Chap3——网络空间安全基本机制

拟态防御

- 发展概况
  - **2013年**: 拟态防御理论开始产生。
  - **2016年**: 拟态防御理论得到进一步的发展。
  - **2018年**: 拟态防御理论得到广泛的应用和认可。
- 安全目标
  - **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。
- 基本思想和原理
  - 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**。
  - 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
  - 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

移动目标防御

- 发展概况
  - **1970年代**: 初期的移动目标防御概念出现。
  - **2009年**: 移动目标防御技术逐渐受到关注。
  - **2011年**: 移动目标防御技术逐步实践应用。
  - **2014年至今**: 移动目标防御成为重要的网络安全防护手段。
- 安全目标
- 基本思想和原理
  - 1. **动态网络**: 通过不断在网络系统的多个配置之间进行转移变换, 例如更改开放的网络端口, 网络配置, 软件等。
  - 2. **增加随机性和不确定性**: 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, 从而增加攻击难度、有效削弱攻击者对防御机制的适应和突破能力。
  - 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

沙箱

- 发展概况
  - **20世纪70年代**: 早期的沙箱技术开始出现。
  - **20世纪80年代至90年代末**: 沙箱技术得到了进一步的发展和应用。
  - **2000年以后**: 随着互联网的普及和技术的进步, 沙箱技术得到了广泛的应用和发展。
- 安全目标
- 沙箱的基本思想和原理
  - **沙箱环境**: 一个受限的、与外部隔离的操作系统环境。
  - **程序的运行**: 在沙箱内部运行的程序只能对沙箱内部的资源进行访问, 对沙箱外部的资源的访问则被限制。
  - **安全规则配置**: 通过配置安全规则, 可以控制程序能够使用的资源集, 例如内存空间, 文件系统空间, 网络等资源。
- 沙箱与其他技术的关系
  - **软件错误隔离**: *沙箱可以看成是软件错误隔离思想在网络防御中的应用*。软件错误隔离的目标是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。
  - **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*。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。
  - **虚拟化**: *沙箱也可以被视为虚拟化技术的一种特定实例*。虚拟化技术能够模拟完整的主机, 如微软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

入侵容忍

- 发展概况
  - **20世纪80年代**: 入侵容忍技术开始出现。
  - **20世纪90年代末**: 入侵容忍技术得到进一步的发展和应用。
  - **2000年以后**: 随着互联网的普及和技术的进步, 入侵容忍技术得到了广泛的应用和发展。
- 安全目标
- 基本思想和原理
- 入侵容忍的安全能力和核心机制
  - **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**
  - **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**
- 互联网设计原则

可信计算

- 发展概况
  - **1999年**: 可信计算平台联盟 (Trusted Computing Platform Alliance, TCPA) 成立。
  - **2003年**: 可信计算组织 (Trusted Computing Group, TCG) 成立, 主推可信计算发展。
  - **2006年**: 可信平台模块 (Trusted Platform Module, TPM) 被广泛接受和应用。
  - **2007年以后**: 可信计算的理念和技术得到进一步推广和应用。
- 安全目标
- 基本思想和原理
- 关键技术概念
  - **背书密钥**
  - **安全输入和输出**
  - **内存屏蔽/受保护的执行**
  - **密封存储**
  - **远程认证**
  - **可信第三方**