一种远程应急工具的实现方式

麦海新　张士华　周肃然
中国联合网络通信有限公司东莞市分公司　广东　东莞　523009

摘　要：随着信息技术的迅猛发展，网络安全事件日益频发，对网络应急响应提出了更高的要求。本文针对当前网络安全事件应急处置中存在的痛点，提出了一种基于虚拟化技术的远程应急工具实现方式，旨在实现网络安全事件应急处置的高效、规范、有序开展。通过深入分析应急处置的三大痛点，本文给出了具体的解决方案，并对其优缺点及应用场景进行了详细探讨。

关键词：远程应急工具；网络安全；虚拟化；内网穿透；应急处置

引言

近年来，网络安全事件呈现出高发态势，对网络应急响应速度和效率提出了严峻挑战。然而，当前应急处置体系存在时间长、技能要求高、工具杂乱不规范等问题。为了解决这些痛点，本文提出了一种基于虚拟化技术的远程应急工具实现方式，旨在通过远程接入机制，实现快速、高效的应急处置。

1 网络安全事件应急处置的痛点分析

1.1 应急处置时间长

网络安全事件的应急处置时间长，这一痛点主要源于多个因素。首先，网络安全事件的突发性和不确定性使得响应团队往往需要在第一时间与客户进行初步沟通，以了解事件的具体情况和影响范围。这一沟通过程可能因客户对技术细节的不了解而耗费时间。其次，根据事件的性质，需要从有限的人力资源中调配具备相关专业技能的工程师前往现场处置。这种人力资源的调配不仅受到地理位置和交通状况的影响，还可能因为工程师的专业技能与事件性质不完全匹配而延误时间。最后，当现场工程师无法独立解决问题时，需要进一步的电话求助或远程支持，甚至可能需要从其他地区调配更专业的工程师，这一过程同样会增加应急处置的总体时间。在整个处置流程中，对单个工程师的依赖、专业技能的匹配问题以及跨地域的协作难度都是导致应急处置时间长的重要因素。这些因素不仅影响了响应速度，也可能因时间延误而加剧网络安全事件的负面影响[1]。

1.2 应急人员技能要求高

工程师在网络安全事件应急处置中的角色至关重要，但这一岗位对个人能力的要求也极高。在计算机技术迅猛发展的背景下，信息网络日益复杂，其中蕴藏的敏感信息和重要数据吸引了全球各地的安全威胁。从信息泄露、窃取到数据篡改、删添，再到计算机病毒等恶意攻击，每一种安全事件都需要工程师具备深厚的专业知识和丰富的实战经验来迅速应对。他们不仅需要精通各种网络安全技术和工具，还要能够在复杂的网络环境中准确识别威胁、分析攻击路径，并迅速制定有效的应对策略。然而，当前安全专业人才的市场供需矛盾依然突出，高级网络安全工程师的稀缺性使得这一岗位的挑战更加严峻。

1.3 应急处置工具不规范

应急处置工具的标准化问题在网络安全领域显得尤为重要。随着信息网络的高速发展，网络架构和技术的多样性及兼容性带来了诸多挑战。在应对客户网络问题时，工程师需要使用多种应急处置工具进行网络接入、控制、扫描和问题处理。然而，由于工具软件的不统一，工程师在切换使用不同工具时可能会遇到操作障碍，这不仅影响了处置效率，还可能因操作不熟练而引发新的问题。同时，在处理敏感和重要数据时，为确保数据安全和客户隐私，工程师需要进行详细的取证和记录。但现实中，他们可能需要一边操作，一边使用手机或相机进行拍照记录，这种分散注意力的方式显然降低了工作效率，并可能增加操作失误的风险。

2 远程应急工具的实现方式

本方案以虚拟化技术为核心，构建了一个高效、便捷的网络安全应急响应系统。通过集成多种应急工具于一个便携式应急终端上，并结合远程接入技术，实现了对网络安全事件的快速响应和有效处置。如图1所示：

2.1 应急终端设计与部署

应急终端作为本方案的关键组成部分，采用了先进的X86平台工控小主机，并安装了EXSI虚拟化软件，以此搭建一个功能强大的虚拟化小型局域网。该终端可提前部署在客户机房作为备用，或在应急仓库中由协作人员快速携带至现场[2]。

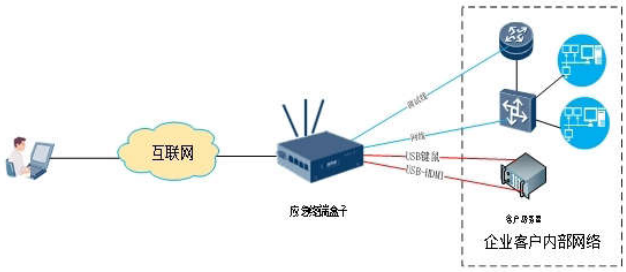

图1 远程应急工具的实现方式示意图

2.1.1 外部接口设计

①无线WIFI接口：此接口设计用于灵活接入互联网，可通过现场的公共WIFI热点或手机设置的热点进行连接。一旦连接成功，它将通过预设的安全通道与远程管控平台进行通信，确保数据传输的安全性。在需要更高级别的安全保障时，WIFI模块可以替换为物联卡模块，通过私有的APN（接入点名称）网络进行接入，从而进一步提高数据传输的私密性和安全性。

②双物理网络接口：应急终端配备两个物理网络接口，分工明确且功能独立。其中一个接口专用于管理功能，通过利用现场已有的网络环境，与远程管控平台进行稳定连接，实现对应急终端的实时监控与配置更新。另一个接口则专注于业务操作，直接接入客户的内部网络，以便进行及时有效的网络安全应急处置工作。

③USB扩展接口：为满足多样化的应急需求，应急终端还配备了USB接口。这一接口不仅支持外接视频采集器、键盘鼠标模拟器等设备，实现对孤立无援或网络隔离的主机设备进行远程操控，还可连接移动存储设备，便于在远程操控现场与应急团队之间进行必要的数据共享与交换。这一设计显著提升了应急响应的灵活性和效率[3]。

2.1.2 内部结构特点

应急终端以虚拟化技术为核心，选用EXSI虚拟化平台为基础，内部预装了多样化的系统和专业软件工具，以满足快速响应需求。为保障平台的稳定性和可靠性，特别采用快照技术，实现系统状态的一键恢复。同时，终端内部构建了一个高效的小型局域网，网络架构如图2所示：

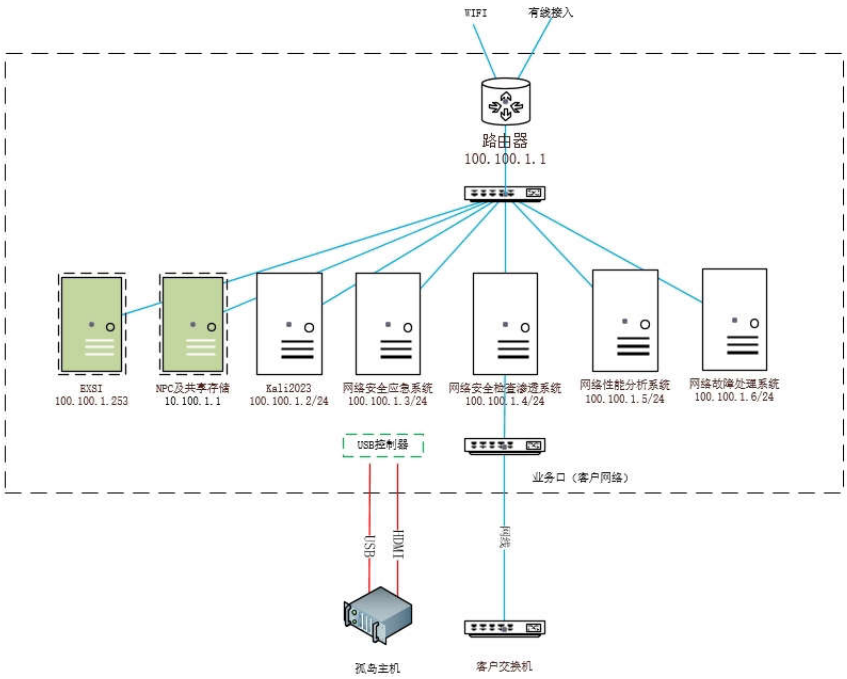

图2 网络架构示意图

2.2 应急终端系统组成及功能

应急终端系统的构建基于EXSI虚拟化平台，采用web管理界面，实现对虚拟机资源的灵活分配与高效利用。系统主要由以下几个核心模块构成：

①虚拟路由器模块：作为虚拟局域网的中枢，它担负着管理WIFI或有线网络连接的重任，确保应急终端能够顺畅接入互联网。此外，其内嵌的内网穿透客户端功能强大，支持包括HTTP代理、TCP/UDP隧道、SOCKS代理以及P2P连接等多种安全隧道技术。这一设计使得应急工程师能够远程接入现场网络，并利用应急终端进行及时有效的处置工作。

②预置系统及软件虚拟机：系统内置了包括KALI在内的多个系统及软件虚拟机，这些工具涵盖安全扫描、渗透测试以及系统分析等多个方面，能够对客户内网进

行全面深入的问题排查与分析。

③孤岛设备远程操控管理：对于网络隔离或无法联网的孤岛设备，采用创新的USB键鼠模拟与USB视频采集卡方案，以实现远程键盘鼠标操作及屏幕内容的实时回传。具体而言，运用CH9329+CH340方案，通过专用的模拟线将应急终端与孤岛设备的USB端口直接相连，从而达成对键盘鼠标的远程操控。为了获取孤岛设备的屏幕显示内容，将USB视频采集卡插入设备的HDMI显示器输出接口。若设备仅有VGA接口，则可添加转换器以适应。推荐使用搭载MS2130芯片的USB采集卡，它支持YUY2格式，能够实现1080P 60Hz的全高清显示输出。采集卡捕获屏幕内容后，会将其回传至应急终端，使得可以远程查看孤岛设备的屏幕显示。此方案无需在孤岛设备上安装任何额外软件，确保了操作的简便性和兼容性。

④存储与共享管理：系统提供了充足的存储空间，并支持FTP、SMB、WEBDAV等多种共享存储方案，满足了数据存储与共享的多样化需求。

⑤远程协作与应急审计：系统内置了远程协作机制，支持屏幕共享、操作共享以及多人远程协作等功能。同时，通过应急审计及日志管理模块，能够对应急过程进行详细的日志记录和操作录屏，确保所有操作的可追溯性和取证需要。

2.3 应急业务流程

应急业务流程简述如下：首先，应急工程师需携带应急终端赶赴现场。随后，通过有线或WIFI等方式，使应急终端接入并通过认证后连接到管理平台。接着，根据现场情况，应急终端会通过有线方式接入内网，或利用USB接口（包括键鼠模拟和HDMI采集卡）直接接管应急主机。应急团队和监管人员随后远程接入平台，在经过远程认证和授权后，将获得对应急终端的操作权限。在此过程中，应急工程师将进行远程操控，协同开展应急工作，而监管人员则负责全程监控，确保应急流程的合规性。同时，平台会通过堡垒机技术，全程审计并记录应急工程师的操作，并进行屏幕录制以取证。应急工作完成后，工程师需上传详细的应急报告供监管人员审核。最后，所有相关资料将被打包留存，应急终端则通过快照技术恢复到初始状态，以备下次使用[4]。

3 优缺点分析及应用场景

3.1 优点

一是提高应急效率：通过提前部署或就近调度使用应急终端，可快速到达应急现场，缩短响应时间。二是降低技能要求：远程应急工具使得应急工程师无需奔赴现场，降低了对现场人员的技能要求。三是规范化应急工具：通过提前内置部署在应急终端的规范化工具，确保应急处置的高效性和规范性。

3.2 缺点

虽然远程接入功能强大，但通过互联网进行连接存在一定的安全风险，尽管可以通过加密技术来降低这种风险，但仍建议在必要时才启用应急终端。其次，远程接入的流畅度受网络线路质量影响，这可能对操作的顺滑性造成一定影响，但不会对整体的应急处置效果产生根本性影响。同时，应急终端在现场需要有稳定的互联网接入环境。

3.3 应用场景

本文提出的远程应急工具适用于常态化应急场景和突发事件应急场景。在常态化应急场景中，可作为服务支持设备定期开展网络安全巡查、检测等工作；在突发事件应急场景中，可快速调配至现场进行应急处置。

4 推广应用前景价值

4.1 安全保障价值

该远程应急工具在提升网络安全防护能力、有效应对网络攻击以及保障信息系统的稳定运行方面具有积极作用。通过高效、规范的应急处置流程，能够及时发现并处置网络安全事件，降低损失和风险。

4.2 社会治理价值

该工具对于促进社会治理现代化、保障公民权益和维护社会稳定具有重要意义。通过加强网络安全事件的应急处置能力，有助于提高政府对网络安全事件的响应速度和处置效率，进而保障公民的个人信息安全和社会稳定。

结语

本文针对网络安全事件应急处置的痛点问题，提出了一种基于虚拟化技术的远程应急工具实现方式。该工具具有高效、规范、有序的特点，能够有效提升网络安全事件的应急处置能力。通过对其优缺点及应用场景的分析，展示了该工具在安全保障和社会治理方面的价值。未来可进一步推广应用于各类网络安全应急场景中，为提升网络安全防护能力和社会治理水平贡献力量。

参考文献

[1]林友凯,陈锦明,何荫虎.便携式应急通信终端设计[J].科技资讯,2019,17(16):27+31.

[2]徐文全.应急救援便携式卫星站通信业务终端集成问题研究[J].数字通信世界,2023(03):182-184.

[3]谌德军,孙志昆,姚怡,等.便携式宽窄带融合卫星通信终端在应急通信的应用及实践[J].卫星应用,2021(12):49-53.

[4]史永祥.基于北斗短报文的便携式应急通信终端设计与实现[J].数字通信世界,2024,(05):4-6+11.