基于 SPARTA 框架的 HAS4 决赛攻击路径分析

雷思磊，荆美倩，龙　森
（酒泉卫星发射中心，甘肃　酒泉　732750）

摘　要：太空网络面临的安全威胁越来越多，美国自 2020 年起，连续四年举办黑掉卫星（Hack-A-Sat，HAS）挑战赛，并发射真实卫星“月光者”用于 HAS 比赛。太空攻击研究与战术分析框架 SPARTA 是针对太空网络安全的对抗战术和技术知识库。借助 SPARTA 框架，详细分析了第四届 HAS 决赛中攻击使用的战术技术，对于深入理解 SPARTA 框架、太空网络安全具有一定借鉴意义。

关键词：Hack-A-Sat（HAS）；SPARTA；太空安全
中图分类号：TP309；TN915.08　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.04.003
引用格式：雷思磊，荆美倩，龙森. 基于 SPARTA 框架的 HAS4 决赛攻击路径分析［J］. 网络安全与数据治理，2024，43(4)：19-23.

Analysis of attack path in HAS4 finals based on SPARTA framework

Lei Silei，Jing Meiqian，Long Sen
（Jiuquan Satellite Launch Center，Jiuquan 732750，China）

Abstract：Security threats to the space network are increasing. Since 2020，the United States has held the Hack-A-Sat Satellite Hack Challenge for four consecutive years，and launched the real satellite "Moonlighter" for the HAS competition. SPARTA，a framework for the analysis of space attack research and tactics，is a knowledge base of adversarial tactics and techniques for space cybersecurity. With the help of the SPARTA framework，the tactical techniques used in the attack in the 4th HAS finals are analyzed in detail，which has certain reference significance for in-depth understanding of the SPARTA framework and space network security.

Key words：Hack-A-Sat（HAS）；SPARTA；space security

0　引言

网络攻击技术的不断演进对网络安全防护能力的要求与日俱增，现有的安全评价和监测方法对安全保护水平的要求无法覆盖网络攻击技术手段和方法的发展变革[1]。2013 年，MITRE 组织为了摆脱网络安全治理中防御方所面临的困境，参考现实中发生的真实网络安全攻击事件，创建了对抗性攻击战术、技术、知识库框架（Adversarial Tactics，Techniques，and Common Knowledge ATT&CK）。该框架随着新技术、新应用、攻击行为等的发展而不断丰富，内容强大、实战性好，逐渐得到业界的广泛认可，成为网络安全领域了解攻击行为、方法以及相应应对措施的主要工具。

随着太空技术在经济、政治、军事等诸多领域的影响力不断增大，太空安全的重要性日益显现，而在网络化时代，太空安全必然与网络安全紧密联系在一起。针对太空网络安全的独特性，2022 年 10 月 19 日，美国 Aerospace 公司发布了太空攻击研究与战术分析框架 SPARTA（Space Attack Research & Tactic Analysis）。SPARTA 也是采用类似 ATT&CK 的矩阵表示法，基础元素同样也是战术、技术和程序（Tactics，Techniques and Procedures，TTPs），其中，战术是攻击者想要实现的目标；技术或子技术是攻击者可以采用的攻击方式以及目标实现路径；程序是攻击者可以使用的技术、子技术[2]。本文基于 SPARTA 框架分析了 HAS4（即第四届黑掉卫星挑战赛）决赛的攻击路径，证明了 SPARTA 框架的适用性、覆盖性。

1　SPARTA 框架介绍

SPARTA 框架最新版本是 v1.5.1，发布于 2023 年 11 月 9 日，涵盖了 9 种战术，83 种技术，129 种子技术。9 种战术分别为侦察、资源开发、初始访问、执行、持久化、规避防御、横向运动、信息泄露和危害，每种战术主要作用如下，涉及的技术如图 1 所示[3]。

注：战术括号中的数字表示该战术下有多少种技术，技术括号中的数字表示该技术下有多少种子技术。

图 1　SPARTA 框架战术及其技术

（1）侦察：主要是收集航天器、飞行软件、发射、供应链等相关信息，为下一步攻击行为做好准备。

（2）资源开发：主要是攻击者为后续攻击行动，构建、破坏相关基础设施，获取网络、非网络能力，并进行相关部署。

（3）初始访问：攻击者试图与目标航天器建立通信、访问、指令执行的渠道，可以的渠道包括供应链、通信链路、交会对接、地面实体、外围设备等。

（4）执行：攻击者试图对目标航天器展开攻击行为，包括利用执行恶意代码、破坏地理围栏、操控内部代码、干扰、欺骗、修改参数、侧信道攻击、动能物理攻击等手段。

（5）持久化：攻击者试图修改、欺骗目标航天器上的访问控制机制，以获得合法、持续非授权控制，包括利用后门、替换加密密钥等方式。

（6）规避防御：攻击者尽量避免被目标航天器的安全防御系统检测到，包括利用伪装、破坏日志、禁用防御机制等方式。

（7）横向运动：攻击者在航天器各个子系统之间或者不同的航天器之间移动，以实现攻击面的扩大，包括

利用托管载荷、星间链路、总线等方式。

（8）信息泄露：攻击者试图获取相关信息，包括利用窃听、带外链路、临近操控、攻击地面系统等手段。

（9）危害：攻击者实现欺骗、干扰目标航天器，使通信链路劣化，目标航天器拒绝服务，数据丢失或被破坏等目的。

2 HAS 介绍

每年在美国的拉斯维加斯都会举行 DEFCON 极客大会，在 2019 年的 DEFCON 27 会议上，主办方宣布要举行 Hack-A-Sat（简称 HAS）太空信息安全挑战赛。比赛分为两个阶段：资格赛和决赛，采用积分制，资格赛中积分靠前的 8 支参赛队将进入决赛[3]。

从 2020 年开始，已经连续开展了四届 HAS。HAS 是结合了信息安全与航天两个领域的比赛，在其题目设置上也体现了这一点，与传统的信息安全夺旗赛不同。一般的卫星运行包括三部分：地面部分、链路部分和空间部分。HAS 的赛题也是从这三个部分设置的。在题目中除了传统的逆向工程、通信数据截获分析、加密解密等信息安全知识，还结合了天文学、天体力学的相关知识，体现太空信息安全的特殊性[4]。HAS 涉及的技术相当广泛，既有与硬件 CPU 相关的，也有与飞行软件相关的，还有与信号处理相关的，对参赛者能力水平、知识面的要求很高[4]。

HAS4 是在 2023 年 4 月 1 日至 2 日举办了资格赛，决赛于 2023 年 8 月 11 日至 12 日举行。在决赛之前，2023 年 5 月 5 日，SpaceX 和 NASA 发射了一颗供黑客攻击的卫星“月光者”（Moonligher），将其送入近地轨道，用作实验性的“黑客沙盒”，进入决赛的队伍将对该卫星展开渗透攻击，发现其中的漏洞，并对漏洞进行控制利用[5]。

HAS4 决赛可以分为两个阶段的挑战，分别是地面段、空间段，这两个阶段又各自分为若干子阶段，每个子阶段分别有对应的目标，如下：

（1）地面段挑战

①Finalpass：要求攻击者破解地面系统的一个密码管理器，并借此获取管理员权限。

②Web：要求攻击者分析地面 Web 系统的漏洞，找出隐藏其中的敏感信息。

（2）空间段挑战

①Script Kiddies：要求攻击者利用二进制逆向技术，实现控制卫星向外发送指定的遥测信息。

②Shutterbug：要求攻击者控制卫星对非地理围栏内（non-geofence）的目标进行拍照。

③Unintended Bug：要求攻击者利用 GPS 欺骗技术，控制卫星对地理围栏内（geofence）的目标进行拍照。

④Ironbank：要求攻击者使用侧信道攻击的方式，解析星上软件，并实现非授权执行特殊敏感指令。

⑤Christmas in August：要求攻击者攻击卫星上的 GPS 模块，使其输出错误信息，让卫星误认为其工作在南北纬 80°以上。

3 HAS4 决赛攻击路径分析

3.1 地面站挑战

3.1.1 Finalpass

该阶段使用到 SPARTA 中的战术技术分别是：

（1）“侦察”中的收集供应链信息：包括软件供应链信息，攻击者可以操纵更新或分发机制、修改源码，或用插入恶意代码的版本替换安全可靠版本；FPGA、ASIC 等硬件供应链信息，攻击者可以修改供应链中的固件或硬件，可以插入后门，并对系统进行深度控制；软、硬件漏洞信息；目标航天器制造商的商业伙伴信息等。

（2）“初始访问”中的入侵地面系统：攻击者入侵地面系统，可以执行破坏飞行软件部署、重放攻击、破坏加密秘钥和身份验证方案，并对地面网络进行拓扑测绘。入侵方式包括破坏地面系统的前端处理器、指控软件等；操纵、修改目标航天器的在轨升级软件。

（3）“持久化”中的修改地面系统：地面系统被配置用于操控目标航天器，攻击者通过入侵、修改地面系统，实现持续非法操控、访问目标航天器。

在该阶段中，攻击者首先获取了地面系统中的密码管理软件的执行文件，可以以管理员登录，也可以创建新用户，攻击者需要获取管理员账号的密码。通过逆向分析该二进制文件，发现该软件实现过程中使用了多线程，登录是一个线程，创建新用户是另外一个线程，两个线程之间有一些公共变量没有使用锁，导致如果在使用管理员账号登录的时候，同时创建新用户，就可以直接修改管理员账号的密码为新建用户的密码，攻击者可以据此修改管理员密码，获取管理员权限。

3.1.2 Web

该阶段使用到 SPARTA 中的战术技术是“初始访问”中的入侵地面系统。

在该步骤中，攻击者可以通过 Web 浏览器方式访问地面系统的一个应用平台，其 URL 形式如下：

https：//moonlighter-facts. dc31. satellitesabove. me/admin/admin. html

通过对该平台进行测试，发现其中存在路径遍历漏洞，利用如下 URL 可以获取敏感文件 passwd（一般为 Linux 平台的账号密码存储文件）：

http：//moonlighter-facts. dc31. satellitesabove. me/../../../../etc/passwd

3.2 空间段挑战

3.2.1 Script Kiddies

该阶段使用到 SPARTA 中的战术技术是“侦察”中的收集飞行软件开发信息：包括飞行软件的开发环境、编译后的程序文件、测试工具、源码和故障管理系统。

在该阶段中，攻击者可以通过 UDP 连接到卫星平台，需要向卫星发送特定的代码，获取指定的遥测信息，但是这个特定的代码未知，同时，攻击者收集到了卫星平台上的 UDP 接口程序的编译文件 script_ udp. so，为此，攻击者需要二进制逆向该文件，分析出特定的代码。为增加难度，该步骤中卫星平台的处理器架构是近几年崭露头角的 RISC-V。最终分析出特定代码与卫星动作的关系如表 1 所示。

表 1 特定代码与卫星动作的关系

特定代码	卫星动作
0	发送 GPS 坐标信息
1	照相
2	发送照片
3	特定遥测信息
4	发送相机电源信息

3.2.2 Shutterbug

该阶段仅操控卫星平台的光学摄像平台对非地理围栏内的目标进行拍摄，未使用 SPARTA 中的攻击战术技术。

3.2.3 Unintended Bug

该阶段使用到 SPARTA 中的战术技术分别是：

（1）“侦察”中的收集航天器设计信息：包括固件、加密算法、总线、软件、控制、载荷、电源、故障管理、环境控制系统等。

（2）“侦察”中的收集飞行软件开发信息：包括飞行软件的开发环境、编译的二进制文件、测试工具、源代码和故障管理。

（3）“执行”中的欺骗攻击：攻击者通过伪造总线数据、GNSS 信号、传感器信号时间信息等各种数据，以此导致航天器工作异常。

在该阶段中，攻击者获取了航天器上的部分软件，包括 script_ udp. so、GPS. so 等，以及 GPS 模块的协议说明，需要拍摄地理围栏内的目标照片。按照航天器的设计，地理围栏内的目标是不允许拍摄的，为此，攻击者分析软件信息、GPS 模块的协议说明，发现在解除 GPS 模块的部分限制之后，可以通过 FIX 指令直接修改 GPS 模块输出的位置信息，从而欺骗航天器。当航天器位于地理围栏之内时，修改 GPS 模块输出，使航天器误认为还处于非地理围栏区域，进而可以控制星载相机进行拍照。

3.2.4 Ironbank

该阶段使用到 SPARTA 中的战术技术包括：

（1）“侦察”中的收集航天器设计信息：参考 3.2.3 中对于收集航天器设计信息的解释。

（2）“侦察”中的收集飞行软件开发信息：参考 3.2.3 中对于收集飞行软件开发信息的解释。

（3）“执行”中的侧信道攻击：获取加密硬件或软件运行时产生的各种泄漏信息，从而加以分析，得到敏感内容，包括电磁攻击、功耗攻击、时间攻击等方式。侧信道攻击分为被动、主动两种。被动侧信道攻击侧重于收集时间、功耗、电磁泄露等信息，分析后获取加解密数据。主动侧信道攻击通过在运行时对硬件主动施加外部刺激（如时钟毛刺、电压或电磁辐射），引发加解密异常。

在该阶段中，攻击者要求向一个星载应用发送指令，以获取敏感信息。攻击者得到该应用的二进制文件后，通过逆向分析，可以得出与该应用通信的指令格式，如图 2 所示。

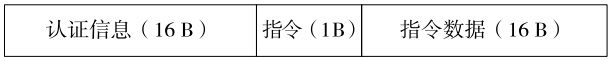

图 2 与星载应用的通信指令格式

其中起始的 16 个字节是认证信息，当执行受保护指令时，星载应用会将这 16 个字节认证信息与秘钥进行对比，如果一致，则执行受保护指令，反之，则不允许执行。在秘钥对比的过程中，是逐字节对比的，如果某字节对比不一致，那么立即退出，如果某字节对比一致，那么稍停顿后再对比下一字节，如此就可以使用基于时间的侧信道攻击，逐个字节推测出秘钥信息，从而实现执行受保护指令的目的。

3.2.5 Christmas in August

该阶段使用到 SPARTA 中的战术技术包括：

（1）“侦察”中的收集航天器设计信息：参考 3.2.3 中对于收集航天器设计信息的解释。

（2）“侦察”中的收集飞行软件开发信息：参考 3.2.3 中对于收集飞行软件开发信息的解释。

（3）“执行”中的欺骗攻击：参考 3.2.3 中对于欺骗攻击的解释。

（4）“危害”中的破坏：攻击者可能会破坏命令、数

据、子系统，或试图破坏目标航天器本身。

在该阶段中，攻击者通过分析软件信息、GPS 模块的协议说明，以及通过 FIX 指令直接修改 GPS 模块输出的位置信息，从而欺骗航天器，让航天器误认为自身处于南北纬 80°以上，从而破坏航天器的正常工作。

4 结论

HAS 是近年来获得广泛关注的太空信息安全活动，SPARTA 也是 2022 年公布的太空攻击研究与战术分析框架，其确定的许多战术、技术（子技术）、过程已在实验室以及太空网络安全事件中得到验证。本文使用 SPARTA 框架分析了 HAS4 决赛攻击战术技术，显示出了 SPARTA 框架的覆盖性、适用性。未来随着 SPARTA 框架的不断丰富，其在太空网络安全威胁狩猎、风险管理、威胁情报、安全解决方案评估、合规管控测试、攻击模拟等方面会有广阔用途。

参考文献

[1] 张福，程度，鄢曲，等. 基于 ATT&CK 框架的网络安全评估和检测技术研究 [J]. 信息安全研究，2022，8（8）：751－759.

[2] 雷思磊，温占伟，荆美倩. 基于 SPARTA 框架的 KA-SAT 卫星网络遭攻击流程分析 [J]. 网络安全技术与应用，2024（2）：16－19.

[3] Space Attack Research & Tactic Analysis (SPARTA)[EB/OL]. [2024－03－09]. https：//sparta-aerospace-org/.

[4] 雷思磊，仇婕，马婷婷. AES 缓存碰撞攻击在美国太空安全挑战赛中的应用 [J]. 信息技术与网络安全，2022，41（3）：32－37.

[5] ISS National Laboratory. Moonlighter, the world's first hacking test bed in space, to launch with five other small satellites on spaceX CRS－28 [EB/OL]. (2023－05－30) [2024－03－09]. https：//www. issnationallab. org/spx28-moonlighter-cube-sat-afrl/, 2023.

（收稿日期：2024－03－09）

作者简介：

雷思磊（1984－），男，硕士，高级工程师，主要研究方向：网络安全。

荆美倩（1989－），女，本科，工程师，主要研究方向：信息通信。

龙森（1992－），男，本科，助理工程师，主要研究方向：信息通信。

（上接第 11 页）

作者简介：

刘子龙（2000－），男，硕士研究生，主要研究方向：工业控制系统信息安全风险评估。

周纯杰（1965－），男，博士，教授，主要研究方向：工业互联网及工业信息物理系统安全。

胡晓娅（1974－），通信作者，女，博士，教授，主要研究方向：工业通信网络及工业互联网技术。E-mail：huxy@hust. edu. cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部