



1

网络空间安全基本机制

发展历程：（安全即受控）

【现实信息-信息流】

最早是信息（秘密）的**保密**，保护符号表示信息通信（敌对环境下链路）保密（及校验（及身份（及新鲜性）））→模拟/数字信号的.....

数字化信息的**完整性**，数字化信息的**非否认性/匿名性**

【系统行为-控制流】（涉及到系统、操作、交互）

计算机（可控环境下访问）的安全

系统完整性、可用性、操作的非否认及可追溯性、交互时身份真实性、授权（合规性）、操作的实时与事后审计

【+虚拟信息与行为】

网络虚拟空间（无边界虚拟环境中）的**广义安全**

常用的机制

信息：陷门与函数映射（密码算法，加密、签名等方案）

交互：认证

系统：隔离（系统设计（设计、测试、分析、验证等）

操作：访问控制 审计 异常检测

管理机制（运筹学（最优化）、控制理论、博弈论、概率论、图论）

2

网络空间安全基本安全机制

加密

完整性检验（校验等）

认证

隔离

审计

可靠性（应对故障，冗余、恢复等）

一致性

3

网络空间安全形势

网络安全问题层出不穷，严重威胁和影响人类社会活动和发展的诸多方面

- 病毒、恶意程序
- 漏洞和后门
- 隐私泄露
- 泄密、窃密
- 针对电力系统等基础设施网络的攻陷
-

本周网络安全基本态势

| | | |
|-----------------|----------|--------|
| 境内计算机病毒程序传播次数 | •2950.4万 | ↑23.6% |
| 境内感染计算机病毒程序主机数量 | •20.2万 | ↓12.0% |
| 境内被篡改网站总数 | •3735 | ↓11.5% |
| 其中政府网站数量 | •20 | ↓28.6% |
| 境内被植入后门网站总数 | •1046 | ↓5.8% |
| 其中政府网站数量 | •5 | ↓66.7% |
| 针对境内网站的假冒页面数量 | •185 | ↓38.9% |
| 新增信息安全漏洞数量 | •457 | ↓28.7% |
| 其中高危漏洞数量 | •163 | ↑39.3% |

表示数量与上周相同 ↑表示数量较上周环比增加 ↓表示数量较上周环比减少

怎么防？

4

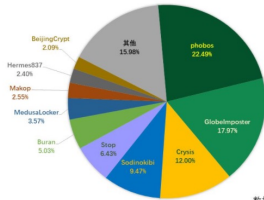
网络安全问题的危害——以勒索病毒为例

2020年勒索病毒“中毒”计算机超3700万，二次勒索日渐兴起

- B站知名UP主被攻击、德国医院遭勒索导致病患死亡、富士康1200台服务器沦陷.....
- 2020年中，360反勒索服务共接收并处理勒索病毒攻击求助3800余例，其中超过3700例确认遭受勒索病毒攻击
- 企业大量设备“中毒”的情况较多“二次勒索”模式逐渐流行，所造成的安全风险和经济损失较往年更为严重

怎么防？

2020年反勒索服务处置勒索病毒家族占比



数据来源：反勒索服务统计数据

5

如何解决网络空间安全问题？

修修补补的思维模式

- “兵来将挡水来土掩”
- 只能防住一个或几个小点



系统性思维模式

- 从全局性、关键性问题出发的系统性防御
- 力求解决核心安全问题



请举出成功案例

6

系统性防御思想——网络空间安全新机制

探索网络空间安全机制、构建安全的网络环境，是网络安全研究人员孜孜以求的目标

- 寻找解决安全问题的系统性思想、方法或模型，为实现网络空间安全提供有力的指导
- 逐步形成了零信任网络、可信计算等代表性的网络空间安全基本机制



7

基本前提和出发点

- 网络是一个复杂的分布式系统，漏洞和攻击的存在不可避免
- 网络空间安全机制的目标从来不是彻底根除攻击，而是实现让网络在有攻击的情况下仍然可以正常工作。围绕这一目标，研究人员按不同的思路展开设计，形成了不同的安全机制



8



9

本章主要内容

| 安全机制 | 原理概要 | 知识点 |
|--------|--------------|---|
| 沙箱 | 限制、隔离 | <ul style="list-style-type: none">发展概况安全目标基本思想和原理 |
| 入侵容忍 | 容忍、容错 | |
| 可信计算 | 可信根、信任链 | |
| 移动目标防御 | 动态、异构、不确定 | |
| 零信任网络 | 从来不相信, 始终在校验 | |

10

第1节 沙箱

- ✓ 发展概况
- ✓ 安全目标
- ✓ 基本思想和原理

11

思想来源

- 设想:
当遇到一些来源不明、意图无法判定的程序时, 直接安装使用会带来巨大的风险, 如果程序中嵌入了恶意代码, 那么主机将可能被破坏和攻陷。
- 如何降低或避免这种风险?

The image shows an Android security warning dialog with the text: "您的手机和个人数据更容易受到从未知来源获取的应用程序的攻击。对于因使用这些应用程序而造成的手机损坏或数据丢失, 您同意自行承担全部责任。" (Your phone and personal data are more susceptible to attacks from applications obtained from unknown sources. For damage to your phone or loss of data caused by using these applications, you agree to bear full responsibility on your own.)

12

沙箱发展概况

上世纪70年代

沙箱技术思想出现

- 1971年兰普森 (Lampson) 关于访问控制的相关论文中出现了沙箱的思想雏形

80年代-90年代

沙箱技术逐渐发展成熟

2000以后

沙箱技术在工业界广泛应用

- Linux内核沙箱Seccomp
- 苹果的Apple App Sandbox
- Google的Sandbox API
- Java 虚拟机
- 微软的Windows沙盒

到底什么是沙箱？具有什么本质特征？沙箱用到的系统设计思想是什么？

关键词：间接 隔离

13

沙箱的安全目标

沙箱的安全目标主要是防范恶意程序对系统环境的破坏

- 沙箱通常用于执行未经测试或不受信任的程序。这些程序主要来自未经经验证或不受信任的第三方、用户或网站，可能包含对计算机系统造成危害的病毒或其他恶意代码
- 恶意程序要对系统进行入侵或者破坏，需要获得文件读、写等必要的操作权限。如果能够对权限进行限制和隔离，就能有效限制恶意程序的破坏能力和范围，沙箱则是为此设计的一种防御机制

14

沙箱的核心思想——隔离

- 通过隔离程序的运行环境、限制程序执行不安全的操作，防止恶意程序对系统可能造成的破坏，限制可信性不能保证的程序

15

沙箱的内部工作机理

- 沙箱环境
- 访问
- 规则

16

沙箱与软件错误隔离

从“隔离”的角度看，沙箱可以看成是软件错误隔离思想在网络防御中的应用

- 软件错误隔离：利用软件手段限制不可信模块造成的危害，通过隔离保证系统鲁棒性，限制程序执行违反安全策略的操作，从而实现限制恶意行为的目的



17

沙箱与访问控制

从访问控制的角度看，沙箱的本质是面向程序的访问控制

- 访问控制能够对权限进行管理，防止信息越权篡改和滥用
- 基于访问控制，沙箱可以限制程序的资源访问能力，既满足其正常的访问需求，又保证整体系统安全



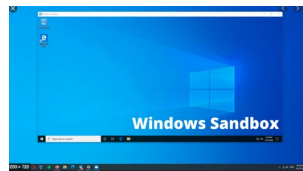
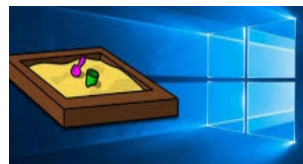
是什么给了“访问控制”的设计机会？

18

沙箱与虚拟化

从提供高度受控环境的角度上看，沙箱也可以被视为虚拟化技术的一种特定实例

- 虚拟化技术的一个典型应用是虚拟机，虚拟机能够模拟完整的主机，在虚拟机内部软件的操作不会对外部系统造成负面影响，实现了沙箱“隔离”的效果。
- 微软 2019 年推出的 Windows Sandbox（又叫Windows沙盒）就是一种轻量化的虚拟机，它基于 Windows 容器技术建立，能够像正常系统一样运行大部分程序，即使 Windows 沙盒被恶意程序攻陷，也不会影响到用户操作系统的安全。



19

第2节 入侵容忍

- ✓ 发展概况
- ✓ 安全目标
- ✓ 基本思想和原理

20

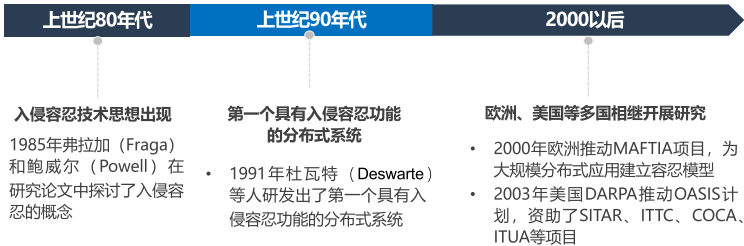
思想出发点

- 漏洞的存在和攻击的发生难以避免，尽管部署了先进的防御系统，也难以避免会存在一些“漏网之鱼”的入侵和攻击发生
- 既然依靠“堵”和“防”还不够，有什么办法能增加系统的安全性，使堵不了、防不住的情况下系统能够正常工作？

21

入侵容忍的发展概况

事件概要



22

入侵容忍的安全目标

入侵容忍的安全目标主要是在攻击可能存在的前提下使系统的机密性、完整性和可用性能够得到一定程度的保证

- 机密性：特定机密的信息不被攻击者窃取
- 完整性：指特定的数据不被删除或篡改
- 可用性：指系统所提供的服务能够持续可用

入侵容忍属于“生存技术”的范畴，即在攻击、故障事件发生时，入侵容忍机制能够使系统在一定的时间内保证其功能的运转并完成任务。

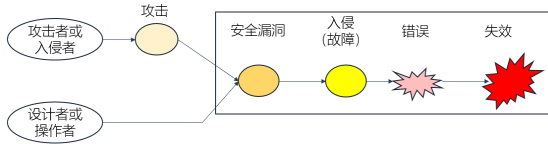
与传统防御机制不同，入侵容忍允许系统存在安全漏洞并假设攻击能够成功，在此前提下研究如何防止系统失效的发生，并保证系统的可用性和鲁棒性

23

攻击漏洞入侵混合错误模型

又称AVI系统故障模型，即Attack, Vulnerability, Intrusion composite fault model

- 系统的失效过程可以用攻击漏洞入侵混合错误模型来表示
- 系统从遭受攻击到最终失效涉及到的环节包括：攻击者（入侵者）攻击、安全漏洞利用、入侵（故障）、错误发生、系统失效

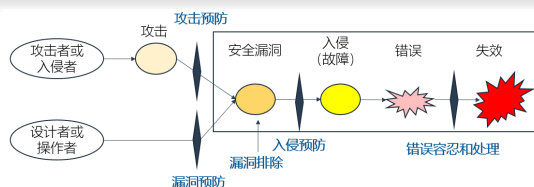


24

入侵容忍的基本原理

通过对AVI模型中的环节进行预防、排除、容忍和处理，防止系统失效，以一定的概率保证系统的安全性

- 入侵容忍的关键要素包括攻击预防、漏洞预防、漏洞排除、入侵预防、错误容忍和处理等
- 本质上，入侵容忍是一种使系统维持幸存性的技术；通过容忍防御环节的疏漏，来提升系统的安全性，是网络防御的最后一道防线



25

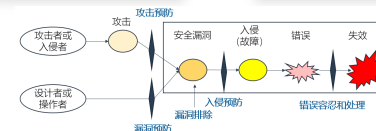
入侵容忍的安全能力和核心机制

安全能力

- 阻止和预防攻击
- 检测攻击、评估攻击造成的危害
- 在遭受攻击后，及时维护和恢复关键数据、关键服务或完全服务

核心机制

- 安全通信机制
- 入侵检测机制
- 入侵遏制机制
- 错误容忍和处理机制等



错误容忍和处理是入侵容忍的核心，是系统在攻击和异常发生时仍然能够提供有效的服务的关键

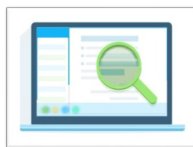
26

错误容忍和处理

错误容忍和处理旨在阻止产生灾难性失效，具体包括错误检测和错误恢复

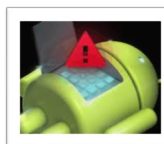
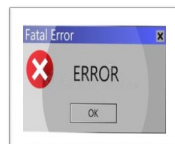
错误检测

- 目的：限制错误传播、触发错误恢复和故障处理机制
- 包括完整性检测和日志审计等



错误恢复

- 目的：使系统从入侵造成的错误状态中恢复，恢复关键数据和服务
- 包括：
 - 前向恢复
 - 后向恢复
 - 错误屏蔽等



27

互联网设计原则(Clark' 88)

In order of importance:

0. Connect existing networks

- initially ARPANET, ARPA packet radio, packet satellite network

1. Survivability

- ensure communication service even with network and router failures

2. Support multiple types of services

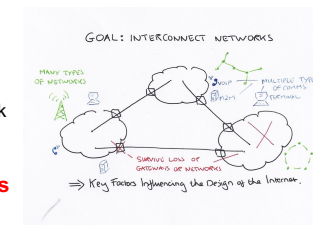
3. Must accommodate a variety of networks

4. Allow distributed management

5. Allow host attachment with a low level of effort

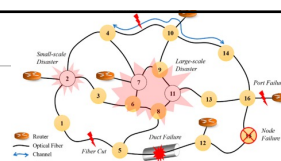
6. Be cost effective

7. Allow resource accountability



28

1. Survivability



- Continue to operate even in the presence of network failures (e.g., link and router failures)
 - as long as network is not partitioned, two endpoints should be able to communicate
 - any other failure (excepting network partition) should be **transparent** to endpoints
- Decision: maintain e-e transport state only at end-points
 - eliminate the problem of handling state inconsistency and performing state restoration when router fails
- Internet: **stateless** network-layer architecture
 - No notion of a session/call at network layer
- Grade: A-**
 - routing algorithm failover path is non-optimal, non-traffic sensitive (Note: ISPs worry about this)

29

第3节 可信计算

- ✓ 发展概况
- ✓ 安全目标
- ✓ 基本思想和原理

30

思想出发点

- 由于计算机设备软硬件结构透明，频繁出现病毒或恶意代码植入、黑客窃取权限和入侵等安全事故，导致程序、系统不可信
- 如何才能从根本上实现“可信”？
- 从这个角度出发，可信计算组织（Trusted Computing Group）提出了可信计算的安全机制



31

可信计算发展概况

国外：以TCG为主推动可信计算的诞生和发展

| 1999 | 2003 | 2006 | 2007以后 |
|---|---|--|--|
| <ul style="list-style-type: none"> 由 Intel、微软、IBM 等计算机巨头共同发起了可信计算平台联盟 (TCPA) | <ul style="list-style-type: none"> TCPA 改组为可信计算组织 TCG，致力于将可信计算技术在个人计算机中推广和实现 | <ul style="list-style-type: none"> IBM 为 Xen 虚拟机设计虚拟 TPM (可信平台模块) | <ul style="list-style-type: none"> Intel 等多家芯片厂商相继推出自己的 TPM 芯片 微软公司先后在 Windows 操作系统的多个版本中使用 TPM 实现 BitLocker 驱动器加密 |

- 可信计算平台联盟：Trusted Computing Platform Alliance, TCPA
- 可信计算机组织：Trusted Computing Group, TCG
- 可信平台模块：Trusted Platform Module, TPM

32

可信计算的安全目标

可信计算的总体目标是提升计算机系统安全性和可信性，包括系统数据的完整性、数据的安全存储和平台可信性的远程证明等

- 可信计算认为，传统的信息安全系统以防止外部入侵为主，这些措施只封堵外围，没有从根本上解决产生不安全的问题
- 解决这些问题重点需要从芯片、硬件结构、操作系统等方面综合采取措施保证系统的安全和可信，从而在根本上提高安全性能，达成安全可信的目标

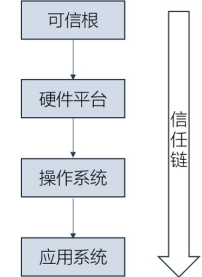


33

可信计算的核心思想

从信任根出发构建信任链

- 首先建立一个可信根。可信根的可信性由物理安全、技术安全与管理安全共同保证。
- 基于可信根建立一条信任链，从可信根开始到硬件平台、操作系统、应用系统逐级传递信任关系，将信任扩展到整个系统，从而确保系统整体可信



34

可信计算的核心思想

可信计算最本质的问题是信任问题

- 强调从可信根出发解决系统结构中的安全问题，即通过信任链确保每一个环节的身份可信，从而保证从起点的可信根到后续的可信应用的信任关系是可靠的，为计算机系统安全提供一体化的安全保证



35

可信计算关键技术概念

可信计算包含六个关键技术概念



基于这六个关键技术，即可构建一个完全可信系统（即符合TCG规范的系统），使计算全程可测可控、不被干扰和篡改，使计算结果可预期，实现信息的可信传递和安全可信

36

第4节 移动目标防御

✓ 发展概况

✓ 安全目标


✓ 基本思想和原理

37

思想出发点

• 当系统的内部结构保持不变时，攻击者可以进行足够多次的尝试寻找系统的漏洞从而将系统攻破，并在类似的系统中复现攻击

• 如果系统内部是动态变化的，攻击者还能达成攻击目标吗？



38

移动目标防御发展概况

1970年代

• 移动目标防御 (MTD) 概念的起源可以追溯到70年代计算机安全领域中的错误容忍及可配置计算、网络多样性等相关概念

2009年

• 美国网络和信息技 术 研 发 计 划 (NITRD) 对 MTD 的有效性和效率进行了相关描述

2011年

• 美国国家科学技术委员会在《可信网络空间：联邦网络安全研发战略规划》中将移动目标防御确定为四大“改变游戏规则”的研发主题之一

2014年至今

• ACM连续举办了数场移动目标防御研讨会 (ACM Workshop on Moving Target Defense)



39

移动目标防御的安全目标

移动目标防御的安全目标主要是增加攻击者的难度、使攻击难以达成，从而瓦解攻击

• 传统的信息系统一般以静态的配置运行，外部攻击者可以利用系统的静态性、确定性和相似性环节来构造系统漏洞的攻击链，实现攻击

• 移动目标防御旨在改变传统信息系统的这一弱点，从而挫败外部攻击



40

10

移动目标防御的基本思想

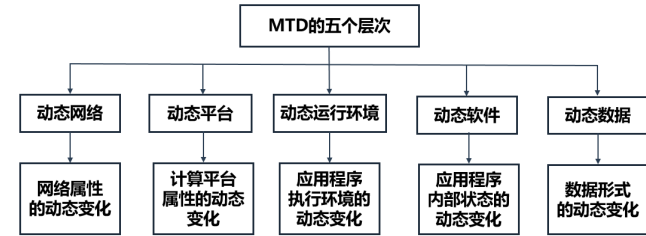
“动态” + “异构”

- 从动态、随机和多样化的角度设计的一种防御机制
- 建立一种动态、异构、不确定的网络空间目标环境
- 增加攻击者的攻击成本

本质:通过增加系统的随机性和不可预测性来防范网络攻击

41

移动目标防御的五个层次



- 动态网络: 通过不断地在网络系统的多个配置之间转移变换 (例如更改开放的网络端口, 网络配置, 软件等)
- 通过在网络、平台、环境、软件和数据等多个层次增加随机性和不确定性, 增加攻击难度、有效削弱攻击者对防御机制的适应和突破能力

42

MTD代表性的具体技术

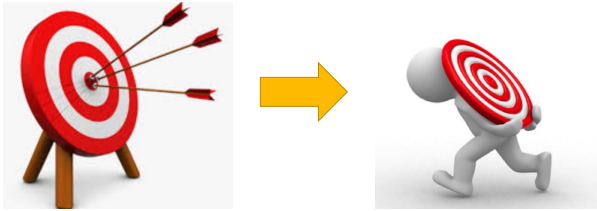
- | | |
|---|---|
| <ul style="list-style-type: none">• IP地址跳变• 端口跳变• 动态路由• 网络和主机身份随机化 | <ul style="list-style-type: none">• 地址空间随机化• 指令集合随机化• 数据存放形式随机化• |
|---|---|

以主动防御的方式应对动态适配的攻击者

43

MTD的本质

MTD的本质在于以不确定的方式进行“转移变换”, 使攻击者难以摸清系统内部的变化规律、无法找到攻击的突破口



- 相反, 如果转移变换的机制是确定性的, 则MTD的优势将消失, 因为攻击者有可能利用足够的时间观测出转移变换的规律, 使这种转移变化在攻击者的视角变为“可预测”, 则无法达成防御目标。

内置隐式的动态随机性, 是移动目标防御能够有效挫败攻击的重要因素

44

第5节 零信任网络

- ✓ 发展概况
- ✓ 安全目标
- ✓ 基本思想和原理

45

思想出发点

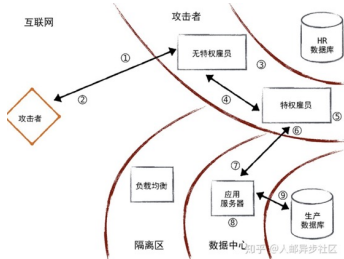
- 传统的从外网到内网的边界安全模型依赖于在网络边界进行安全检查，试图把攻击阻挡在边界之外。但内网是否绝对安全？



46

思想出发点

- 攻击者可以在办公网络中横向移动，最终进入生产网络
- 随着内部威胁、高级持续攻击等新型安全威胁的出现，“内网”的安全问题越来越复杂，单靠网络边界已经无法划清安全的界限



用新的视角来重新审视网络边界和安全的关系，产生了零信任网络安全机制

47

零信任网络发展概况

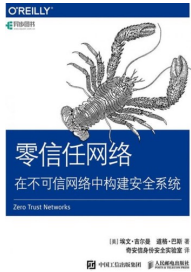
| 2010 | 2017 | 2018 |
|---|--|---|
| <ul style="list-style-type: none">零信任网络的概念最早由福雷斯特研究公司 (Forrester) 的分析师约翰·金德瓦格 (John Kindervag) 在 2010 年提出 | <ul style="list-style-type: none">2017 年，谷歌建立了基于零信任架构实践的新一代企业网络安全架构 BeyondCorp | <ul style="list-style-type: none">2020 年，美国国家标准与技术研究院 (NIST) 发布了《零信任架构》研究报告 |

越来越多领先的IT平台供应商和网络安全供应商，开始将零信任的思想和架构运用于企业实际的解决方案

48

零信任网络的五个基本假设

- 网络无时无刻不处于危险的环境中
- 网络中自始至终存在外部或内部威胁
- 网络的位置不足以决定网络的可信程度
- 所有的设备、用户和网络流量都应当经过认证和授权
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来



——摘自 埃文·吉尔曼，道格·巴斯
《零信任网络——在不可信网络中构建安全系统》

49

零信任网络的核心思想

“从来不相信，始终在校验” (Never Trust, Always Verify)

- 零信任模型不依靠建立隔离墙来保护可信的资源，而是接受“不可信”或“坏人”无处不在的现实，试图让全体资源都拥有自保的能力
- 零信任默认不应该信任企业网络内部和外部的任何人/设备/应用，需要基于认证和授权重构访问控制的信任基础。

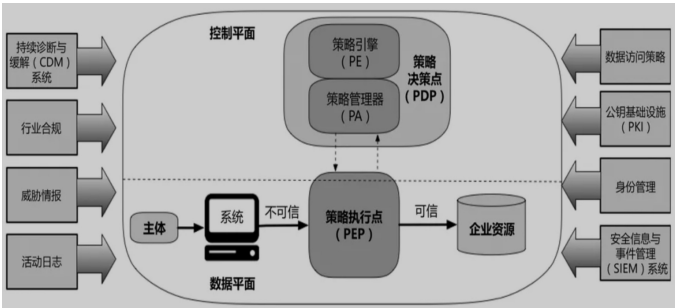


零信任对传统访问控制机制进行了范式上的颠覆
其本质是以身份为基石的动态可信访问控制

50

零信任网络架构

美国国家标准与技术研究院 (NIST) 于2020年8月发布的《零信任架构》研究报告给出了零信任架构的理想模型

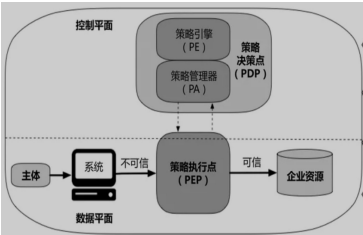


51

零信任网络架构

美国国家标准与技术研究院 (NIST) 于2020年8月发布的《零信任架构》研究报告给出了零信任架构的理想模型

- 核心逻辑组件由策略决策点（包括策略引擎、策略管理器两个子组件）和策略执行点组成
- 外部还有多个提供输入和策略规则的数据源，包括持续诊断与缓解系统、行业合规系统、数据访问策略、公钥基础设施等

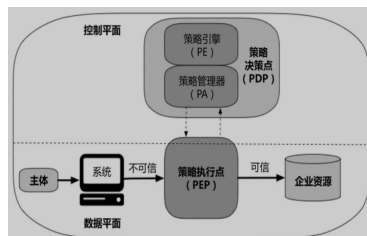


52

零信任网络控制平面

零信任的安全机制主要在控制平面中的核心逻辑组件实现，控制平面对数据平面进行指挥、配置：

- 策略引擎负责最终决定是否授予访问权限
- 策略管理器负责建立或切断主体与资源之间的通信路径（通过发送指令到策略执行点）
- 策略执行点负责启用、监控并最终结束访问主体和企业资源之间的连接



所有对敏感资源的访问请求首先需要经过控制平面处理，包括设备和用户的身份认证与授权

53

零信任网络的7条基本原则

NIST的报告中提出了零信任架构的设计和部署应当遵循的基本原则：

- 所有的数据源和计算服务都被认为是资源
- 所有的通信必须以最安全的方式进行，与网络位置无关。网络位置并不意味着信任
- 对单个企业资源的访问的授权基于每个连接授予的。在授予访问权限之前评估请求者信任级别。访问权限还应授予完成任务所需的最小权限
- 对资源的访问由策略决定，包括客户身份、应用/服务和请求资产的可观察状态，可能还包括其他行为及环境属性

54

零信任网络的7条基本原则

NIST的报告中提出了零信任架构的设计和部署应当遵循的基本原则：

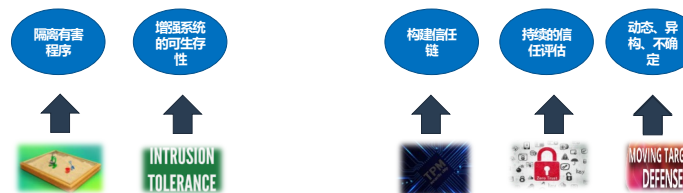
- 企业对所有资产的完整性和安全态势进行监控和测量。没有资产是天生可信的。企业评估资源请求时，也评估资产的安全态势
- 所有资源身份认证和授权是动态的，并且在允许访问之前严格执行。这是一个不断的循环过程，包括访问、扫描和评估威胁、调整、在通信中进行持续信任评估
- 企业尽可能收集有关资产、网络基础架构和通信现状的信息，并利用这些信息改善其安全态势

55

网络空间安全基本机制小结

- 每一种安全机制对应不同的出发点和核心思想
- 从不同角度思考，衍生和发展出了不同的安全机制和防御思想

不同的侧重点：

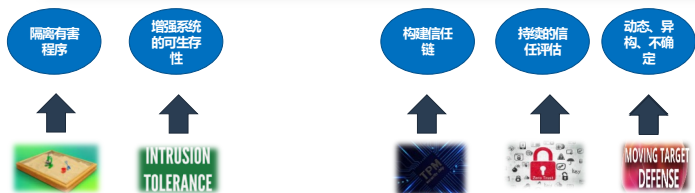


56

新机制可能带来新的问题

在增加新安全特性的同时，也可能同时引入了一些新的挑战或问题：

- 可信计算中可信根本本身的安全问题
- 拟态的冗余带来的成本和开销问题



如何完善已有的安全机制、增强已有安全能力，以及更进一步，如何探索新的、全面高效的安全机制，是值得深入研究和探讨的问题

57

思考和探讨

- 可信计算和零信任网络有哪些异同点
- 本章介绍的安全机制是否可以按照静态防御和动态防御进行分类？请给出理由
- 本章介绍的安全机制是否可以按照主动防御和被动防御进行分类？请给出理由
- 你认为本章介绍的安全机制有哪些优势和不足？
- 如果请你来设计一套新的校园网安全机制，你会从哪个角度去思考和设计？谈谈你的看法。

58

主要内容

网络空间安全基本机制的发展历程、安全目标和核心思想



59