中国科学院网络安全保障与服务工程
信息安全自主技术示范应用项目指南

一、指南说明

“十二五”中国科学院网络安全保障与服务工程的主要目标是增强我院网络与信息安全保障和监管能力，以基础设施为支撑，以应用与服务为重点，依托院内信息安全优势力量，构建特色鲜明、使用便捷、保障有力、自主可控的全院信息安全保障技术体系，在深度和广度上确保我院信息化设施的安全运行，有力保障我院科技创新和组织管理活动，充分应对开放的互联网环境。针对我院信息化对特定安全技术的迫切需求，现开展若干自主信息安全技术的应用示范，以引领我院在信息化建设过程中安全技术的自主创新和推广应用。

本指南由院信息化工作领导小组办公室（以下简称“院信息办”）公开发布，目的是确定院网络安全保障与服务工程信息安全自主技术示范应用项目的承担单位与工作内容等。项目承担单位接受院信息办的指导，接受院聘请的监理专家的监督。

项目主要目标：

针对我院院信息化对特定安全技术的迫切需求，开展若干自主信息安全技术的应用示范，推动我院在信息化建设过程中安全技术的自主创新和推广应用。作为建设项目，项目最终研发的成果必须在院公共信息化基础设施上部署应用。

项目申请要求：

1. 本指南面向院内单位公开发布。

2. 项目牵头申请单位必须是院内法人单位。

3. 对项目负责人的要求

（1）对项目内容有较全面的认识和理解，具备组织实施项目的能力。

（2）具有副高级及以上技术职称的院属人员，并在所申报项目的技术方面有两年以上的工程或研究工作经历。

（3）“十二五”院信息化专家咨询委员会委员原则上不能作为项目负责人。

二、指南内容

1. 方向一

1.1 项目名称

信息安全大数据分析与挖掘云服务平台应用与示范

1.2 项目目标

针对海量信息安全数据中的用户行为模式发现、网络攻击行为检测等任务，开发基于云计算的信息安全大数据分析与挖掘云服务平台，提供多种并行数据转换规则和并行数据挖掘算法，支持信息安全大数据的预处理、入侵模式分类、聚类、入侵模式关联分析、用户行为异常发现等多种并行数据挖掘算法把数据挖掘算法抽象成服务提供给用户，用户按需使用计算资源，并在中国科技网上部署，为我院用户提供服务。

1.3 主要工作内容

1. 开发部署并行数据挖掘工具库，支持信息安全数据预处理、入侵模式分类、聚类、入侵模式关联分析、用户行为异常发现等多种并行数据挖掘算法，支持从大量的、动态的、模糊的信息安全数据中基于模式挖掘的用户行为异常检测和基于数据挖掘的入侵检测。

2. 研究数据挖掘算法内部并行化与外部多任务之间分布式协同执行问题，实现高效并行算法。

3. 开发信息安全数据挖掘任务工作流及相关业务系统间的业务协同机制，实现数据挖掘任务的定制、参数设定、过程监控、结果展示、比较和分析。

4. 开发并行信息安全数据分析与挖掘云服务平台，在该平台上支持对信息安全大数据的联机在线分析，支持数据挖掘任务的定制、参数设定、过程监测、结果比较和展示。

5. 实现基于模式挖掘的用户行为异常检测和基于数据挖掘的入侵检测。

1.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. 开发完成信息安全大数据处理的算法工具库，包括数据预处理、入侵模式分类、聚类、入侵模式关联分析、用户行为异常发现等多种并行数据挖掘算法，用于基于模式挖掘的用户行为异常检测和基于数据挖掘的入侵检测。

2. 完成多种并行算法对信息安全大数据的测试，测试规模至少达到 TB 级规模。

3. 完成在中国科技网上部署信息安全大数据分析与挖掘云服务平台，并在该平台上进行用户行为异常检测和基于数据挖掘的入侵检测的数据挖掘应用验证。

2. 方向二

2.1 项目名称

应用安全云服务平台

2.2 项目目标

建设并部署应用安全云服务平台，对我院各分散的应用系统提供防护。系统支持对应用层攻击进行实时拦截，支持漏洞、挂马、篡改、敏感信息的不间断监测，能够基于平台所获取的海量异构日志数据、应用层数据流以及内容数据，对存在的安全隐患进行分析，达到异常行为检测和安全状态预测的要求。

2.3 主要工作内容

1. 建设云基础平台，提供数据中心和虚拟资源管理系统。

2. 建设应用安全服务平台，从防护、监测、分析三个层面，逐层深入，对应用安全提供全方位立体的保护，主要建设内容包括实时攻击防护服务、远程安全监测服务、安全分析预测服务、事件审计分析服务以及用户自服务六方面。

3. 建设支撑运维平台，保障服务的稳定性、安全性、可扩展性以及开放性，支撑核心服务的运行。

2.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. 构建包括数据中心和虚拟资源管理系统的云基础平台，并部署在中国科技网。

2. 采用业务流与基础设施低耦合的架构，支持基础设施更新升级。

3. 保证不变动原有网站部署环境的情况下快速接入。

4. 支持网站应用安全服务类型按需选择、防护性能按需选择两方面的要求。

5. 提供安全状态查询接口，实现与我院“科技云”、“管理云”和“教育云”等云环境的对接。

6. 建设完成后能够支撑为 500-1000 网站服务的应用安全服务平台，并保证系统的可用性、可靠性、安全性。

3. 方向三

3.1 项目名称

云环境安全保障示范系统

3.2 项目目标

面向我院“十二五”期间重点部署建设的“科技云”、“管理云”和“教育云”，依据云计算环境在部署架构、实现方式、构建技术等方面的特点，从基础设施层、虚拟化层和云终端层三个层次出发，搭建云环境安全保障示范系统。系统通过安全隔离、基线防护、安全检测、安全运维管理等方式，

建立全生命周期的信息安全保障体系，提高信息化应用环境的安全保障力度，降低安全事件风险，为我院云计算环境的建设和部署工作提供示范。

3.3 主要工作内容

云环境安全保障示范系统主要依据相关安全标准体系和“科技云”、“管理云”和“教育云”系统的实际安全需求，通过在基础设施层、虚拟化层和云终端层实施各种安全技术手段来保障云环境的安全。主要任务如下：

1. 基础设施安全保障模块：提供拓扑结构安全分析功能，保障云环境基础设施物理架构的安全性；提供数据加密和访问控制功能，保障云环境中用户数据的隐私性，避免云环境中的恶意用户非法窃取和利用相关资源。

2. 虚拟化层安全保障模块：提供虚拟机安全隔离、虚拟机镜像安全检测、数据迁移监控等核心功能，有效防止虚拟机之间的相互渗透及通过虚拟机安全漏洞进行违规操作，保障虚拟机化环境的安全。

3. 云终端安全保障模块：提供违规行为检查、安全配置基线审查等功能为云计算环境接入终端的安全提供保障。

4. 安全运维管理模块：依据相关安全标准规范实施系统整个生命周期内的安全运维管理，并进行可视化呈现和多维分析。

3.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. 系统在“科技云”、“管理云”和“教育云”中部署应用，实现对基础设施、虚拟化层和云终端的全生命周期安全防护，提供 3 个层面共 10 项安全功能：拓扑结构安全分析、数据加密、访问控制、虚拟机镜像安全检测、虚拟机安全隔离、数据迁移安全监控、违规行为检查、配置基线审查、可视化显示、多格式报告生成和导出。

2. 提交设计报告、使用手册、技术总结报告、实施总结报告、示范应用报告等 5 份技术文档。

3. 提交安全保障效果的自评估报告。

4. 方向四

4.1 项目名称

IPv6 网络安全工具

4.2 项目目标

针对 IPv6 网络协议特征，依据全院 IPv6 网络应用环境，研究开发 IPv6 网络安全工具。工具提供 IPv6 下的入侵检测、局域网扫描检测、中间人攻击检测、组播欺骗检测等功能；同时能够作为 IPv6 网络漏洞测试工具，进行邻居主机发现、

端口发现、数据包分片攻击、重定向攻击等; 并能够统计 IPv6 各种报文流量，发现异常。

4.3 主要工作内容

1. 开发 IPv6 网络安全检测工具。通过分析常见异常攻击的行为特征，构建 IPv6 安全检测规则，与源攻击进行规则匹配。协议特征和攻击特征的相应规则存储在相应数据库中。该工具由数据包捕获、协议解码、规则分析与告警四部分组成，包含入侵检测、内网扫描检测、中间人攻击检测、组播欺骗检测等子工具。

2. 开发 IPv6 网络测试攻击工具。模拟常见的网络攻击行为，进行邻居主机发现、端口发现、数据包分片攻击、重定向攻击等，从而测试 IPv6 网络安全漏洞。

3. 开发 IPv6 流量统计工具。根据协议内容进行流量统计，基于 IP 地址、攻击事件、应用协议等条件产生详细的异常流量报表。

4.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. IPv6 网络安全检测工具能够检测 IPv6 环境下 10 种以上类型的网络攻击，包括：中间人入侵检测、Smurf 攻击检测、MTU 攻击检测、MLD 攻击检测、重定向攻击检测等。

2. IPv6 网络测试攻击工具具有 10 种以上类型的测试攻击方式，包括：邻居欺骗测试、分片数据包攻击、重定向攻击、路由欺骗测试等。

3. 能够进行 IPv6 流量统计，产生包括 IP 地址、攻击事件、应用协议等详细内容的流量报表。

4. IPv6 安全工具部署在中国科技网。

5. 方向五

5.1 项目名称

计算机终端安全检查工具

5.2 项目目标

针对全院终端存在的突出安全问题，为办公计算机终端提供全面、强大且易于管理的终端安全检查工具，能够检测和分析终端安全状态，对终端配置进行检查和修复，有效降低终端安全运行维护工作量，提高管理效率，确保计算机终端安全稳定运行。

5.3 主要工作内容

1. 主机安全检测。针对每一个接入终端，可全面扫描并显示其安全状态，包括系统漏洞情况，病毒木马入侵情况、安全策略配置情况、安全防护措施（防毒软件和防火墙）配置情况、设备变化情况、流量异常情况、软件安装情况等，实时报告各项安全状态检测结果，方便用户及时了解本机安全状况，维护终端安全。其中，“系统漏洞检测”能够判断终端补丁安装情况，存在的漏洞及其严重程度，并推荐下载补丁。

2. 主机安全配置自动修复。对终端安全配置中存在的问题，能够自动一键修复，并在完成后对配置有效性进行检查。

5.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. 开发完成终端安全检测工具，并部署在计算机终端上使用，实现对终端的配置和安全状态的检查及修复。

2. 工具的主要功能包括：主机安全状态扫描、病毒查杀、主机安全配置检测、主机软件安装管理、主机安全配置自动修复等功能。

3. 工具采用图形化界面，用户操作简单。

4. 安全工具装机数量达到 2000 台以上。

6. 方向六

6.1 项目名称

移动终端安全检查工具

6.2 项目目标

针对我院移动终端安全这一薄弱环节，研究开发在 Android、iOS 等主流操作系统上可运用的移动终端安全检查工具，实现移动终端漏洞的安全监控与扫描，恶意软件和代码的查杀，以保证移动终端及其所承载的我院业务应用的安全可靠。

6.3 主要工作内容

1. 移动终端系统体检与杀毒。实时扫描终端系统及已安装的软件，发现病毒木马和恶意软件，彻底查杀；随时检查终端的健康状况，快速清理垃圾。

2. 移动终端上网安全保护。移动终端连接不安全 Wi-Fi 时提醒，恶意软件下载提醒，推迟安全更新提醒，点击欺诈链接提醒，保证移动终端安全上网。

3. 数据安全与备份。可提供重要数据信息备份，不收集用户信息，用户隐私绝对安全。

6.4 考核指标

申请单位依据下列考核指标内容（包括但不限于），提出定性、定量的考核指标。

1. 实现对移动终端的安全保护，主要功能包括：手机体检、实时病毒木马查杀、应用程序恶意代码扫描与清除、系统恢复、检测与处理结果报告。

2. 实现对移动终端的安全上网保护，主要功能包括：WiFi 安全警告、恶意软件下载警告、不安全链接警告、安全更新提醒等，保证实用性与可操作性。

3. 实现 1000 台以上移动终端的安装部署。

三、遴选原则

1. 支持我院特色的网络信息安全应用需求。

2. 支持能部署应用在院公共信息化基础设施上的网络信息安全技术。

3. 优先支持有一定网络信息安全技术及服务基础的申请团队。

4. 经费支出中以设备采购为主的项目不支持。

5. 已有同类成熟商业产品的网络信息安全项目不支持。

四、经费与年限

院信息化发展经费资助额度见下表，鼓励各申请单位配套经费支持项目的研发。项目完成时间截至年限为2014年12月31日。

序号	项目名称	经费（万元）
1	信息安全大数据分析与挖掘云服务平台应用与示范	90
2	应用安全云服务平台	90
3	云环境安全保障示范系统	60
4	IPv6网络安全工具	45
5	计算机终端安全检查工具	45
6	移动终端安全检查工具	45

五、申报要求

1. 通过Email提交项目申请书的电子版至“十二五”院网络安全保障与服务工程的总承担单位院计算机网络信息中心（以下简称“网络中心”），申报截止时间是2013年5月31日。

网络中心联系人：汪　洋

联系电话：010-58812267

Email: wangyang@cnic.cn

院信息办联系人：吴丽辉

联系电话：010-68597554

2. 通过形式审查进入评审答辩阶段，再提交申请书纸质版。

3. 遴选出的项目承担单位与网络中心签订任务书，并报院信息办备案。