Chap3

> Credit to @Saltyp0rridge

沙箱

发展概况

沙箱技术的发展历程：

- **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。

P13 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。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。因此，沙箱通过隔离和限制程序的权限，有效地防止了这些恶意程序的破坏。

P14 沙箱的基本思想和原理

沙箱的核心思想是**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，恶意程序对系统可能造成的破坏被限制在最小范围内。

P15 沙箱的内部工作机制主要由以下几个方面构成：

- **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

- P16 **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。
- P17 **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。
- P18 **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

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。

入侵容忍

发展概况

入侵容忍技术的发展历程：

- **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 P22

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。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。

基本思想和原理

入侵容忍的核心思想是**即使存在安全漏洞并且攻击能够成功，也要防止系统失效，并保证系统的可用性和鲁棒性**。系统的失效过程可以用攻击漏洞入侵混合错误模型（AVI模型）来表示，即Attack, Vulnerability, Intrusion composite fault model。

入侵容忍的基本原理包括攻击预防、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。

P26 入侵容忍的安全能力和核心机制

入侵容忍的安全能力主要包括：

- **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**

入侵容忍的核心机制主要包括：

- **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**

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。具体包括错误检测和错误恢复，旨在阻止产生灾难性失效。

互联网设计原则

Clark'88 的互联网设计原则

强调了包括入侵容忍在内的多种要素，如连接现有网络、生存性、支持多种类型的服务、容纳多种网络、允许分布式管理、允许低努力的主机连接、成本有效性和资源可追溯性等。在这些原则中，生存性（即入侵容忍）是非常重要的一点，确保通信服务在网络和路由器故障下仍可持续运行。

可信计算 P33

发展概况

可信计算的发展历程：

- **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。

在中国，自2000年开始，相关研究团队也开始进行可信计算的研究。

安全目标

可信计算的目标是提升计算机系统的安全性和可信性，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。这需要从芯片、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。

基本思想和原理

可信计算的核心思想是从信任根出发构建信任链。首先建立一个可信根，其可信性由物理安全、技术安全与管理安全共同保证。然后，基于可信根建立一条信任链，将信任扩展到整个系统，从而确保系统整体的可信性。可信根通常以 TPM 形式实现，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。

关键技术概念

可信计算包含以下六个关键技术概念：

- **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**

基于这六个关键技术，我们可以构建一个完全可信的系统，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。

类免疫防御

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”。

1. 对攻击威胁的特征进行提取和编码
2. 借助免疫系统算法和模型生成相应的“抗体”
3. 以一种自适应的方式实现对攻击威胁的识别和清除

移动目标防御

发展概况

移动目标防御的发展历程：

- **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

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。它旨在改变传统信息系统静态配置运行的弱点，从而挫败外部攻击。

基本思想和原理

移动目标防御的基本思想是 “动态”+“异构”，即通过**增加系统的随机性和不可预测性来防范网络攻击**。这种防御机制从动态、随机和多样化的角度进行设计，目的是建立一种动态、异构、不确定的网络空间目标环境，以增加攻击者的攻击成本。

移动目标防御具有五个层次。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。

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。如果转移变换的机制是确定性的，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。

拟态防御

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**。其目标包括：

- **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

“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**。
- 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。

零信任网络

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。

从来不信任，始终在校验，不应该信任企业网络内部和外部的任何人/设备/应用。

P75 七条原则