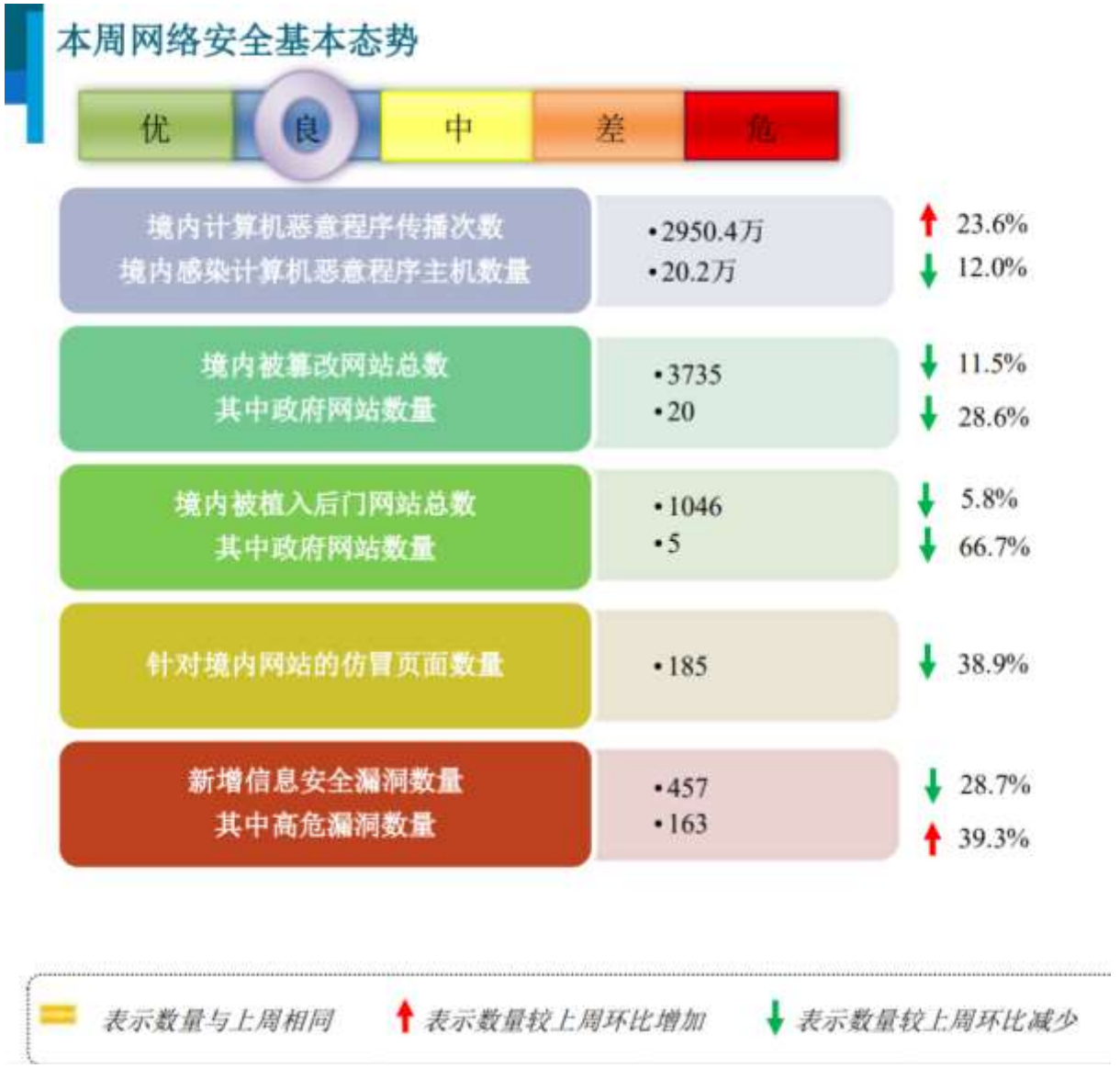
网络空间安全基本机制

李琦
清华大学网研院

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

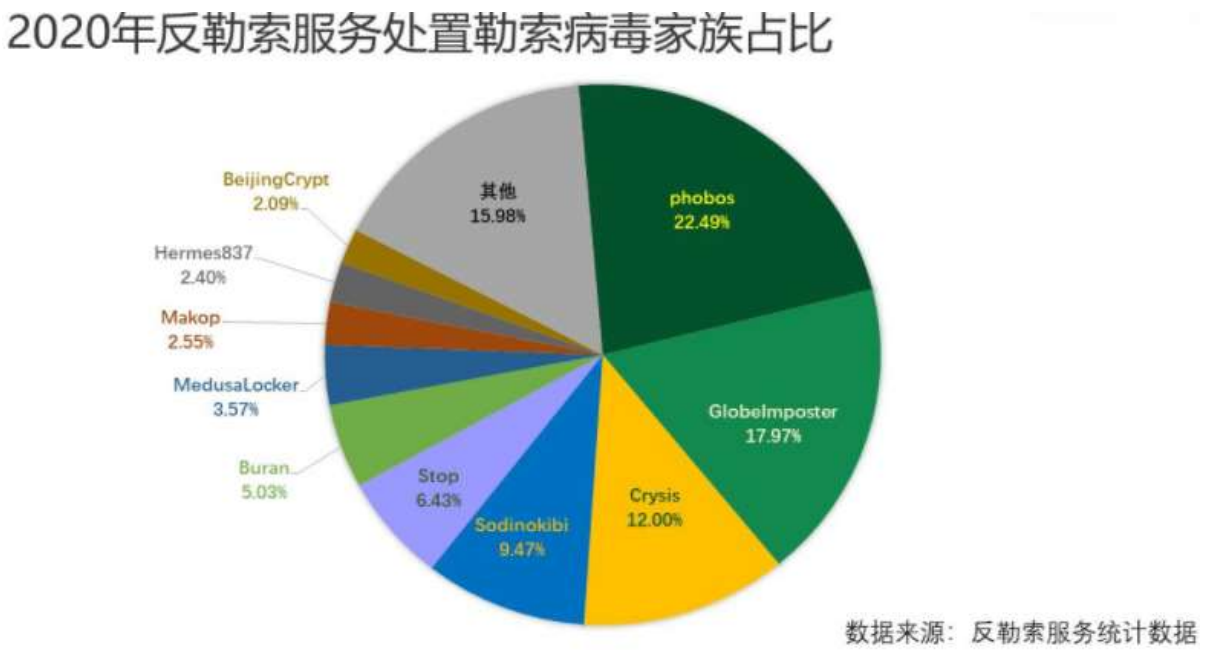
- 病毒、恶意程序
- 漏洞和后门
- 隐私泄露
- 泄密、窃密
- 针对电力系统等基础设施网络的攻陷
- ……



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



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

系统性防御思想——网络空间安全机制

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、拟态安全、可信计算等代表性的网络空间安全基本机制

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

检查软件是否有害

让系统不失效

让系统具备免疫能力

让计算可预期

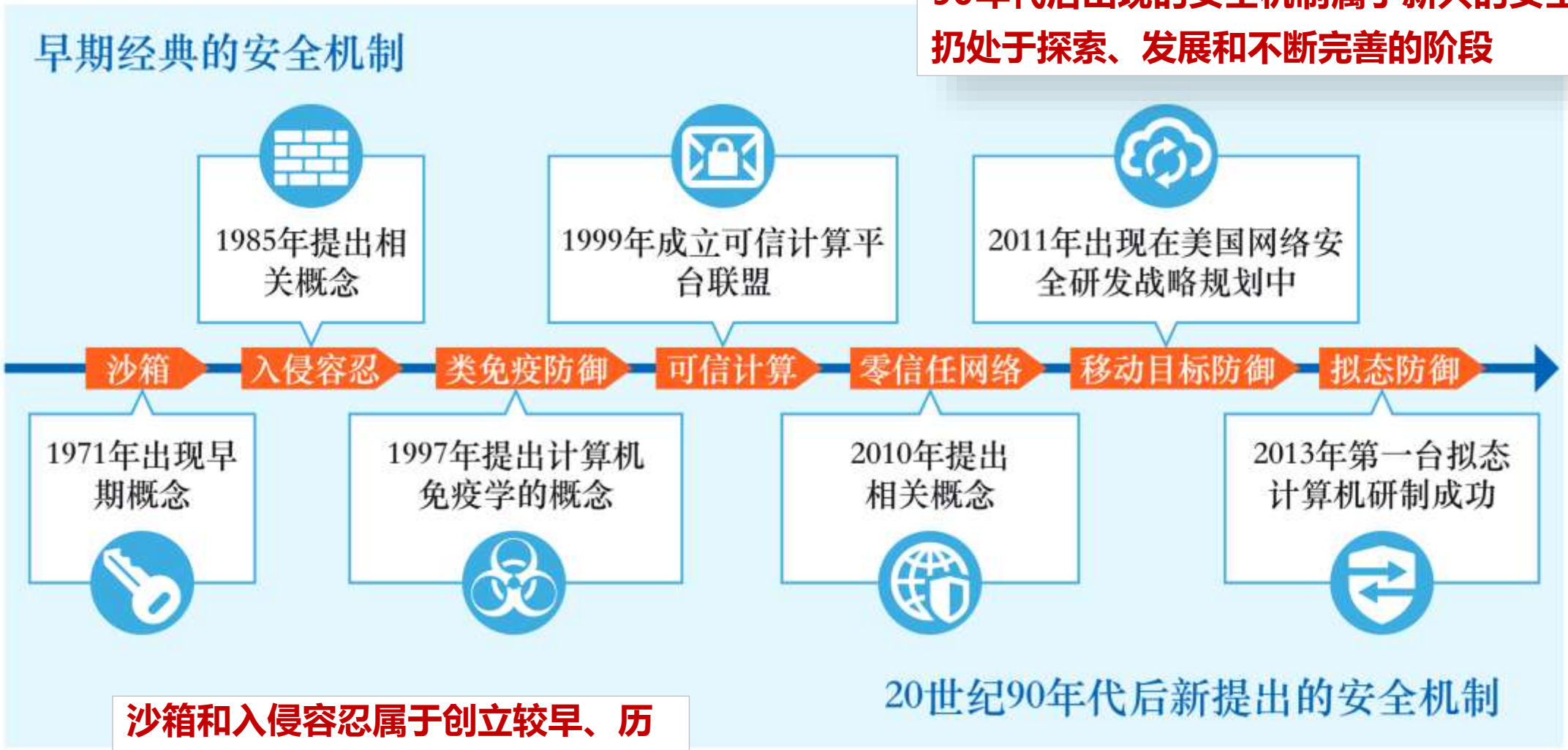
操作前检查权限

让攻击者不容易定位目标

使系统不可测、攻不破

代表性的网络空间安全基本机制

90年代后出现的安全机制属于新兴的安全机制，扔处于探索、发展和不断完善的阶段



沙箱和入侵容忍属于创立较早、历史较久的经典安全机制

讨论

畅所欲言

有没有可能设计实现一种绝对安全的网络系统?

本章的内容组织

第一节
沙箱

- 发展概况
- 安全目标
- 基本思想和原理

第二节
入侵容忍

- 发展概况
- 安全目标
- 基本思想和原理

第三节
可信计算

- 发展概况
- 安全目标
- 基本思想和原理

第四节
类免疫防御

- 发展概况
- 安全目标
- 基本思想和原理

第五节
移动目标防御

- 发展概况
- 安全目标
- 基本思想和原理

第六节
拟态防御

- 发展概况
- 安全目标
- 基本思想和原理

第七节
零信任网络

- 发展概况
- 安全目标
- 基本思想和原理

第1节 沙箱

- 发展概况
- 安全目标
- 基本思想和原理

思想来源

- 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？

沙箱发展概况

20世纪70年代 | 20世纪80年-90代末 | 2000年以后

沙箱技术思想出现

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

沙箱技术逐渐发展成熟

沙箱技术在工业界广泛应用

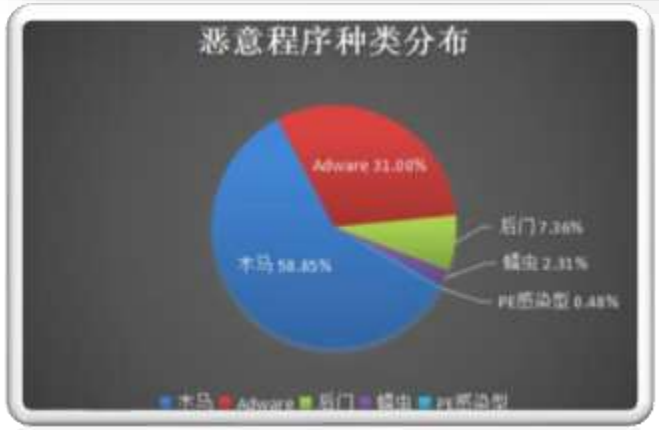
- Linux内核沙箱Seccomp
- 苹果的Apple App Sandbox
- Google的Sandbox API
- Java 虚拟机
- 微软的Windows沙盒

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

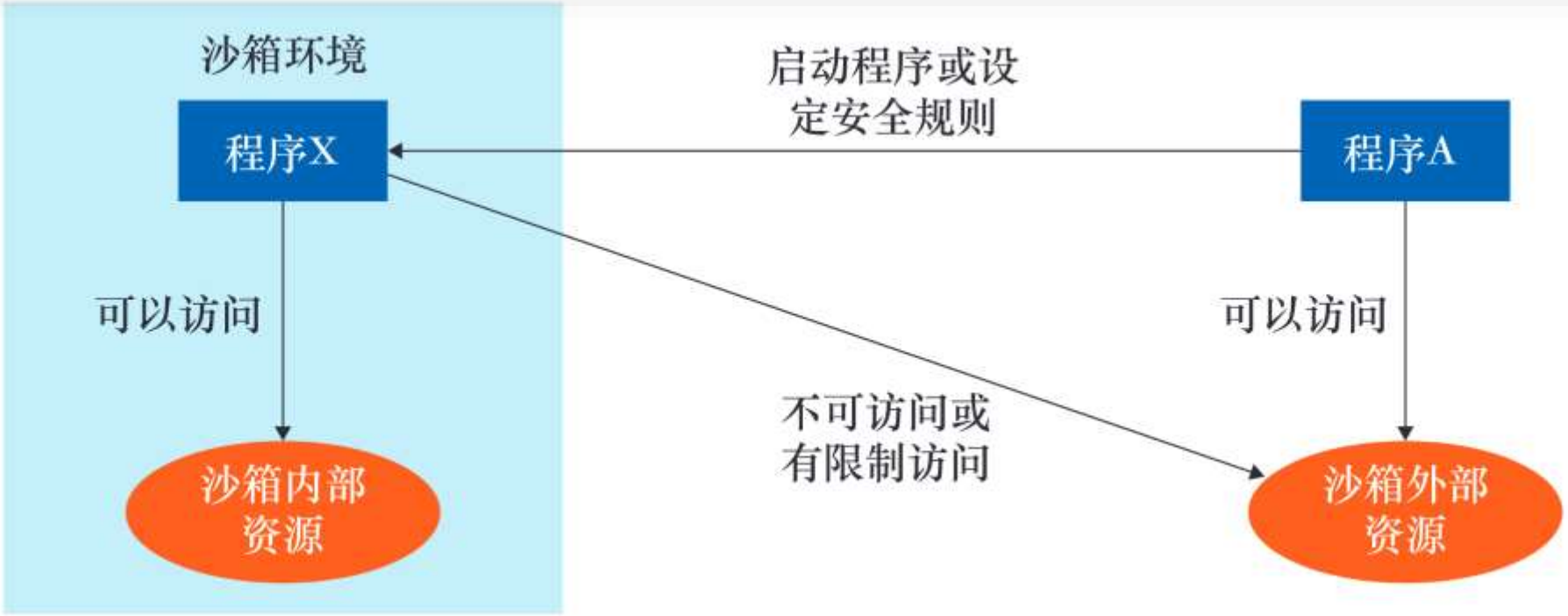


沙箱的核心思想——隔离

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

沙箱的内部工作机理

- 沙箱环境：某种受限的、与外部隔离的操作系统
- 沙箱内部运行可信性无法保证的程序X，与沙箱外部的程序不同，程序X只能对沙箱内部的资源进行自由的访问，不能访问或只能根据安全规则有限制地访问沙箱外部的资源
- 通过配置安全规则，可以控制程序X能够使用的资源集（如内存空间，文件系统空间、网络等资源），使程序X无法对沙箱外部资源环境造成破坏



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

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

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

第2节 入侵容忍

- 发展概况
- 安全目标
- 基本思想和原理

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、防不住的情况下也系统能够正常工作?

入侵容忍的发展概况

入侵容忍技术思想出现

- 1985年弗拉加（Fraga）和鲍威尔（Powell）在研究论文中探讨了入侵容忍的概念

第一个具有入侵容忍功能的分布式系统

- 1991年杜瓦特（Deswarte）等人研发出了第一个具有入侵容忍功能的分布式系统

欧洲、美国等多国相继开展研究

- 2000年欧洲推动MAFTIA项目，为大规模分布式应用建立容忍模型
- 2003年美国DARPA推动OASIS计划，资助了SITAR、ITTC、COCA、ITUA等项目

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

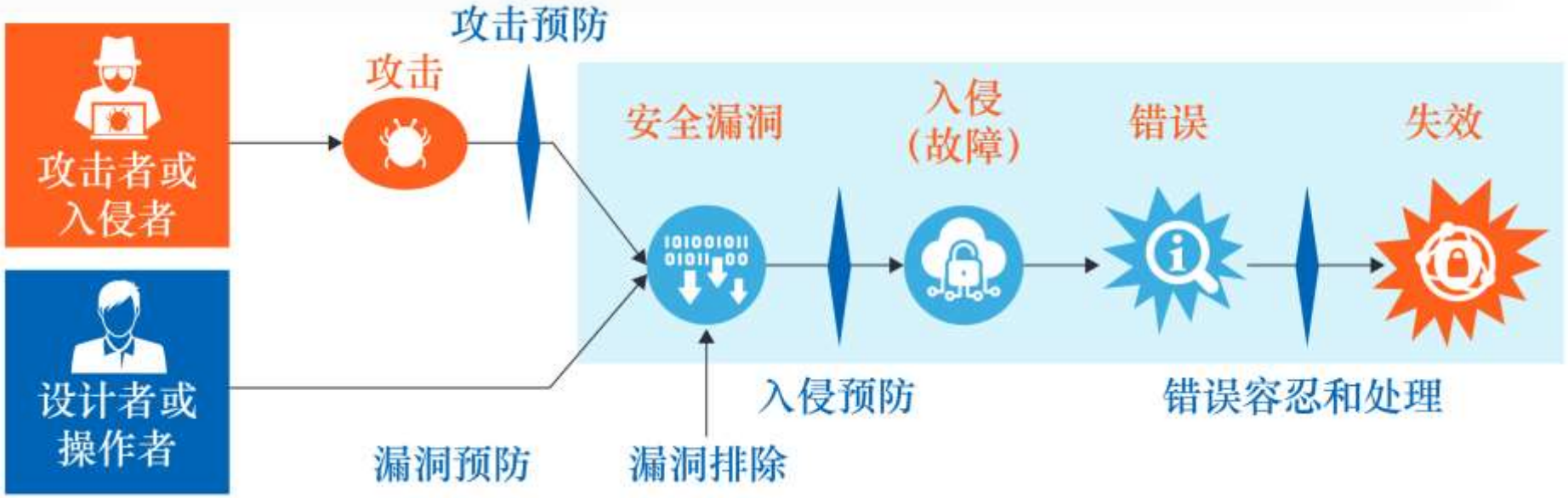
入侵容忍属于“生存技术”的范畴，即在攻击、故障事件发生时，入侵容忍机制能够使系统在一定的时间内保证其功能的运转并完成任务。

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

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

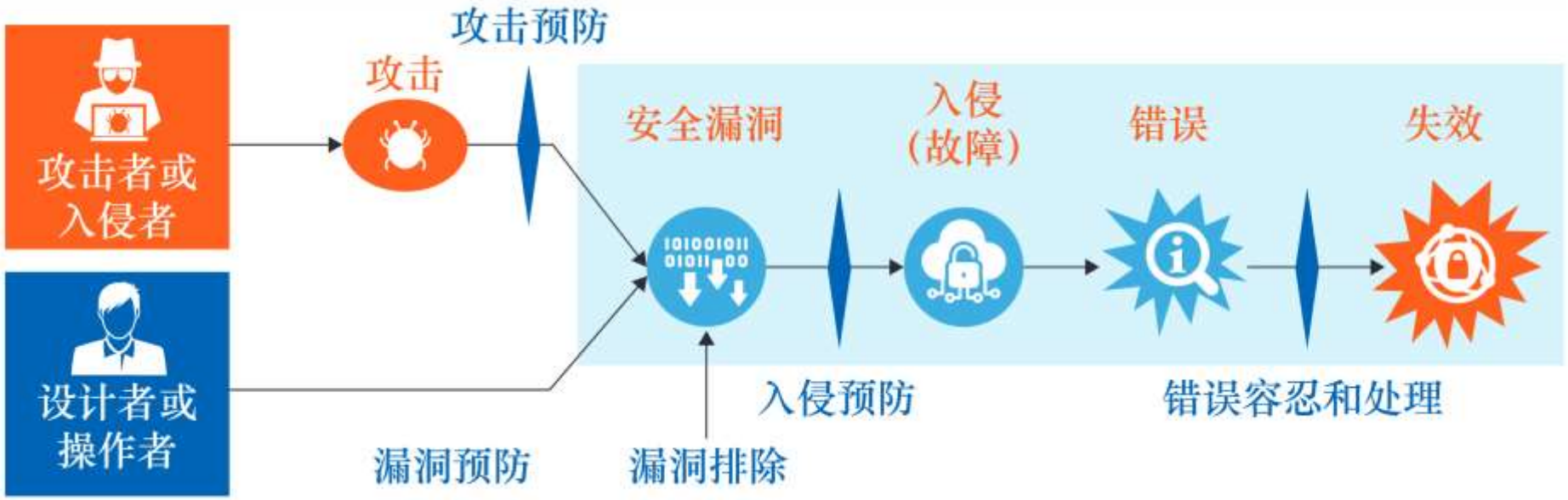
- 系统的失效过程可以用攻击漏洞入侵混合错误模型来表示
- 系统从遭受攻击到最终失效涉及到的环节包括：攻击者（入侵者）攻击、安全漏洞利用、入侵（故障）、错误发生、系统失效



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



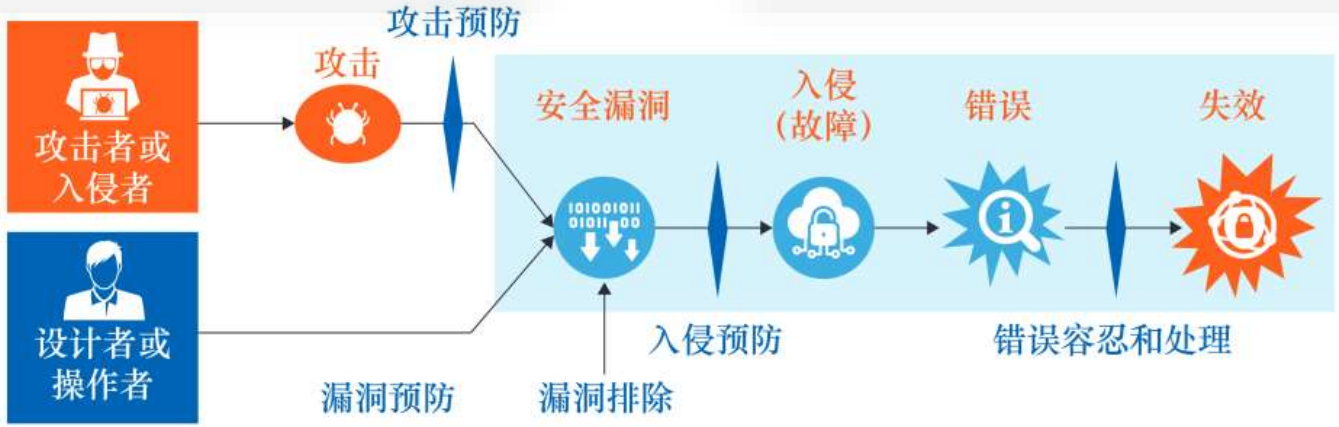
入侵容忍的安全能力和核心机制

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

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

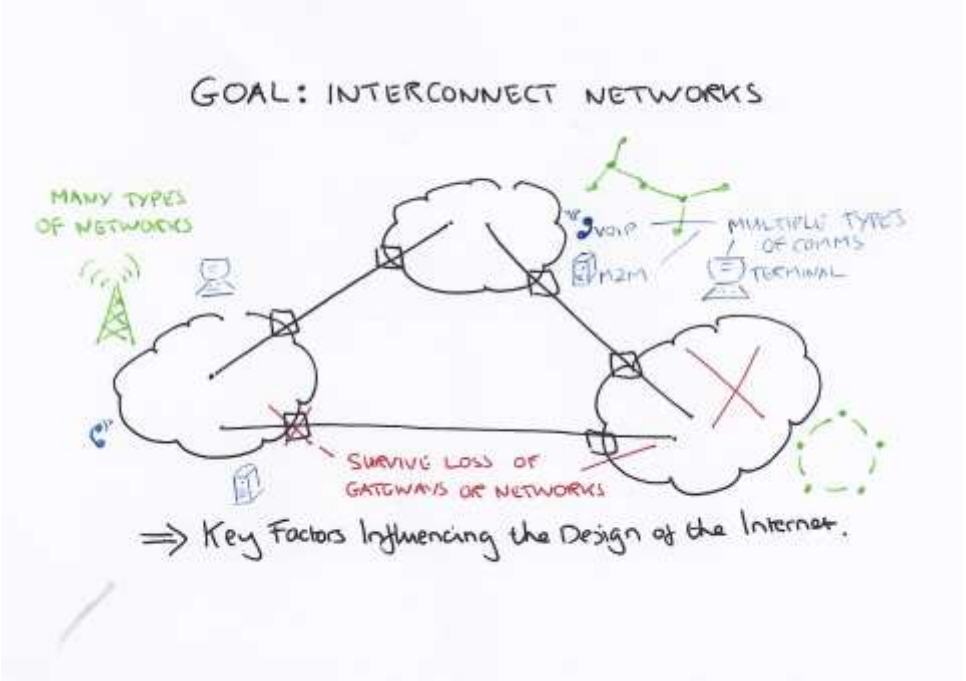
错误恢复

- 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

互联网设计原则(Clark’88)

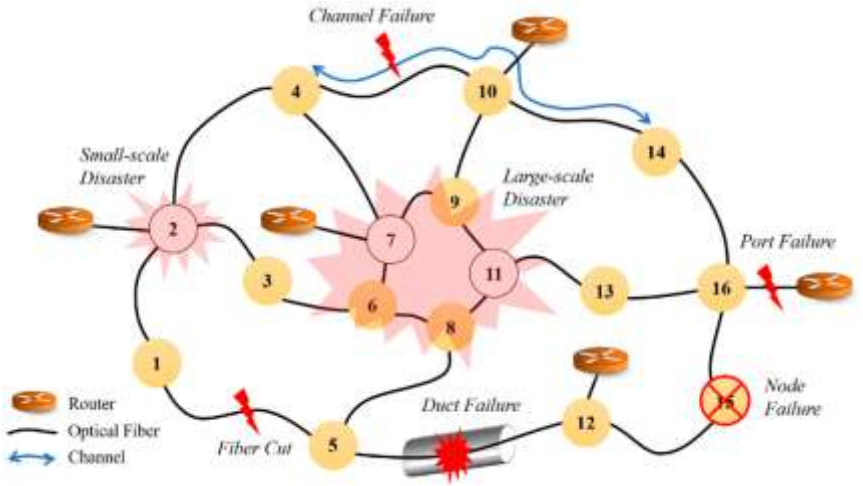
In order of importance:

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



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)



第3节 可信计算

- 发展概况
- 安全目标
- 基本思想和原理

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

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
• 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）	• 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	• IBM为Xen虚拟机设计虚拟TPM（可信平台模块）	• 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Window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

可信计算发展概况

国内：相关研究团队相继开展研究

2000	2005	2008	2014以后
• 武汉瑞达和武汉大学采用可信计算的思想研制了“国内第一款可信计算机”	• 联想研制了自己的TPM芯片和可信计算机	• 中国可信计算联盟（CCTU）成立）	• 中关村可信计算产业联盟成立 • “白细胞”操作系统免疫平台推出，宣告可信计算3.0产业化时代到来

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

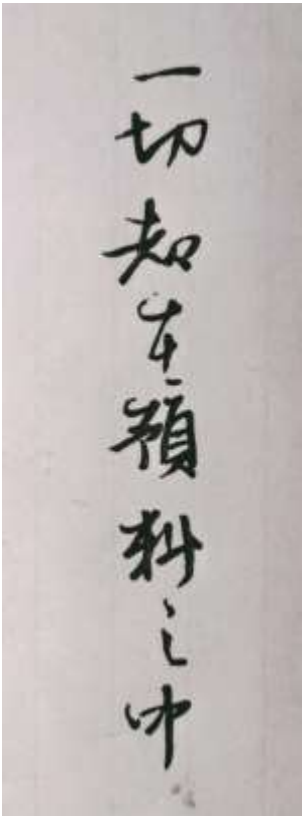
- 解决这些问题重点需要从芯片、硬件结构、操作系统等方面综合采取措施保证系统的安全和可信，从而在根本上提高安全性能，达成安全可信的目标

什么是可信?

可信的通俗解释：可以相信、可以信赖（摘自百度百科）

- 可信计算组织认为，当一个实体的行为总是按照预期的方式达到预定的目标时，它就是可信的

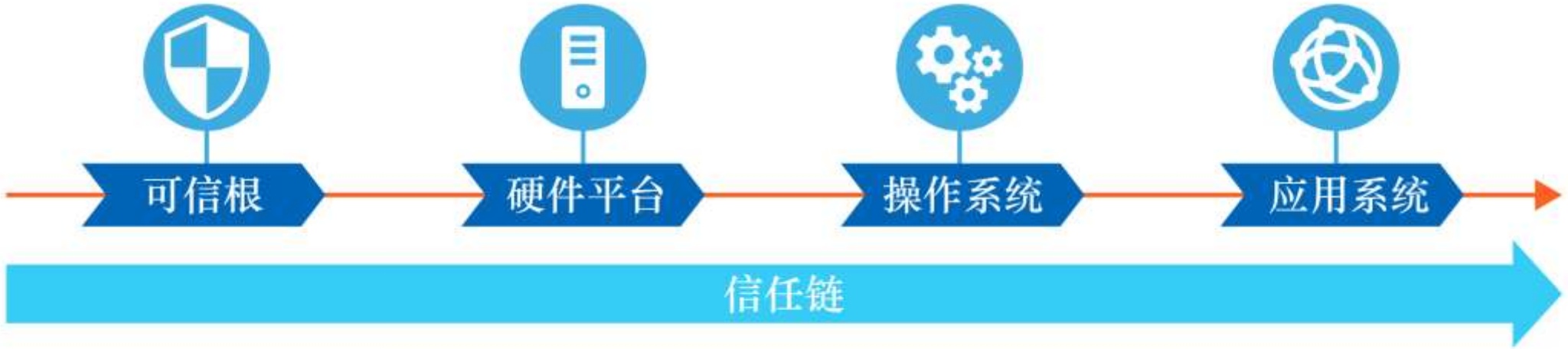
- 对于计算机系统而言，如果系统每一个部件的行为都可知或者可预期时，就能够保证系统的安全可信



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



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

- **可信根**通常以 TPM 的形式实现，是一种加密处理器，能够提供基于硬件的安全相关功能。可信根受到非常严格的保护，具有物理上防篡改、防探测的属性，能够确保恶意软件无法篡改 TPM 的安全功能，从而使可信根能够抵抗攻击，承担起可信计算系统信任基点的重要角色

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

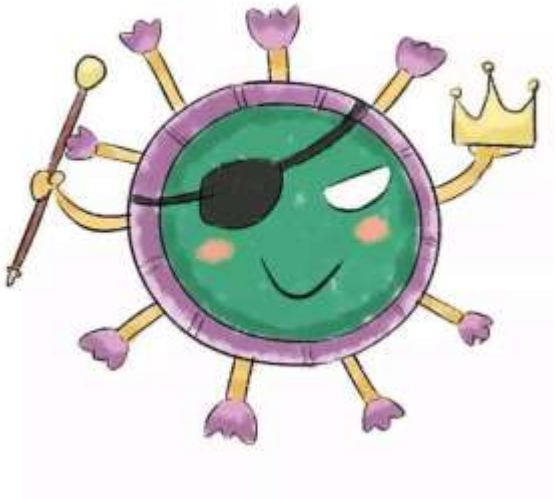
第4节 类免疫防御

- 发展概况
- 安全目标
- 基本思想和原理

思想出发点

- 计算机病毒和生物学中的病毒有一定的相似性，都能够在目标系统中复制、传播并造成破坏
- 在生物学中，免疫机制能够有效抑制病毒传播，通过消灭和清除病毒保证机体健康
- 在计算机系统中，是否也能够借鉴生物学中的免疫机制从而实现计算机系统的安全？

生物病毒疫苗

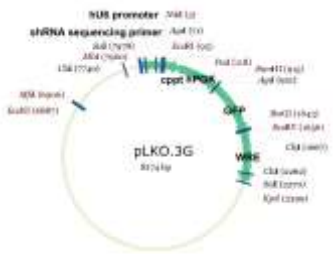


灭活疫苗

即在体外培养新冠病毒，然后将其灭活，使之没有毒性，但这些灭活病毒仍能刺激人体产生抗体

重组蛋白疫苗

通过基因工程方法，大量生产新冠病毒最有可能作为抗原的S蛋白，把它注射到人体，刺激人体产生抗体



腺病毒载体疫苗

用经过改造后无害的腺病毒作为载体，装入新冠病毒的S蛋白基因，制成腺病毒载体疫苗，刺激人体产生抗体

核酸疫苗

包括mRNA疫苗和DNA疫苗，是将编码S蛋白的基因，mRNA或者DNA直接注入人体，利用人体细胞在人体内合成S蛋白，刺激人体产生抗体

类免疫防御发展概况

类免疫防御的思想可以追溯到1987年“计算机病毒”这一词汇的提出。此后，不断有计算机研究人员将计算机的安全问题和生物学中的问题进行比较和分析

1987	1997	1997-至今
• 科恩（Cohen）等人在论文中提出了计算机病毒的概念	• 福雷斯特等人在1997年发表的论文“Computer immunology”（计算机免疫学）中正式建立了免疫系统和计算机安全的联系	• 研究人员围绕如何借鉴自然免疫系统来设计计算机免疫系统开展研究 • 类免疫防御的思想逐步被应用于恶意代码检测、入侵检测、未知攻击检测等领域

类免疫防御的安全目标

- 类免疫防御的目标是使计算机系统像生物系统一样，具有发现和消灭外来安全威胁（病毒、入侵）的能力，从而实现计算机系统的安全

- 类似生物免疫学中的抗体识别抗原，计算机类免疫防御系统通过设计安全机制检测、识别和清除安全威胁，使系统对安全威胁“免疫”

计算机系统中的免疫

“识别” + “清除”

- 识别正常和非正常信息
- 修改、隔离或删除有害信息

维持系统的安全状态

提升系统的安全性能

类免疫防御的实现思路

- 对攻击威胁的特征进行提取和编码
- 借助免疫系统算法和模型生成相应的“抗体”

以一种自适应的方式实现对攻击威胁的识别和清除

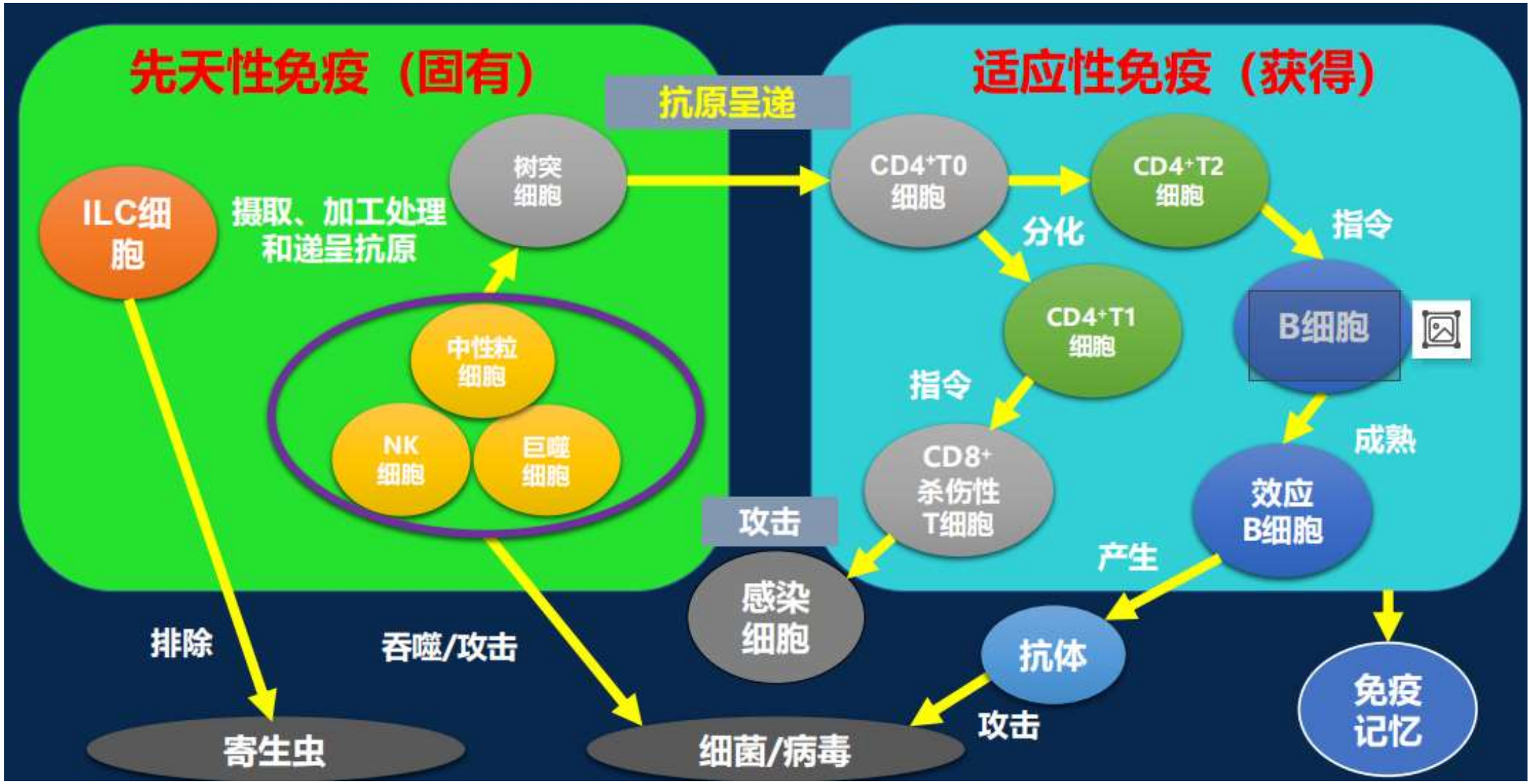
类免疫防御与生物免疫的类比

以恶意代码检测为例

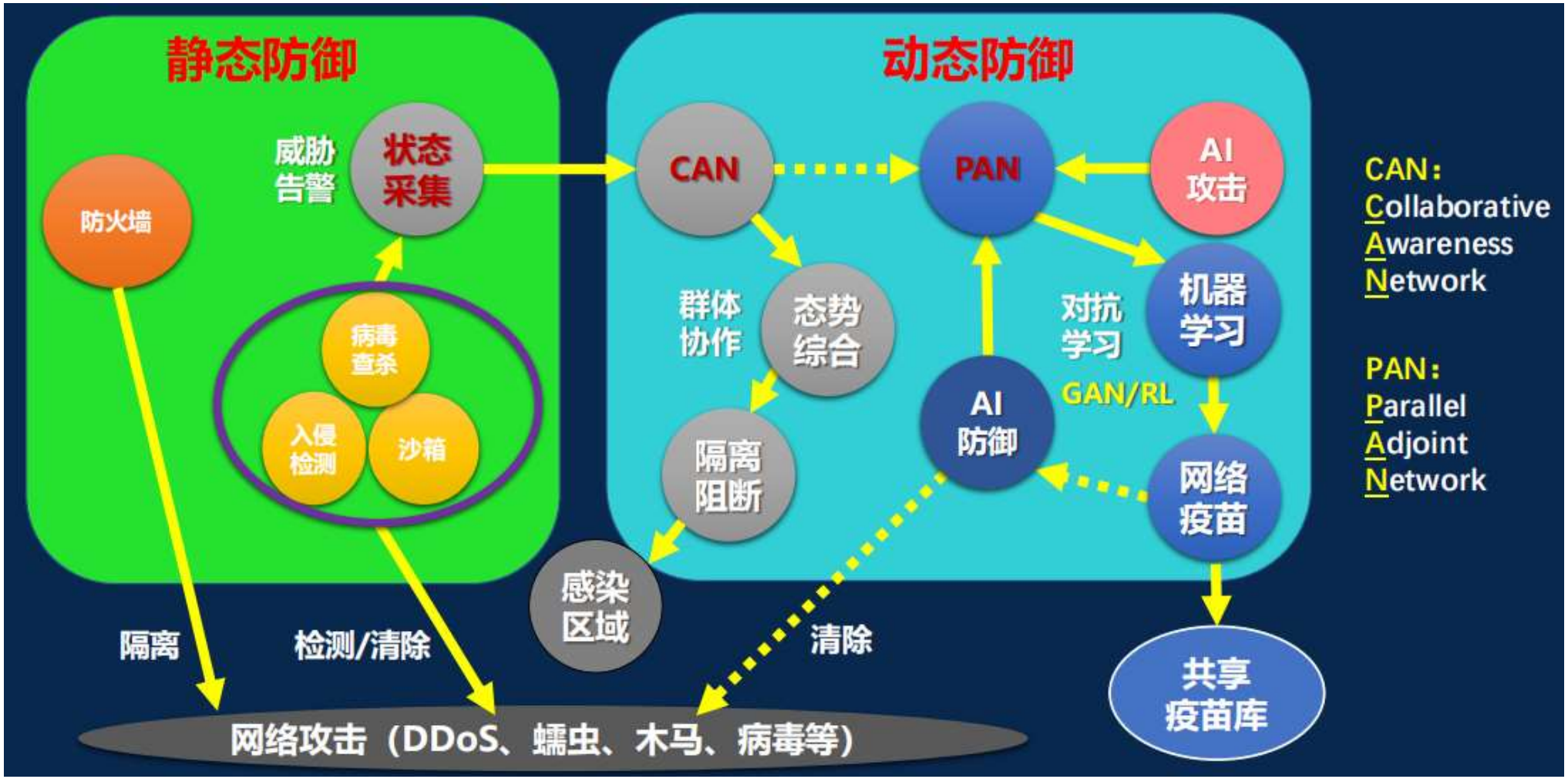
生物免疫	类免疫防御
生物体内的微生物	计算机系统内的各种资源
疾病发作	恶意代码破坏计算机系统
自身细胞	正常文件
抗原	恶意代码文件
抗体	恶意代码特征
生物疫苗	恶意代码疫苗
疫苗注射	恶意代码特征库更新
抗原清除	恶意代码清除

针对不同的安全威胁设计相应的免疫机制，使系统具备免疫能力

先天性免疫与适应性免疫基本模型（于全院士）



类生物免疫的自适应安全防御（于全院士）



第5节 移动目标防御

- 发展概况
- 安全目标
- 基本思想和原理

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？

移动目标防御发展概况

1970年代	2009年	2011年	2014年至今
• 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	• 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	• 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	• ACM连续举办了数场移动目标防御研讨会（ACM Workshop on Moving Target Defense）

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

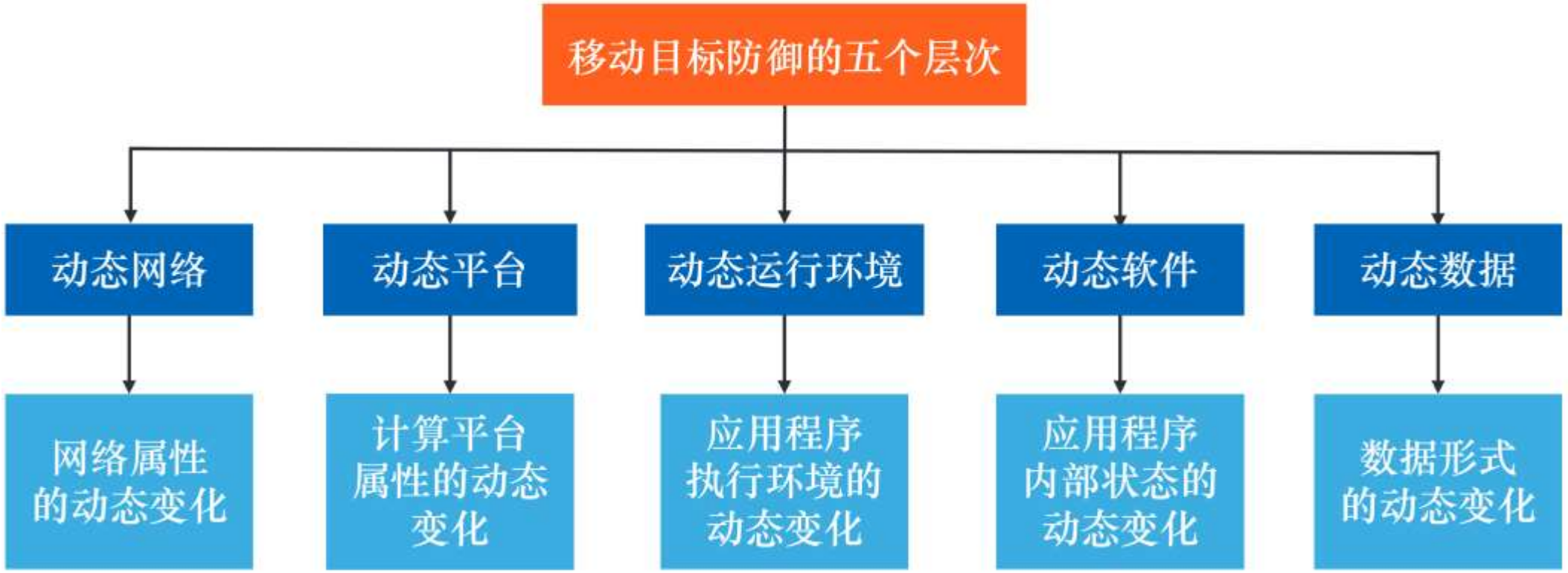
移动目标防御的基本思想

“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

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

MTD代表性的具体技术

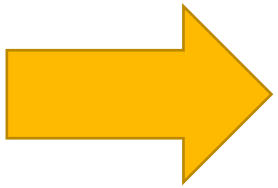
- IP地址跳变
- 端口跳变
- 动态路由
- 网络和主机身份随机化

- 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

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

第6节 拟态防御

- 发展概况
- 安全目标
- 基本思想和原理

思想出发点

- 网络空间安全的一个重要目标是确保有漏洞的系统难以被攻破，并且在遭受攻击时仍然正常运行
- 借鉴异构冗余的思想，通过运行多个执行同样功能的异构硬件或者软件系统，是否就可以实现系统难攻击和攻不跨的目标?

结合移动目标防御动态变化、异构、不确定的设计思想，产生了拟态防御的安全机制

灵感来源

- 战争：八卦阵——以阵形变换进行防御
- 射击：固定靶、活动靶、随动靶
- 通信：抗干扰——跳频、跳时、跳规程、跳结构
- 生物：拟态章鱼、变色龙、叶尾壁虎等自然界的伪装高手

https://haokan.baidu.com/v?vid=6245352048310755527&&

许多技术思想的起源都受到自然或者社会现象的启发

拟态和拟态现象

- 拟态：生物学名词，指某些动物的形态、色泽或斑纹等极似他物，借以蒙蔽敌害，保护自身的现象。如尺蠖之极似树枝，凤蝶幼虫之极似鸟粪等。亦指人在外表上所模拟的形态
- 拟态现象或拟态伪装：是一个生物学概念，指一种生物在形态、行为等特征上模拟另一种生物，从而使一方或双方受益的生态适应现象

按防御行为分类可将其列入基于内生机理的主动防御范畴，这种防御行为又可称为“拟态防御”

拟态防御发展概况

拟态防御理论是国内研究团队首创的主动防御理论（邬江兴院士团队）

2013

- 2013年9月第一台拟态计算机——主动可重构计算机体系结构（PRCA）原理样机研制成功

2016

- 2016年1月“拟态防御原理验证系统”通过了上海市科学技术委员会组织的历时4个多月的测试和验证

2018

- 2018年4月全球首套拟态防御网络设备在郑州上线，标志着拟态防御理论的发展迈上新的台阶

拟态防御的安全目标

拟态防御的安全目标主要是对攻击者形成“测不准”效应、获得内生安全/广义鲁棒控制功能

- 扰乱或阻断未知漏洞或后门利用的攻击链，缩短外部攻击者和内网攻击者嗅探系统特征及规律的时间窗口，作为倍增器放大传统安全措施的效能

- 大幅增加了漏洞的利用难度，降低了攻击的有效性；通过对未知漏洞或后门进行主动防御，有效抑制“有毒带菌”底层构件造成的安全威胁，解决不确定威胁的问题

拟态防御的基本思想

“动态” + “异构” + “冗余”

- 在功能等价的条件下，以提供目标环境的动态性、异构性、冗余可靠为目的
- 通过网络、平台、环境、软件、数据等结构的主动跳变或快速迁移来实现动态变化、弹性可靠的拟态环境
- 扰乱攻击链的构造、使攻击的代价倍增、难以生效

拟态防御的基本思想

“动态” + “异构” + “冗余”

- 以防御者可控的方式动态变化
- 对攻击者则表现为难以观测、无法预测
- 大幅度增加包括未知的可利用的漏洞和后门在内的攻击难度和成本

对不确定性威胁形成主动防御

拟态安全主动防御体系基础架构

基于随机化和多样化内核构建的拟态防御安全模型是整个防御体系的核心

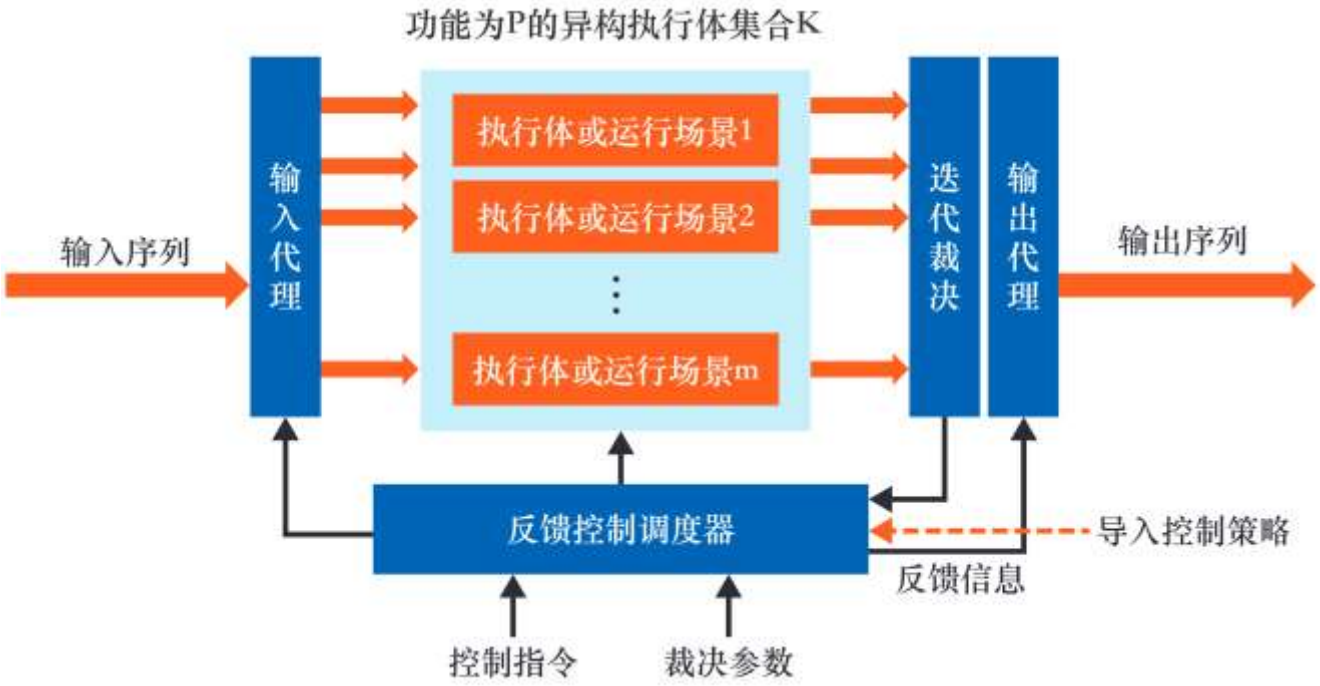
主动防御特性体现在：

- 以异构性、多样或多元性改变目标系统的相似性、单一性
- 以动态性、随机性改变目标系统的静态性、确定性
- 以异构冗余多模裁决机制识别和屏蔽未知缺陷与未明威胁
- 以高可靠性架构增强目标系统服务功能的柔韧性或弹性
- 以系统的不确定属性防御针对目标系统的不确定性威胁

随机化和多样化内核——动态异构冗余构造

拟态构造：动态异构冗余构造

- 包括异构执行体集合、策略裁决、反馈控制等要素
- 具有多维动态重构、迭代裁决、反馈控制调度等功能
- 自带随机、多样、冗余等属性
- 以系统的不确定属性防御针对目标系统的不确定性威胁



实现在呈现功能等价条件下的“测不准效应”，可以同时应对“基于暗功能的攻击”和“软硬件随机性故障”等内生安全问题

第7节 零信任网络

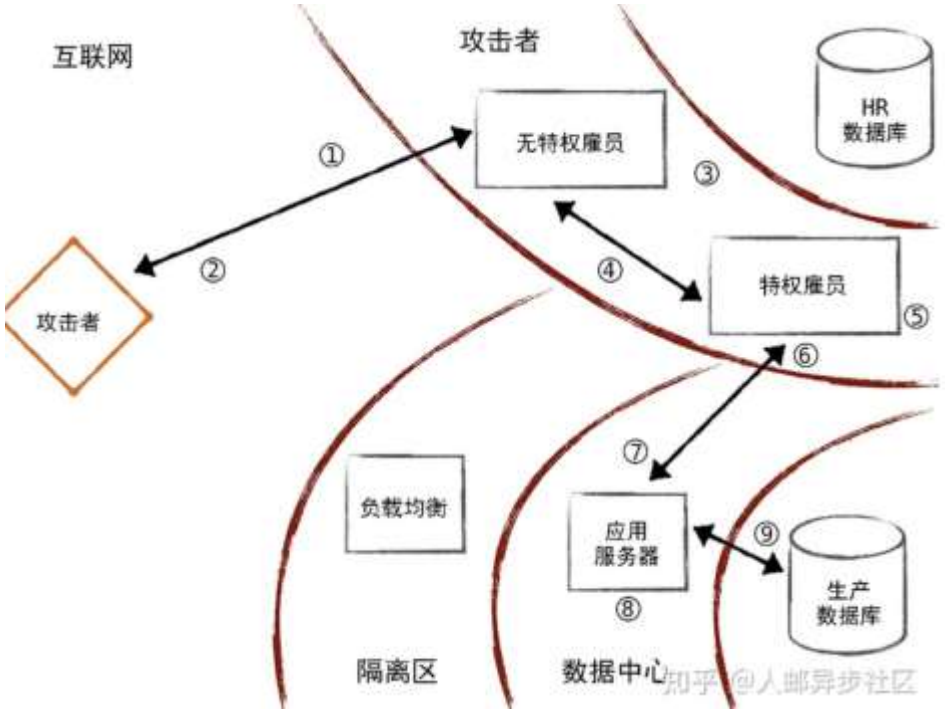
- 发展概况
- 安全目标
- 基本思想和原理

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？

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

零信任网络发展概况

2010

- 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

2017

- 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

2018

- 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

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》

零信任网络的核心思想

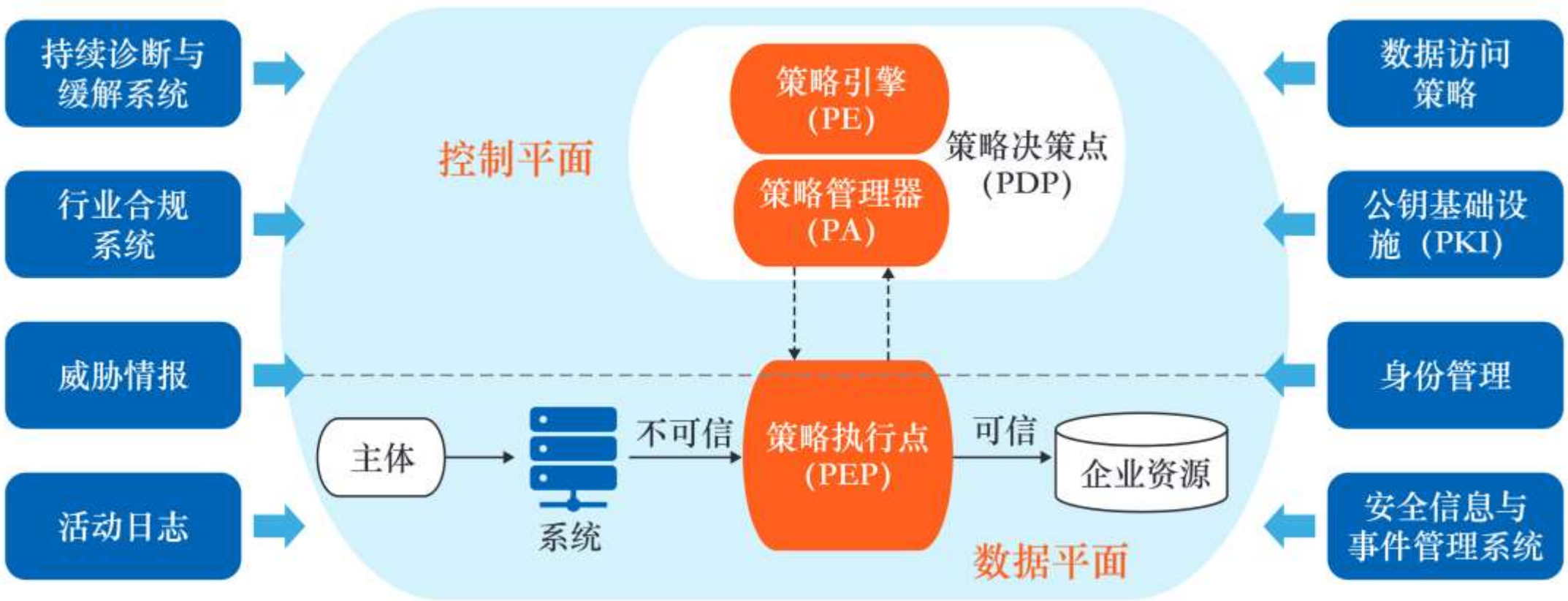
“从来不信任，始终在校验”（Never Trust, Always Verify）

- 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

零信任网络架构

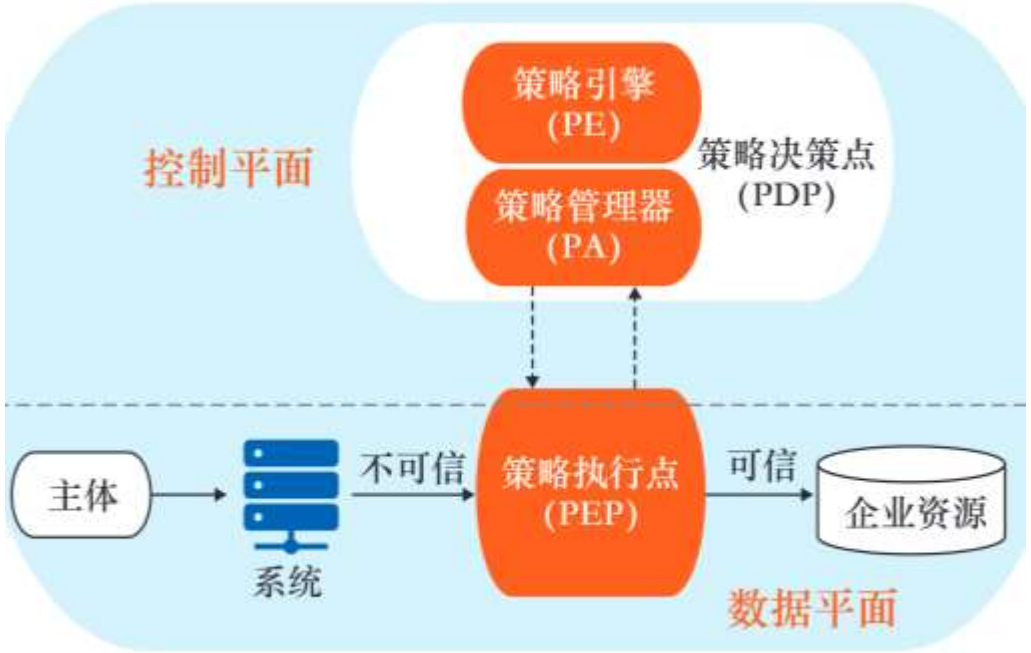
美国国家标准与技术研究院（NIST）于2020年8月发布的《零信任架构》研究报告给出了零信任架构的理想模型



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

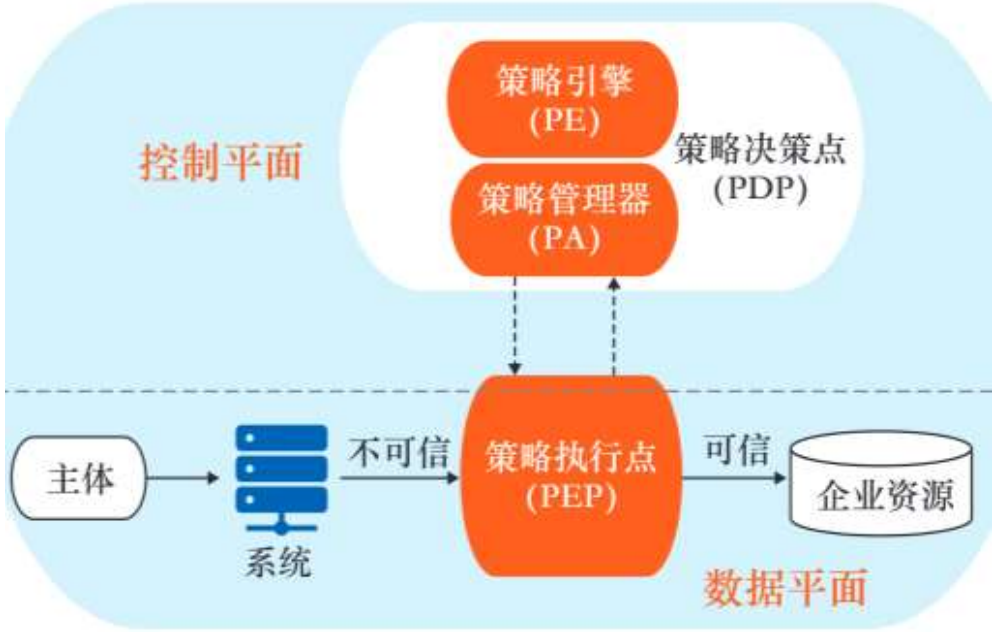
- 核心逻辑组件由策略决策点（包括策略引擎、策略管理器两个子组件）和策略执行点组成
- 外部还有多个提供输入和策略规则的数据源，包括持续诊断与缓解系统、行业合规系统、数据访问策略、公钥基础设施等



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

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

零信任网络的7条基本原则

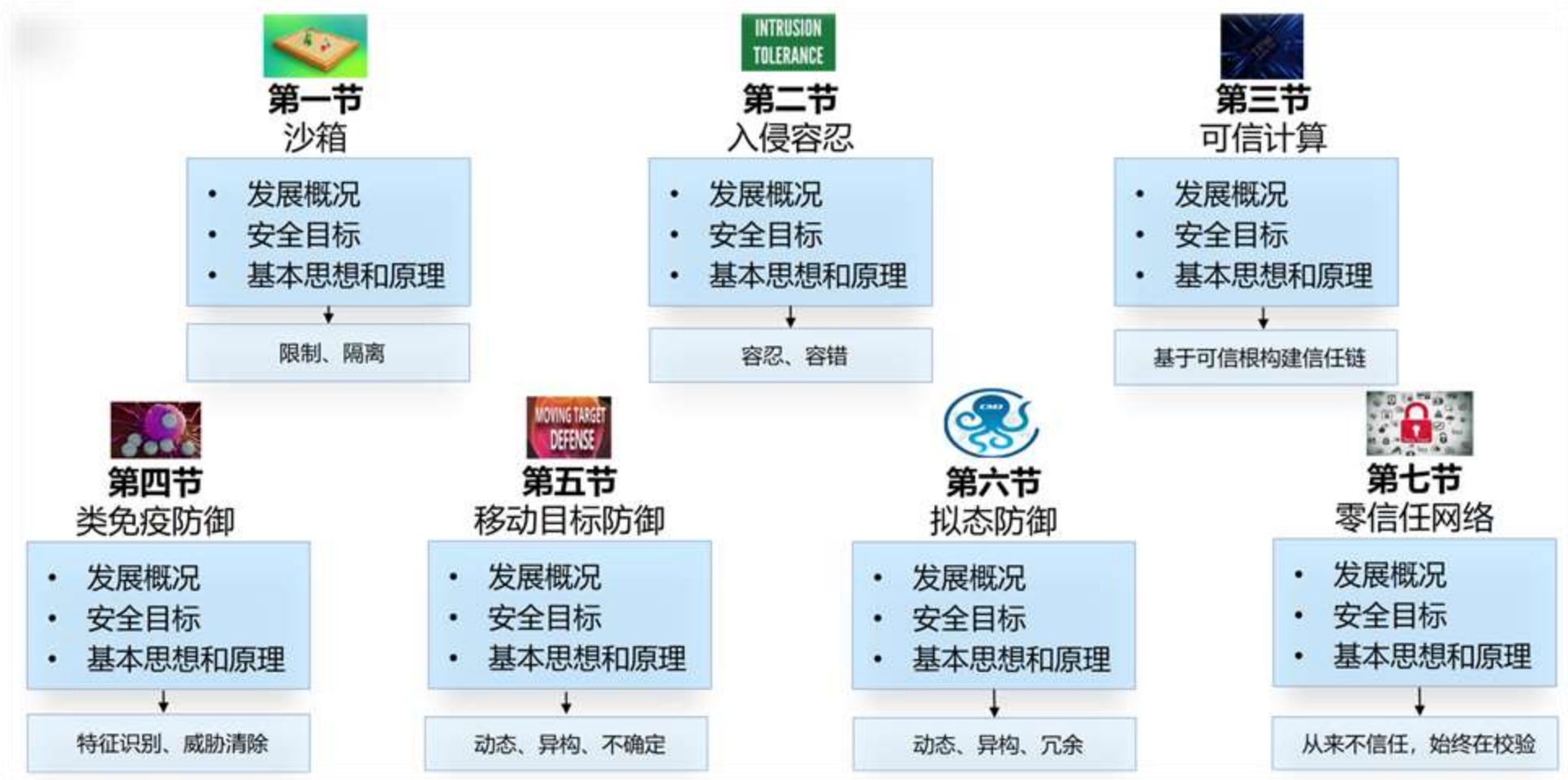
NIST的报告中提出了零信任架构的设计和部署应当遵循的基本原则：

- 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

第8节 总结和展望

网络空间安全基本机制

- 回顾了网络空间安全基本机制的发展历程，着重介绍了七种经典的网络空间安全基本机制，对每一种安全机制的出发点、安全目标和核心思想进行了分析和探讨



展望：完善已有机制并探索新一代安全机制

已有的安全机制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，如何持续完善解决?

- 沙箱中漏洞的利用造成隔离机制的绕过
- 可信计算中可信根本身的安全问题
- 入侵容忍和拟态的冗余设计带来的成本和开销问题
- 移动目标防御中动态跳变对效率的影响
- 零信任网络中权限检查导致的开销问题

绝对安全的网络系统有可能存在吗?