



文章编号:1001-9081(2019)07-1991-06

DOI:10.11772/j.issn.1001-9081.2018122475

服务器管理控制系统威胁建模与应用

苏振宇^{1,2*}, 宋桂香², 刘雁鸣², 赵媛²

(1. 高效能服务器和存储技术国家重点实验室(浪潮集团), 济南 250101; 2. 浪潮电子信息产业股份有限公司 安全技术部, 济南 250101)

(*通信作者电子邮箱 suzhy@inspur.com)

摘要:基板管理控制器(BMC)作为大型嵌入式系统负责对服务器进行控制和管理,针对BMC的脆弱性以及面临的安全威胁,提出一种服务器管理控制系统的威胁模型。首先,为了寻找威胁,根据BMC的硬件结构和软件架构建立了数据流图(DFD);其次,采用威胁六要素(STRIKE)方法进行威胁发现,得出全面的威胁列表;然后,为了对威胁进行细化描述,建立了威胁树模型,得出具体的攻击方式并对威胁进行量化;最后,针对STRIDE分类的威胁制定了应对策略,给出了BMC威胁的具体防护方法,满足了机密性、完整性、可用性等安全目标。分析结果表明,所提模型能够全面识别BMC的安全威胁,基于该模型提出的BMC具体防护方法已作为安全基线应用于设计过程中,提升了服务器整体安全性。

关键词:基板管理控制器;威胁建模;数据流图;威胁树;安全威胁

中图分类号: TP309; TP311.522 **文献标志码:**A

Threat modeling and application of server management control system

SU Zhenyu^{1,2*}, SONG Guixiang², LIU Yanming², ZHAO Yuan²

(1. State Key Laboratory of High-end Server and Storage Technology, Inspur Group, Jinan Shandong 250101, China;

2. Security Technology Department, Inspur Electronic Information Industry Company Limited, Jinan Shandong 250101, China)

Abstract: Baseboard Management Controller (BMC) is responsible to the control and management of server as a large embedded system. Concerning the problem of vulnerability and security threats of BMC, a threat model of server management control system was proposed. Firstly, in order to discover threats, a Data Flow Diagram (DFD) was established according to the hardware and software architecture of BMC. Secondly, a comprehensive threat list was obtained by using Spoofing-Tampering-Repudiation-Information disclosure-Denial of service-Elevation of privilege (STRIDE) method. Thirdly, a threat tree model was constructed to describe the threats in detail, and the specific attack modes were obtained and the threats were quantified. Finally, the response strategies were formulated for the threats classified by STRIDE, and the specific protection methods of BMC were obtained, which met the security objectives such as confidentiality, integrity and availability. The analysis results show that the proposed model can fully identify the security threats of BMC, and the protection methods of BMC based on the model have been used in the design process as security baselines, which improves the overall security of server.

Key words: Baseboard Management Controller (BMC); threat modeling; Data Flow Diagram (DFD); threat tree; security threat

0 引言

基板管理控制器(Baseboard Management Controller, BMC)是服务器的管理控制系统,用户通过Web管理界面监视服务器的物理特征,如各部件的温度、电压、风扇工作状态、电源供应以及机箱入侵等。BMC是服务器中相对独立的重要管理控制单元,通常基于进阶精简指令集机器(Advanced RISC Machine, ARM)搭载精简的Linux操作系统,采用Web页面的方式进行带外网络管理。BMC给用户提供便利的同时也面临着各种安全威胁和挑战,因此采用威胁建模可以帮助设计者确定BMC系统中的威胁、攻击、漏洞和对策。

威胁建模是一项工程技术,在系统设计的早期阶段启动并贯穿于整个软件生命周期的迭代过程,目的是帮助设计者

了解所需要保护的资产、如何保护资产、实现的优先级、承担的风险等。在威胁建模过程中,设计者必须始终认为自己就像一个攻击者^[1],假设软件产品的所有输入都是恶意的,而且所有信任边界可以在第一层面,即软件产品之间的首个互动层和最终用户层进行突破。

针对不同的软件应用场景,研究人员已经提出多种软件威胁建模的方法:文献[2]针对Web应用可能存在安全漏洞的模块进行了形式化的分析建模,采用了扩展的有限状态机模型;文献[3]同样针对Web服务面临的安全威胁,提出一种基于威胁六要素(Spoofing-Tampering-Repudiation-Information disclosure-Denial of service-Elevation of privilege, STRIDE)模型的安全评估方法,为用户提供了Web服务安全性的参考评价和防护策略;文献[4]以集成电路(Integrated Circuit, IC)卡互

收稿日期:2018-12-14;修回日期:2019-01-28;录用日期:2019-03-08。

作者简介:苏振宇(1983—),男,山东济南人,高级工程师,硕士,主要研究方向:信息安全、应用密码学;宋桂香(1978—),女,山东郓城人,高级工程师,主要研究方向:信息安全、安全测评;刘雁鸣(1989—),男,山东聊城人,工程师,硕士,主要研究方向:安全测评;赵媛(1988—),女,山东聊城人,工程师,硕士,主要研究方向:信息安全。



联网终端产品为研究对象,提出了以软件安全开发生命周期和威胁树分析的威胁建模过程;文献[5]中提出一种面向对象的威胁建模方法并根据评估结果确定了优先级,制定了缓和方案;文献[6]中提出一种面向嵌入式系统的威胁建模方法,分析了嵌入式系统可能存在的威胁漏洞并以威胁树的形式建立了威胁模型。

以上研究成果对威胁建模有较好的理论指导作用,但也存在一定不足,缺少对复杂系统的威胁建模研究。复杂系统的威胁建模需要考虑硬件、软件等多种威胁因素,因此本文的主要工作是针对服务器中重要的管理控制系统 BMC 进行威胁建模研究,采用 STRIDE 方法和威胁树分析了 BMC 的安全威胁,制定应对方案作为服务器 BMC 系统安全设计的参考依据,以便在实际应用中规避风险并加强对常见漏洞的关注。

1 风险分析

1.1 攻击趋势

服务器的安全分为物理安全和系统安全:物理安全是基础,系统安全是保障。当前对服务器的攻击逐渐由上层软件攻击趋向对底层硬件和固件的攻击,这是由于固件代码在特权的位置进行操作,固件一旦被破坏,经历很长的时间也不容易被检测出,因此,仅仅通过采取防火墙级别或服务器软件和操作系统层面对网络进行保护的方法不足以应对安全威胁。随着互联网应用的普及,越来越多的企业把关注的重点放在服务器外围乃至数据中心网络的安全防护方面,而忽视了对服务器硬件和固件的安全防护。当斯诺登曝光美国国家安全局(National Security Agency, NSA)内部的“产品目录”(软硬件攻击工具)以及方程式(Equation Group)等犯罪组织利用恶意间谍软件频繁发动网络攻击事件之后,服务器的硬件和固件安全问题才得到了高度的重视,为此,2017年5月美国发布了平台固件抗性指南 SP800-193^[7],用于指导服务器固件的安全合规性;2017年6月我国施行《网络安全法》后,业界对服务器产品安全性的关注和要求也越来越高了。

1.2 BMC 系统结构

目前主流两路以上的服务器都具有 BMC。BMC 与主处理器和主板上各元件相连接,监测主板上的温度传感器、CPU 状态、风扇速度和电压传感器等,提供重新引导服务器的远程电源控制功能,并且提供对基本输入输出系统(Basic Input and Output System, BIOS)配置和操作系统控制台信息的远程访问。BMC 可以和主系统共享网络接口采用带内管理方式,或者单独集成专有的网口采用带外管理方式。

BMC 通常独立于服务器 CPU 和操作系统,接通主板电源就处于加电状态,因此无论用户在开机还是关机的状态下都可以对服务器的运行状况进行监控。BMC 芯片与主板硬件单元的连接如图 1 所示。BMC 以高性能的 ARM 芯片为控制核心,通常采用 AST2300/2400/2500^[8]系列的芯片,BMC 芯片与南桥、同步动态随机存储器(Synchronous Dynamic Random Access Memory, SDRAM)、串行外设接口(Serial Peripheral Interface, SPI)的 Flash 存储器等硬件模块连接,实现服务器平台的多种管理功能,如虚拟存储功能、通用串行总线(Universal Serial Bus, USB)虚拟介质、Web 管理界面、监控传感器功能、用户管理功能等。BMC 一旦发现系统中的单元出现异常,立即采取记录事件、报警、自动关机或重启动等措施。

BMC 的软件功能主要提供服务器故障诊断、远程控制、远程配置部署、远程固件更新、系统信息监测等功能;对外提供完备的协议或服务,如智能平台管理接口(Intelligent

Platform Management Interface, IPMI)、简单网络管理协议(Simple Network Management Protocol, SNMP)、Web 界面、syslog 日志模块、安全外壳协议(Secure SHell, SSH)、远程登录服务 Telnet、系统虚拟化模块(Kernel-based Virtual Machine, KVM)等。

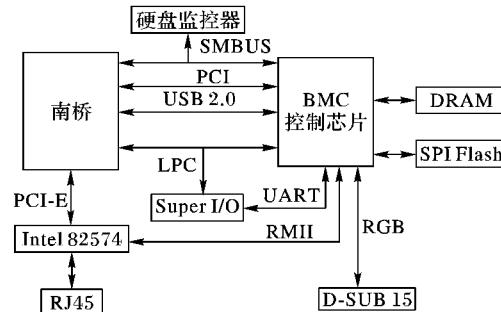


图 1 BMC 硬件结构
Fig. 1 BMC hardware architecture

其中 IPMI 是运行于 BMC 上的服务器管理协议^[9],目的是使服务器管理工具和不同厂商生产的 BMC 之间的通信标准化。IPMI 的主要特征是日志记录及恢复控制功能均独立于主处理器、BIOS 和操作系统。用户可以利用 IPMI 监视服务器的温度、电压、电扇工作状态、电源供应以及机箱入侵等,为系统管理、恢复以及资产管理提供信息。

1.3 BMC 风险要素

物理服务器涉及到的安全问题有一半以上出自 BMC,所以 BMC 的安全对服务器安全的重要性不言而喻。一旦利用 BMC 漏洞发起攻击,入侵者可以获得 BMC 访问权,入侵服务器获得服务器的控制权,进而从存储器中复制数据,对操作系统作修改,安装永久的后门,获取服务器的证书,加载拒绝服务攻击,或者清除硬件驱动等,最终导致服务器的业务直接中断或瘫痪。有些厂商的服务器存在 BMC 不经过鉴权访问的风险;而有些厂商服务器的 BMC 则存在安全漏洞,入侵者可模仿合法用户,查看用户记录及执行事务。工信部曾发现美国某芯片厂家的 BMC 管理芯片存在安全漏洞,会窃取用户数据向外发送,并且无法关掉或屏蔽。

BMC 面临的安全威胁比较多,主要如下。

1) 协议安全问题。超文本传输协议(Hyper Text Transfer Protocol, HTTP)、IPMI、SNMP、Telnet 等协议的脆弱性,例如 IPMI 允许零密码和匿名登录、HTTP 数据明文传送、SNMP V2.0 通信不加密、Telnet 缺少口令保护和强力认证等。

2) Web 应用程序安全问题。存在跨站脚本攻击、安全配置错误、敏感信息泄露、跨站请求伪造(Cross Site Request Forgery, CSRF)等风险。

3) ARM Linux 操作系统安全问题。存在弱口令、端口入侵、病毒木马入侵^[10]、网络窃听等风险。

2 威胁建模流程

2.1 安全目标

在威胁建模之前首先应确定安全目标,这是 BMC 系统威胁建模最重要的步骤,只有明确了 BMC 中需要保护的对象,即非法攻击者攻击的对象,才能够有助于理解潜在攻击者的目标,并将注意力集中于那些需要密切留意的应用程序区域。安全目标通常涉及数据及应用程序的机密性、完整性、不可否认性、身份验证、授权等,具体如下。

1) 机密性。防止未经授权的信息泄露。在 BMC 应用的带外管理环境中,维护信息的机密性是 BMC 应用的重要保



障。

2)完整性。防止信息未经授权的更改,保证信息不被偶然或故意地破坏。

3)不可否认性。保证信息的发送者不能抵赖或否认对信息的发送。

4)身份验证。提供身份证明的实体才能访问 BMC 的应用和数据,否则不能访问 BMC 资源。

5)授权。根据访问权限授予主体访问 BMC 服务资源的许可,保证发送方被授权发送消息。

只有满足了以上五方面的安全要求,BMC 才能投入应用,安全才会得到保障。

2.2 模型的选择和定义

常见的威胁模型有资产模型、攻击者模型和软件模型。

1)资产模型。先确认软件的所有资产,然后分析攻击者怎样攻击,以及怎样应对每个威胁,资产到威胁没有直接关系。

2)攻击者模型。先确认软件的攻击者可能有哪些,然后分析对应攻击者的攻击方法以及怎样应对攻击。

3)软件模型。先分析软件是如何组装在一起的,然后分析组成软件的各模块可能存在的安全威胁以及应对方法。该模型相对而言是最好用的,因为建立清晰的软件模型有助于寻找威胁,应避免陷入到软件功能正确与否的细节中。图表是软件建模的最佳方法,其中数据流图(Data Flow Diagram, DFD)通常是威胁建模最理想的模型,在讨论威胁时可进行图表的完善。

结合以上分析,在威胁发现阶段为了全面寻找威胁,采用了 DFD 模型结合 STRIDE 方法来识别威胁。在威胁量化阶段,采用了威胁树模型,对威胁进行细化和对具体攻击方式进行量化。

定义 1 DFD 模型。 DFD 描述为一个五元组〈外部实体、过程、存储、数据流、信任边界〉,其中:

外部实体 系统应用外部不受控制的元素,与系统有交互或被系统调用。

过程 系统内部管理数据的任务,通常会基于数据处理或执行一个任务。

存储 表示存储但没有修改数据的地方。

数据流 表示系统中数据的移动方向。

信任边界 出现在一个组件不信任边界另一侧的组件时。

定义 2 威胁树模型(TM)。 TM 是由一个或多个节点构成的威胁树, $TM = (N, A, L)$,其中:

N 是非空有限 AND/OR 节点的集合,AND 是指构成父节点的子节点之间是“逻辑与”关系,只有实现所有子节点时才能实现父节点;同理,OR 代表“逻辑或”,当实现任一子节点时就能实现父节点。

A 是属性集合,包括攻击成本 Co 、攻击成功概率 P 和攻击危害程度 Da 。各属性之间的关系为: $Da = P/Co$, $Co \in [0, 100]$, $P \in [0, 1]$ 。

L 是攻击路径, $L = \{\langle N_1, N_2, \dots, N_k \rangle \mid N_1, N_2, \dots, N_k \in \text{叶节点}\}$ 。一条攻击路径 $\langle N_1, N_2, \dots, N_k \rangle$ 是 TM 的一个最小割集,即实现威胁树根节点所需的相关叶节点构成的集合。

根据对威胁建模的形式化描述,以 BMC 用户手册、软件架构文档等作为建模的输入,设计工具采用了微软威胁建模软件 Threat Modeling Tool 2016^[11],具体建模流程为:

1)根据 BMC 系统结构,利用 Threat Modeling Tool 绘制系

统的主体数据流图,并根据实际情况进行参数配置;

2)针对各个功能模块,考虑是否存在特有的数据流,对数据流图进行完善;

3)用建模软件生成威胁点并逐条分析,得到初步的系统威胁列表;

4)进行思维发散,考虑各主体的威胁点是否有遗漏,并补充威胁列表;

5)使用威胁树对数据流图中各主体再进行逐个分析,进行威胁量化;

6)分析列表中各条威胁对应的解决方案,识别安全需求和非需求。

3 绘制数据流图

对 BMC 功能及使用方法的理解有助于有针对性地确定威胁可能发生的位置,因此为了识别 BMC 的威胁,需要对系统进行分解应用,基于 BMC 的物理部署特性、应用程序、子系统的组成和结构等,采用体系结构图表的表达方式,即绘制数据流图,以便将威胁定位于某一特定区域,为后续识别对应威胁的解决方案打下基础。

在绘制数据流程时,需要根据 BMC 的结构以便确定信任边界、数据流、数据入口点和数据出口点。确定信任边界主要用于注明在 BMC 设计过程中需要特别关注的区域,而且必须能够确保相应的安全措施可以将所有入口点保护在特定的信任边界内,并确保入口点可以充分验证通过信任边界的所有数据的有效性。确定数据流是指从入口到出口跟踪 BMC 应用模块的数据输入输出,这样做可以更全面地找出尽可能多的威胁。入口点和出口点都是应用程序遭攻击的地方,是在进行威胁建模时需要重点考虑的。

绘制数据流图过程中,参考了 BMC 用户手册、软件架构文档等,作为威胁建模的输入。数据流图分为外部实体、过程(加工)、数据流和数据存储等 4 个元素,根据 BMC 硬件结构及软件架构,利用微软威胁建模工具 Threat Modeling Tool 2016 绘制了数据流图,如图 2 所示。表 1 是对数据流图各元素的分解。

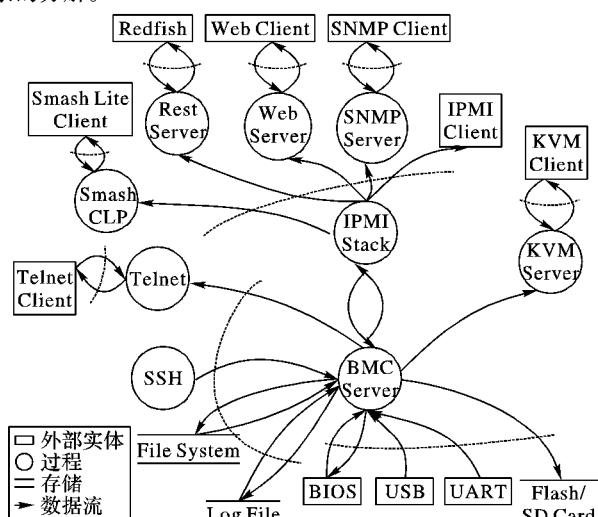


图 2 威胁模型

Fig. 2 Threat model

图 2 中:外部实体用矩形框表示,例如 Web 客户端(Web Client)、IPMI 客户端(IPMI Client)等。

过程用圆形表示,例如 BMC 服务(BMC Server)、Web 服



务 (Web Server)、IPMI 协议栈 (IPMI Stack) 等。

存储用平行线表示, 例如文件系统 (File System)、日志 (Log File) 和 Flash/SD 卡存储区。

数据流用带箭头的线表示, 箭头表示移动的方向, 例如客户端 Web 请求 (Web Client-Web Server)、Web 应答 (Web Server-Web Client) 等。

信任边界通常存在于不同隐私级别的元素之间 (例如 Web Server 与 Web Client 之间), 或存在于在一样的隐私级别之间运行的不同组件之间 (例如 BMC Server 与 Telnet 之间)。信任边界的确定需要考虑系统里的所有要素是否具有相同级别的权限, 并且每个要素是否可以访问系统里的所有其他要素。

表 1 BMC 数据流图元素

Tab. 1 Elements of BMC data flow diagram

DFD 元素	数据流图内容
外部实体	Web Client, SNMP Client, Redfish, Smash Lite Client, IPMI Client, KVM Client, Telnet Client, BIOS, USB, UART
过程	BMC Server, IPMI Stack, Web Server, SNMP Server, Rest Server, Smash CLP, KVM Server, Telnet, SSH
存储	File System, Log File, Flash/SD Card
数据流	用于连接外部实体-过程-过程-过程-存储之间的所有箭形线

在利用 Threat Modeling Tool 绘图的过程中, 需要对每个元素进行参数配置, 例如 Web Server 是否采用了 HTTPS、数据存储是否加密等, 此时需要结合 BMC 系统的实际情况进行配置, 对于不能确定的配置选项保持默认设置即可。

4 威胁分析

4.1 确定威胁

完成 BMC 威胁模型的数据流图后, 需要确定可能影响应用程序和危及安全目标的威胁和攻击, 采用了 STRIDE 方法进行威胁发现。STRIDE 是一种启发式的方法, 目的是帮助寻找威胁。STRIDE 是由假冒 (Spoofing)、篡改 (Tampering)、否认 (Repudiation)、信息泄露 (Information disclosure)、拒绝服务 (Denial of Service) 和提升权限 (Elevation of privilege) 的英文词首字母构成^[12]。Threat Modeling Tool 即采用 STRIDE 方法进行威胁发现。

当检测数据流图无错误后, 运行 Threat Modeling Tool 自动分析功能后会按照数据流图的各元素自动生成 BMC 的初始威胁报告, 报告中对每个标识出的威胁进行了描述, 并且标注了对应 STRIDE 威胁中的分类。

需要说明的是, 通过工具生成的初始威胁列表是比较复杂的, 而且其中有的数据流威胁是不需要关注的, 例如 Telnet 服务不需要关注 Telnet 到 BMC Server 的过程, 由于攻击不到 LPC (Low Pin Count) 总线协议所以不需要关注 BMC 与 BIOS 之间的请求-应答过程, 因此需要结合 BMC 的实际对数据流图中的各主体再进行逐个分析以便完善威胁列表。最后需要进行发散思维, 检查各主体的威胁点是否有遗漏, 可以利用头脑风暴分析方法, 补充那些工具没有识别出来, 但 BMC 实际存在的威胁, 例如 USB 存在 BadUSB 攻击、BMC 串口未采取访问控制机制等。

经过分析、筛选、补充之后得到完善的 BMC 威胁列表如表 2 所示。表中按照 BMC 数据流图中的各元素进行分类, 列出了每个模块有哪些安全威胁, 以及每条威胁对应的 STRIDE 分类, 由此得到了适用于 BMC 系统的威胁类型。

4.2 威胁量化

在威胁量化阶段, 从攻击者的角度进行 BMC 威胁分析, 归纳起来大致分为两类:

- 1) 对数据的攻击, 例如窃听、篡改、重复攻击等;
- 2) 对系统的攻击, 例如未授权访问、授权违例、拒绝服务等。

表 2 威胁列表

Tab. 2 Threat list

BMC 模块	对应数据流图元素	威胁描述及对应的 STRIDE 分类
File System	写文件 读文件	数据篡改 (T) 越权访问 (E); 敏感信息泄露 (I)
Log File	写日志 读日志	存储空间不足 (D) 未授权访问 (E); 敏感数据泄露 (I)
Web	Web Client 请求 Web Server	未授权访问 (E); CSRF 攻击 (T); 远程执行代码 (E) 否认接收数据 (R); 拒绝服务攻击 (D)
	Web Server 应答	篡改客户端浏览器 (T); 数据发送到攻击者目标 (S)
SNMP	SNMP Client 请求 SNMP Server SNMP Server 应答	欺骗 (S); 篡改数据 (T); 远程执行 SNMP Server 端代码 (E) 拒绝服务、或被中断数据传输异常 (D) 数据发送到攻击者目标 (S);
SmashCLP	Smash Lite Client SmashCLP SmashCLP 应答	信息泄露 (S); 篡改数据、特权攻击 (T); 远程执行代码 (E) 拒绝服务、或被中断数据传输异常 (D) 数据发送到攻击者目标 (S);
KVM	KVM Client 请求 KVM Server KVM Server 应答	未授权访问 (E); 篡改数据 (T) 拒绝服务、或被中断数据传输异常 (D) 否认接收数据 (R); 数据发送到攻击者目标 (S)
IPMI	IPMI Client 请求 IPMI 应答	未授权访问 (E); 篡改数据 (T) 数据发送到攻击者目标 (S)
Telnet	Telnet 请求 Telnet 服务 Telnet 应答	被攻击者欺骗 (S); 篡改数据 (T); 数据嗅探 (I) 捕获、重放没有序列号或时间戳的分组或消息 (T) 数据发送到攻击者目标 (S)
SSH	SSH 请求	对 BMC 未授权访问 (S)
Flash/SD card	写 Flash/SD 卡	数据篡改 (S)
USB	USB 请求	BadUSB 攻击 (S)
UART	串口请求	未授权访问 (E)

利用威胁树进行威胁的分级细化。威胁树是通过树形结构描述系统存在的各种攻击, 用根节点表示给定系统所面临威胁的抽象描述, 逐层细化威胁, 直到用叶节点表示具体攻击方式。

构建的 BMC 的威胁树如图 3 所示, 根节点 A 代表攻击 BMC, 进一步分解为下一级节点 A1 (服务攻击)、A2 (协议攻击) 和 A3 (硬件攻击); A1 ~ A3 之间的“OR”代表并列的关系, 即单独实施某一类攻击就可以实现对 BMC 的攻击。之后对 A1 ~ A3 分别进行逐层分解, 直到细化为叶节点, 即能够实施的具体攻击手段, 如表 3 所示。例如, 服务攻击 (A1) 中的 Web 攻击 (A11), 分解为暴力破解口令 (A111)、跨站请求伪造攻击 (A112) 和拒绝服务攻击 (A113) 三种具体攻击方式, 该三个叶节点直接也为“OR”关系。

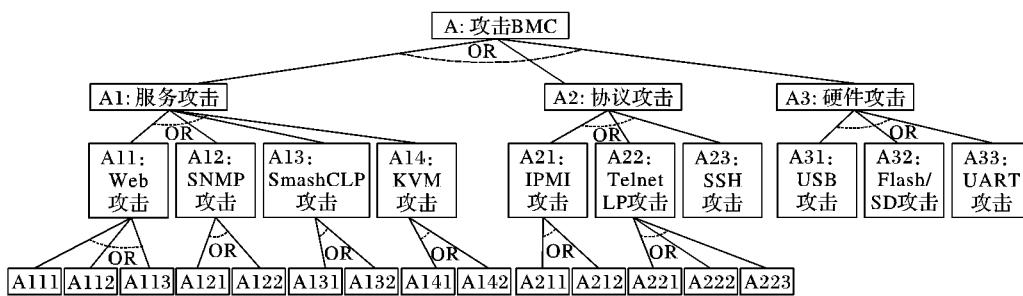


图3 BMC 威胁树

Fig. 3 BMC threat tree

为了评估对 BMC 不同攻击方法的成本效益差异,需要对各叶节点进行威胁量化,确定各个攻击方式的优先级,从而有针对性地制定应对措施或缓解方案,为此根据威胁量化公式: $Da = P/Co$,为叶节点威胁量化地评估属性。 Da 反映了从攻击者的角度进行成本效益评估的结果,其值越大,成本效益越高,反之越低。量化标准取决于安全专家的实际经验、安全事件的统计信息及主观期望等方面^[13]。表3中对每个叶节点进行了威胁量化,列出了 Co 、 P 值,计算得出了对应的 Da 值。

表3 威胁量化
Tab. 3 Threat quantification

叶节点	攻击描述	Co	P	Da
A111	暴力破解口令,权限提升	20	0.1	0.0050
A112	跨站请求伪造攻击	30	0.5	0.0170
A113	拒绝服务攻击	40	0.2	0.0050
A121	未授权访问攻击	20	0.1	0.0050
A122	篡改数据	80	0.2	0.0025
A131	未授权访问攻击	20	0.1	0.0050
A132	特权攻击	80	0.3	0.0038
A141	拒绝服务攻击	40	0.2	0.0050
A142	监听、信息泄露	90	0.1	0.0011
A211	暴力破解口令,权限提升	20	0.1	0.0050
A212	篡改、信息泄露	70	0.2	0.0029
A221	未授权访问	20	0.1	0.0050
A222	数据篡改	80	0.2	0.0025
A223	嗅探、重放攻击	100	0.4	0.0040
A23	SSH 未授权访问	20	0.1	0.0050
A31	Flash/SD 数据篡改	70	0.8	0.0114
A32	BadUSB 攻击	80	0.7	0.0088
A33	UART 未授权访问	20	0.9	0.0450

4.3 威胁应对

针对由 STRIDE 方法得到的威胁,具体应对策略如下。

- 1) 假冒(S)。采取建立用户身份,并对身份验证的策略。
- 2) 篡改(T)。采取数据完整性检测的策略,通常使用杂凑密码算法实现。
- 3) 否认(R)。采取数字签名的策略,通过非对称算法保证通信双方的不可抵赖性。
- 4) 信息泄露(I)。采用对称加密的策略,使未授权的对象不能获取有效信息。
- 5) 拒绝服务(D)。采用设置异常处理机制的策略,使系统在需要时执行正常操作,满足可用性。
- 6) 提升权限(E)。采用授权和访问控制的策略,授权是授予主体访问客体的许可,访问控制是限制主体对客体进行访问的范围。

根据威胁量化阶段的分析,针对威胁的具体分类,制定了

威胁的具体防护和应对方法,如表4 所示。

表4 威胁防护方法
Tab. 4 Threat protection methods

威胁类别	威胁细分	防护方法
Web 服务威胁	Web 跨站请求伪造攻击	对客户端含有敏感信息的 Form 表单提供令牌、验证码等不可预测的随机信息
Web 服务威胁	Web 客户端暴力破解口令,权限提升	对每一个需要授权访问的页面核实用户的会话标识是否合法,防止统一资源定位地址(Uniform Resource Locator, URL)越权
Web 服务威胁	Web 服务端拒绝服务攻击	设置 Web 会话超时机制,并且在超时后及时清除会话信息,减少会话劫持
SNMP 服务威胁	SNMP 客户端未授权访问攻击	对用户的输入在服务端进行最终校验,一旦发现数据不合法禁止访问
SmashCLP 服务威胁	SmashCLP 客户端篡改数据	使用杂凑算法对传输的数据进行加密,保证数据的完整性
KVM 服务威胁	SmashCLP 客户端未授权访问	实现用户的权限分立,且仅授予所需的小权限
KVM 服务威胁	SmashCLP 客户端特权攻击	使用对称算法加密传输数据
KVM 服务威胁	KVM 服务端拒绝服务攻击	KVM 服务端加入异常处理机制,并进行输入验证
KVM 服务威胁	KVM 监听、信息泄露	对客户端进行输入验证,校验内容包括输入类型和数据长度
IPMI 协议威胁	IPMI 客户端篡改、信息泄露	使用加密通道 HTTPS 传输数据
IPMI 协议威胁	IPMI 客户端口令破解,权限提升	设置口令的长度和复杂度要求,禁止使用弱口令
Telnet 协议威胁	Telnet 请求未授权访问	Telnet 协议请求过程进行强制访问控制
Telnet 协议威胁	Telnet 协议嗅探、重放攻击	增加序列号、实现强完整性验证
Telnet 协议威胁	Telnet 客户端数据篡改	使用加密通道 HTTPS 传输数据
SSH 协议威胁	SSH 请求未授权访问	SSH 协议请求过程加入访问控制机制
硬件威胁	Flash/SD 数据篡改	对 BMC 的二进制镜像文件添加数字签名,在固件更新时需校验签名值
硬件威胁	USB BadUSB 攻击	禁用 USB-HID 协议
硬件威胁	UART 未授权访问	增加用户名/口令的身份验证机制,验证通过后允许操作 UART 口

最后,为了加强对 BMC 最常出现漏洞的关注,需要识别安全需求和非需求,作为设计阶段的依据和参考。安全需求即各类威胁对应的安全属性,即威胁的具体防护方法、威胁应



对或设计阶段的注意事项,表 4 中的 BMC 威胁防护方法都可以作为安全需求。非需求为软件产品内部不会处理的安全隐患,无法通过软件内部实现来规避威胁,此种威胁可通过操作指南、警告和提示等进行说明。例如对于 BMC 的 Telnet 等存在安全缺陷的协议,通过在用户手册中建议用户进行安全参数配置、默认关闭协议等方式来规避威胁。

通过 BMC 威胁建模,将识别出的威胁应对方案转化为设计阶段的安全需求和非需求,从而满足了威胁建模的安全目标,安全目标对应的安全措施主要有:

1) 机密性。对于 BMC 的 Web 应用环境,利用高级加密标准(Advanced Encryption Standard, AES)^[14]对 Web 服务的请求和响应进行加密,保证数据的机密性。

2) 完整性。对于 BMC 的固件二进制镜像文件,利用 256 位安全散列算法(Secure Hash Algorithm, SHA-256)^[15]进行完整性校验。

3) 不可否认性。在 BMC Web 服务环境中,对于传输的可扩展标记语言(eXtensible Markup Language, XML)消息,利用数字签名算法 RSA(Rivest-Shamir-Adleman)^[16]对 XML 进行签名操作保证发送行为的不可否认性。

4) 身份验证。对于 BMC 可以使用多种不同的身份验证方式,例如通过用户名/口令、指纹/声音、基于令牌的身份验证等方式。

5) 授权。使用授权策略以限制访问不同的资源集合,包括文件、Web 页面、应用程序接口、日志等。

5 结语

为了提升服务器的安全可靠性,需要在系统开发设计阶段的早期考虑安全问题。本文针对 BMC 面临的攻击趋势和安全威胁,提出了针对大型嵌入式系统的威胁模型,根据从模型得到的威胁制定了应对策略和具体防护方法,作为设计阶段的输入,在设计阶段就考虑安全风险,防患于未然,从而提升服务器的安全性。由于威胁建模不可能一次识别系统所有可能的威胁,而且应用程序需要不断增强其功能并作出调整以适应不断变化的外部需求等诸多原因,因此建模过程不是一次性的过程,需要结合实践不断总结完善,包括对模型的完善以及对威胁的分析等,因此威胁建模是不断反复和迭代的过程。后续研究方向是在 BMC 的设计、编码等开发阶段中实现具体的威胁防护方法,并且在测试阶段引入安全性测试,根据测试出的安全漏洞进一步调整和优化威胁模型。

参考文献 (References)

- [1] JAMES R, ANMOL M. 软件安全: 从源头开始 [M]. 丁丽萍, 卢国庆, 李彦峰, 等译. 北京: 机械工业出版社, 2016: 48–50. (JAMES R, ANMOL M. Core Software Security: Security at the Source [M]. DING L P, LU G Q, LI Y F, et al, translated. Beijing: China Machine Press, 2016: 48–50.)
- [2] 李栋. 基于扩展 FSM 的 Web 应用安全测试研究 [J]. 计算机应用与软件, 2018, 35(2): 30–35. (LI D. Research on Web application security testing based on extended FSM [J]. Computer Applications and Software, 2018, 35(2): 30–35.)
- [3] 姜莉. 一种基于 STRIDE 模型的 Web 服务安全评估方法研究 [D]. 长沙: 湖南大学, 2010: 28–35. (JIANG L. Research on a security evaluation method based on STRIDE model for Web service [D]. Changsha: Hunan University, 2010: 28–35.)
- [4] 王宇航, 高金萍, 石竑松, 等. 基于威胁建模的 IC 卡互联网终端安全问题定义方法 [J]. 北京理工大学学报, 2017, 37(12): 1259–1264. (WANG Y H, GAO J P, SHI H S, et al. A method of the security problem definition on the IC card international terminal based on the threat modeling [J]. Transactions of Beijing Institute of Technology, 2017, 37(12): 1259–1264.)
- [5] 何可, 李晓红, 冯志勇. 面向对象的威胁建模方法 [J]. 计算机工程, 2011, 37(4): 21–26. (HE K, LI X H, FENG Z Y. Approach to object oriented threat modeling [J]. Computer Engineering, 2011, 37(4): 21–26.)
- [6] 徐超, 何炎祥, 陈勇, 等. 面向嵌入式系统的威胁建模与风险评估 [J]. 计算机应用研究, 2012, 29(3): 826–828. (XU C, HE Y X, CHEN Y, et al. Embedded system oriented threat modeling and risk evaluation [J]. Application Research of Computers, 2012, 29(3): 826–828.)
- [7] ANDREW R. NIST special publication 800-193: platform firmware resiliency guidelines [EB/OL]. (2018-05-22) [2018-12-13]. <https://doi.org/10.6028/NIST.SP.800-193>.
- [8] ASPEED Technology Inc. AST2500/AST2520 integrated remote management processor A2 datasheet [EB/OL]. (2017-05-12) [2018-12-13]. <http://www.ASPEEDtech.com>.
- [9] Intel Corporation, Hewlett-Packard Company, NEC Corporation, et al. Intelligent platform management interface specification V2. 0 [EB/OL]. (2015-04-21) [2018-12-13]. <https://www.intel.de/content/www/de/de/servers/ipmi/ipmi-intelligent-platform-mgt-interface-spec-2nd-gen-v2-0-spec-update.html>.
- [10] 刘煜堃, 诸葛建伟, 吴一雄. 新型工业控制系统勒索蠕虫威胁与防御 [J]. 计算机应用, 2018, 38(6): 1608–1613. (LIU Y K, ZHUGE J W, WU Y X. Threat and defense of new ransomware worm in industrial control system [J]. Journal of Computer Applications, 2018, 38(6): 1608–1613.)
- [11] Microsoft Trustworthy Computing. Microsoft threat modeling tool 2016 getting started guide [EB/OL]. [2018-12-13]. <http://microsoft.com/security/sdl>.
- [12] SHOSTACK A. 威胁建模: 设计和交付更安全的软件 [M]. 姜常青, 班晓芳, 梁杰, 等译. 北京: 机械工业出版社, 2015: 45–47. (SHOSTACK A. Threat Modeling: Designing for Security [M]. JIANG C Q, BAN X F, LIANG L, et al, translated. Beijing: China Machine Press, 2015: 45–47.)
- [13] 杨洋, 姚淑珍. 一种基于威胁分析的信息安全风险评估方法 [J]. 计算机工程与应用, 2009, 45(3): 94–96. (YANG Y, YAO S Z. Risk assessment method of information security based on threat analysis [J]. Computer Engineering and Applications, 2009, 45(3): 94–96.)
- [14] National Institute of Standards and Technology. FIPS PUB 197: announcing the Advanced Encryption Standard (AES) [S/OL]. (2001-11-26) [2018-12-13]. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>.
- [15] National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS) [S/OL]. (2015-08-10) [2018-12-13]. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.
- [16] National Institute of Standards and Technology. FIPS PUB 186-3: Digital Signature Standard (DSS) [S/OL]. (2009-06-11) [2018-12-13]. https://csrc.nist.gov/CSRC/media/Publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf.

SU Zhenyu, born in 1983, M. S., senior engineer. His research interests include information security, applied cryptography.

SONG Guixiang, born in 1978, senior engineer. Her research interests include information security, security testing and evaluation.

LIU Yanming, born in 1989, M. S., engineer. His research interests include security testing and evaluation.

ZHAO Yuan, born in 1988, M. S., engineer. Her research interests include information security.