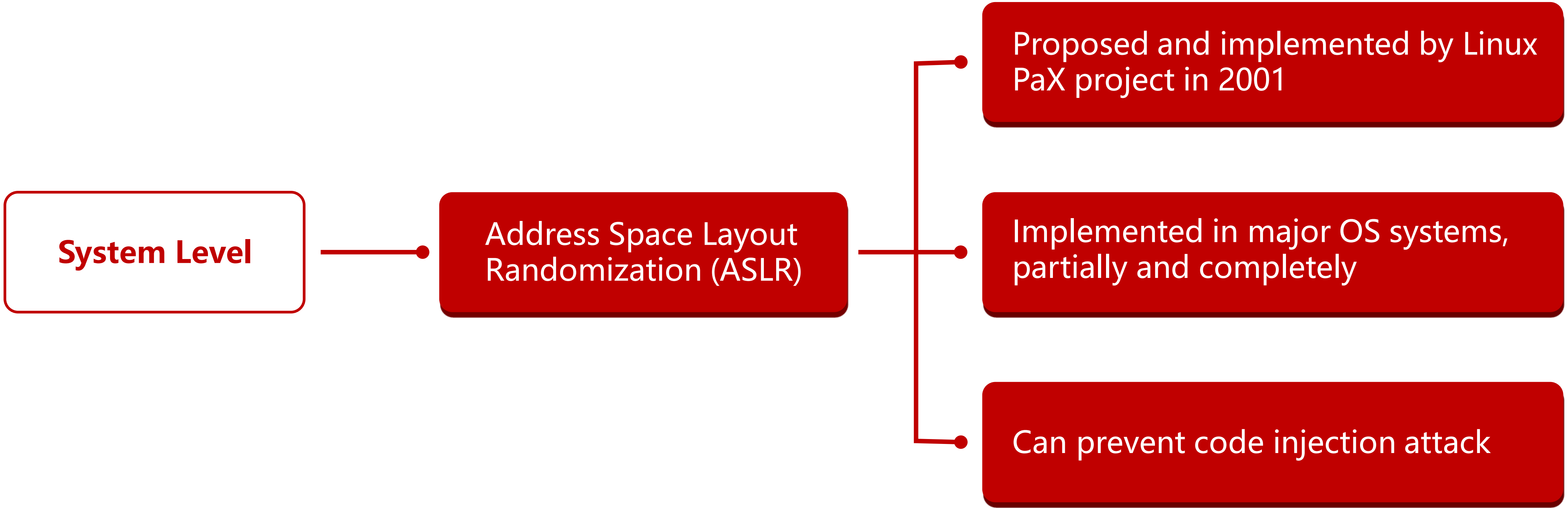
基础架构多样性

主动变化 避免威胁。减少攻击面，增加攻击者攻击难度

在暗处，因动态变化，攻击者每次侦查、分析的结果均不相同，攻击者甚至不知道多次侦查的结果是否为一个目标

不基于特征码，**不依赖经验**

目前研究态势



System Level

Address Space Layout Randomization (ASLR)

Proposed and implemented by Linux PaX project in 2001

Implemented in major OS systems, partially and completely

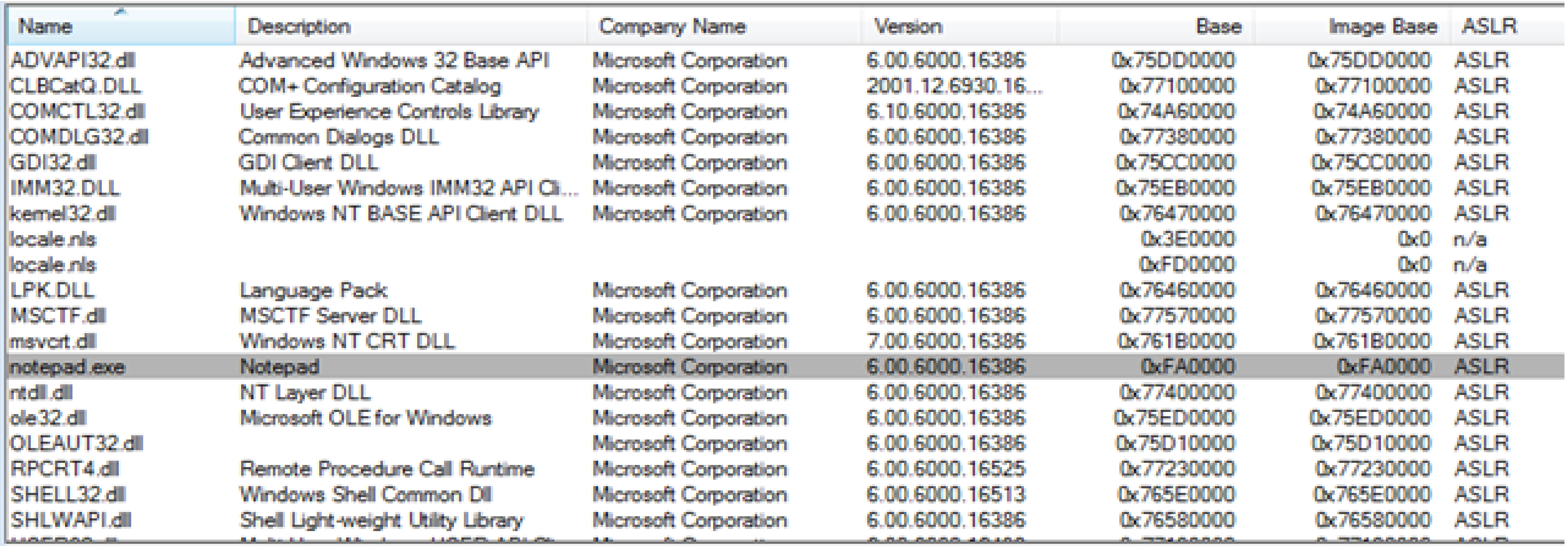
Can prevent code injection attack

目前研究态势

Moving Target Defense Research

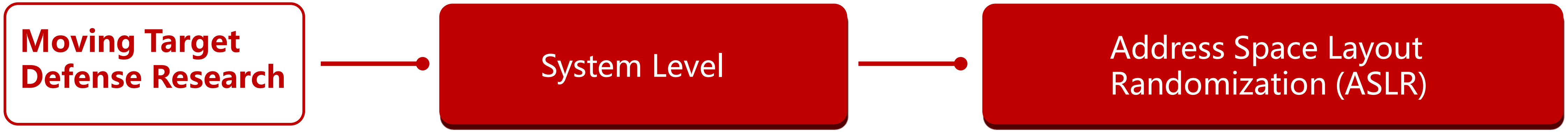
System Level

Address Space Layout Randomization (ASLR)



Name	Description	Company Name	Version	Base	Image Base	ASLR
ADVAPI32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.00.6000.16386	0x75DD0000	0x75DD0000	ASLR
CLBCatQ.DLL	COM+ Configuration Catalog	Microsoft Corporation	2001.12.6930.16...	0x77100000	0x77100000	ASLR
COMCTL32.dll	User Experience Controls Library	Microsoft Corporation	6.10.6000.16386	0x74A60000	0x74A60000	ASLR
COMDLG32.dll	Common Dialogs DLL	Microsoft Corporation	6.00.6000.16386	0x77380000	0x77380000	ASLR
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.00.6000.16386	0x75CC0000	0x75CC0000	ASLR
IMM32.DLL	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	6.00.6000.16386	0x75EB0000	0x75EB0000	ASLR
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.00.6000.16386	0x76470000	0x76470000	ASLR
locale.nls				0x3E0000	0x0	n/a
locale.nls				0xFD0000	0x0	n/a
LPK.DLL	Language Pack	Microsoft Corporation	6.00.6000.16386	0x76460000	0x76460000	ASLR
MSCTF.dll	MSCTF Server DLL	Microsoft Corporation	6.00.6000.16386	0x77570000	0x77570000	ASLR
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	7.00.6000.16386	0x761B0000	0x761B0000	ASLR
notepad.exe	Notepad	Microsoft Corporation	6.00.6000.16386	0xFA0000	0xFA0000	ASLR
ntdll.dll	NT Layer DLL	Microsoft Corporation	6.00.6000.16386	0x77400000	0x77400000	ASLR
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	6.00.6000.16386	0x75ED0000	0x75ED0000	ASLR
OLEAUT32.dll		Microsoft Corporation	6.00.6000.16386	0x75D10000	0x75D10000	ASLR
RPCRT4.dll	Remote Procedure Call Runtime	Microsoft Corporation	6.00.6000.16525	0x77230000	0x77230000	ASLR
SHELL32.dll	Windows Shell Common Dll	Microsoft Corporation	6.00.6000.16513	0x765E0000	0x765E0000	ASLR
SHLWAPI.dll	Shell Light-weight Utility Library	Microsoft Corporation	6.00.6000.16386	0x76580000	0x76580000	ASLR

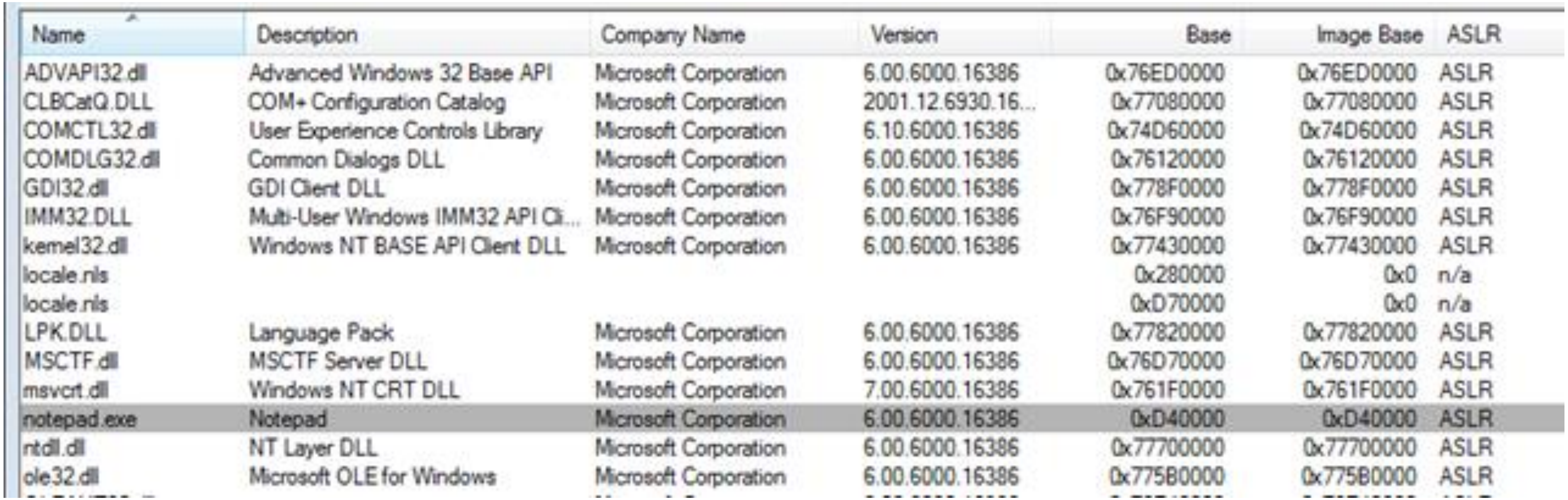
目前研究态势



Moving Target Defense Research

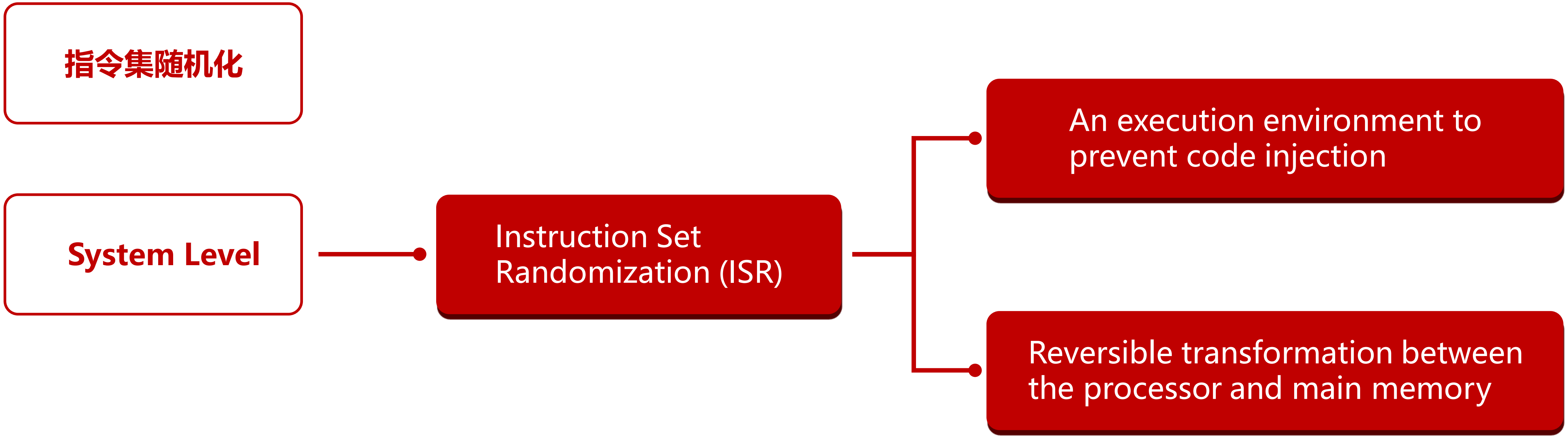
System Level

Address Space Layout Randomization (ASLR)



Name	Description	Company Name	Version	Base	Image Base	ASLR
ADVAPI32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.00.6000.16386	0x76ED0000	0x76ED0000	ASLR
CLBCatQ.DLL	COM+ Configuration Catalog	Microsoft Corporation	2001.12.6930.16...	0x77080000	0x77080000	ASLR
COMCTL32.dll	User Experience Controls Library	Microsoft Corporation	6.10.6000.16386	0x74D60000	0x74D60000	ASLR
COMDLG32.dll	Common Dialogs DLL	Microsoft Corporation	6.00.6000.16386	0x76120000	0x76120000	ASLR
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.00.6000.16386	0x778F0000	0x778F0000	ASLR
IMM32.DLL	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	6.00.6000.16386	0x76F90000	0x76F90000	ASLR
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.00.6000.16386	0x77430000	0x77430000	ASLR
locale.nls				0x280000	0x0	n/a
locale.nls				0xD70000	0x0	n/a
LPK.DLL	Language Pack	Microsoft Corporation	6.00.6000.16386	0x77820000	0x77820000	ASLR
MSCTF.dll	MSCTF Server DLL	Microsoft Corporation	6.00.6000.16386	0x76D70000	0x76D70000	ASLR
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	7.00.6000.16386	0x761F0000	0x761F0000	ASLR
notepad.exe	Notepad	Microsoft Corporation	6.00.6000.16386	0xD40000	0xD40000	ASLR
ntdll.dll	NT Layer DLL	Microsoft Corporation	6.00.6000.16386	0x77700000	0x77700000	ASLR
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	6.00.6000.16386	0x775B0000	0x775B0000	ASLR

目前研究态势



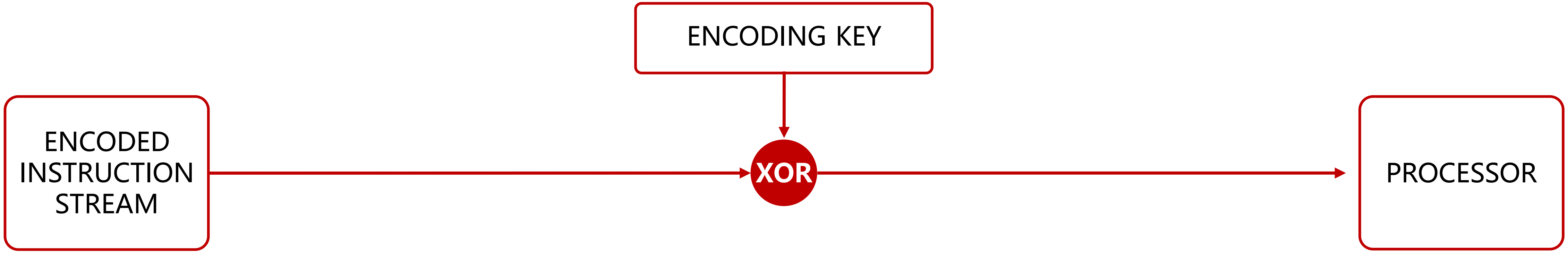
指令集随机化

System Level

Instruction Set Randomization (ISR)

An execution environment to prevent code injection

Reversible transformation between the processor and main memory



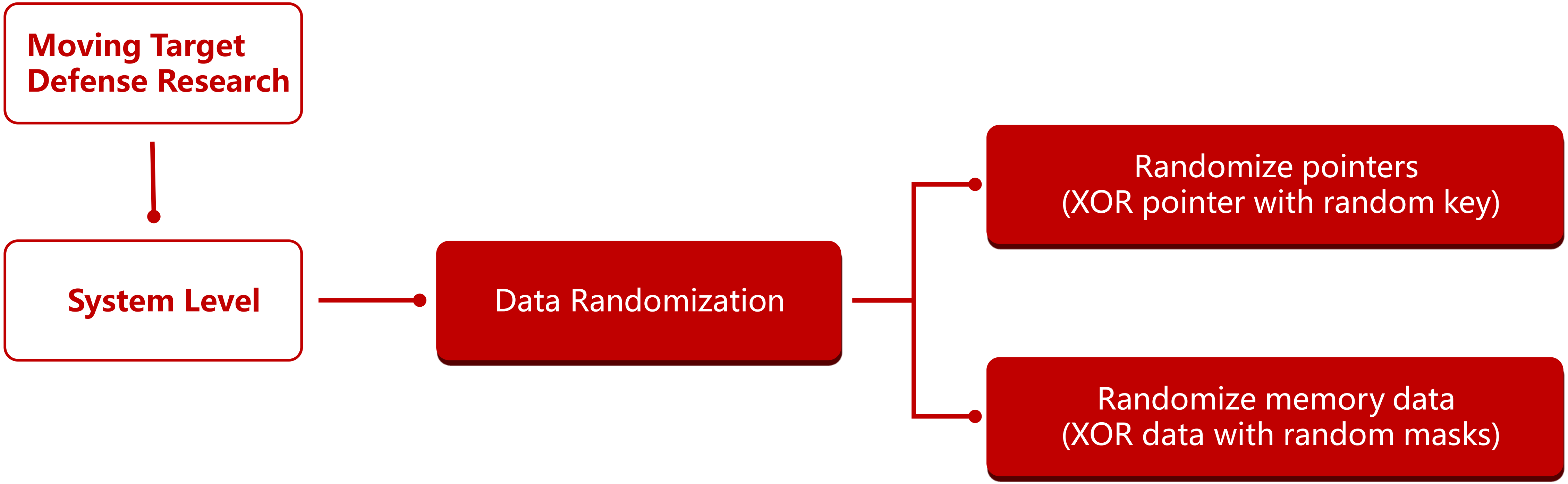
ENCODING KEY

ENCODED INSTRUCTION STREAM

XOR

PROCESSOR

目前研究态势



Moving Target Defense Research

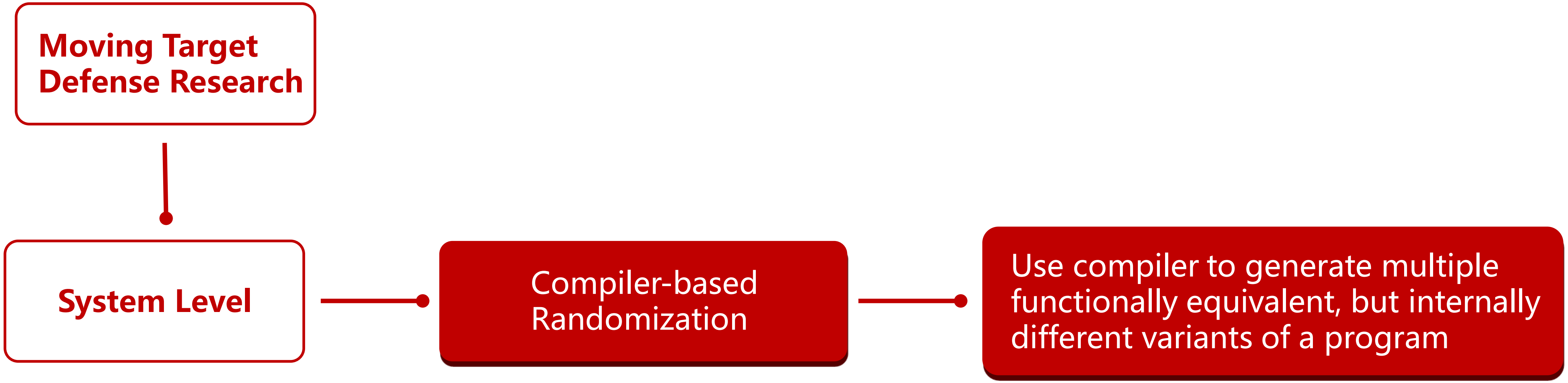
System Level

Data Randomization

Randomize pointers
(XOR pointer with random key)

Randomize memory data
(XOR data with random masks)

目前研究态势



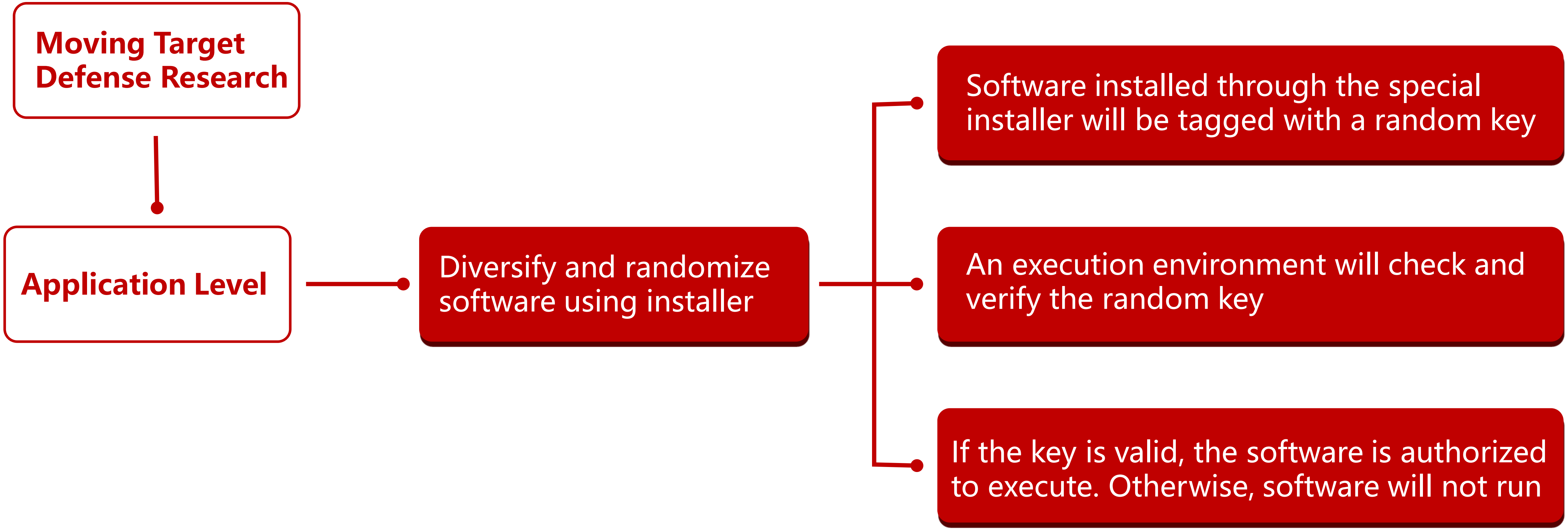
Moving Target Defense Research

System Level

Compiler-based Randomization

Use compiler to generate multiple functionally equivalent, but internally different variants of a program

目前研究态势



Moving Target Defense Research

Application Level

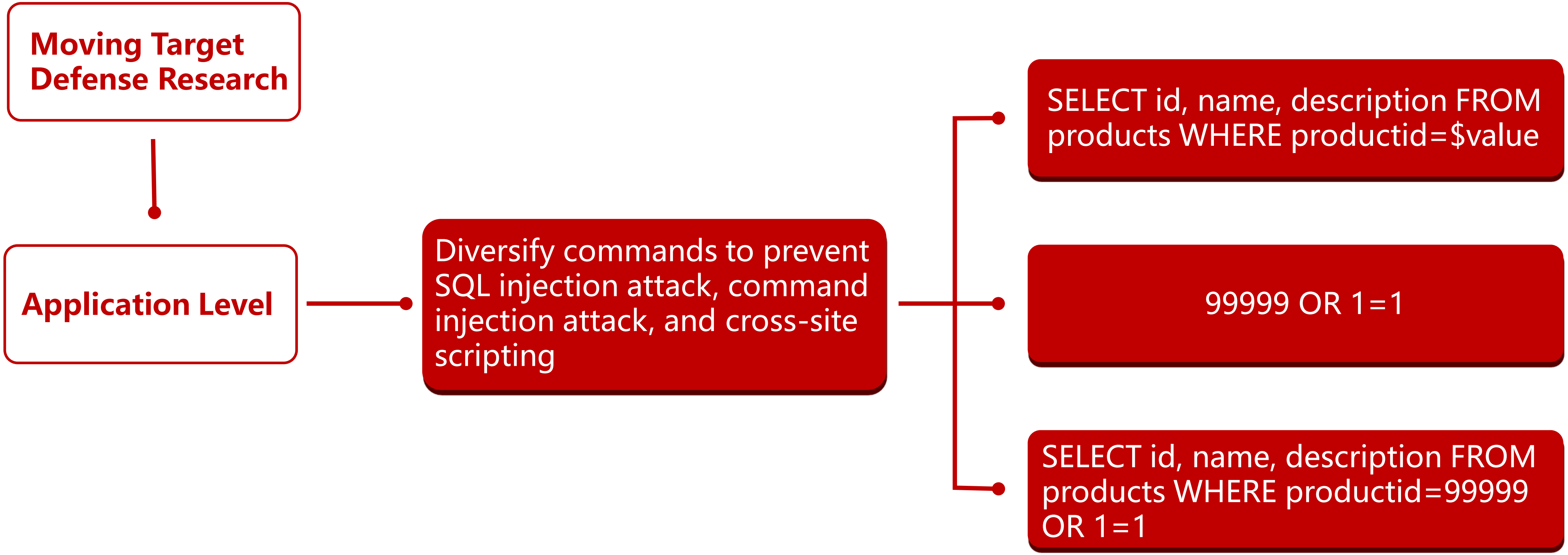
Diversify and randomize software using installer

Software installed through the special installer will be tagged with a random key

An execution environment will check and verify the random key

If the key is valid, the software is authorized to execute. Otherwise, software will not run

目前研究态势



Moving Target Defense Research

Application Level

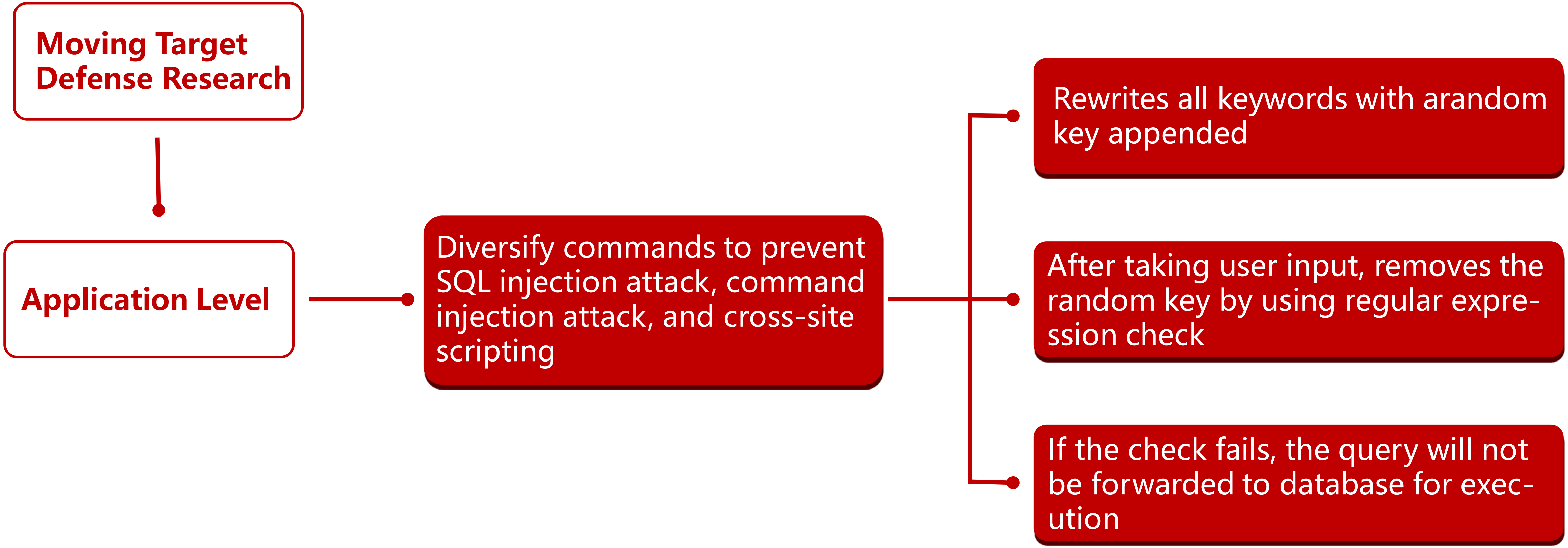
Diversify commands to prevent SQL injection attack, command injection attack, and cross-site scripting

SELECT id, name, description FROM products WHERE productid=$value

99999 OR 1=1

SELECT id, name, description FROM products WHERE productid=99999 OR 1=1

目前研究态势



Moving Target Defense Research

Application Level

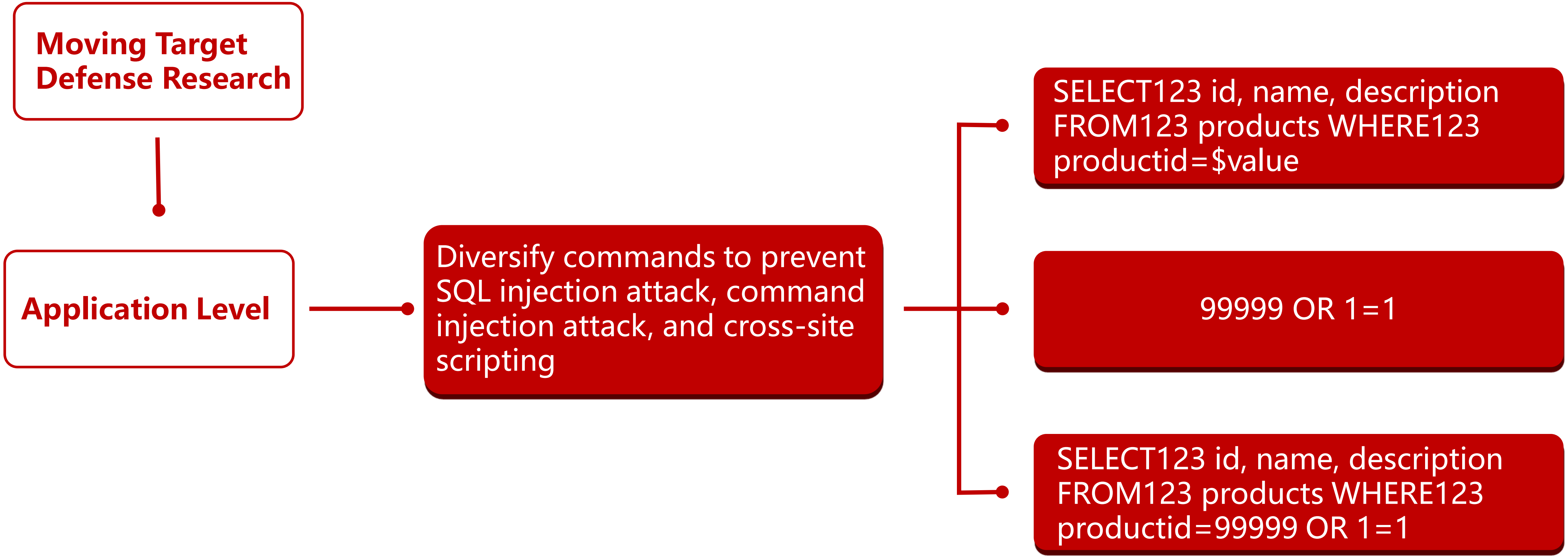
Diversify commands to prevent SQL injection attack, command injection attack, and cross-site scripting

Rewrites all keywords with arandom key appended

After taking user input, removes the random key by using regular expression check

If the check fails, the query will not be forwarded to database for execution

目前研究态势



Moving Target Defense Research

Application Level

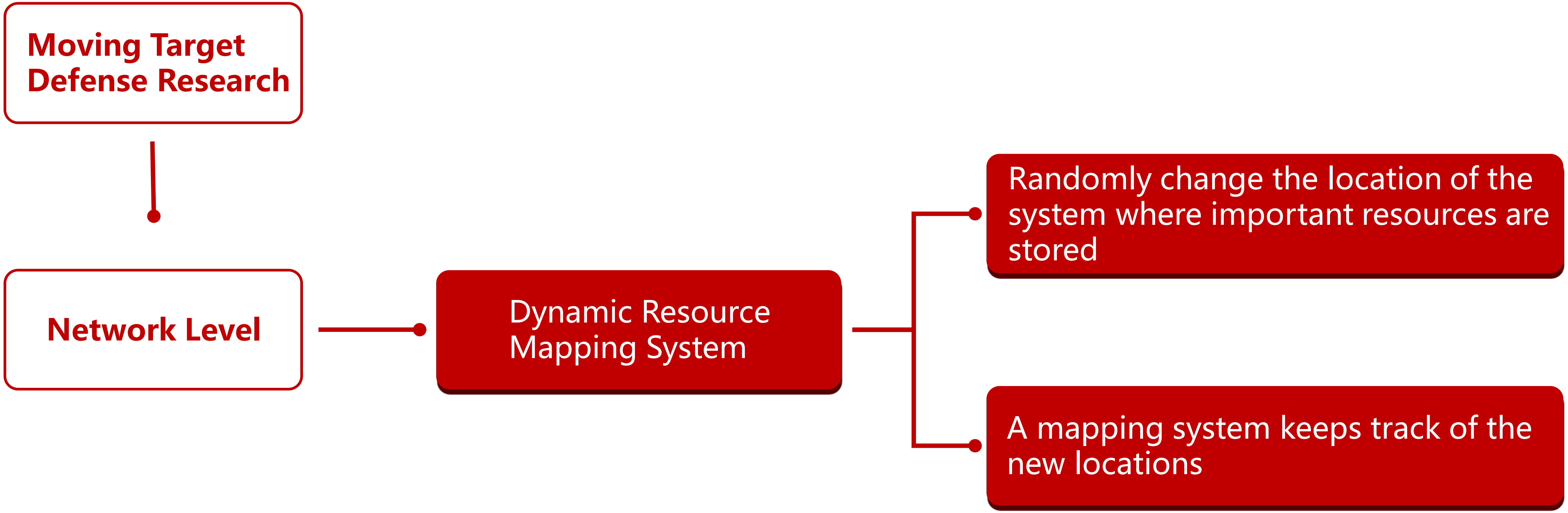
Diversify commands to prevent SQL injection attack, command injection attack, and cross-site scripting

SELECT123 id, name, description FROM123 products WHERE123 productid=$value

99999 OR 1=1

SELECT123 id, name, description FROM123 products WHERE123 productid=99999 OR 1=1

目前研究态势



Moving Target Defense Research

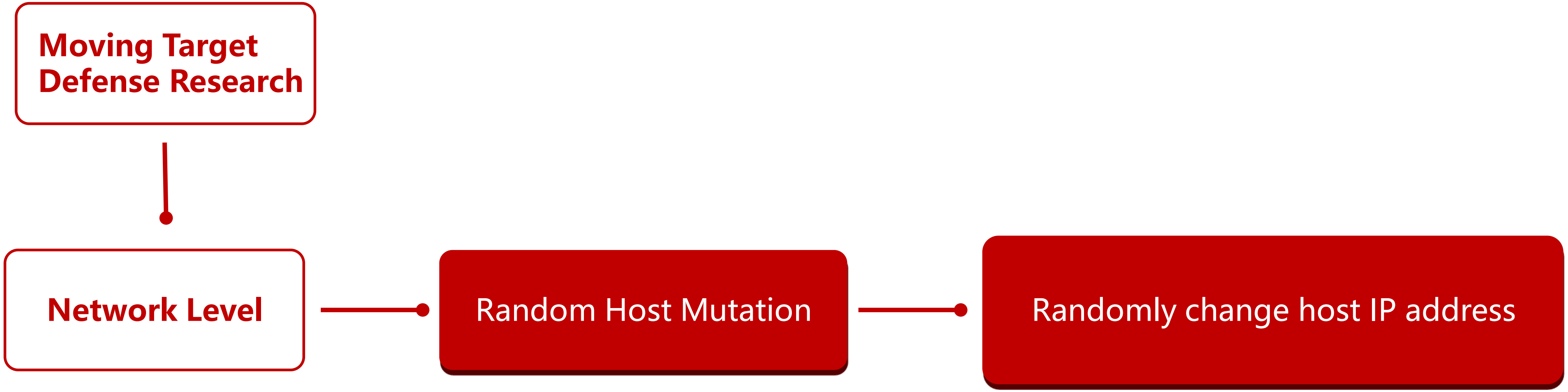
Network Level

Dynamic Resource Mapping System

Randomly change the location of the system where important resources are stored

A mapping system keeps track of the new locations

目前研究态势



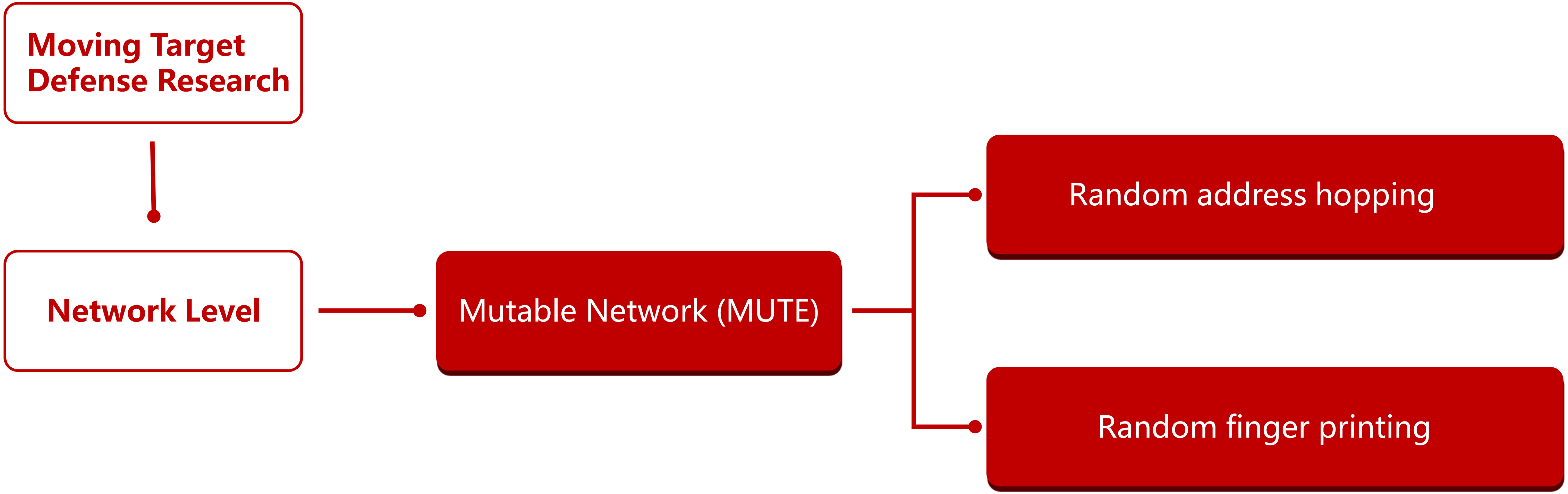
Moving Target Defense Research

Network Level

Random Host Mutation

Randomly change host IP address

目前研究态势



Moving Target Defense Research

Network Level

Mutable Network (MUTE)

Random address hopping

Random finger printing

商业应用

MORPHISEC
Moving Target Defense

SHAPE

VEDA 卫达安全

解决方案

内网安全
解决方案

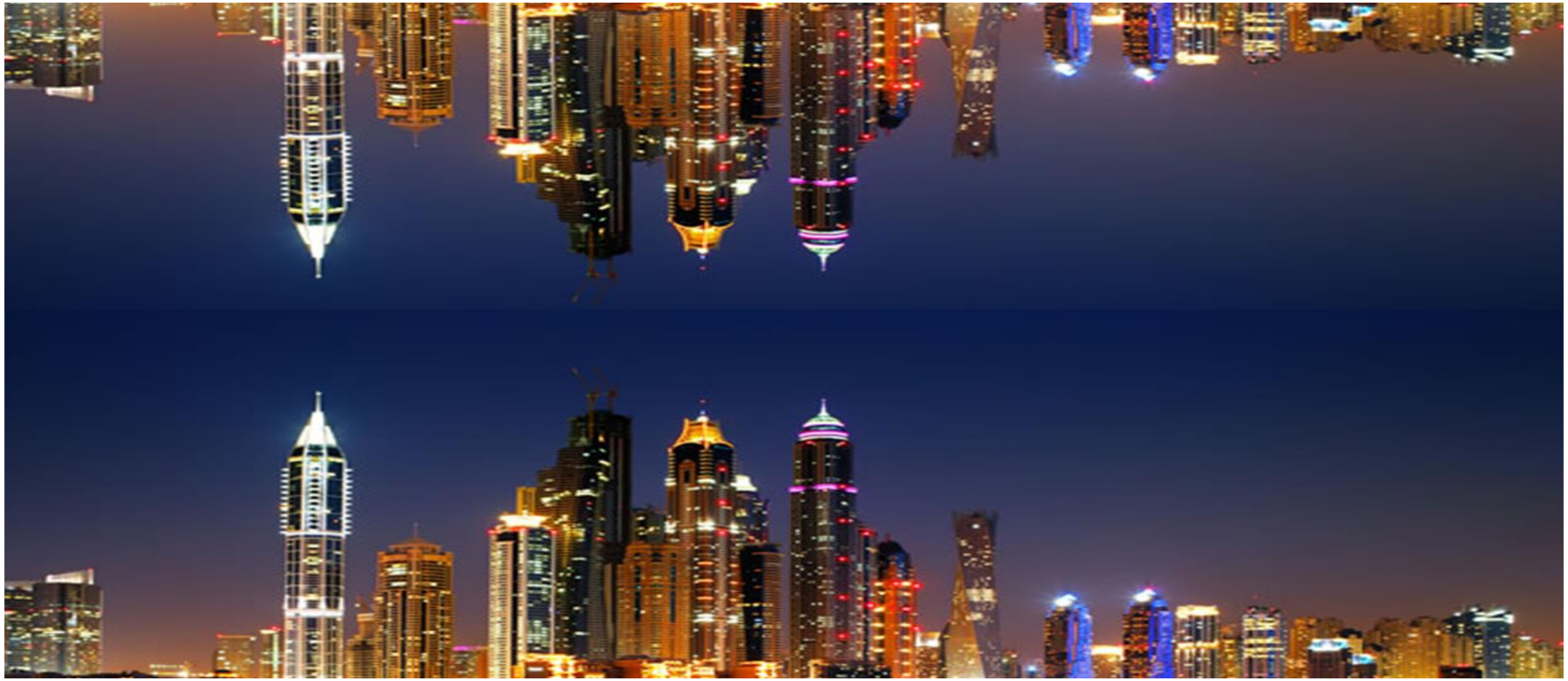
“幻境”内网动态防御系统

办公网

生产网

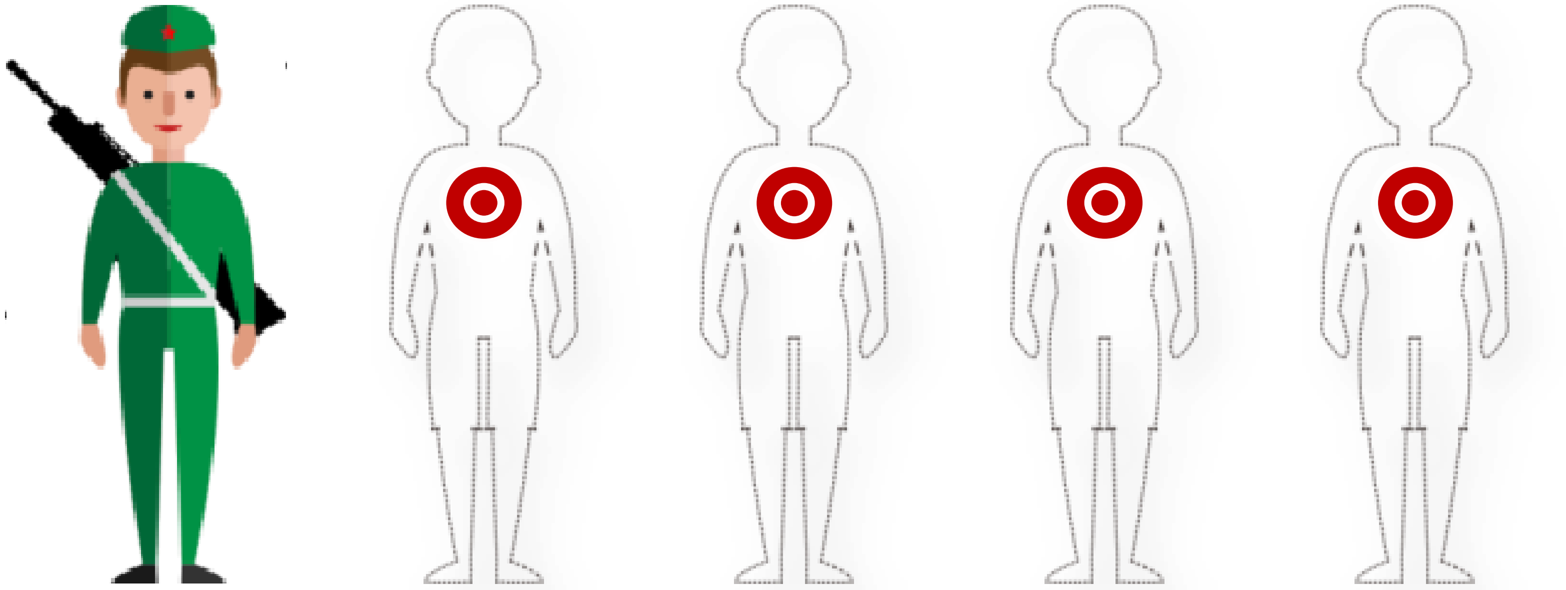
业务网

镜像世界



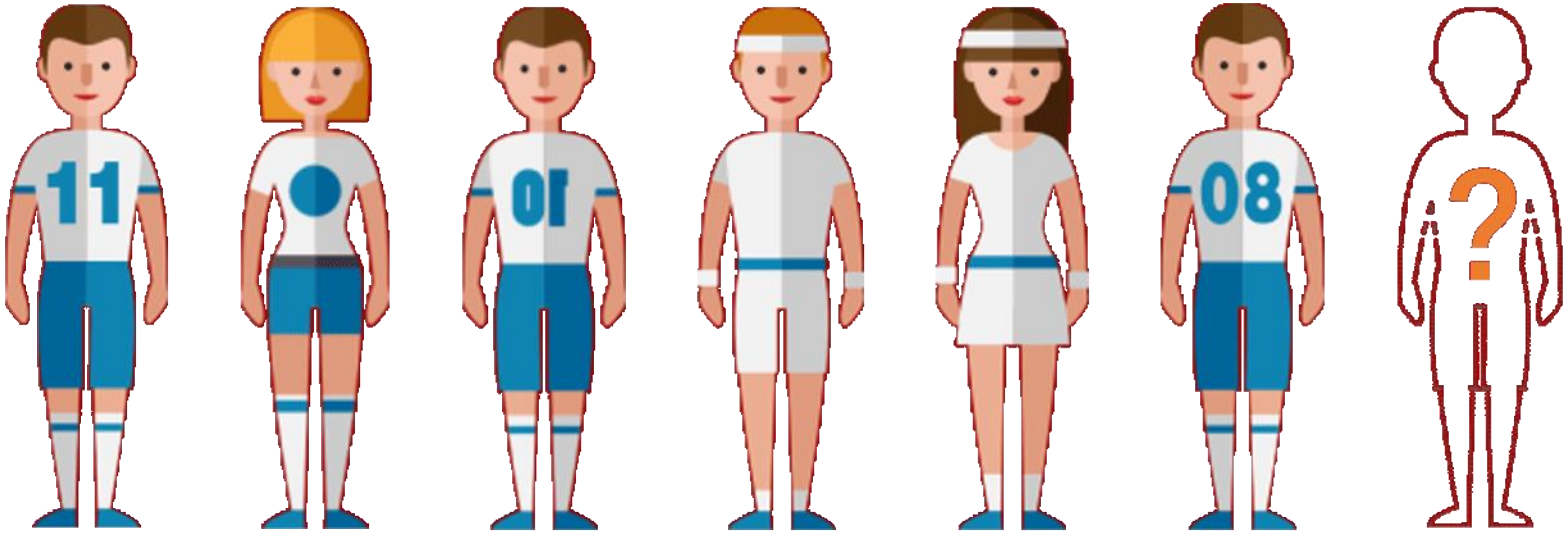
给每个终端构建镜像世界，将攻击约束到虚假网络中

虚拟哨兵



构建亿级极具诱惑力的哨兵节点，诱捕攻击者(瞒天过海)

移形换影



网络拓扑结构、IP地址、指纹信息动态变化

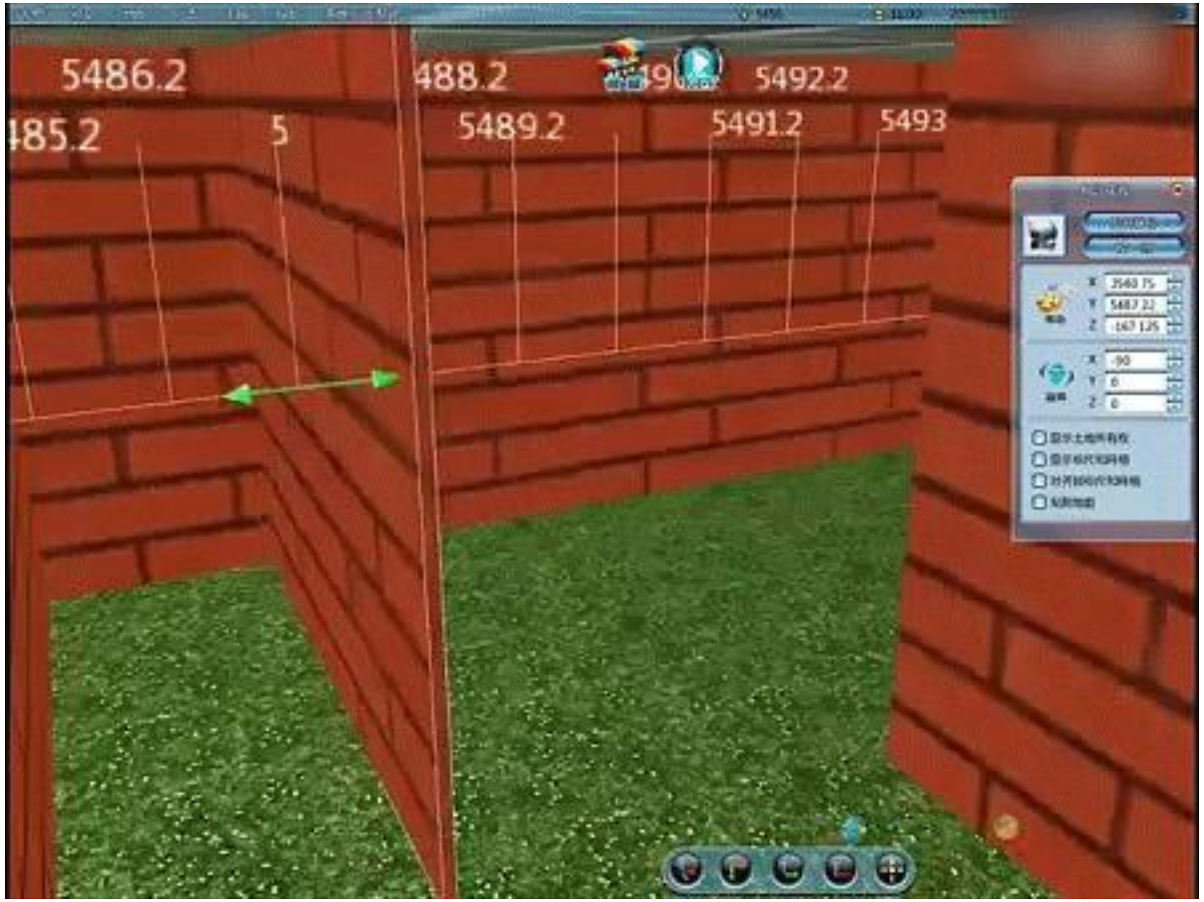
全息伪装

【无中生有】

全息虚拟大量与真实节点功能一致的伪装节点，让黑客无法分辨真假

幻境

- 不断变换的迷宫
- 全息隐藏真实拓扑
- 布满诱捕陷阱
- 兵法、谋略
- 进得来、动不了
- 一动必被捉



幻境

2019全球悬赏500万

奖励突破幻境的黑客

卫达再次为“幻境”加高筹码，将悬赏奖金从100万提高至 500万 ，邀请全球黑客高手前来挑战。

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE