关于接入网防雷接地应用技术探析

刘 鉴
中国通信建设集团设计院有限公司第四分公司，河南 郑州 450000

[摘要]近年来，随着家集客业务的蓬勃发展，GPON 技术应用前景十分的广泛，从早期的 FTTB 过渡到 FTTH 建设，最大的变化是：由有源特性延伸到无源的建设模式，能够极大的降低建设、管理和运营成本，提高运营商的投资回报率，增加新的收益模式；GPON 网络的体系结构非常适合接入网建设，使运营商可以快速有效地开展业务并易于进行网络扩展。其次，通过综合业务区一级分析点的网络搭建，二级分纤点的资源延伸，极大的满足了家集客业务的建设需求。
[关键词]三级法；接地电阻；土壤电阻率
DOI：10.33142/sca.v3i1.1556 中图分类号：Z88 文献标识码：A

Discussion on Application Technology of Access Network Lightning Protection and Grounding

LIU Yin
The Fourth Branch of China Communications Construction Group Design Institute Co., Ltd., Zhengzhou, Henan, 450000, China

Abstract: In recent years, with vigorous development of home collection business, GPON technology has a wide application prospect. The biggest change from early FTTB to FTTH construction is that active characteristic extends to passive construction mode, which can greatly reduce cost of construction, management and operation, improve return on investment of operators and increase new income mode. Architecture of GPON network is very suitable for access network construction, so that operators can quickly and effectively carry out business and easy to carry out network expansion. Secondly, through network construction of the first level analysis point in comprehensive business area and resource extension of the second level fiber distribution point, it greatly meets construction demand of home customer service.
Keywords: three level method; grounding resistance; soil resistivity

引言

在接入网不同的场景和需求方式下，施工工艺和标准参差不齐，存在不同的工程质量问题和安全隐患，特别是因雷击接地等造成的物质或人身危害，都造成了极大的损失。为了确保人员安全和通信设备的安全和正常工作。本文针对目前接入网室外型分纤点和用户端分纤箱等常用的无源通信设备在接地防雷方面一些安全措施，进行技术方面的探讨。

1 原有光纤分纤点的接地电阻测试方法

在新建接入网工程时，需要出具现场勘察报告，对其建设方案上联的通信局站或一级光纤分纤点进行接地电阻的测试。目前，国内常用的是三级法和三角形法测量。本文以三级法作为范例。

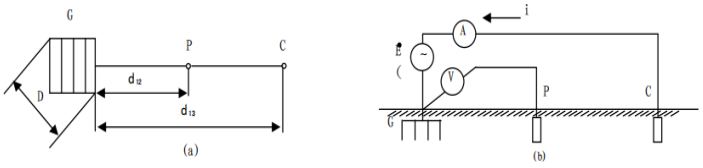
1.1 极法测试方法

（1）电流极与接地网边缘之间的距离 d_{13}，应取接地网最大对角线长度 D 的 4 倍～5 倍，电压极到接地网的距离 d12 宜为电流极到接地网距离的 50%～60%。测量时，沿接地网和电流极的连线应移动三次，每次移动距离宜为 d_{13} 的 5%。

（2）若 d_{13} 取 4D～5D 有困难，在土壤电阻率较均匀的地区，可取 2D，d_{12} 可取 D；在土壤电阻率不均匀的地区或城区，d_{13} 可取 3D，d_{12} 可取 1.7D。

（3）可采用几个方向的测量值互相比较，也可用三角法和直线法对比互校。

（4）电流极和电压极均应可靠接地。如下图所示：



（a）电极布置 （b）原理接线

图 1-1 三极法

基于 Android 系统漏洞的通用攻击模型研究

巫忠跃 黄 钟 何 洋
成都国信安信息产业基地有限公司，四川 成都 610000

[摘要]系统漏洞存在会给 Android 平台的运行安全带来比较大的威胁，通过各种修补技术，例如移动操作、漏洞利用等等，可以显著提高 Android 生态系统的应用安全性。基于此，文章主要分析平台漏洞存在造成的安全隐患，并结合 Android 系统漏洞通用攻击模型探讨模型建设、模型利用、模型攻击实施过程，评估漏洞对于系统安全性的影响。
[关键词]Android 系统；漏洞；通用攻击模型
DOI：10.33142/sca.v3i1.1534 中图分类号：TP316;TP309 文献标识码：A

Research on General Attack Model Based on Android System Vulnerability

WU Zhongyue, HUANG Zhong, HE Yang
Chengdu Guoxin'an Information Industry Base Co., Ltd., Chengdu, Sichuan, 610000, China

Abstract: Existence of system vulnerabilities will bring great threat to operation security of Android platform. Through various repair technologies, such as mobile operation, vulnerability utilization and so on, application security of Android ecosystem can be significantly improved. Based on this, the paper mainly analyzes security risks caused by platform vulnerabilities, discusses model construction, model utilization, model attack implementation process and evaluates impact of vulnerabilities on system security.
Keywords: Android system; vulnerability; general attack model

引言

当前移动互联网正处于快速发展过程当中，Android 系统由于其开放性受到了广大用户的喜爱和支持。作为应用最为广泛的一种移动智能手机操作系统，Android 在人们的日常生活、社交、通信、移动办公当中都是重要的角色，担任媒介功能。由于其自身存储了大量的信息，因而也很容易受到恶意攻击。

1 Android 系统漏洞带来的安全隐患

从美国某互联网移动公司给出的统计数据可以看出，2017 到 2018 年，Android 系统曝光漏洞 272 个，给用户带来了非常大的安全隐患。而到了 2018 年上半年，这一数据更是达到了 257，增长幅度超过 40%，有一些漏洞严重影响了用户的隐私和敏感数据。甚至造成应用层面的代码受到威胁，严重影响系统的业务安全。长期以来，Android 系统由于业务的碎片化问题，使得漏洞补丁需要经过较长的周期才能够部署到用户的终端设备之上，这增加了安全风险隐患。一些不法分子甚至会利用已经公开的系统漏洞来进行攻击，该种行为已经形成了价值超过 20 亿美元的黑色产业链，例如意大利知名控制软件商曝光的信息泄露问题，就集成了 oday 漏洞等多个公开漏洞，利用完整的代码达到恶意窃取用户信息、恶意控制音响设备的目的，获取非法收入[1]。

2 基于 Android 系统漏洞通用攻击模型

2.1 Android 系统利用通用模型

2.1.1 漏洞分析基础

Android 系统生态存在的安全隐患来自多个方面，例如信息方面、扣费方面、应用软件方面、网络安全等方面。目前，从黑色产业链条的形成方式来看待 Android 系统漏洞的实现，可以对攻击路径进行有效拓展，建成可用模型。系统漏洞基于结构化描述，可以对已经获取到的攻击行为进行结果研究，利用漏洞识别系统，进一步提起代码检测，对安全预警进行有限元分析。漏洞系统检测验证的指令执行，主要是搜集特定机型信息、创建有力的攻击环境、编写 Sherlock 指令，触发该指令，对漏洞检验和验证进行相关系统介绍。例如北京某科学技术公司采用的漏洞检测模型，就覆盖了目前市场上的三星、华为、小米、魅族、酷派、联想等多个品牌，建立了有效的数据映射反应系统，在检测信息基础之上选用不同的漏洞信息模型，制定适配的漏洞脚本利用信息。

近年来，随着移动互联网的快速发展，Android 平台迅速在全球范围内推开已经成为应用用户最多、使用范围最广、平台操作最为便利的移动智能手机操作系统，作为日常用户社交、通信、移动办公的重要媒介，Android 平台也存在用

户隐私暴露敏感数据泄露等相关的危险。因而恶意攻击系统分析模型要针对这种现象，不断探讨各类漏洞曝光存在的安全隐患。结合 cv 公开披露的漏洞数据库，进行总体探讨，遏制这种井喷之势，避免漏洞发展造成系统的安全威胁，提高数据安全管理的有效性，促进业务安全和代码安全，避免由于版本碎片化的问题影响 Android 系统的未来发展，不断提高终端设备的应用价值，促进安全建设。

2.1.2 漏洞资源库

漏洞资源库主要是对现有的漏洞数据进行深入挖掘，基于大数据算法进行传输、存储、收集，对于漏洞当中存在的交易进行捕捉。漏洞信息交换和漏洞售卖过程都会被漏洞资源数据库所记录，整体的展现出漏洞的具体覆盖、映射和利用情况。目前已经可以通过漏洞信息映射和漏洞脚本库来全面进行披露。

一方面，可以应用系统漏洞库进行 Android 信息查找，包括公开漏洞和未公开漏洞集合都可以进行全面暴露分析。在漏洞资源库分析的过程当中，要对持续爆开的公开漏洞进行攻击分析，这种黑色产业链条目前已经成为了一种攻击利器。根据意大利知名软件控制商给出的信息泄露数据显示，超过 400gb 的数据被曝光，不仅包含多个 Android 平台的系统源代码，还包括多个完整的利用代码。很多不法分子和集团都通过这种恶意利用的行为，探讨非法信息，实现监控用户行为盗取音视频资料的目的。该公司发布的这种现象也成为地下黑客攻击手段的一次泄漏问题，从这个角度来看，通过攻击代码工程的高度规范化、隐蔽性，在世界范围内已经引起了越来越大的重视，只有对攻击者的攻击方案进行分析，披露现有安全机制的短板和缺陷，才能够促进安全应用体系的完善，不断引入新的保护机制，促进安全管理水平的提高，对抗攻击能力，缓解系统漏洞危险，逐渐实现代码段读取保护特征，禁止实行一些盗用指令，提高缓冲技术的完善程度。

另一方面，通过信息映射库进行动态把握，通过终端识别脚本利用等方法进行自动查询，脚本厂商补丁就可以获得映射库的影响数据。除此之外，还可以针对某种机型和某个漏洞编写的利用脚本，获取相应的漏洞代码，通过运行该代码获得指定的执行顺序。在系统漏洞分析的过程当中，还要通过版本分析探讨内核因素，通过控制主机自动控制访问方式对于内核的安全体系进行策略分析，不断通过增强安全机制和缓解技术，为 Android 平台提供天然的保护，针对这种漏洞利用手段进行反推式分析，绕过安全机制，避免漏洞利用成功。从这个角度来看，只有不断增强和演化安全机制、弥补现有的缺陷，才能够避免安全事件发生，造成信息数据泄露，影响平台运行的安全性。

从这个角度来看，Android 系统的平台攻击与防守是一场持续激烈的战争，只有从制度发展、代码保护、平台建设综合入手，才能够增加利用防护的安全效果，避免出现公开披露漏洞，不断完善反应机制。现有的攻击主要来自物理攻击、恶意应用、网络威胁、云端数据泄露等多个维度，只有不断利用大数据技术云端网络系统技术，避免恶意操作造成严重危害，通过应用签名方式、平台安全操作方式、权限设置方式、沙箱方式，才能够减少系统状态受到的威胁。

2.1.3 业务资源攻击

对于 Android 系统存在的漏洞，每进行一次攻击都会对原系统发生一定的改变，简单来说，整个漏洞资源的获取要分为攻击前提、动作和后果三个分析行为，不论采取哪一种单独的攻击行为都要对漏洞系统进行充分利用。

首先，在攻击之前要对前提进行分析，通过扩散、传播、复制，判断 Android 系统漏洞存在的状态。不法分子可以借助各种技术和工具，实现用户隐私信息盗取的行为，达到恶意破坏系统恶意扣费的目的，这种问题也给 Android 用户的隐私保护和财产安全带来了巨大的系统威胁，只有在原有的安全保护基础之上不断完善应用软件系统，提高安全网络的划分程度，才能够促进系统的升级，避免恶意攻击给 Android 系统造成隐患和危害。

其次，连接被攻击主体与攻击主体，获得相映的特点信息进行准确定位。通过模拟方式对于现有的黑色产业链进行定位分析。可以进一步发现模型的应用方式与应用路径。避免安全攻击对于现有的安全评估模型造成系统损害，从整个生态系统的角度进行优化评估，及时的发现评估框架，避免出现漏洞，利用和攻击提高通用模型的设置完善程度。

再次，对漏洞进行攻击，对原有生态系统进行改变，使原有的生态系统运行模式受到破坏，无法恢复到原本的运行状态，也无法接收到外界的指令。基于结构方式进行系统性分析可以促进 Android 系统通用模型的不断完善，利用现有的数据库进行漏洞模拟探讨，根据覆盖情况、映射情况和利用情况全面的探知漏洞检测的实际结果，对于漏洞信息映射库和漏洞利用脚本库进行信息反馈。

最后，在不破坏原有生态系统名称的情况下，改变状态切换模块实现最终的控制行为。上述几种控制行为可以单独采用或多种组合采用，危害程度也不断升级。不断强化安全应用级别，通过系统漏洞标示最终识别安全脚本，建设这种数据库可以提高厂商补丁的映射补充程度，利用脚本索引等方式进行快速的完善和补充，全面提高系统补丁的应