

基于自然免疫原理与可信计算的自主可控信息系统研究

柳伟¹, 慈林林², 刘利平¹

(1. 北京理工大学计算机学院, 北京 100081;

2. 北京信息高技术研究所, 北京 100085)

摘要: 信息领域的竞争是一种体系竞争, 针对单一防御手段无法应对立体攻击的问题, 构建了一种基于自然免疫原理与可信计算的自主可控信息系统。该系统包括可信网络基础功能部分、用户行为度量子系统、软件行为度量子系统和容错子系统, 通过在基础功能部分增加安全机制的方式实现了信任链的扩展、可信网络接入控制模型与基于角色访问控制模型的融合, 以及可信终端全生命周期的可信接入。

关键词: 自主可控信息系统; 可信计算; 软件行为; 用户行为; 容错系统

中图分类号: TP311.134.3

文献标识码: A

doi: 10.11959/j.issn.2096-6652.201920

Research of independent and controllable information system based on natural immune system and trusted computing

LIU Wei¹, CI Linlin², LIU Liping¹

1. School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China

2. Beijing Institute of Information High Technology, Beijing 100085, China

Abstract: The competition in the field of information is a kind of system competition. Aiming at the problem that a single defense method cannot cope with the comprehensive attack, an independent and controllable information system based on natural immune system and trusted computing was constructed. The system includes trusted network basic function subsystem, user behavior measurement subsystem, software behavior measurement subsystem and fault-tolerant subsystem. The advantage of this way of adding security mechanisms to basic functionality is the extension of the chain of trust, integration of trusted network access control model and role-based access control model and trusted access of trusted terminal throughout life cycle can be achieved.

Key words: independent and controllable information system, trusted computing, software behavior, user behavior, fault-tolerant system

1 引言

信息安全涉及国家安全, 工业控制系统等关键信息系统的信息安全尤其如此。当前, 世界各国纷纷强调信息安全, 我国也旗帜鲜明地提出信息系统的“自主可控, 安全可信”。因此, 自主可控信息系统具有重要的研究价值^[1]。

随着攻击手段的升级, 即使是在与因特网物理隔离的高可靠性信息系统的可信链中, 依然存在

诸多可以被利用的薄弱环节。

信息领域的竞争是一种体系竞争, 任何时候都要构造自我保护法则。本文依托信息系统安全控制课题, 以“自主可控”为手段, “安全可信”为目的, 以构建融合安全控制、指挥控制和发射控制于一体的某可信分布式系统为目标, 将网络安全研究理念从被动防御转向主动防御, 从关注脆弱性安全转向关注结构性安全, 从关注外部威胁转向提高自身能力, 重点探索可信可控软硬件环境的构建方法和实

现技术^[2-4]。

2 相关研究

2.1 自然免疫系统

生物免疫系统是抵御病原体(例如寄生虫、真菌、细菌和病毒等)侵袭有机体的重要保卫系统。整个免疫系统由免疫器官(脾脏、胸腺、骨髓、淋巴结、扁桃体和阑尾和小肠集合淋巴结等)、免疫细胞(淋巴细胞、单核吞噬细胞、中性粒细胞、嗜碱粒细胞、嗜酸粒细胞、肥大细胞和血小板等)及免疫分子(干扰素、白细胞介素、肿瘤坏死因子、补体和免疫球蛋白等)组成。免疫系统面对外来入侵病原体或外来抗原时能调动细胞和分子积极防御,限制病原体在体内繁殖并将其彻底消灭。

作为开放复杂巨系统,自然免疫系统具有自组织性、自学习性、适应性、分布性、动态性、多样性、记忆性和鲁棒性。自然免疫系统对于复杂系统的研究能够提供理论借鉴和求解思路^[5-6]。

2.2 可信计算

可信计算(trusted computing)技术是一种主动防卫技术,其基本思想可以概括为“信任传递(transitive trust)”,即可信计算从根入手通过完整性度量和标签机制建立基础信任体系。

在计算机系统中建立一个信任根,由信任根通过完整性度量方法建立一条信任链,通过一级度量一级、一级信任一级的方式将信任关系逐步从信任根扩展到整个计算机系统。在可信平台中,可信度量根核(core root of trust for measurement, CRTM)是平台执行可信度量根(root of trust for measurement, RTM)时的执行代码。平台启动时, CRTM 最先获得执行控制权并对下一个执行模块的代码进行度量。从信任根芯片、主板、基本输入输出系统(basic input output system, BIOS)到操作系统一级度量一级、一级保证一级地逐级安全加固确保系统安全。作为信任的源头, CRTM 的正确性和完整性受物理方法保护。

可信网络是可信计算机机制和网络接入控制机制的结合,也是可信计算平台应用的扩展。可信网络增强了网络访问控制的互操作安全性,其基本思想是在终端接入网络之前对用户身份进行认证,用户身份认证通过后再对终端平台完整性进行度量。若完整性度量值满足网络接入安全策略,则允许终

端平台接入网络;否则将终端平台隔离到指定区域并对其进行安全修补和升级。可信网络连接将终端计算环境的可信扩展到了网络,使网络计算环境变得可信。可信网络连接突破了原有的被动防御模式,将大部分潜在攻击抑制在了攻击发生之前,在用户、终端平台和网络之间建立了信任关系,实现了网络和终端平台的可信连接。

目前可信度量研究还集中在静态可信度量方面,“一级度量一级,一级信任一级”的“信任传递”思想描述的信任链扩展本质上还是基于数据完整性度量机制的静态度量。这种完整性度量机制只能保证可信平台在启动初始阶段的软硬件资源符合预期安全策略要求,但终端平台启动之后,在其上动态运行的系统软件和应用软件能否按照预期运行却得不到保证。

3 基于自然免疫原理与可信计算的自主可控信息系统

为弥补静态度量的不足,对具体的信息系统应采取按需定制、系统综合化的措施来增强动态可信,即既要基于可信计算硬件平台研究动态可信评测理论和方法,也要基于可信网络通过增加安全机制的方式进行动态评测。在保证信息系统各要素可信的同时,通过信息系统各部分之间相互联系、相互制约得到“1+1>2”的效果^[7-12]。

3.1 自主可控的可信源头

构建自主可控的可信生态环境要求从硬件、固件、操作系统等底层安全入手减少不可控环节。可信平台模块是所有信任发起的源头,是自主可控硬件设备中的重点。本节给出了具有主动度量功能的自主可信密码模块(trusted cryptography module, TCM)设计原理和具有 TCM 功能模块的自主可控设备主板设计原理。

自主 TCM 结构与可信赖平台模块(trusted platform module, TPM)结构不同,其度量起点设置在 TCM 内部。在可信计算平台其他部件不加电的情况下,给 TCM 加电使其最先启动。在 BootRom 工作之前,完成对 BootRom 中关键数据的度量工作。由 TCM 对 BIOS 进行度量,保证了对 BIOS 的客观监控能力。TCM 和 BootRom 芯片之间的连接总线不通过南桥连接,而是采用直接互联的方式连接。这样就避免了间接连接方式可能造成的信息不真实或信息窃取问题,使得读取的内容更为可信。

TCM 内部维护着预先设定的用户管理表以及预设为管理员和普通用户的设备使用权限信息,这使得可信计算机具备了在开机之前对用户进行身份认证的能力。除以上创新之外,自主 TCM 还集成了自主知识产权的密码算法。

此外,为了防止恶意软件篡改权限,TCM 还增加了对平台底层硬件设备资源(硬盘、并口设备、串口设备、网口设备、USB 和 PCI)和可信平台控制模块资源(各类寄存器、密码引擎、密钥和各类证书)的访问控制功能。

安全可信硬件模块采用 PCI-E/mini PCI-E 接口形式嵌入主板,并基于 Xilinx FPGA 实现主动度量逻辑 SPI-LPC 协议转换和 PSRAM-PCI-E 协议转换。利用自主研发硬件驱动在 PEMON 和操作系统上进行的命令测试,验证了可信硬件模块 PCI-E 通路能够正确地提供可信命令通信。

3.2 自主可控信息系统的数学定义与描述

令 Σ 、 I 、 Ω 、 O 、 M 分别表示系统、系统输入、系统组成、系统输出和输入输出间映射,则系统可用四元组描述为

$$\Sigma = (I, \Omega, O, M)$$

其中, $O = M(I)$ 。

因此,可将自然免疫系统定义为

$$\Sigma_{NIS} = (I_{NIS}, \Omega_{NIS}, O_{NIS}, M_{NIS})$$

其中,输入自然免疫系统的各类抗原 I_{NIS} 包括自身蛋白或某种病原体。 Ω_{NIS} 包括免疫器官、免疫细胞和免疫分子。若用 A 表示抗原全体, S 表示自身蛋白集合, NS 表示病原体集合,则有

$$\begin{cases} S \cup NS = A \\ S \cap NS = \emptyset \\ I_{NIS} \in A \end{cases}$$

对应地,有

$$O_{NIS} = M_{NIS}(I_{NIS}) = \begin{cases} 0, & I_{NIS} \in S \\ 1, & I_{NIS} \in NS \end{cases}$$

类似地,自主可控信息系统可以定义为

$$\Sigma_{TIS} = (I_{TIS}, \Omega_{TIS}, O_{TIS}, M_{TIS})$$

其中,自主可控信息系统的输入 I_{TIS} 包括可信终端身份验证信息、终端平台完整性验证信息、用户输入命令序列、程序系统调用序列、设备执行状态序列和程序控制流标签异或运算值等。 Ω_{TIS} 包括可信

网络基础功能部分、用户行为检测子系统、软件行为检测子系统和容错子系统,不同的信息系统具有不同的 Ω_{TIS} 。令输入论域 T 由符合预期集合 N 与不符合预期集合 $\neg N$ 共同构成。

则有

$$\begin{cases} N \cup \neg N = T \\ N \cap \neg N = \emptyset \\ I_{TIS} \in T \end{cases}$$

对应地,有

$$O_{TIS} = M_{TIS}(I_{TIS}) = \begin{cases} 0, & I_{TIS} \in N \\ 1, & I_{TIS} \in \neg N \end{cases}$$

定义 1 自主可控信息系统检测性能。若令 ρ_{HR} 表示系统 Σ_{TIS} 的检测率,则检测率可以定义为

$$\rho_{HR}(\Sigma_{TIS}) = P(O_{TIS} = 1 / I_{TIS} \in \neg N)$$

相应地,系统 Σ_{TIS} 的漏检率 ρ_{MR} 与虚警率 ρ_{FAR} 可分别定义为

$$\rho_{MR}(\Sigma_{TIS}) = P(O_{TIS} = 0 / I_{TIS} \in \neg N)$$

$$\rho_{FAR}(\Sigma_{TIS}) = P(O_{TIS} = 1 / I_{TIS} \in N)$$

则自主可控系统 Σ_{TIS} 的防御性能可以表示为

$$PD(\Sigma_{TIS}) = \alpha \rho_{MR}(\Sigma_{TIS}) + \beta \rho_{FAR}(\Sigma_{TIS})$$

其中, α 与 β 分别为漏检率和虚警率权值。理论上,虚警率对性能 $PD(\Sigma_{TIS})$ 的贡献越大,则 $PD(\Sigma_{TIS})$ 越小,表示自主可控信息系统的性能越好。

定义 2 自主可控信息系统鲁棒性。若系统 Σ_{TIS} 的内部构成 Ω_{TIS} 包含 n 个检测子系统或代理,即 $\Omega_{TIS} = \{l_1, l_2, \dots, l_{n-1}, l_n\}$ 。当其中有 k 个子系统或代理失效时,产生系统 Σ_{TIS}^* 且其内部构成变为 $\Omega_{TIS}^* = \{l_1, l_2, \dots, l_{n-k}\}$ 。如果 σ 为规定指标且满足

$$\frac{PD(\Sigma_{TIS}^*) - PD(\Sigma_{TIS})}{PD(\Sigma_{TIS})} \leq \sigma$$

则称自主可控信息系统 Σ_{TIS} 具有 k 级鲁棒性。

定义 3 自主可控信息系统自适应性。若内部构成为 $\Omega_{TIS} = \{l_1, l_2, \dots, l_{n-1}, l_n\}$ 的系统 Σ_{TIS} 包含 n 个检测子系统或代理,随着入侵时间 T 发生变化, Σ_{TIS} 变为内部构成为 $\Omega_{TIS}^* = \{l_1, l_2, \dots, l_{n-k}\}$ 的系统 Σ_{TIS}^* 。若其防御性能、感知威胁时间或感知威胁所耗费资源满足 $PD(\Sigma_{TIS}^*) < PD(\Sigma_{TIS})$ 或 $t^* < t$ 或 $r^* < r$,则称系统 Σ_{TIS} 具有自适应性。

定义 4 自主可控信息系统动态防护性。若内部组成为 $\Omega_{TIS} = \{l_1, l_2, \dots, l_{n-1}, l_n\}$ 的系统 Σ_{TIS} 在一段

运行时间 T 内包含激活的子系统代理集合为 $\Omega_{\text{TIS}}^* = \{l_1, l_2, \dots, l_{n-k}\}$ ，假设时间段 T 内存在 $t_1, t_2, \dots, t_j$ 的关键时间点，若在关键时间点 t_i 有 $\Omega_{\text{TIS}}^* \subseteq \Omega_{\text{TIS}}$ ，且当 $1 \leq i \leq j$, $1 \leq h \leq j, i \neq h$ 时有 $\Omega_{\text{TIS}}^* \neq \Omega_{\text{TIS}}^*$ ，则称系统满足动态性。若存在某个时刻 t_m ($1 \leq m \leq n$)，当 $t_i \geq t_m$ 时有 $\Omega_{\text{TIS}} = \bigcup_{i=1}^m \Omega_{\text{TIS}}^*$ ，则称系统满足完备性。当系统同时满足动态性和完备性时，称其具有动态防护性。

3.3 自主可控信息系统的设计原理

自然免疫系统与自主可控信息系统在检测任务、运行环境与检测方法方面类似。

(1) 检测任务

自然免疫系统能够识别“自体”与“异体”，并通过消灭“异体”和耐受“自体”的方式维持自然免疫系统平衡；自主可控信息系统要准确及时地检测、响应针对系统的攻击并能容忍系统正常范围内的变化。

(2) 运行环境

自然免疫系统运行在各类新旧病毒、细菌、真菌和寄生虫等病原体从生的生物世界中；自主可控信息系统则位于充斥着各类已知、未知计算机病毒和攻击手段的网络世界中。

(3) 检测方法

自然免疫系统利用已知“自体”特征区分“自体”与“异体”或利用已知“异体”特征确定并消灭有害“异体”；自主可控信息系统通过比对待检测对象与“自体”或“异体”模型完成检测。

自然免疫系统表示其“自体”的细胞蛋白质几乎不发生变化，“自体”的定义明确、稳定。相对地，自主可控信息系统中用于表示其“自体”的用户操作、软件行为、资源访问等都在一定范围内随时间动态变化，其“自体”的定义并不非常明确和稳定。

自主可控信息系统通过类比自然免疫系统可以得到如下启示。

(1) 多层防护性

生物体采用多层防护抵御外界物质侵入，这些防御层包括：皮肤、黏膜、体液环境（PH、温度等）、炎症反应、适应性反应（T 细胞介导的细胞免疫、B 细胞介导的体液免疫等）。现有基于边界防护的计算机安全系统默认边界内部的活动都是可信的。因此，自主可控信息系统的设计应当采用多层联合防御机制，使整个系统达到高安全性。不同层有不同

的检测对象，各层间并联互补。

从防护层次的角度来看，自主可控信息系统的系统组成 Ω_{TIS} 包括 5 层，即

$$\Omega_{\text{TIS}} = \{l_1, l_2, l_3, l_4, l_5\}$$

- l_1 层负责检查可信平台终端加电前用户身份是否合法，该层主要通过自主设计计算机系统结构和密钥卡来实现，只有持有有效密钥卡的用户才能启动可信平台。

- l_2 层负责检查可信平台完整性与平台身份验证，该层主要通过自主可信终端、可信密码模块（TCM）与可信网络连接（TNC）架构来实现。满足平台鉴别（平台身份验证和平台完整性验证）的可信终端允许接入可信网络。

- l_3 层负责用户行为检测，该层主要通过用户行为子系统完成检测。 l_3 层动态评测结果能完善可信网络接入控制与授权机制，使网络达到全生命周期的可信接入。

- l_4 层负责软件行为检测，该层主要通过软件行为子系统完成检测功能。为达到网络全生命周期可信， l_4 层的动态评测结果也用于完善可信网络接入控制与授权机制。

- l_5 层负责检测因瞬态故障引起的控制流错误和设备执行状态序列，确保其输出结果的可靠和正确，该层主要通过相应的容错子系统完成。 l_5 层的动态评测结果既可用于启动备份系统，也可用于完善可信网络接入控制与授权机制。

(2) 多样性

自然免疫系统包括淋巴细胞、巨噬细胞和中性粒细胞等多种免疫细胞，这些免疫细胞散布在体内不同的淋巴结中，每个细胞个体都能检测一个或多个病原体。因此，自然免疫系统能够检测多种病原体。自主可控信息系统防御子系统代理各具特色，且防御子系统代理多样化可以增加子系统代理之间的多样性，防止单个子系统代理的脆弱性在整个系统中蔓延。这些代理包括可信平台身份验证检测代理、可信平台完整性验证检测代理、用户命令序列检测代理、系统调用序列检测代理和设备控制状态检测代理等。每种代理若干，分布于网络的不同位置。各种代理能够独立检测并相互通信合作。即

$$\Omega_{\text{TIS}} = \left\{ \bigcup_{\substack{i=1 \sim 5 \\ j=1 \sim k_i}} a_{ij} \right\}$$

其中， i 为代理种类数， k_i 为每类代理的个数。

(3) 独特性

不同的自然免疫系统所含的免疫细胞集合有所不同,这使得每个自然个体对病原体的防御能力也不相同。对于不同的代理集,位于不同检测位置的同类检测代理由于所用规则集合不同,同类检测代理的个体检测性能会有差异,这种差异增强了系统的抗攻击能力,使得系统不会因为一个某类检测点被攻破而导致全局同类所有检测点被攻破。即

$$\Omega_{TIS} \neq \Omega_{TIS}^* \Rightarrow a_{ij} \neq a_{ij}^*$$

(4) 协同性

自然免疫系统采用信号协同机制激活淋巴细胞,这使得生物体很少出现自免疫疾病。无论是 T 淋巴细胞还是 B 淋巴细胞,被激活时都要收到两个信号:第一个信号为阈值信号,即一定时间内淋巴细胞所黏合病原体数超过某一阈值后触发的信号;第二个信号为协同信号。对于 B 淋巴细胞来说, T 协助细胞提供协同信号;对于 T 淋巴细胞来说,其自身组织受损释放的化学信号充当协同信号。信号协同机制使得淋巴细胞“自体”不会被误识别为“异体”。自主可控信息系统的“自体”定义随时间在一定范围内波动(不是非常明确和稳定),可以通过引入信号协同机制降低虚警概率。

假设只有自主可控信息系统 Σ_{TIS} 的系统组成中的 l_1, l_2, l_3, l_4 都异常并收到 l_5 协同信号时 Σ_{TIS} 才报警,由定义 1 可知,对于具体防护层 i ,其检测率和虚警率分别为

$$\begin{cases} \rho_{HR}(l_i) = P(O_i=1/I_{TIS} \in \neg N), & i = \{1, 2, 3, 4, 5\} \\ \rho_{FAR}(l_i) = P(O_i=1/I_{TIS} \in N), & i = \{1, 2, 3, 4, 5\} \end{cases}$$

由于采用信号协同机制,各检测层采用并联互补抵御入侵。

$$\rho_{HR}(\Sigma_{TIS}) = P(O_{TIS}=1/I_{TIS} \in \neg N)$$

即有

$$\begin{cases} P\left(\bigcup_{i=1}^5 O_i=1/I_{TIS} \in \neg N\right), & i = \{1, 2, 3, 4, 5\} \\ \{O_i=1\} \subset \left\{\bigcup_{i=1}^5 O_i=1\right\}, & i = \{1, 2, 3, 4, 5\} \end{cases}$$

所以

$$\rho_{HR}(\Sigma_{TIS}) > \rho_{HR}(l_i), \quad i = \{1, 2, 3, 4, 5\}$$

若 l_1, l_2, l_3, l_4 层检测到疑似入侵, l_5 层作为协同信号 Σ_{TIS} 报警。

$$\rho_{FAR}(\Sigma_{TIS}) = P(O_{TIS}=1/I_{TIS} \in N)$$

而

$$\{O_i=1\} \cap \{O_j=1\} \subset \{O_i=1\}, \quad i = \{1, 2, 3, 4\}$$

可得

$$\rho_{FAR}(\Sigma_{TIS}) < \rho_{FAR}(l_i), \quad i = \{1, 2, 3, 4, 5\}$$

又由系统 Σ_{TIS} 防御性能评价公式得

$$PD(\Sigma_{TIS}) < PD(l_i), \quad i = \{1, 2, 3, 4, 5\}$$

即自主可控信息系统的多层协同防御机制性能较普通可信网络更加优异。

(5) 动态防护性

生物体检测器集合不可能大到覆盖整个抗原空间,因此只能在某一时刻利用抗原细胞的分裂和死亡改变抗原空间子集,使其分布在生物体中尽量覆盖抗原空间。大约每 10 天,所有淋巴细胞检测器就能更新一次,这样就在时间和抗原空间上得到了平衡。自主可控信息系统以时间为代价换取待检测“自体”空间。某时刻 Σ_{TIS} 只通过“自体”检测器全体的子集检测。某时刻系统有一个或若干个代理工作且随时间变化,则代理也随之发生变化。对于某一子系统来说,所有代理都异步串行工作。经过一段时间,所有检测器都被激活完成一遍检测。

设 A 为 t 时刻的检测代理工作集合。若在 $[t_i, t_h]$ 内系统能完成一次全系统检测,则 Σ_{TIS} 满足动态防护完备性条件,系统具有动态防护性。

(6) 鲁棒性

生物免疫系统的检测和记忆高度分布且无集中管控应答,检测器和感受器局部协作。变化的细胞分裂和死亡使得免疫系统将资源分配到最需要的地方,并能耐受很多错误,例如去掉脾脏器官。自主可控信息系统无集中控制,具有高安全性,不会因局部点的失效使整个信息系统失败。 Σ_{TIS} 包含多个检测子系统和检测代理,每个检测子系统和若干检测代理能检测到某一类或多类威胁。多个检测子系统协同工作能检测到绝大多数威胁,少数代理失效不会显著降低整个系统的防御能力。某节点检测代理失效只会使得该节点检测不到某类威胁,而该节点依然可以检测到其他类型的威胁。但这种“漏检”很可能引起系统行为偏离预期而被其他类型的检测代理检测到。同样,由于检测代理失效,产生的虚警与其抑制虚警作用相抵消,虚警率变化也很小。同理,代理失效前后误检率变化也小。由定义 1 与定义 2 可知,

$$\frac{PD(\sum_{TIS}^*) - PD(\sum_{TIS})}{PD(\sum_{TIS})} = \frac{\alpha\rho_{MR}(\sum_{TIS}^*) + \beta\rho_{FAR}(\sum_{TIS}^*) - \alpha\rho_{MR}(\sum_{TIS}) - \beta\rho_{FAR}(\sum_{TIS})}{\alpha\rho_{MR}(\sum_{TIS}) + \beta\rho_{FAR}(\sum_{TIS})} \leq \sigma。$$

(7) 适应性

B 淋巴细胞受到初次进入生物体抗原刺激后增生。当亲合力达到阈值后, B 淋巴细胞被克隆扩增, 产生新的 B 淋巴细胞, 而亲合力值小于阈值的 B 淋巴细胞被消除。被克隆扩增的 B 淋巴细胞一部分变为记忆细胞, 另一部分变为浆细胞。初次应答后, 记忆细胞使得自然免疫系统再次遇到相同抗原或相似抗原时能迅速反应, 发生二次应答。自主可控信息系统受克隆选择启发, 能够自动调节 $\sum_{TIS}$ 子系统检测器的“自体”集合。具有更高亲和力的命令序列“自体”、系统调用序列“自体”和设备执行状态序列“自体”在遇到新序列时自动调整“自体”表示。不常用的“自体”表示会被移除。

系统 $\sum_{TIS}$ “自体”表示随时间 T 优化后, Ω_{TIS} 变为 Ω_{TIS}^* 且 $\sum_{TIS}$ 变为 $\sum_{TIS}^*$ 。由定义 3 可知, $PD(\sum_{TIS}^*) < PD(\sum_{TIS})$ 或检测时间 $t^* < t$ 或消耗资源 $r^* < r$ 满足适应性条件。因此, 系统 $\sum_{TIS}$ 具有适应性。

3.4 自主可控信息系统架构

本文基于自然免疫原理提出了包含系统可信基础功能、内部用户行为度量功能、软件行为度量功能和容错功能的多子系统、多代理和多组件的自主可控信息系统架构。

(1) 自主可控信息系统可信基础功能部分

自主可控信息系统可信基础功能部分的全部硬件设备均采用自主设计的可信计算机原理样机, 保证了信息源头的可控和可信, 并采用开源可信网络连接 (TNC) 架构将自主终端可信扩展到网络中, 使可信网络初步具备可信平台身份验证与完整性度量功能。可信基础功能架构为用户行为度量子系统、软件行为度量子系统和容错子系统预留了功能接口, 以便将其结果作为网络接入控制的评判依据。

(2) 内部用户行为度量子系统

可信网络信任链扩展机制只能保证整个系统启动初期接入可信网络的软硬件资源符合预期安全要求。根据“重点防内”的要求, 信息系统启动后, 作为系统操作人员的内部用户行为是否合法可信并不能得到保证。因此, 需要构建用户行为度量子系统度

量内部用户操作是否符合预期, 并将评测结果作为评判依据, 完善可信网络接入控制与授权机制, 以期实现内部用户操作的全生命周期可信接入。

(3) 软件行为度量子系统

信息系统一旦被“震网”“舒特”类攻击成功入侵, 即使内部用户操作命令正确、系统前端显示正常, 系统依然可能按照攻击者的意图执行。因此, 构建软件行为度量子系统, 度量应用程序行为是否符合预期, 并将评测结果作为评判依据用于完善可信网络接入控制与授权机制, 能保证可信平台运行程序的全生命周期可信接入。

(4) 容错子系统

自主可控信息系统的工控设备工作环境特殊, 需要具备抗恶劣环境能力^[9-10]。容错子系统通过添加、对比控制流检测指令和检查设备执行状态的方式增强工控设备应对软错误的“免疫”能力。控制设备程序运行时先检查控制流标签, 待执行完程序的某一阶段后, 将设备反馈执行状态与预先存储的标准执行状态相比较。若控制流标签检测结果或设备执行状态检测结果与预期不一致, 则采取相应的措施; 否则, 继续执行控制设备程序的下一阶段, 以此类推。

自主可控信息系统将可信基础功能与用户行为度量子系统、软件行为度量子系统和容错子系统相结合。在静态度量功能的基础上实现动态度量功能, 使可信网络终端达到全生命周期的访问接入控制。可信终端接入网络前, 可信基础功能部分先对终端身份进行识别, 并对终端平台完整性进行度量。若度量结果满足接入控制系统的安全策略要求, 则允许终端接入网络; 否则, 拒绝该终端接入并对其进行隔离修复。当终端的安全属性达到接入控制系统安全策略要求时, 允许其接入网络; 接入网络后由终端行为收集器收集内部用户行为、软件行为和控制状态, 并与元数据点存储数据度量对比。若用户行为、软件行为和控制状态依然符合安全控制策略, 则继续保持终端平台的接入状态; 否则采取相应的措施。这种架构将终端的可信状态延续到了网络中, 使可信网络具有了动态度量能力。平台全生命周期可信接入的实现提升了整个网络的安全性、可控性及可信性。

可信基础功能架构包括 3 个实体、3 个层次以及若干接口组件, 该架构在传统网络接入层上增加了可信评估层和可信度量层。这里的实体指的是网络中具有对应角色的逻辑实体, 不一定是物理实体。本章架构包括接入请求者 (access requestor,

AR)、策略执行者(policy enforcement point, PEP)和策略决策者(policy decision point, PDP)3个实体。其中,AR负责提交接入认证请求和收集端点设备的各种安全状态信息;PDP依据安全策略对AR提交的平台身份验证、完整性验证和行为动态评测结果等安全状态信息进行判定,并动态调整AR的网络访问权限;PEP接收可信端接入请求信息、可信端安全状态信息并转发给PDP,随后执行PDP的网络访问控制决策。

AR包含网络接入请求者(network access requestor, NAR)、TNC客户端(TNC client, TNCC)、完整性度量收集器(integrity measurement collector, IMC)和平台行为收集器(platform behavior collector, PBC)4个功能组件。

PDP实体包括网络接入授权者(network access authority, NAA)、TNC服务器(TNC server, TNCS)、完整性度量验证器(integrity measurement verifier, IMV)和终端行为检测器(platform behavior verifier, PBV)4个功能组件。

PEP只有策略实施点组件,其主要指能将端点设备接入可信网络的各类接入设备,包括802.1x的自主可信交换机、防火墙、VPN(虚拟专用网)网关等。PEP类设备只包括其本身,而没有按功能分层。

不同实体中的组件依据功能的不同又被分成网络访问层、可信评估层和可信度量层3个抽象层。网络访问层从属于传统的网络互联和安全层,支持传统的网络连接技术,例如VPN和802.1x等;可信评估层进行平台认证、完整性评估和软件行为可信评估;可信度量层收集和校验请求访问者的完整性相关信息和行为相关信息。

架构中实体间的互操作通过接口来实现。完整性度量收集接口IF-IMC是IMC同TNCC之间的接口;完整性度量校验接口IF-IMV是IMV与TNCS之间的接口;TNC客户服务接口IF-TNCCS是TNCC和TNCS之间的接口。厂商定制的IMC-IMV消息接口IF-M是IMC和IMV之间的接口。网络授权传输协议接口IF-T负责AR实体和PDP实体之间的信息传输,在这两个实体中,维护该接口的组件为NAR和NAA。策略执行点接口IF-PEP是PDP和PEP之间的信息传输接口。PDP通过IF-PEP接口指示PEP对AR进行某种程度的隔离以便对AR进行修复,修复完成之后方可授权AR访问网络。

元数据访问端(MAP)负责存储和提供与AR有关的状态信息,例如设备绑定、用户绑定、注册地址绑定、认证状态、终端策略遵从状态、可信终端标准行为库(包括用户命令序列库、系统调用序列库及设备执行状态库)和授权状态等。这些信息可能对策略的制定和执行有用。

MAP客户端(MAPC)负责将与AR有关的状态信息发布给MAP或处置来自MAP的与AR有关的状态信息,MAPC可能不会与AR直接连接。用户行为分析与监控模块负责命令输入数据与MAP中用户命令“自体”模式间的度量评测。软件行为分析与监控模块负责系统调用序列数据与MAP中软件行为“自体”模式间的度量评测。设备执行状态分析与监控模块负责设备执行状态序列与MAP中设备执行状态序列“自体”模式间的度量评测。

可信终端的全程访问接入由平台初始状态、内部用户行为、软件行为和终端执行状态评测结果共同决定。如果终端不符合相关的安全策略,架构为其提供隔离区并进行修补。架构提供的用于修补的实体是配置与修补应用(provisioning & remediation application, PRA)程序和配置与修补资源(provisioning & remediation resource, PRR)。架构提供的平台可信服务接口IF-PTS封装了可信软件栈(trusted software stack, TSS)的相关功能,为AR的各个组件提供密钥存储、非对称加解密、随机数、平台身份和平台完整性报告等功能。完整性度量日志主要用于保存平台组件的度量信息。若终端平台完整性验证没有通过,AR可以通过PRA访问PRR,对相关的组件进行更新和修复直到通过完整性验证。多个安全域可以通过跨域可信网络接入控制组成跨域自主可控信息系统。图1所示为自主可控信息系统基础功能架构。

3.5 自主可控信息系统授权逻辑过程

对自主可控终端进行动态评测的目的是完善其访问接入控制,实现其全生命周期的身份与授权管理。

对内部用户行为的动态可信评测、对软件行为的动态可信评测和对设备执行状态的动态可信评测都是从不同的评测角度将度量机制的粒度细化到行为层面。这3种动态评测相互补充、相互协作,保证了系统运行后的动态可信性。这种基于可信网络基础架构与安全机制的结合实现可信、可控的方式不但符合可信网络的本质,而且实现了终端计算环境中可信度量机制向网络的扩展和静态度量向

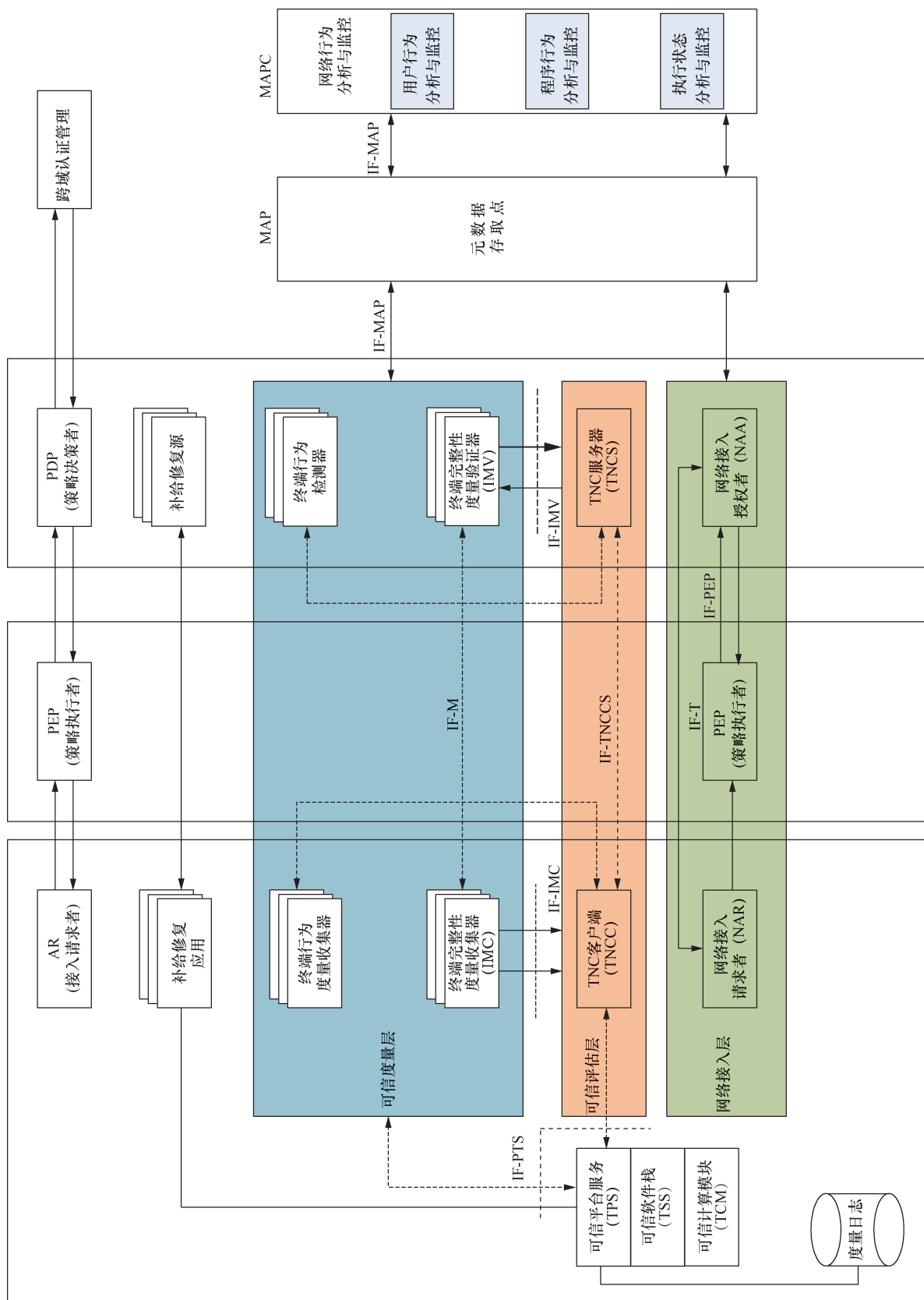


图1 自主可控信息系统基础功能架构

动态度量的扩展,使得信息系统架构在为上层应用提供可信度量和可信报告的同时能将计算机信任设备丰富的安全功能以标准服务接口的形式通过网络提供给策略中心使用。

将可信网络接入控制模型与基于角色的接入控制模型相结合更能适应当前复杂多变的网络环境,控制用户对资源的访问。基于角色的接入控制模型本身不能很好地支持可信信息及属性的动态改变和全生命周期的授权决策。现有可信网络可控性技术仅在终端接入网络前进行授权决策,即授权判断是由终端接入网络的请求驱动,终端一旦接入网络就可以无限制地使用网络资源。倘若终端接入网络后受到破坏,依然可能危及整个网络的安全,所以这种危害隐蔽性更强、危害性更大。

因此,自主可控信息系统需要全新的可信网络接入模型及时、自动地调整受损可信终端的接入权限,确保终端平台全生命周期的可信。这种模型不但要保证终端初次接入网络时的可信,也要保证接入网络后与组织安全策略实时一致的全生命周期的可信。

本文提出的可信网络连接全生命周期接入与授权控制模型将内部用户行为度量结果、软件行为度量结果和设备执行状态度量结果作为系统进行授权判断的重要依据和组成部分。控制模型在终端接入网络前进行授权判断,在终端接入网络后也会根据用户行为动态评测结果、软件行为动态评测结果和设备执行状态评测结果实时地调整网络接入授权,实现可信的全程接入控制。

4 结束语

针对目前可信网络信任链扩展机制的不足,本文基于自然免疫系统原理构建了自主可控信息系统架构。该架构包含可信网络基础功能部分、用户行为度量子系统、软件行为度量子系统和容错子系统,将可信网络接入控制模型与基于角色的接入控制模型相融合。自主可控信息系统通过这种在网络体系架构层面上增加安全机制的方式,解决了可信终端全生命周期可信接入的问题。

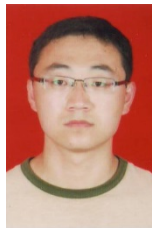
参考文献:

- [1] 慈林林,杨明华,田成平,等.可信网络连接与可信云计算[M].北京:科学出版社,2015.
CI L L, YANG M H, TIAN C P, et al. Trusted network connectivity and trusted cloud computing[M]. Beijing: Science Press, 2015.
- [2] 沈昌祥,张焕国,王怀民,等.可信计算的研究与发展[J].中国科学:信息科学,2010(2):139-166.

SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing[J]. Scientia Sinica Informations, 2010(2): 139-166.

- [3] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学:技术科学,2007,37(2):129-150.
SHEN C X, ZHANG H G, FENG D G, et al. Information security review[J]. Scientia Sinica Technological Sciences, 2007, 37(2): 129-150.
- [4] 郑南宁.人工智能新时代[J].智能科学与技术学报,2019,1(1):1-3.
ZHENG N N. The new era of artificial intelligence[J]. Chinese Journal of Intelligent Science and Technology, 2019, 1(3): 1-3.
- [5] HOFMEYR S A, FORREST S. Architecture for an artificial immune system[J]. Evolutionary Computation, 2000, 8.
- [6] FORREST S, BEAUCHEMIN C, HOFMEYR S. Computer immunology [J]. Immunological Reviews, 2010, 216(1): 176-197.
- [7] KANUPARTHI A K, ZAHRAN M, KARRI R. Architecture support for dynamic integrity checking[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(7): 321-332.
- [8] FERREIRA R S, VARGAS F. ShadowStack: A new approach for secure program execution[J]. Microelectronics Reliability, 2015, 55(9-10): 2077-2081.
- [9] ZHANG X D, CLARK M, RATTAN K, et al. Controller integrity monitoring in adaptive learning systems towards trusted autonomy[J]. IEEE Transactions on Automation Science and Engineering, 2016: 1-11.
- [10] ASOKAN N, MANTYLA J, SERAFAT R. Method and device for verifying the integrity of platform software of an electronic device[P]. 2018.
- [11] GAMBARDALLA M, DORIGO M. Ant colony system hybridized with a new local search for the sequential ordering problem[J]. INFORMS Journal on Comput., 2014, 12(3): 237-255.
- [12] XAYPANYA T, MALINOWSKI R E. Power grid universal detection and countermeasure overlay intelligence ultra latency hypervisor[P]. 2015.

[作者简介]



柳伟(1984-),男,北京理工大学计算机学院计算机应用专业博士生,主要研究方向为可信计算等。



慈林林(1956-),男,教授,博士生导师,主要研究方向为智能计算、人工智能计算、抗恶劣计算、智能信息处理等。



刘利平(1986-),男,北京理工大学计算机学院计算机应用专业博士生,主要研究方向为可信计算等。