安全+
SECURITY
2010/04 总第 008
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

10

中国网络安全发展十年

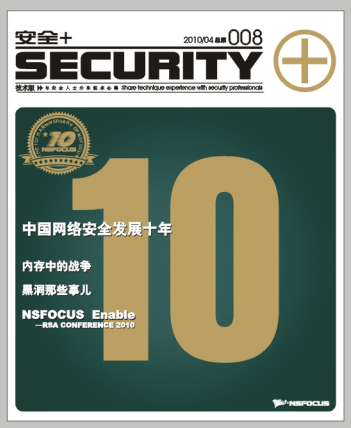
内存中的战争

黑洞那些事儿

NSFOCUS Enable
—RSA CONFERENCE 2010

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

2010/04 总第 008

安全+ SECURITY+

目录 CONTENTS

中国网络安全发展十年

首席战略官　赵粮

摘要：本文主要分为三部分内容。“轨迹”部分对十年的安全市场进行了简要的回顾；“发展”部分则对十年间发展背后的驱动力和发展趋势进行了分析和总结；“反思与动议”部分提出了针对业界的一些思考，并发出倡议和期望。

关键词：网络安全　轨迹　发展　反思　动议

1. 序曲

从历史的角度看，十年的时间不是很长。上世纪 50 年代 IBM 开始了现代意义的“商业机器”销售；1980 年 PC 个人电脑出现 [PC];1988 年华为成立；1991 年万维网概念提出；1989 年 CERT 诞生；1993 年 Checkpoint 成立；1994 年 Checkpoint 开始销售其第一台商业防火墙、ISS 成立、Cisco 开始销售 PIX 防火墙、ChinaNet 连入国际互联网、中国首部信息安全法规条例诞生 [SecHis];1995 年 ISS 开始销售其网络扫描器、天融信成立；1996 年启明星辰成立；1997 年 ISS 开始销售其运行于 Windows NT 4.0 上的 RealSecure 1.0 入侵检测系统 [IDS]、NetScreen 成立，笔者走出校门，入职中国电信数据局，开始网络安全旅途；1998 年产地中国的 CIH 病毒爆发；2000 年 4 月绿盟科技成立，11 月推出冰之眼入侵检测系统；…… 拂去淡淡的灰尘，发生在上个世纪的这些往事都还历历在目。

十年的时间也不短，已经足够发生太多事情，这十年恰恰是中国网络安全市场风起云涌的十年，多少弄潮儿竞相风流的十年。当前正值“青春期”、活跃在第一线的安全专业公司很多成立于 2000 年前后。

让我们一起回首这十年，回味这十年的潮头风雨，并希冀借此对明天的方向发现一些蛛丝马迹。

2. 轨迹

笔者在 2006 年 11 月的电信安全论坛上曾提出一个不太成熟的阶段定义 [TelecomSec2006]，按照某个阶段的主导技术和产品特征定义了 Security 0.1, Security 1.0, Security2.0。本文在此基础上进行了一些调整，将其用于本节的轨迹回顾。

图 1 中国安全市场阶段与主导技术特征

• Security 0.1 – 安全专注于传统的反病毒和基于防火墙的网络隔离控制。

• Security 1.0 – PDR 模型获得广泛接受，防火墙、反病毒、入

侵检测和漏洞评估、安全服务成为市场主导。

• Security2.0 – 关注点从简单的防止攻击和入侵，发展到应用和数据安全，NIDS 涅槃成为 NIPS，内部控制安全体系从“老三样”发展到基于 AAAA 的综合防御体系，强调安全管理的“内功”，安全管理和技术更加强调信息交互，以及相关、挖掘和展现。

• Security NG – Web 和云计算的迅猛发展，给安全业界带来了多方位的思考。一大片蓝海空间展现在人们的面前。

Security 0.1

作为一个相对公认的观点，中国的网络安全市场实际起步于 2000 年前后。在此之前，从社会和媒体关注、商业公司、从业人员、市场容量等各种角度来看，安全市场都非常薄弱。虽然称呼不同，或称为“元年”，或称为“导入期”[Intro]，或称为“古典期”，或称为 Security v0.1[Security0.1]。但是，这个阶段对后面十年的影响是深远的，很多后来业界的骨干都是在这个阶段开始接触网络安全、下决心进入这个“行业”为之奋斗的。

该时期的特点为：市场关注迅速提高，需求增长很快，增长率较高，技术变动较大。行业中的企业主要致力于提升用户安全意识，开辟新用户和占领市场，但此时技术方面限于反病毒、防火墙、入侵检测、网络扫描以及相关的安全服务，技术标准尚不成熟，行业竞争状况和用户特点等尚不明朗。这段时间的大部分网络安全专业企业利润很少甚至是亏损。

绿盟科技也正是从此开始了自己的十年创业征途。

Security 1.0

从 2000 年以来到 2003 年前后，该时期的一个重要标志是以 PDR 模型为代表的安全意识获得广泛的接受，以安氏、天融信、绿盟科技、启明星辰、中科网威、联想网御等为代表的主要网络安全企业基本上明确了自己的核心技术和市场竞争地位；安全产品“老三样”逐渐成为安全市场中明显的主导分支，成为 IT 或安全项目中的标准采购项目，“老三样”是指反病毒、防火墙、入侵检测和漏洞评估等。而以扫描渗透评估加固、安全管理体系建设咨询为主要内容的安全服务也获得了大量的实践机会并逐渐成熟。

按照 IDC 的统计口径，2001 年国内安全产品的销售额为 1.295 亿美元，防火墙产品的销售额为 0.63 亿美元，占到中国网络安全产品市场的 48.9%；防病毒产品的市场份额达到 25.6%，其销售额达到 3310 万美元；入侵检测与漏洞评估产品的市场规模为 1730 万美元，其市场份额为 13.4%；网络 3A 产品的市场份额为 10.3%；而加密软件产品在中国安全产品市场上份额仅为 1.9%。

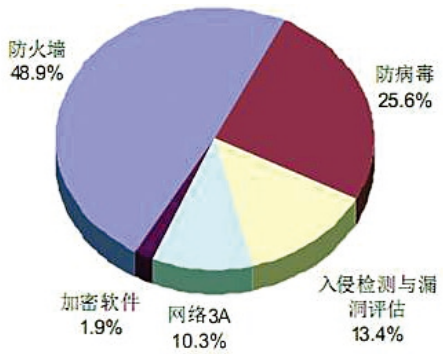


图 2 2001 年中国网络安全市场规模和分布（数据来源：IDC 2002）

作为对比，图 3 是 Gartner2003 年版的安全技术曲线，可以看到，同时期的国际市场上，MSSP（从技术上说，这就是国内正在快速上升期的安全管理中心 SOC）、IDS 都已走过“光环期”、进入“争议期”。

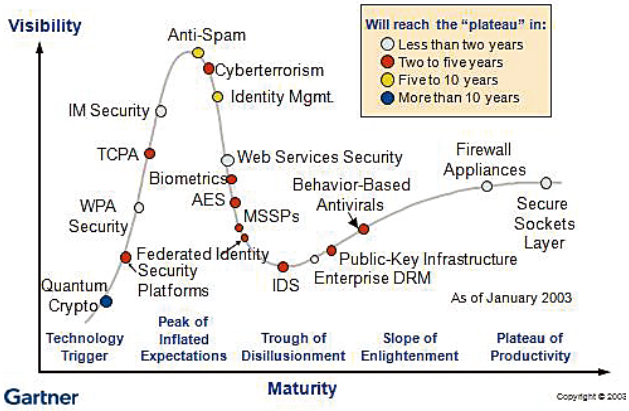


图 3 Gartner 安全技术演化图 2003

在此阶段，绿盟科技通过三年的摸爬滚打，逐步明确了自己的产品和竞争战略，建立了自己在安全专业服务、冰之眼 - 网络入侵检测、黑洞 - 抗拒绝服务、极光 - 远程安全评估等四个领域的国内领导者地位。这四个技术领域凝聚并见证了绿盟科技十年征途上的专注、成长和收获。

Security 2.0

2004 年到 2009 年上半年前后，该时期的重要市场活动是围绕着安全管理中心和 AAAA 为代表的安全运维实践的竞争。关于市场竞争的描述请参见笔者在 2005 年关于战国时代一文 [Warring]。

这是绿盟科技耕耘和收获的一个阶段，NIDS 产品逐渐成熟，成为国内市场的领导产品，并前瞻性地成功转向网络入侵防御系统 NIPS。在愈演愈烈的网络攻击威胁下，黑洞获得运营商和大型互联网数据中心的广泛认可，高端的流量清洗产品通过与运营商合作，进入安全运营管理 MSSP 市场，并在北京奥运会期间大放异彩。

这是绿盟科技承前启后的一个阶段，在技术和产品研发上持续投入和探索，在 Web 扫描和 Web 应用防火墙、企业安全计划 ESP、安全配置核查、安全审计、内容安全管理、桌面安全等方向推出了新产品。

这也是绿盟科技开始走向海外、实现蓝色梦想的一个重要阶段。在 2005 年绿盟科技产品获得 CVE 兼容性认证、2007 年获得西海岸 West Coast 产品认证、2008 年四月绿盟科技首次亮相美国 RSA 安全峰会……

此阶段业界有两个围绕着 IDS 和 UTM 的争论比较引人注目：IDS 技术走向何方？UTM 会成为防火墙、IPS/IDS/IDP、防毒墙等的终结者吗?

关于 IDS 的命运

从国际数据上看，在 1998 年到 2002 年间，IDS 的销售额大幅攀升，CSI/FBI 统计数据显示，IDS 的购买比例从 1998 年 43%，上升到了 2002 年的 73%。但是，另一方面，在 2003 年，国际上关于 IDS 前途的争论也已经如火如荼了，Gartner 在 2003 的报告中更是大胆预测了 IDS 和 IPS 的死刑 [GartnerIDS]。在 2004 年的技术走向 Hype 图中，大家可以清楚地看到赠与 IDS 的那个唯一的红色死亡标志。

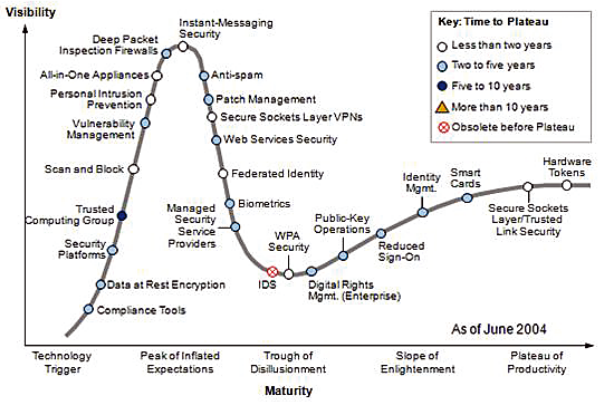


图 4 Gartner 在 2003-2004 年给 IDS 判了死刑

著名 IDS 开源软件 Snort 的作者、Sourcefire 的 CTO Martin Roesch 在 2005 年承认 IDS 技术的实际使用效果不太理想，例如告警太多、检测策略很难调优等，但是 Martin 认为通过不断优化检测技术、与漏洞检测关联等新技术，IDS 将会更加实用。

现在来看，Deborah Radcliff 在 2004 年发表的观点具有相当的前瞻性和透视力 [NWIDS] – “在线实时阻止的 IPS 将会在 2-3 年内逐渐超过检测模式的 IDS；IDS 逐渐成为更大的安全信息管理 SIM 框架的一部分，从而获得 SIM 系统更为强大的监视和报表能力的支持。然后，IDS 地位会逐渐下降，成为事后型取证分析等方面的工具，大概在 5 年左右的时间内，基于攻击签名的 IDS 将被融合后的合规性、终端和内核安全等产品替代”。在此话题上，Gartner 的预测被证明过于武断，“内网检测 + 边界阻止”双模式、相互补充和共存成为后来事实上的产品发展轨迹。

关于 UTM

UTM 自诞生之日起，争论就一直伴随着它。2004 年 IDC 首度提出“统一威胁管理”概念，同时将多种安全特性集成于一个硬件设备里，提供一项或多项安全功能。UTM 相关的定义和讨论大家可以在很多媒体发现。从下图笔者在 2006 年做的技术趋势分析上可以看到 [Trend2006]，UTM 正处于备受期待、光芒四射的顶部。但是，在后面几年的发展过程中，人们发现过于复杂的功能组合、性能方面不尽人意、管理运维方面的挑战等使得 UTM 无法承担关键核心网络的保护任务 [UTM]。

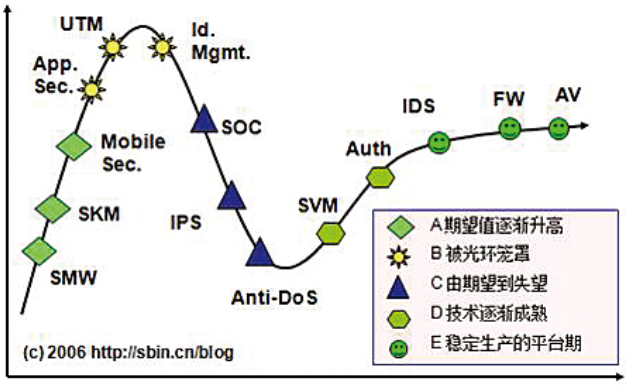


图 5 2006 年笔者关于安全技术趋势的分析

随着 UTM 的主力倡导者 Fortinet 在 2009 年 11 月成功上市，UTM 完成了一次成功表演。在此之前，防火墙技术成就了 Checkpoint、SonicWall(1999 年 11 月)、NetScreen(2001 年 12 月)，入侵检测和漏洞评估技术成就了 ISS(1998 年 3 月)、

Sourcefire(2007 年 3 月)，安全信息事件管理技术成就了 ArcSight（2007 年 9 月）。

Security NG

云计算的声音响彻 IT 业界，从 2009 年上半年开始，以 RSA 大会云安全联盟 CSA 成立为标志，云安全迅速成为业界的关注焦点。云安全有两种含义，它们分别是：

- 云自身的安全保护 Security for Cloud
- 使用云的形式提供和交付安全 Security from Cloud

关于云计算的定义和架构模型、云安全的架构模型等请参考云安全联盟的官方网站 [CSA] 以及最新发布的云安全指南 [CSASG]。云计算对安全产品的影响参见 [CSRoadmap]。可以预见，云计算将会对网络安全市场产生深远影响，从产品技术创新、营销、交付、支持等各个环节再造“适者生存”的传奇。

安全进入云时代，也是绿盟科技快速发展、冲入全球安全市场的一个阶段。2009 年 12 月，绿盟科技成为 CSA 在亚太地区的第一个企业成员，组织了云安全指南中文版项目 [CSASGCN]。在 2010 年的 RSA 大会上展出了独具特色的云安全解决方案，如图 6 所示。

在绿盟科技引以为豪的技术储备 - 知识库基础上，通过面向服务的架构 SOA，多种原子服务可以灵活地构架成为最为满足客户和伙伴需要的云服务或相对传统的交付形式，大幅提升产品情报互动、互操作能力，提升客户响应时间、性能和客户体验，降低客户整体拥有成本，同时能够降低公司的研发、制造和交付成本。

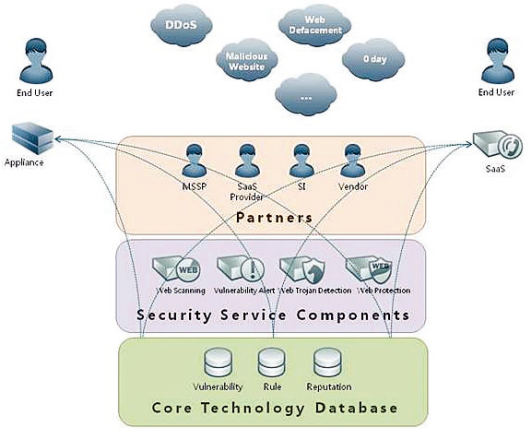


图 6 绿盟科技云时代安全架构图

“云”并不新，也不是“所有”，云代表的是一个新思维—面向互联网和创新的思维。欢迎您与绿盟科技一同关注云计算和云安全，并积极参与、引导、变革安全的未来。

3. 发展

中国的安全业界走过了重要的十年，防火墙、入侵检测、安全专业服务、安全管理中心 SOC、AAA/AAAA、应用安全、Web 安全、数据安全、云安全…… 回首这一个个脚印，我们希望理清发展的脉络，发现其内在的“导航仪”，希望能看清未来的方向。

本节希望通过四个话题的讨论和读者产生一些“脑力激荡”。

威胁的蔓延

从本质上说，安全威胁是安全业界得以产生、得以生存的原动力，

是网络攻防矛盾中最变化多端的一方。从每年各个权威机结构发布的威胁报告上，可以不断的阅读来发现人类的创造力和新思维。

安全发展的十年中，处于对立面的威胁方也完成了从孩童期到成熟期的发育，从单纯的好奇、挑战、成名等发展到基于投入回报 ROI 的、有组织的、具有很强针对性的入侵攻击。

在经济利益驱使下，为了获得更大的商业利益，网络安全威胁呈现了下面的一些特点，这些特点将会对安全保护技术的发展产生深远的影响:

- 应用越广泛的软件和系统遭到的入侵和破解也越严重，威胁方投入的资源也越大。
- Web 有关的安全威胁和漏洞已明显超过了传统的操作系统和设备。
- 利用“社会工程”的安全威胁和攻击入侵事件越来越频繁—“人”成为最难打“补丁”的一环。
- 安全威胁和攻击蔓延到信用卡处理中心、开发中心、下载中心等更容易产生超额“回报”的对象。而这些地方传统上被认为是“可信任的”。

关于边界的演化

从安全保护的角度看，来自威胁方的变化只是“动因”之一，另外一个很重要的考量就是互联网计算模式的改变。

大家从自己的切身体验可以知道，3G/4G 的用户在不远的将来肯定会迅速上升。漫游、移动用户肯定越来越多。大家发现企业 VPN 上的在线用户数迅速增加，边界安全策略越来越令人困扰、难以操作。大家忧心忡忡地谈及企业的传统边界正在逐渐被“销蚀”、甚至消亡。以防火墙为代表的传统边界防护方案在诞生二十多年后面临着越来越多的挑战。

“城墙”是一个很好的比喻，能帮助说明这个趋势可能是无法避免的。古代因为经济活动简单、城市规模很小，城墙加城门的架构很好的满足了安全和交通的需要。同时，没有一个现代城市是被围在城墙里的。分布式的视频监控系统、移动巡查系统、快速响应系统等使得城市的安全性和方便性获得新的平衡。

安全保护的焦点将会从基于 IP 为代表的位置（Where）转向数据和用户（What, Who）。因为，后者在新的时代更为“稳定”。

发展的驱动力

现在越来越多的人同意这个观点：安全的本质是管理，“七分管理、三分技术”。与成熟的企业管理理论相比，安全管理总是显得有点另类。至今关于企业安全管理的绩效考核仍然是一个热门的研究课题。下面几个例子是业界充满矛盾的一些地方：

- 发生安全事件并不代表安全管理失败；不发生安全事件也不代表安全管理成功。
- 如果以不发生安全事件作为目标，如何评价是否投资过度?
- 业界遵循的很多“最佳实践”却没有任何实实在在的数据证明这些“最佳实践”带来多少安全水平的提升，就像传统行业中汽车安全带、避雷针做的那样。
- 当前很多安全管理 OLA/SLA 是基于事务性的，而不是面向商业目标的。同时，找不到这些目标与商业目标之间的清楚而准确的关

系定义。

这些矛盾为未来安全业界提供了发展的契机。如何将网络空间中的安全活动以更加“可读”的方式呈现出来? 如何借给安全管理员“一双慧眼”让他更准确地发现网络空间的违规活动? 如何帮助安全管理建立起相对标准通行的度量指标体系? ……

在安全可视化、可度量、可管理方面的努力将会帮助安全管理活动获得更多的理解和商业支持，从而使其更健康、可持续的发展。

关于安全的未来

人类总是对未来充满好奇。我们也不会例外。在病毒木马僵尸地下经济愈演愈烈的黑云压城面前，安全技术和安全业界有没有能力有效地对抗威胁、保护社会和经济?

著名安全思想家 Bruce 认为网络安全如同社会，杀人盗窃等各种犯罪行为，从很久很久以前已经伴随着人类有数千年的历史了。虽然我们仍然无法根除甚至制止这些犯罪，但并不妨碍社会的发展和进步。我们虽然生活在有犯罪、并不安全的社会里，但没有关系，社会是有相当的弹性和自我恢复能力的 [Bruce]。

在此话题上 Gartner 有一个分析很有意思 [Security2013]。Gartner 依然采用传统的四象限分析法 – 横向维度是安全水平、纵向维度是安全控制水平，如图 7 所示。

- 从左下角开始，“道高一尺、魔高一丈”，安全技术无法提供更高的保护水平，“破坏总比建设和保护容易”，恶意黑客大量增多，网络陷入混乱和恐慌之中。
- 右下角，安全生命周期 SDL 大获成功，IT 系统内置网络安全保护措施异常强壮，可以防止任何网络空间的黑客攻击。
- 左上角，SDL 不甚理想，一次又一次不断提升的网络攻击，迫使 IT 和安全厂商不停地提升安全保护能力，双方陷入拉锯战和持久的军备竞赛。
- 右上角，“魔高一尺、道高一丈”，安全技术处处占得先机，成功的 SDL 使得 IT 系统坚不可摧，使得网络攻击和“黑客”成为传说。

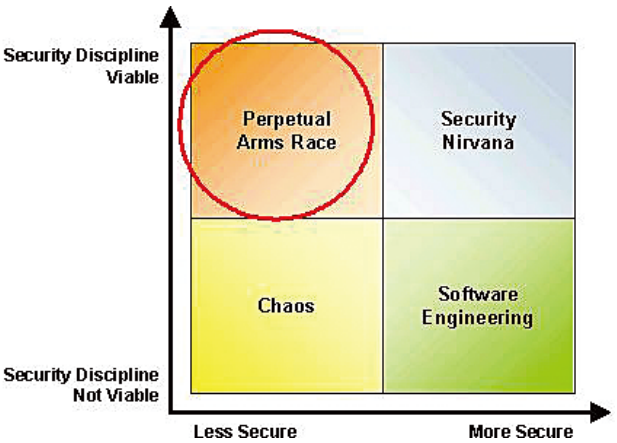


图 7 Gartner 关于安全未来的分析

面对这样的四个象限，不知道您心中会选择哪个未来?

Gartner 的观点是红圈左上角—军备竞赛，也就是说，选择了与 Bruce 类似的观点，攻防生态环境会维持微妙的平衡。安全业界的未来既不会好风凭借力，直上云霄、也不会秋风萧瑟两不知。

4. 反思与动议

总体来说，中国网络安全市场规模偏小，发展偏慢，整个市场在 2009 年的营收规模大概为百亿元左右。与国际市场相比，

McAfee 一家公司在 2008 财年的营收就有 16 亿美元；与国内的互联网和网游业相比，根据 2010 年初文化部发布的《2009 年中国网络游戏市场白皮书》[NetGame]，2009 年中国网络游戏市场规模为 258 亿元人民币，同比增长 39.5%。腾讯公司在 2009 年的全年营收达 124.4 亿元，其中单网游业务的收入就达 54 亿元 [qq]。

笔者无意在此评价国家在网游方面可能存在的政策导向，以及网游带来的消极社会效应，而是希望通过对市场和技术的反思总结，更有针对性地协作努力为网络安全的健康发展做出积极贡献。

提倡分享与协作

我们经常痛苦的发现我们国内的论坛上，不管是社会方面的、还是技术领域的，很多论坛会流于灌水、相互的攻击和谩骂等，能够冷静地、心平气和地坐下来就技术讨论技术的论坛、邮件列表属于凤毛麟角。而在国外的技术论坛和列表中，有不少订户和成员来自国内，却很少看到来自国内用户的贡献。在此表面下，隐藏着的是国内业界在互动互操作、标准化、信息共享等协作方面和发达国家之间存在的巨大差距。这个差距伤害了中国业界的技术创新能力和发展能力，同时也非常不利于从业者的个人提高。

举个简单的例子，国内围绕着 ISO27001 系列提供安全服务的机构不在少数，可是如果通过 Google 查询 “ISO27001 安全 ”，查询普通网页的结果可以发现一些国内新闻媒体浮夸的市场报到，如果查询 PDF/PPT/DOC 等相对高质量的原创内容时，能够得到的大都是台湾和香港同胞的贡献。

引用一个说法：若要走得快，一个人走；若要走得远，一起走。网络安全行业需要更多的共享和协作! 更多的 “我共享、我成就、共同发展” 的精神!

加强数据收集和积累

在 “发展驱动力” 一节已经提到，安全业界普遍匮乏实际的运营指标、运营记录、安全事件、事件根源分析等基础数据，众多的所谓 “最佳实践” 是建立在各种调查问卷和安全顾问、专家的个人经验和观察上的。我们知道，这些调查问卷大都没有公开调查问卷的问题设计、答卷人的分布和选择过程、分析过程等，经常看到各种调查问卷结果之间的相互矛盾和冲突，结果并不十分可信。

为此，笔者呼呼政府主管部门和服务支持共建单位等一起，持续地收集整理分析并公开重要安全事件的过程、根源分析以及经验教训。这样，在漏洞库之外，安全事件经验库将会为企业、组织、IT 管理层、CISO/CSO/ 安全经理和架构师们提供大量的、更多实际行动指南的 “宝典”，也会非常有效地校准安全 “最佳实践” 和现有的安全标准和规范。

提高安全标准开发过程中的开放性、加强持续改进

当前，在某种程度上，我们是国外安全标准的 “消费国”，我们在安全标准框架等方面还比较依赖国外组织和同行，在相关开发过程中比较被动，很少或者基本上没有参与。这一点在整个亚太地区较为明显。掌握标准代表着对未来的主导权和话语权。一方面重视并积极参与国际范围内相关安全标准的研究和开发活动，同时，另一方面，我们需要敞开胸怀，借鉴国外先进的标准开发模式和应用过程中的经验教训，而不仅仅是引入标准的文档条文。

PCI-DSS 是目前国际上最受关注的安全标准之一，它覆盖银行、电子商务、在线支付等众多领域 [PCIDSS]。自 1996 年 9 月份发布 PCI-DSS v1.1 到 2008 年 12 月发布 v1.2，PCI-DSS 获得广泛的支持和推广部署，其标准机构 SSC 倾力打造了一个开放的生态环境 – 标准的开发委员会、授权扫描商 ASV、合格安全审核师 QSA、每两年一个循环的标准升级系统等等。

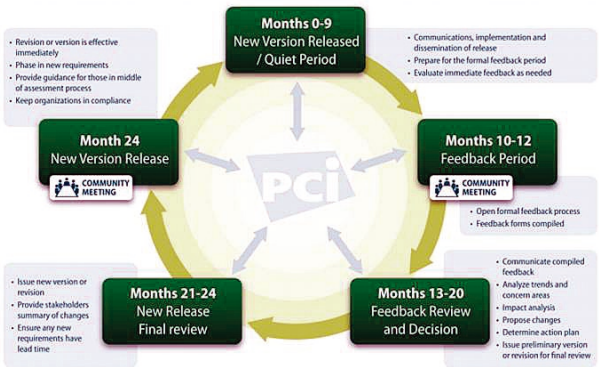


图 8 PCI-DSS 标准定期审核升级系统

另一方面，随着几次重要安全事件的爆发，业界对 PCI-DSS 的质疑也不绝于耳 [Register]，尤其是发生于 2009 年 1 月份的 Heartland 信用卡资料被窃事件。由于 Heartland 刚刚通过 PCI-DSS 的审查，所以，在 Heartland 因为该安全事件而损失惨重的同时 [Heartland]，PCI-DSS 的权威性、信用卡处理商、授权审核师 QSA、PCI 标准机构 SSC 之间的责任划分等受到很大争议。另外，标准中模糊不清的地方、实施过程中的成本过高、一刀切等问题也被广泛提到。

希望以上面 PCI-DSS 成功的做法和教训为例，对业界在像等级保护、网上银行系统信息安全通用规范等诸多标准开发活动提供参考。

参考文献和链接

[SecHis] http://www.chinabyte.com/cbspecialnocss/467/8645467.shtml

[PC]http://zh.wikipedia.org/zh-cn/%E4%B8%AA%E4%BA%BA%E7%94%B5%E8%84%91

[IDS] http://www.sans.org/reading_room/whitepapers/detection/the_history_and_evolution_of_intrusion_detection_344?show=344.php&cat=detection

[Telecomsec2006] http://www.cnii.com.cn/cniizt/2006dxhywlxxaqgllt/index.htm

[Security0.1] http://sbin.cn/blog/2006/05/10/go-security-20/

[Intro] http://www.studa.net/jingji/090910/14184019.html

[Warring] http://sbin.cn/blog/2005/12/29/china-security-warring-wtates-period-final/

[Trend2006] http://sbin.cn/blog/2006/01/13/security-trends-2006/

[GartnerIDS] http://www.softpanorama.org/Security/Whitepapers/ids_roadmap.shtml

[NWIDS] http://www.networkworld.com/research/2004/110804ids.html?page=1

[UTM] http://sbin.cn/blog/2008/11/07/firewall-utm-ips/

[CSA]http://cloudsecurityalliance.org

[CSASG] http://www.cloudsecurityalliance.org/csaguide.pdf

[CSRoadmap] http://sbin.cn/blog/2009/06/01/cloud-computing-1/

[Bruce] http://sbin.cn/blog/2009/02/04/2009security/

[Security2013]http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&id=979112&ref=g_BETAnoreg

[NetGame] http://news.ccidnet.com/art/1032/20100119/1982751_1.html

[qq] http://game.people.com.cn/GB/48644/48662/11167211.html

[NewSchool] Adam Shostack, Andrew Stewart, "The New School of Information Security", Addison-Wesley, 2008

[PCIDSS] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[Register] http://www.theregister.co.uk/2009/09/23/data_security_survey/

[Heartland] http://www.ctg.com/infosecurity/pdf/security_insights_feb_2009-musing-on-heartland-breach.pdf

[CSASGCN] http://www.cloudsecurityalliance.org/guidance/csaguide-cn.v2.1.pdf

十年回望之漏洞扫描与检测

产品管理中心　李晨

摘要：脆弱性（漏洞）是引发信息安全问题的重要原因之一，脆弱性检测产品是一种针对系统、设备、应用的脆弱性进行自动化检测的工具，广泛应用于信息系统安全建设和维护工作，成为度量信息系统风险的一种基础手段。本文回顾了绿盟科技核心产品线——脆弱性检测类产品线这十年的发展历程，并结合信息安全的发展变化，对未来风险检测类技术及产品的发展趋势进行论述。

关键词：信息安全　漏洞扫描　风险评估　法规遵从　风险管理

伴随着绿盟科技的成长，绿盟脆弱性检测类产品线不断发展、创新，目前已经成为业界的领导品牌。其中业内最为熟知的绿盟远程安全评估系统（原名“极光”远程安全评估系统）早在公司成立时就已经研发，其 V1.0、V2.0 版本是绿盟科技在为客户实施风险评估项目中所使用的扫描工具。2001 年 3 月 10 日，绿盟远程安全评估系统的第一个商业版本正式面世，推出了全球首款基于嵌入式 BSD 系统的硬件安全扫描设备。十年来，绿盟远程安全评估系统获得了市场的广泛认可，荣获诸多殊荣。2004 年底，在某运营商集团网络安全漏洞扫描器产品测试中，该产品从七家厂商的送测产品中脱颖而出，获得第一名的成绩；此外，产品于 2008 年 3 月成为亚太地区惟一一款获得 WestCoast Labs（西海岸实验室）认证的 Vulnerability Assessment 类产品。

历经十年的不间断技术创新和产品研发，目前绿盟科技已经跻身全球漏洞扫描产品的领导厂商之一，绿盟远程安全评估系统已经成为这一领域的领导品牌，得到运营商、金融、互联网、政府机构、大中型企业以及风险测评机构等用户的广泛认可，绿盟科技也成为国内惟一一家能够面向全行业用户提供多层次漏洞管理解决方案的专业厂商。

辉煌十年

新生

2001 年 3 月 10 日绿盟科技第一款商用漏洞扫描器——极光远程安全评估系统（NSFOCUS Aurora RSAS）3.0 版本发布。当时全球漏洞扫描器产品还处于起步阶段，以 Nessus 为代表的漏洞扫描工具软件特别流行。但是，Nessus 运行于 Linux 系统环境中，安装和操作都较为复杂，性能也无法满足大网的评估需求。极光远程安全评估系统定位于帮助管理员完成对大网段主机系统的快速评估，其利用远程扫描技术收集和测试网络的信息和远程系统安全漏洞，以发现网络潜在风险。相对于软件的扫描工具，其简易的操作和直观的报告尤其得到用户的喜爱。产品具备几个当时最为领先的技术特点：

1. 基于嵌入式 BSD 系统的硬件安全扫描设备。提高性能、稳定性和自身安全性，适合大网评估，大大地的提高了用户的工作效率。

2. 即插即扫。用户只需将扫描设备连入网络，作少量设置就可以开始检测，并且还可自定义扫描计划。

3.B/S 架构，提供安全 HTTP（SSL）的远程管理。通过 HTTPS 的远程安全管理，

用户无需安装任何管理软件，即可操作和管理扫描器设备。

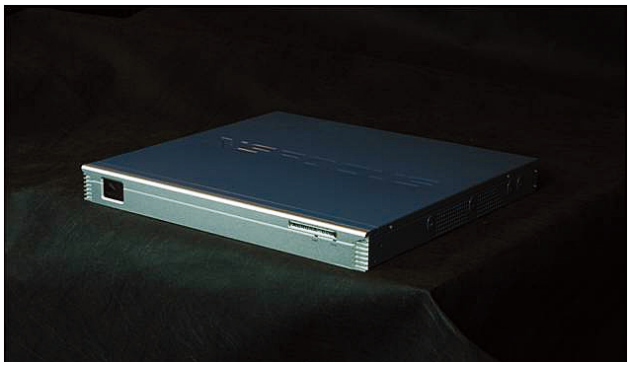


图 1 第一款绿盟远程安全评估系统

初露锋芒

某运营商集团为加强网络与信息安全工作，于 2004 年底组织了七家安全厂商的漏洞扫描器产品测试，其中不乏国际知名的安全厂商，如美国 ISS 公司。这次测试内容涵盖了功能测试、漏洞扫描能力测试、性能测试等多项测试指标，最终极光远程安全评估系统获得综合排名第一的好成绩，取得了客户的认可，这也充分证明了这款产品的优异性能。

修炼

2006 年 7 月 11 日，绿盟远程安全评估系统 V4.0 发布，该版本结合安全技术发展，风险管理方式的变化情况，完成漏洞扫描工具到安全评估专家系统的转变。该版本最值得关注的是提供 Open VM(Open Vulnerability Management 开放漏洞管理) 工作流程平台。以往的漏洞扫描产品只是定位在评估工具，能扫描出漏洞但并不能反映客户环境中资产的真实风险状况，无法将 IT 资产的漏洞从发现到消除进行闭环。通过 Open VM 工作流程平台，以资产为核心，将资产、漏洞和威胁紧密结合，把漏洞生命周期管理的循环过程划分为漏洞预警、漏洞检测、风险管理、漏洞修复、漏洞审计五个阶段，将先进的漏洞管理理念贯穿于整个产品实现过程之中，形成资产风险可管、可控。

出关

2008 年 3 月 10 日，绿盟远程安全评估系统一举获得英国西海岸实验室（West Coast Labs）的权威认证，同时也是亚太地区漏洞扫描产品首次通过西海岸实验室的认证 。之前，从 1996 年至今，全球只有 IBM（ISS）、McAfee 等五家企业通过实验室 Vulnerability Assessment 类产品的认证。

在严格的测试中，绿盟科技安全产品的表现和国际顶尖公司的产品相比毫不逊色。成熟的技术优势、完善的功能应用、稳定的系统给实验室的专家们留下了极为深刻的印象。该认证的通过，标志着绿盟科技漏洞扫描核心技术已达到世界水平。通过了全球的权威认证，拿到了国际化的品质保证书和市场通行证，走出了迈向国际市场的第一步。

冲天

2008 年 6 月 6 日，绿盟远程安全评估系统发布划时代的版本——V5.0。

V5.0 侧重对网络风险进行全方位管理和分析，网管员可以对所有信息资产设备进行资产风险管理。对于大规模网络用户，由于网

图 2 绿盟科技开放漏洞管理 Open VM 过程图

络资产繁多、IP 地址记忆非常繁琐，绿盟远程安全评估系统以资产为核心，通过资产管理与用户组织结构或网络拓扑结构的紧密结合，进一步优化了漏洞管理的流程，更加符合企业客户的漏洞管理需求。

针对 Web 应用安全检查的需求，V5.0 创新地融入了 Web 应用安全漏洞的扫描功能。综合应用了很多业内领先的技术，如模拟点击智能爬虫技术、主动挂马检测及核心调度引擎，为用户提供精准的检测结果及最高效的检测效率。可以应用于网站管理员进行 Web 上线前安全测试、上线后周期性安全评估以及企业安全管理员进行统一的风险监控与管理。相比传统 Web 扫描器仅局限于提供 Web 应用层的漏洞扫描，该产品能够为 Web 应用系统提供最为全面的漏洞检测范围，包含 Web 应用（SQL 注入漏洞、跨站脚本漏洞、CGI 漏洞，以及网页挂马等漏洞）、Web 服务及支撑系统（网络层、操作系统层、数据库）等多层次全方位的安全漏洞扫描、审计、渗透测试和辅助逻辑分析。


Product
Certification
NSFocus
westcoast labs

图 3 West Coast Labs 认证证书

再展凌云志

2008 年 11 月 17 日，绿盟脆弱性检测产品线发布国内第一款专门针对安全配置检查与管理的产品——绿盟安全配置核查系统。

随着信息系统的网元设备越来越多，网络结构越来越复杂，因此对大量不同种类的网元设备进行统一规范的配置，并有效的检查与管理，就成为了安全运维人员面临的新问题和新挑战。

针对上述需求，绿盟科技推出了业内首款专注于“业务安全配

置检测与管理”的新产品——绿盟安全配置核查系统（NSFOCUS BVS）。该产品具备完善的安全配置库，并可以实现对网络资产设备自动化的安全配置检测、分析。该系统的应用，大大提高安全配置检查的方便性、准确性，在节省时间成本的同时，让安全配置维护工作变得有条不紊而且简单、易于操作。该产品的推出，进一步完善了绿盟科技以资产为核心的脆弱性安全管理整体解决方案，并填补了国内该领域内空白。

展望

脆弱性检测与管理是一项极具挑战的课题，是信息安全工作过程中治本的方式，只有通过对风险的控制与消除才能从根源上消除安全威胁。面临千变万化的攻击手法，，单纯采取被动防御的技术手段越发显得力不从心，更多的用户开始关注风险的管理与度量，侧重在“事前”尽量降低甚至规避风险，因此脆弱性检测将在信息安全技术发展的下个十年扮演越来越重要的角色。结合安全趋势和用户信息建设的变化，笔者认为脆弱性检测与管理将会有如下几个发展趋势：

检测技术的转变

1. 传统系统漏洞检测向应用漏洞扫描转变

近年来不断发展和广泛应用的各种应用系统中存在的安全漏洞也越来越多的被披露出来，攻击者从关注操作系统的漏洞向应用漏洞转变。针对应用的攻击技术相对简单，影响范围大，特别是近几年针对 Web 应用安全漏洞的攻击逐渐成为主流的攻击方式。利用网站操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等，黑客能够得到 Web 服务器的控制权限，从而轻易篡改网页内容或者窃取重要内部数据，甚至在网页中植入恶意代码（俗称“网页挂马”），使得众多网站访问者受到侵害。因此漏洞扫描器将会着力研究并迅速发展针对 Web、数据库等重要应用的检测能力。

2. 检测引擎平台化，支持扫描插件的用户扩展性

漏洞检测产品的核心技术是检测方法，即使用插件或者叫做扫描模块技术。每个插件都封装一个或者多个漏洞的测试手段，主扫描程序通过调用插件的方法来执行扫描。面对大量不同应用的检测需求，仅仅依靠扫描产品厂商对漏洞的研究将不能够支撑用户的使用需求。因此，需要扫描器具有非常强的扩展性，支持灵活添加新的插件以便增加新的漏洞检测方式。在插件编写规范公布的情况下，由用户或者第三方公司甚至可以自己编写插件来扩充软件的功能。同时这种技术还使得软件的升级维护都变得相对简单。

3. 源代码审计将成为脆弱性检测产品类别里的新兴产品

大部分的漏洞扫描器都是针对上线后，即以黑盒方式对已经完成开发的系统进行渗透测试。而自动的源代码分析是在生命周期早期安全性测试的最有效的方法，因为它允许在不需要完全的应用程序的情况下，对任意代码段进行评估。通过在所涉及的代码中精确查明弱点，以及详述有关缺点的类型、关键的程度，以及如何修补它的信息，来提供最有价值的结果，以形成更高质量的产品并降低应用程序整个生命周期的成本。风险检测类产品将涵盖该类型技术，更注重“事前”根源的预防。

4. 传统漏洞的检测向业务逻辑的检测转变

业务系统越来越庞大，业务逻辑也越发复杂，很多的攻击手法都不再是针对底层系统漏洞，而是利用系统在设计时考虑不周的逻辑错误进行攻击。由于业务逻辑的关注点主要集中在业务规则的制定、业务流程的实现等与业务需求有关的系统设计，业务逻辑的设计错误，隐含的风险漏洞都将对系统的可靠运行产生致命的影响。因此如何检测逻辑错误，并呈现攻击路径，将是检测类产品的技术发展中的一个非常有挑战性的转变。

应用及管理方式的转变

1. 独立的评估工具向大规模部署，集中监控管理、整体度量转变

“数据集中”、“统一管理”都是现在信息化建设的主要思想。特别是一些规模较大的传统企业，由于其组织结构复杂、分布点多、更需要整合资源，统一监管。以前的脆弱性检测产品基本都是用于单个网络的评估，数据相对分散，不能够满足大范围的脆弱性评估与度量。因此采用使用大规模分布式部署扫描引擎，多台扫描引擎协同工作，下级单位利用自己的扫描器来维护自己网络的安全，同时由于所有的扫描结果都发送到上级单位，由管理监控中心统一监管，这样总部就能直接了解到整体网络的安全情况，可对各系统间的数据共享并汇总，方便形成全网络、全系统各级单位的统一风险分析和管理。

2. 产品提供向服务提供转变

中小企业安全维护人员相对较少，精力相对有限，但是脆弱性管理是企业信息系统维护管理中必不可少的部分，因此越来越多的中小企业选择采用脆弱性评估服务的方式，即 Security as a Service。越来越多的传统漏洞管理厂商也利用自己的核心技术和服务为客户提供基于可托管式的漏洞管理服务。这种服务的一个最大的特点就是基于“云”端，采用透明模式，用户无需购买设备，无需改变网络结构，并且帮助用户节省人力成本。

3. 单纯脆弱性检测向法规遵从管理转变

全球各地的政府机构、企业都面临着监管者提出的法规遵从性要求，更多的用户正在为不能有效地根据法规要求进行信息系统的风险管理，并在为如何证明自己遵从法规而忧虑。“合规”已经成为企业最为重要的日常工作。作为针对脆弱性进行度量管理的工具，脆弱性检测产品帮助企业安全管理者实现内外部 IT 审核自动化，摆脱繁琐的手工操作与面对面的问答，轻松实现风险管理与合规性遵从。

小结

可以预见，脆弱性检测与管理作为企业安全建设中一项日益重要的工作，必将以其特殊性、重要性在信息安全建设的各个方面、各个阶段发挥越来越重要的作用。

绿盟科技根据多年来对脆弱性检测与管理的理解，提出结合资产的脆弱性管理理念，从漏洞管理、策略管理、配置管理等多方面进行脆弱性的检测，面向目标类型提供了系统扫描、应用扫描等检测能力，最终形成整体脆弱性管理与遵从性度量的整体解决方案，帮助用户进行预警、监测、度量、审计的精细化安全风险管理。

历经十年的不间断技术创新和产品研发，绿盟风险检测类产品已经发展到多个系列，多种应用模式的产品组合，并成为国内市场第一品牌。绿盟科技已经跻身全球漏洞扫描产品的领导厂商之一，成为国内惟一一家能够面向全行业用户提供多层次脆弱性管理解决方案的专业厂商。

十年回望之黑洞那些事儿

产品管理中心　崔云鹏

摘要：自上市以来，绿盟黑洞抗拒绝服务攻击产品已经有 8 年历史了，作为国内最早的抗拒绝服务产品，黑洞经历了国内抗 DDoS 的大部分事件，期间有不少令人难忘的故事，特撰文为黑洞做一个简单的回忆录。

关键词：抗拒绝服务攻击　DDoS

很不好意思，用了如此一个很“山寨”的题目，特别是写黑洞的时候，这个题目是有可能冒黑洞开发团队之大不韪的，他们引以为豪的是那些很技术、很原创的东西。抄袭，可以，但是，请远离黑洞。但今天，实在是不想写太技术的东西，只想写一些故事，关于黑洞的故事，并且，说起黑洞，至少在抗拒绝服务攻击的领域里，那是有些时间的产品了，抄袭一个历史畅销书的题目，其实也符合本文的主旨。

先介绍一下黑洞，黑洞是绿盟抗拒绝服务攻击（DDoS）的产品名字，也称为 ADS（Anti-DDoS System），是专门用于清洗网络上 DDoS 攻击的一款硬件设备。网络上大量泛滥的拒绝服务攻击，可以轻易的让 WEB、DNS 等应用的服务器、路由器甚至网络链路阻塞和瘫痪，因此，架设在网络出口的黑洞，将那些恶意流量精确的除掉，只让正常的访问流量进入，成了黑洞的主要功能。

黑洞的生日是 2002 年 10 月 25 日，比绿盟科技公司小了将近 2 岁，不过要是把前面将近两年的对 DDoS 攻击算法的研究和产品开发的时间算上，黑洞今天倒也有理由庆祝一下自己的十周年纪念日了。2002 年，在中国，大部分人都还是用电话线模拟拨号上网，大家对于网络安全，最多停留在安装杀毒软件的级别上，今天已经耳熟能详的网络硬件防火墙在当时也是个新东西，至于黑洞这种专业抗 DDoS 的硬件设备，则更是只有安全专家才能搞清楚了。

事实上，在那个时候，在国内市面上，绿盟科技的黑洞是没有同类产品的，很多时候，遭遇拒绝服务攻击的用户会直接电话找到绿盟，希望借一台设备临时顶一下。绿盟黑洞产品线经理叶晓虎，经常会回忆起当时的情况，那时绿盟科技的开发人员同时也做着技术支持的工作，叶晓虎就经常亲自扛着一台非常笨重的黑洞设备，跑到用户的机房，将设备安装上线，调试好。“很多服务器被拒绝服务攻击缠上，非常麻烦，一天 24 小时，没完没了的打，服务器要么就是关机，要么就是在那里半死不活，那些维护工程师非常头痛”，“我们设备一上线，服务器就活了，效果非常明显”，“就因为我们帮忙解决攻击，以前都是用户请我吃饭的”，叶晓虎经常会回忆那段令人激动的时刻。

可惜的是，黑洞组没有留下最早的产品照片，也没有留下样机，不过，在绿盟科技的生产中心，在备件库里，笔者找到了 2003 年左右的黑洞，拍了照片。（顺便表扬一下生产中心的同事，2003 年的产品，可能使用这个产品的用户早就把旧设备淘汰了，但是按照绿盟科技的备件维修内部规范，生产中心依旧规规矩矩地留存备件，就这点来

说，可能很多厂商是做不到的。）

图 1 早期的绿盟黑洞产品图片

设备给人一种很沧桑、很古老的感觉，很重，一个人搬起来非常吃力，仔细看一下，上面竟然还有个 3.5 寸软盘驱动器。据说这台早期的黑洞相当原始，就有几种防攻击算法，处理性能在现在看来也是小的可怜—10Mbps 流量级别的。但就是这台古董级设备，当年不知挡住了多少次拒绝服务攻击，让那些黑客们摸不着头脑，不知道为什么百试百灵的攻击手段，突然失灵了。

黑洞上市后，很长一段时期，在网络安全的论坛上，黑洞经常就等同于抗 DDoS 产品，黑洞经常也等同于抗 DDoS 技术，很多网友会在网站上发表自己对黑洞、对抗 DDoS 算法的理解，例如有人很严肃地讨论黑洞的反向探测技术，并且写到（原文大意如此）：“黑洞不断向流量的来向发送大量的反向数据，将来向数据报文消灭掉……”。文中描述的黑洞，给人的感觉不像是一台网络安全设备，倒是更像是一台天文物理学的正负粒子对撞机，正在制造正负质子的对撞和湮灭。事实上，绿盟黑洞是有反向探测技术的，但是无法像帖中所述消灭已经发送过来的 DDoS 报文，只是经过反向探测，可以明确区分正常报文和恶意报文，从而在后续的处理中，非常高效而准确地丢弃恶意报文，放行正常报文，只是，这绝不是正负质子的关系。

当然，除去这些轶闻趣事，也有很多对黑洞的恶意研究。黑客论坛上，不断有人公布自己的发现，宣称他们发现了黑洞的弱点，反向推测黑洞的抗 DDoS 算法，并且研讨在黑洞防护下的攻击改进方法。面对这些，有时黑洞研发人员一笑而过，但也有些时候，绿盟的黑洞也面对非常棘手的一个又一个挑战。

这些挑战里面，最著名的就是 CC 攻击了，事实上，CC 攻击最直观的名字应该叫做 Http Get Flood 攻击，它是专门针对 WEB 服务器，由大量的代理服务器或者僵尸主机对 WEB 服务器发起，不断对某个页面进行 Http Get 请求，消耗 WEB 服务器的资源，最终导致 WEB 服务器无法响应正常用户的请求。

但是这类攻击却被称为 CC 攻击—Challenge Collapsar，挑战黑洞，在 DDoS 攻击领域，Collapsar 黑洞就是绿盟的抗拒绝服务产品。事实上，CC 也是黑客在利用新的攻击向抗 DDoS 厂商发起挑战 : 你能战胜我们吗?

早期绿盟黑洞的防护算法大多集中在抗四层攻击上，如著名的 SYN Flood 攻击, 以及其他一些类型如 UDP Flood、ICMP Flood 等，对于应用层攻击，特别是不再伪造 IP 地址的真实主机访问，很难区分每个报文的真伪，而且随着 CC 攻击工具的发展，报文的特征字段几乎不再存在，传统的特征库的作用也越来越小。直到今天，对于防火墙、IPS 等一般安全产品，CC 等应用级别的 DDoS 依旧是

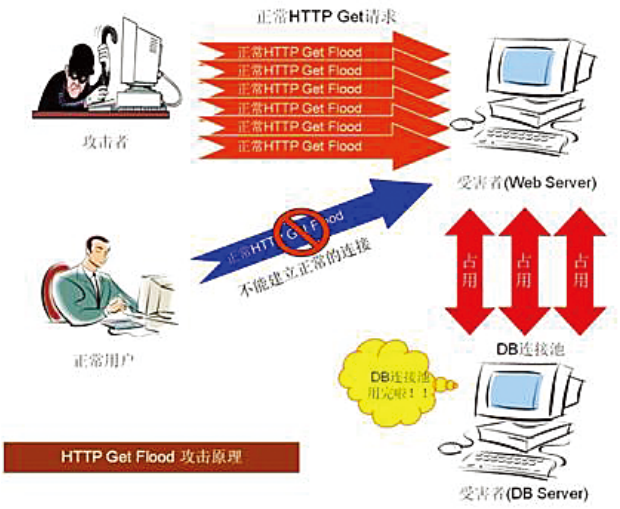


图 2 CC 攻击原理示意图

一个很难解决的难题，因此 CC 以及其变形攻击也至今是黑客的重要 DDoS 攻击手段。

还好，经历过前期一段束手无策后，黑洞很快找到了应对 CC 攻击的算法，而且随着 CC 攻击手法的变化，黑洞自身的防护算法不断改进，到今天为止，绿盟黑洞的抗 CC 防护算法已经有 6 种，用户可以根据自己实际的情况，选择任何一种方便的方式进行防护，CC 对于黑洞来说，已经不再是挑战了，只有 CC 的名字，依旧记录了那段攻防双方的博弈经历。

当然，挑战也不都全是来自黑客攻击者，也有来自同行业产品的竞争、技术对比测试。最让黑洞产品难忘的一次是在 2006 年，东南某省电信的产品对比测试，除了绿盟科技的黑洞，竞争对手全部来自美国，都是著名的抗 DDoS 公司：IPS 厂商 R 公司、IPS 厂商 T 公司、网络厂商 C 公司、以及病毒厂商 M 公司。特别是 R 公司，更是由亚太区技术总监亲自从香港赶来压阵，但最终看到的却是黑洞的完胜。当然，那位技术总监也没有白来，在黑洞测试 ICMP Flooding 等几个防护的过程中，他用手机悄悄地拍下了黑洞的测试界面，因为对于这些攻击的防护，R 公司只顶住了其标称值的 20% 流量。黑洞的开发人员也终于发现，原来，在网络高科技领域，也有很多美国公司需要努力赶超中国厂商的时候，只是，那些内置的防护算法的功效，如何能用手机拍摄获得?

时间一天天过去，绿盟科技的黑洞也继续用自己的防护效果去赢得用户的信任，并且在业内传递着黑洞的口碑。黑洞在电信运营商、银行、证券、互联网、政务办公网，都有着国内最广泛的应用。在北京奥运会、六十周年国庆、在国家级领导人同网友对话等重大事件中，都有绿盟科技的黑洞产品在默默看护着网络的安全。很多用户，在黑洞防护住攻击后，给绿盟科技技术人员致以感谢和赞赏。其实，依我看来，黑洞产品的防护效果应该首先感谢这些使用黑洞的用户，正是由于这些分布全国、遍布各个行业的广泛的应用和复杂的网络环境，使得黑洞每天都在面对各种各样的新型 DDoS 攻击，遍布全国的黑洞部署也成了绿盟科技的发现、收集新型 DDoS 攻击的巨大平台，几乎任何一种新出现的 DDoS 攻击，都会很快反映到全国的某些黑洞上，为黑洞研发人员提供算法研究的素材，并督促黑洞研发人员快速改进算法，提高防护效果。

抗 DDoS 防护算法成了绿盟黑洞的最宝贵的资本，这不同于做

路由器和应用服务，可以根据 RFC 规定做路由协议，或者根据用户的需求分析可完成应用的开发。对于黑客攻防产品、特别是 DDoS 攻防的算法，有时候，防护算法的小小一个字节的不同，对于整个防护效果则是差之千里，而对攻防的算法的效果提升，是没有什么文档可以依赖的，只能立足于广泛的攻防积累，没有时间、没有大量的客户群，黑洞无法达到其现在的防护能力，从这点来说，黑洞是应该真心感谢那些使用黑洞的客户的。

有了 DDoS 防护算法的核心技术，绿盟科技的黑洞产品线也在不断的壮大，在抗 DDoS 领域，黑洞传统的抗 DDoS 清洗设备，拥有了最全的产品系列——从最低端百兆级别的企业级清洗设备，到电信级的数10G 清洗能力的高端集群设备；流量检测分析领域，推出了专业的 NTA 流量分析产品；在僵尸网络发现领域，推出了蜜罐系统，自动捕获那些恶意攻击者和被感染的僵尸主机。全面的产品能力，让绿盟科技可以进一步为行业客户提供完善的抗 DDoS 流量清洗解决方案，在运营商，借助旁路算法技术，借助流量牵引技术，借助流量回注技术，形成了安全岛解决方案；在骨干网络中，建立一个以黑洞为核心的安全岛屿，任何的异常流量都要进入这个安全岛内部去审核一遍，清除异常，让正常访问畅通无阻……

很多时候，绿盟给人的印象就是一个低调的技术型厂商，只是，从长远来看，无论对于任何一个安全产品，技术才应该是最终极、最好的营销宣传手段。绿盟科技用自己这些年的积累，凭借这些抗 DDoS 技术，未来的一段时间里，黑洞能继续做中国最好的抗 DDoS 清洗产品，让绿盟再多几件黑洞那些事儿。

十年回望之入侵检测与防御

产品管理中心 陈星霖

摘要：国内安全市场从 2000 年起到现在，已经跨过了十个年头，而入侵检测产品（IDS）是许多安全公司进入这个市场最初的产品。本文将回顾这十年来，在入侵检测及防御领域中重要的历史时刻，同时针对未来该领域的发展进行展望，并简要回顾了在不同时间段中绿盟科技的入侵检测及防御产品的发展历程。

关键词：NSFOCUS 绿盟科技 入侵检测 入侵防御 IDS IPS NSS Labs

2010 年 3 月 31 日，绿盟科技对外宣布，其入侵防御系统（NSFOCUS IPS）顺利通过国际权威机构 NSS Labs 的严格测试，荣获 NSS Labs Approved 认证，并且被 NSS Labs 认定为最高级别“Recommended”，由此，绿盟科技自主研发的 IPS 产品成为国内安全厂商中惟一获得该权威机构认证的产品。历经十年磨砺，NSFOCUS IPS 实现跨越，进入国际顶尖产品行列。

十年前，诸多安全公司选择了 IDS 产品作为进入国内安全市场的第一款安全产品；十年后，大浪淘沙，业内知名的 IDS 产品并不多了，这十年发生了什么？未来十年又会怎样……

过去的十年

冰冻三尺非一日之寒，无论哪个产品，能在十年的竞争中获得优势，一定与其在这个领域的执着和专注密不可分。

市场萌芽，IDS 产品成为安全市场的敲门砖

2000 年至 2004 年期间，各种蠕虫病毒大肆爆发，红色代码、尼姆达、冲击波，震荡波此起彼伏，它们的各种变种程序更是层出不穷，在互联网上任意肆虐。面对上述基于正常端口工作的蠕虫病毒，传统的防火墙（Firewall）显得束手无策，而入侵检测系统（IDS）则能够利用这些蠕虫病毒的攻击特征，进行检测和预警，这使得 IDS 一时名声大噪，各大安全厂商争先恐后涌入 IDS 市场。

就在国内 IDS 市场刚刚萌动的同时，国际安全厂商正在海外酝酿一场新的技术变革。2000 年 9 月 18 日，Network ICE 第一次将 pass by 的 IDS 技术用于 pass through 模式，在线部署的 BlackICE Guard 产品，通过分析网络流量，直接丢弃恶意数据包，这也是入侵防御系统（IPS）的最早雏形。为了抑制当时较为泛滥的拒绝

服务攻击（D.o.S），早期的 IPS 产品都带有一定抗拒绝服务攻击能力，部分网络厂商、负载均衡厂商借此机会跻身 IPS 市场，从而使得早期的 IPS 市场较为混乱。

绿盟科技是国内最早进入 IDS 市场的安全厂商之一，凭借对入侵检测市场的深刻理解，以及多年来在安全领域的精耕细作，绿盟入侵检测系统（NSFOCUS IDS）自 2001 年上市以来，就一直代表着业界 IDS 的最高水平，持续多年直至今日，该产品仍牢牢占据着国内 IDS 市场的领导者地位。

2004 年，NSFOCUS IDS 做出重大技术变革，在绿盟科技特别定制的安全操作系统之上，NSFOCUS IDS 的引擎架构经过重新设计，检测技术由单包模式匹配，全面进化到完全的状态检测与深入的协议解码。同时，系统的稳定性和处理性能得到极大提升。由此形成的系统主体框架一直沿用到现在，这也成为了今后 NSFOCUS IPS 所采用的基本系统架构。

图 1 早期的 NSFOCUS IDS 产品图片

“IDS 已死？”，IPS 粉墨登场!

随着互联网的普及，公司之间的联系比以往更加密切，更多企业的生产系统，以及运营体系逐渐向互联网迁徙，在发展或提高生产力的同时，安全成为企业尤为关注的重要环节。防火墙和 IDS 在面对趋于复杂的混合性安全威胁时略显苍白，企业迫切需要一种能够积极、主动应对不断变化的安全威胁，有效控制各类网络安全风险的产品，IPS 再次引起人们的关注。

IPS 将入侵检测技术应用到串联网络之中，旨在第一时间对所有出入企业网络的流量进行深度分析和检测，实时阻断攻击。基于其高效的处理性能和精准的检测效率，IPS 重新诠释了网络安全的定义，并从根本上改变了人们保护网络架构和应用系统的方式。

区别于防火墙和 IDS，IPS 具有更精准的检测率和更有效的执行力，能够实现对整个报文流直至应用层的全面检测和保护。系统融合多重检测机制，通过应用状态防火墙、智能协议分析、异常检测、状态签名、关联分析，以及行为建模等多种方法，以确保能准确识别入侵，并在损失发生之前精确拦截攻击，从而持续净化互联网和内网的流量。

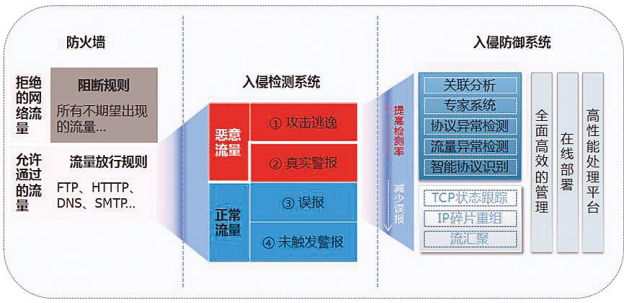


图 2 入侵防御系统和传统安全产品的区别

因为 IPS 能够完全取代 IDS，并提供 IDS 所不具备的关键功能，使得 IPS 产品逐渐成为国内 IT 安全市场上一个新的热点。然而，早期的国内 IPS 市场充斥着传统国际 IPS 厂商的身影，多数国内安全厂商却仍在为 IDS 和 IPS 孰是孰非，为 Gartner 的 “IDS is dead” 论调争论不休。直至 2005 年 9 月，绿盟科技正式推出了国内第一款 IPS 产品—绿盟入侵防御系统（NSFOCUS IPS），终于打破国际 IPS 厂商一统天下的局面。

大浪淘沙，IPS 领军人物出现

自 2007 年起，市场上涌现出越来越多的 IPS 产品，国内 IPS 市场也得到了充足的发展。据国际权威调研机构 IDC 统计分析，IPS 市场是国内 IT 安全市场中，近几年来增长速度最快的子市场之一。与此同时，因为部分用户市场完全覆盖，国内 IDS 市场规模受到 IPS 冲击，增长速度逐渐减缓，甚至成为 2009 年惟一开始负增长的安全子市场。

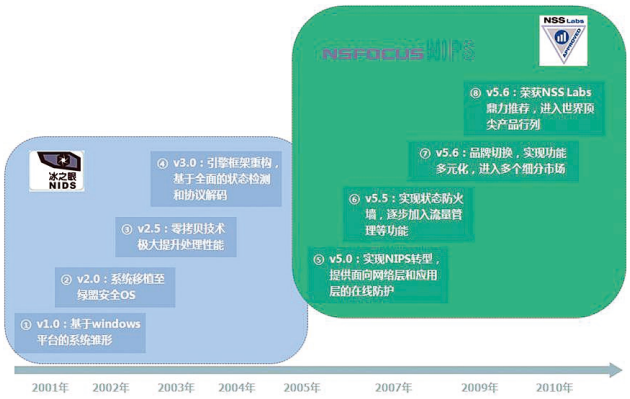


图 3 绿盟入侵检测 / 防御系统（NSFOCUS IDS/NSFOCUS IPS）发展历程

一边是高歌猛进的 IPS 市场，一边是逐渐没落的 IDS 市场，绿盟科技均一直保持平稳增长和绝对的市场统治力。

其实这个市场，也会重复着 IDS 市场的过去，市场兴起的时候诸多厂家争相进入，产品鱼龙混杂，而到了后期，只有专注和坚持的厂家才能活下来，成为真正的领军人物。

- 2004 年至 2009 年，NSFOCUS IDS 连续 6 年进入 IDC 定义的国内 IDS 领导者行列。
- 2006 年至 2009 年，NSFOCUS IPS 连续 4 年进入 IDC 定义的国内 IPS 领导者行列。
- 2009 年 7 月，绿盟科技荣获 Frost&Sullivan 颁发的 “2009 年中国 IDS/IPS 市场增长战略领导者” 奖（2009 China Frost & Sullivan Growth Strategy Leadership Award in the IDS/IPS Network Security Market），由此率先完成历史性突破，成为国内首家获此殊荣的安全厂商。
- 2010 年 3 月，NSFOCUS IPS 荣获 NSS Labs Approved 认证，并被认定为最高级别 Recommended，成为国内安全厂商中唯一获得该权威机构认证的产品。

下一个十年

目前，安全威胁形势已经改变，全球性的安全疫情很难复现，区域性和定向攻击，在数量与精密度上势必持续升高；强制性感染已经成为常态，用户只要浏览到恶意网站就可能被感染；僵尸网络

将永远存在；未来可能还会出现针对虚拟化与云计算环境的攻击方式；当互联网上的所有信息，包括企业网络和社区网络（Facebook、Twitter 等）都承载着对我们有用的信息时，当利益已成为一切罪恶的诱因，网络犯罪不可能消失，未来十年将是信息安全的黄金十年。作为国内 IT 安全市场中增长速度最快的一个子市场，IPS 市场的未来十年生机无限。笔者认为，不断革新的产品技术，以及随需而变的产品策略，将推动 IPS 进入下一个黄金十年，IPS 必然在产品形态、产品架构，以及应用模式等方面发生重大变革。

趋于融合的下一代安全网关

传统的安全网关在应对不断变化的混合型安全威胁，处理丰富的互联网应用时，已经显得力不从心，基于 Botnet 传播的安全威胁，新的 Web 2.0 应用，利用隧道技术的业务程序，都能够轻易绕开防火墙的封锁。

笔者认为，未来将出现趋于融合的下一代安全网关——NGSG（Next Generation Security Gateway），面向安全威胁新趋势，专注于应用层防护的高性能安全网关，NGSG 具有一系列特点，以适应未来 3 ~ 5 年的安全威胁防护趋势:

- 标准的防火墙特性：具备包过滤、网络地址转换（NAT）、状态协议检查和 VPN 等基本功能。
- 拥有较强的应用识别能力，不局限于端口和协议的识别，对于某些限制应用，如 SSL 加密会话，也能准确识别。
- 深度融合入侵防御（intrusion prevention）、内容控制（content control）和 URL 过滤（URL filtering）等多种功能。
- 基于用户身份（users by name）的会话识别和监控，而不仅仅通过 IP 地址进行判断。
- 具备 10Gbps 以上的在线处理能力，不会影响业务系统的正常应用。
- 在上述特性之中，应用安全防护是 NGSG 需要重点解决的问题。针对 WEB、DNS、电子邮件、电子商务、VoIP 和视频会议等各类应用的攻击监控，将成为未来应用安全防护的重点。

IPS、UTM，亦或是防火墙，都将只是 NGSG 发展史上的阶段性里程碑，尽管它们在限定的细分市场内，仍将保持一定规模的增长，但最终必将殊途同归，在不久的将来成为融为一体的下一代安全网关。

基于 SaaS 的安全威胁管理服务

“安全问题的威胁日渐变得复杂，并且其规模和数量使得中小企业无法很好的应对。”RSA 总裁亚瑟•科维洛认为云安全是 2010 年的关键趋势，“旧的管理安全服务供应商只是为用户提供防火墙管理和虚拟专用网。这使我看到了新的外包服务即将诞生：人们需要更多的安全管制，但他们又无法很好地进行全面的管理。在这一基础上，形成了安全云外包服务，或者称为多重安全应用外包服务。”

新的安全威胁总是孕育着新的市场机会。无论是国内中小型企业用户，还是全球范围内的企业级用户，在选择安全解决方案的时候，不仅要考虑方案的完整性和有效性，还要兼顾方案的总体拥有成本，

他们需要的不再是单一的安全产品，而是更具成本效益、更方便透明的一体化安全服务。

新的 Security as a service（SaaS）模式应运而生，基于互联网为全球范围内的用户交付定制化的安全服务，这将打破传统的安全防护方法，用户依托这个平台，可以选择个性化的安全服务，例如基于 IPS 的安全威胁管理。从产品管理、运维，直至警报分析和解决方案建议，SaaS 平台将提供一站式安全贴心服务。

在不久的将来，这个平台还将为全球范围内的企业级用户，提供全面的“安全威胁管理”能力，以及“安全趋势分析”服务，而 IPS/IDS 则将成为依附于这个平台，同时不可或缺的重要组件。遍布于全球的 IPS/IDS 引擎首先将新出现的安全威胁发布到云安全平台，然后基于安全威胁分析引擎处理，形成新的解药，再快速部署到各个节点的 IPS/IDS 产品之中。同时，云安全平台还将依据实时的威胁信息，持续协助用户不断改进安全策略。

随着 IPS 技术的日益完善、用户对 IPS 产品认知的逐步深入，国内 IPS 市场日渐成熟，未来这个市场都将是安全厂商重点发力的领域。随需而变的产品策略，使得 IPS 不断焕发新的青春，无论是作为独立的 IPS 产品，融合多种安全解决方案的 IPS 管理平台，还是为用户提供 SaaS 服务的 IPS 族群，未来的路都还很长。

辉煌十年，不是终结，而是一个新的起点，作为绿盟科技全面拓展国际市场的一把利刃，NSFOCUS IPS 进入国际顶尖产品行列之后，将面临更多的挑战。历经十年磨砺，当我们怀揣梦想，站在群山之巅的时候，我们已经准备好了…

NSFOCUS Enable

—RSA CONFERENCE 2010

国际拓展部　韩永刚

摘要：绿盟科技参加 RSA 大会已经有三年的历史了。三年来，透过绿盟科技在 RSA 大会上的变化，也让我们体会着公司越来越坚实的国际化步伐。

关键词：RSA　变化 合作

NSFOCUS Enable，这是绿盟科技第三次参加 RSA Conference 的主题。三年来绿盟科技在 RSA 大会上的变化，也让我们体会着公司越来越坚实的国际化步伐。早在几年之前，绿盟科技研究部的同事在美国的 Blackhat 技术大会上进行过演讲。随着近三、四年国际化进程的加速，促使绿盟科技成为更多国际专业信息安全会议上的常客。不论是将国际市场最前沿的信息带回国内，还是向海外市场展示来自中国安全公司的实力，与国际同行开展多领域合作，绿盟科技在成为网络安全领域国际化先行者的同时，也成为了一座桥梁。

初探海外

2007 年，绿盟科技已经派专人前往欧洲参加在英国举办的 InfoSec 2007 大型安全展会，了解与熟悉当时的国际信息安全市场。参加 InfoSec 2007 的厂商有超过 300 家，涉及网络安全、漏洞管理、Web 安全，安全增值业务、Email\P2P\IM 应用安全、桌面安全以及内容安全等各个领域。通过对这些领域中国际公司的分析，绿盟科技开始寻求自身与国际市场的契合点与差距，借鉴海外的经验，调整自己的国际化步伐。

亮相 RSA

通过对国际安全市场的不断调研，我们发现在一些关键的技术上，如漏洞管理、抗拒绝服务、入侵保护等，公司已经具备了相当的实力。但与国际知名公司相比，我们还需要更多的磨练，在提升产品成熟度的同时，还需要提升公司整体运营的水平。另一方面，如何开辟新的领域，在技术上保持持久的创新能力，也是公司能够保持高速发展的基础。

2008 年，绿盟科技把眼光转向了信息安全领域中规模最大，也是实力最强的 RSA Conference。RSA 大会每年在美国举行，从 19 年前开始的第一届 RSA Conference，最初只有几十个密码学领域的专家参加，而现今已经是全球安全行业的风向标了。新技术发布、最前沿的热点领域、最准确的市场动向，你都能在这里找到。这里已经成为了全球信息安全行业充分交流与合作的理想平台。

当绿盟科技以展商的身份第一次亮相于 RSA 时，大洋彼岸这个高科技领域的起源之地第一次近距离接触到来自中国的网络安全厂商。此时的绿盟科技可以用兴奋两个字来形容，同行的七八个同事一头扎进数百个安全界最好的厂商中，汲取着营养。交流，不断的交流，去了解最新的动态，也让国际市场了解绿盟科技。2008 年，绿盟科技规模不大的展台，已经成为了一块北美与中国网络安全领域交流的平台。我们展示着绿盟科技最好的技术，而美国安全界的人士在走过绿盟科技的展台时，也都

透出了一种新鲜感，他们同样渴望更多地了解这个来自中国的网络安全厂商，了解中国的信息安全行业。

2008 年的 RSA 有几个重点的领域：一是应用与内容安全，WEB、Email、IM、P2P 等多种应用的安全问题，以及承载在这些系统之上的定制应用与内容安全，都是诸多厂商关注的热点。比如绿盟科技刚刚在 2007 年末发布的 WAF 产品，在北美市场已经逐步步入成熟。二是数据安全，比如 DLP 领域、数据泄露、甚至数据的物理存储安全，都有专门的厂商进行关注。三是安全管理，比如身份管理、行为审计、SIEM、策略管理等，都是热点领域。而在北美提供这些管理平台的厂商不在少数，其中也不乏优秀者。其实从关注领域的差别，我们已经能够看到在北美市场与中国市场无论从客户业务的关注点、资金的集中领域、网络与无线通信技术等方面，还是各方面策略的推动，都有着不小的差异。

通过不断加深对国际安全市场的理解，绿盟科技越来越清晰地看到了自己与国际一流厂商的差距，也看到了我们在技术方面的优势，更加坚定了自己在国际市场上拼搏的决心。意识上的提升将引领公司进入更广阔的空间。“以第一世界的视野，完善产品、服务和运营，开拓国际市场”，成为了公司国际化战略明确的方向指引，我们已经迈出了第一步。

- 2008 年绿盟科技成为了微软 MAPP 计划在中国的第一个合作伙伴。
- 在 2007 年底至 2008 年初，绿盟科技的漏洞管理产品（RSAS），参加了英国西海岸（WCL）实验室的漏洞管理类产品测试，并获得了 Checkmark 认证。当时在全球范围内，总共只有 6 家公司获得此项权威认证。绿盟科技是亚太区的第一家。
- 2007 年至 2008 年，绿盟科技开始投入更多的精力在 WEB 安全及应用安全领域。
- 同年，绿盟科技在日本、新加坡与当地合作伙伴一同，开始了区域市场的拓展。

有备而来

2009 年，在全球都经历了经济危机之后，绿盟科技重返美国旧金山的 RSA Conference。此时的绿盟科技已经少了第一次的兴奋，而更多的是带去自己最拿手的技术与方案。“中国第一个发布 IPS 产品”，“中国第一个发布 WAF 产品”，“2008 北京奥运安全服务提供者之一”…展位上的这些宣传语，无不向国际的同行体现着绿盟科技的自信。其实中国已经是全球网民最多的国家，也是互联网上安全事件发生率最高的国家之一。在实战中不断磨练出来的绿盟科技，有着自己独特的优势。当我们的同事路过 WAF 领域中技术最好的厂商展台时，他们的工作人员认出了绿盟的标志，说到“我知道 NSFOCUS，你们是我们的竞争对手！”对手的重视，就是我们最好的动力。

2009 年的 RSA 是个创新迸发的地方，重新开启的“创新沙盒”环节、对云计算的憧憬以及对云安全问题的聚焦与担忧，SaaS 模式与安全服务的关系、安全协作、合规性以及国家与政府对安全问题的越发关注（GRC，Governance + Risk Management + Compliance），WEB 2.0 时代安全的新动向、身份认证与管理，一切都触动着绿盟科技参会人员的神经。

北美市场在这些创新方面的领先优势，以及良好的创新土壤，都给我们留下了深刻的印象。比如“Innovation Sandbox”环节，优胜者将直接获得风险投资，并能与业内的顶尖专家讨论如何更好地推广自己的产品，并加强公

司的运营。此时的绿盟科技，已经深入地融入进 RSA 会议的进程与方向当中，思考着自己的定位与步伐。

• 2009 年，绿盟科技的互联网组成立，利用云计算方法来提供安全能力与安全交付，成为了公司追逐的新领域。

• 2009 年，绿盟科技成为了 CSA（云安全联盟）在亚太地区的第一个成员，更为深入地参与并推动云安全的发展。

• 同年，绿盟科技多个主力产品线完成产品的国际化版本，并获得海外订单。

深入合作

2010 年，绿盟科技再次来到旧金山。在今年的会场上，绿盟科技高兴地看到已经出现了更多中国网络安全厂商的身影，我们不再孤单。公司展台的风格更加融入国际化的风格，而我们也更为注重市场层面的深度合作。与云安全联盟 CSA（Cloud Security Alliance）的深入沟通，与 Stopbadware 的合作交流，开始进行第一次 NSS Labs 的测试，以及与更多北美主流安全公司开始合作。绿盟科技对于国际安全市场不再陌生，开始展开自己更多的计划。

经历了经济危机的复苏之后，相比 RSA 2009，今年的大会已经有了起色，参展的厂商数量明显增加。云计算也成为了这届会议的强心剂。随着云计算在北美市场的兴起与实际应用，众多的中小安全企业都将目标瞄准了虚拟化安全与云安全。比如在创新沙盒（Innovation Sandbox）环节，竟有近一半的入围者是与云计算与虚拟化相关的，最后的胜出者也是提供了基于虚拟系统的安全防护方案。

而在主题演讲等各个会议主题环节上，各个业内巨头已经不再对云安全的问题有犹豫与怀疑，更多地讨论具体的方案实现以及业务的开展。可见人们已经逐渐在接受并且融入到新的变革当中。而在欧美市场，也已经完成了最初的市场培育阶段，云计算已进入主流。除了网络与通讯巨头，云计算的资源提供商及应用提供商之外，云安全的问题应当是业界最为关心的领域。我们会发现传统的安全更多的以网络传输、边界、数据资产为中心。而这些正在悄悄的改变，未来的互联网与计算环境，你很难再找到明确的边界，物理结构不再清晰，安全问题也转向以身份、数据、业务为中心。置身其中，你会充满了对未来的想象与憧憬。

• 2010 年，绿盟科技的 WAF（WEB 应用防火墙）产品首次出口到北美市场。作为在中国第一个发布 WAF 产品的厂商，绿盟科技在巩固了自己中国 WAF 市场领跑者的地位后，又第一个将 WAF 产品销售到了国际高端市场。

• 2010 年 3 月份，经过半年多的准备，完成了 NSS Labs NIPS 产品测试的绿盟，又再次得到了好消息。中国安全厂商中，有了第一个通过 NSS Labs Approved 认证的厂商，并且我们获得了最高的 “Recommended” 推荐级别。绿盟科技在海外市场的根据地，也即将展开。

绿盟科技是最早开始国际化进程的中国网络安全公司。华为与中兴在海外市场的成功，给中国的高科技企业树立了典范，而中国的网络安全厂商，要想在国际市场上取得成功，无疑还要面对更多的困难与挑战。当我们开始用我们自己的核心技术去换取海外的市场机会；当我们离开国内，面对不同的市场环境，新的客户需求及创新的商务模式时，这一切都是对公司运营成熟度的考验。同时，这些带给我们的动力及价值难以衡量。作为绿盟科技的成员，我们相信一定会有更多来自中国的网络安全公司在国际安全市场上驰骋。就像在跑马拉松，坚持源自信念。

等级保护的实践与探索

行业营销中心　孙铁

摘要：本文基于绿盟科技在长期等级保护实践过程中对等级保护政策、标准及实施的一些理解和成功经验，从业务安全需求与等级保护、流程优化等几个方面进行了总结，同时从实践的角度对等级保护工作提出了建设性意见。

关键词：等级保护　业务安全需求

在《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）1994年颁布以来，经过十几年的摸索和实践，尤其是《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号文件）发布以后，等级保护工作目前已经取得了重大进展：文件和标准体系基本完善、重要信息系统基本完成定级、一些行业已经完成或正在着手进行定级系统的整改工作、有些单位成立了由主要领导牵头的等级保护领导（协调）机构，同时，作为等级保护主管部门，公安部、各地网监部门不断加强对定级工作的监督、检查和指导，为全面贯彻落实国家信息安全等级保护制度提供了有力保障。

但由于等级保护与传统的安全建设内容如风险评估、体系认证、安全集成等有很大的区别，首先其具备一定的强制性，因此初期对信息系统主管单位，也就是最终的责任承担者来讲不可避免的是被动接受，主观能动性相对较低；其次，等级保护涉及的机构比传统的安全建设要多得多，传统的安全建设是简单的甲方、乙方关系，甲方提出需求、乙方满足需求，而由于等级保护是国家意志的体现，重要信息系统等级保护工作所涉及的机构不仅有信息系统主管单位、整改建设实施单位，还有测评机构、行业主管单位、行业监管单位、国家主管单位等，如何协调好这些单位的动作，如何明晰相互的责权利关系，如何在这些单位参与的情况下高效完成等级保护工作，这确实是需要仔细考虑的问题，因此在等级保护具体执行环节还有很大的改进和提升空间。

绿盟科技长期从事等级保护实践工作，协助各行业用户开展了等级保护咨询、建设、整改等工作，同时作为各地测评机构、检查机构的技术支撑队伍，积极参与了各行业、各地测评中心的体系建设，在这个过程中积累了丰富的实践经验，希望通过本文从几个方面的简要讨论，为等级保护工作顺利开展提供参考和借鉴。

1. 等级保护实践经验

1.1 业务安全需求与等级保护要求结合

在等级保护工作中，要保护的对象应是信息系统承载的业务。在定级阶段，系统所定等级的一个重要依据是业务及系统提供服务影响，但在整改阶段，很多系统的建设方法却偏离了定级的初衷，目前有相当一部分系统管理者和使用者认为定级系统的建设整改工作只是满足标准的要求和规定，针对等级保护的标准要求一条一条进行简单对比，僵化的比较，包括部分测评中心也是这样开展测评，使等级保护的建设、整改脱离了保护对象的自身安全需求，演变为标准的符合与不符合，导致保护重点不突出、同质化严重等现象，整改效果受到很大影响。

例如：政府门户网站和电子政务外网同是三级系统，但二者的防护重点和内容是完全不一样的，网站保障重点是防挂马、防篡改、防越权等，而外网的保障重点是：防DDoS攻击、入侵检测、网络安全态势分析及预测，如果采用相同的保障措施，是不可想象的。

因此在实践中，绿盟科技建设、整改方案的设计，坚持业务和系统所提供服务的安全需求是系统安全规划、系统整改设计的核心。在对重要信息系统整改方案设计之前，进行细粒度的业务调研，在此基础上参照等级保护的标准要求，进行建设、整改规划。

经过详尽的业务分析后，在整体安全规划的指导下，将等级保护的标准要求分为三类:

第一类是针对急需解决的系统安全问题采用的技术、管理措施，是本次建设的重点和主要内容;

第二类是系统需要完善的安全内容，但现阶段由于各方面原因暂时难以实施的部分，做为安全规划延续内容，明确提出后期建设计划;

第三类是不适合项，该类要求是不符合当前系统安全特点，在建设整改过程不予考虑。

对于第二类、第三类以及高等级系统采用低等级防护措施的情况，应给予详细的解释说明。

这部分工作应通过业务风险评估等咨询方式完成，也就是说应有具备咨询能力的机构完成。

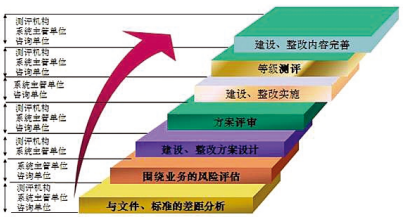
通过这样的设计，使系统承载业务安全需求与等级保护的要求紧密结合，做到即符合合规性要求，又满足自身的实际安全需求。

1.2 等级保护流程优化

如何保证等级保护工作实施有效性，达到即节约成本、又能有效保障相应等级信息系统的目标，流程是至关重要的。笔者在实践中深深体会到：等级保护落地工作不仅仅是一个技术的问题，更为重要的也是一个流程管理问题。传统的定级、建设、测评、整改、检查流程在实践中还是遇到了很大的困难，容易造成系统安全建设时间过长、建设浪费，而且由于测评机构先期工作没有介入，在测评阶段如果出现测评机构与建设方对系统安全建设内容理解不一致，将耗费大量的精力和时间。

在实践中，绿盟科技摸索出了一个比较有效的流程，通过这个流程，可以使等级保护工作更快捷、更有效。在这个流程中没有将系统管理者、测评机构及系统整改建设单位作为检查和被检查关系看待，而是强调三方全程合作、测评机构的早期介入。

在建设中，本着对等级系统进行切实有效安全保障的出发，与测评中心、系统用户在系统的不同阶段进行配合，达成一致，有效降低了测评阶段的分歧、提高了工作效率。整改方案从信息系统主管、整改实施单位、测评机构三方的角度进行了综合评审，意见统一后再开展建设和整改，达到合规、实用、有效的目的。



1.3 标准、要求细化

对于等级保护标准所提出的技术和管理要求，坚持入乎其内，出乎其外的原则。深入分析等级保护所涉及的主要标准，开发

标准具体技术要求与现行成熟技术产品功能性能的对应工具，使抽象的技术要求转化为方便理解的具体技术、产品、管理和服务指标，方便整改方案的设计和实施，在将等级保护工作按文件、标准做细、做深、具体化的同时，也始终站在用户业务安全需求整体保障的高度看待等级保护各项标准，做到标准的灵活运用，将一个个要求转变为一个个方便实施、相互有衔接递进关系的项目，映射在系统安全建设的各个阶段，使等级保护的各项要求在符合信息系统业务安全需求的前提下真正落到实处。

1.4 管理和运维体系设计

信息系统等级保护工作的本质是一个管理问题。在等级保护建设整改阶段，相当一部分单位将重点放在技术体系设计和产品搭建上，而忽略了信息安全管理和运维体系的建设和有效性，严重影响了技术体系效能的发挥。

以往的安全管理体系建设过分的强调技术和管理的分离，在实践中发现这样的管理体系很难真正起到管理的作用，具体实施过程中很难落地，系统的安全体系建设应是技术、管理和运维相互融合的完整的工作体系。如果说安全技术是建筑材料、是手段。安全管理和运维就是真正的粘合剂、是根本。

在等级保护管理和运维体系设计实践中，并没有采用将标准中管理条目和要求展开进行设计，而是结合目标系统的行业及业务特点，设计差异化的管理体系设计，对标准中对管理体系的分类和要求进行归纳、分析，因为在实践中我们发现，大而全、事无巨细的管理体系在实际工作中应用效果并不理想，体系包括四个层面：策略、制度、流程、工作表单，策略和制度层面尽可能精炼，每个制度后面均有相对应的流程和工作表单支撑，使等级保护的管理要求融入到各项制度中，也使各项制度和技术体系通过流程和操作表单实现了落地，同时为日后的审计和回顾打下了良好的基础。

1.5 以过程而不是项目的观点看待等级保护

现在有一个倾向：即认为等级保护工作是一个阶段性的工作，是一个项目，通过一个项目实施就完成等级保护工作，这是需要纠正的。

随着系统承载业务和提供服务的不断变化、安全保障技术的持续完善、新攻击方法和手段的日新月异，信息系统安全保障工作顺应形势不断调整和改进，等级保护工作应该是一个过程，贯穿于信息系统生命周期的各个阶段，是系统安全保障的常态工作。因此绿盟科技在实践中，通过等级保护工作，与信息系统建设、主管单位建立战略合作伙伴关系，提供系统全生命周期的咨询、设计、服务、实施、应急等伴随性技术支持工作，在系统安全体系设计过程中，保证了安全体系建设的持续性。

同时在信息系统等级保护设计和实施中，也避免一蹴而就的偏激和功利做法，而是在深入理解系统安全需求和等级保护建设要求的基础上，采用分阶段、分期的方法，逐步深化系统的等级保护安全建设。采取首先以满足系统主要安全需求为主要目的的安全基线建设，然后以符合等级保护工作要求为主的合规建设，围绕系统自身安全特点对不满足等级保护标准要求的方面进行分析，以决定进一步建设的方向，最后建立技术管理、态势感知平台，在前两个阶

段工作基础上，区分不同的安全问题建设构建相应的有针对性的管理平台，如：网站监控、配置管理、异常流量监测、入侵检测、预警审计等，这样一步步踏实的工作，使统一安全管理和分析成为可能。

2. 建议

随着等级保护实践工程的逐步深入，也感到有几方面工作还有很大的改进、完善空间，如果解决不好将成为等级保护工作进一步推进和大范围展开的瓶颈。

2.1 测评工作的统一、规范

等级测评在等级保护各阶段工作中占有重要地位，可以毫不夸张的说，等级测评是等级保护工作的“腰”，测评机构对政策的理解、测评方法、测评流程直接影响到等级保护工作的整体质量和效果。目前除了国家的几个权威测评机构外，各地、各行业也在积极进行测评中心的建设，但各测评中心对等级保护制度、政策、文件、标准的理解却存在巨大的差异，导致各地测评机构的条件、测评机构的组织架构、测评技术体系、测评流程等极不统一，不同测评机构的测评手段和方法没有可比性，在某种程度上影响了等级保护工作的深入开展。

同时由于测评报告是判断等级保护整改工作是否有效的重要依据，也是在以后安全检查中重要参考文件，因此测评机构所出具的报告是系统管理者、整改建设者、检查单位所关注的重点，但测评手段和方法的不一致导致了用户的迷茫。

建议下一步加大对各地测评机构的行业规范，政策、技能培训，对测评机构的认可，测评人员的选择有更为明晰的制度，使测评机构整体水平得到提升、测评内容和方法统一、规范。

2.2 标准的权威解析

目前指导等级保护各阶段工作的标准已经比较完备，对等级保护各阶段的工作内容提出了明确的要求，但如何将要求转化为具体的建设指标，至少针对目前等级保护工作依据的几个主要标准，需要有更具体的解读。对标准中的理论词汇如强制访问控制、主体、客体等也应结合现实情况给出明确的解释，而不是在理论层面进行描述。

2.3 具备业务及行业特点的方案设计

等级保护的文件和标准具有很强的普适性，但对于不同行业、承载不同业务和行业的信息系统信息安全保障还是具有鲜明的业务特点的，比如运营商和金融行业，等级保护现有的标准体系已经不能够完全表达其行业安全需求，因此应该鼓励重点行业围绕国家文件、标准要求，根据自身特点制定相应的行业标准，使等级保护工作具备鲜明的行业特点，增强其可实施性和针对性。

3. 总结

以上是绿盟科技在等级保护实践过程中的一点经验和体会。经过长期的一线工作，目前绿盟科技已经探索出使等级保护工作切实落地的方法，完成多家单位等级保护安全体系设计、系统整改并协助用户单位通过等级保护测评，同时与这些单位及测评机构一起参与相关系统安全运维工作。

希望在今后为推进国家等级保护工作的进一步深化，更好的成为等级保护制度的宣传者、等级保护政策落地的推进者、设计者和实施者。

运营商新业务催生新安全

行业营销中心 万慧星

摘要：基于行业竞争格局的改变，运营商的业务增长点也在逐渐转变，随之而来的安全焦点也从传统的 DDoS、Web 入侵向着应用、业务在进化，其中发生了很多变化与创新。基于此，本文以运营商行业竞争的特点入手，从新业务模式对安全发展需求、政策监管合规、云计算安全，以及安全增值等几个方面展望运营商的安全发展趋势。

关键词：运营商 业务安全 云计算 合规 新业务 安全增值

2008 年电信业的重组，2009 年 3G 牌照的发放，三大运营商已经具备了全业务竞争的外部条件，各运营商开始依靠自身的优势发力进入对方的领地。随着移动互联网的应用逐渐丰富，移动互联网也越来越普及，给运营商带来了业务发展的新机遇，音乐基地、手机应用工厂、手机支付等新兴业务的发展，也带来了新的增长领域。2010 年电信网、互联网和广电网三网融合的出现，必将促成一个跨边界的新市场，也将给运营商带来新的挑战。

近期以来，与运营商有关的网络安全事件越来越多地呈现在大众面前，从去年 5·19DNS 断网事件、百度域名解析出错事件、业务恶意订购、手机涉黄整治事件的陆续出现，都越来越明确地告诉大家，安全问题、网络安全问题已经不仅存在于电视上、新闻中，而是实实在在地影响着广大互联网用户的正常网络生活。运营商作为互联网与用户间的重要一环，对于安全事件的预防、控制、响应能力就显得尤为关键。

安全自身经过多年的发展，也在持续的改进和创新。一方面，安全防护已经从传统的防火墙、防病毒、IDS 等传统的“老三样”，发展到了以 UTM 综合防护、认证审计的 4A 平台、针对 DDoS 和 WEB 安全的专项防护产品等为代表的“新三样”；另一个方面，安全的模式也在转变和创新，运营商向大客户推出的安全增值服务渐入佳境；基于云计算平台的安全业务似乎也来到了眼前……

DDoS 攻击、Web 入侵仍是安全事件的主旋律，针对运营商特有业务系统的安全事件也已初露端倪，但造成的影响却非常严重。基于互联网对于国家发展的重要价值，安全也受到政府的高度重视，运营商作为互联网的接入和运营单位，政府对运营商也提出了更高的安全管控要求。随着产业环境的变化，新的业务模式层出不穷，而伴随而来的安全问题也相约而至，这些安全问题相比传统网络安全更为复杂，既有的防护策略也将面临严峻挑战。同时，随着互联网越来越成熟，用户对于安全需求越来越多，而运营商是否可以依据自身的安全积累展开安全业务也成为一个热门话题。基于此，本文以运营商行业竞争的特点入手，从新业务模式对安全发展

需求、政策监管合规、云计算安全以及安全增值等几个方面展望运营商的安全发展趋势。

安全与业务结合将越来越紧密

近年来智能手机用户大幅攀升，移动数据业务蓬勃发展，出现在数据业务中的安全事件也时有发生。去年某运营商 A 省公司收到 B 省的几个投诉，告知用户甲从未漫游至 A 省，却在近两个月被 A 省公司无故扣除了业务订购费用，运营商的系统运维人员查询业务系统中相关的订购记录，发现与正常的业务订购记录不一致，且系统中存在不知名程序——明显这又是一起类似 WAP 入侵的非法订购事件。根据对事件的分析，得出两个简单的原因：一、系统安全策略不严格致使非法应用得以部署和执行；二、系统中存在业务流程逻辑的不安全因素，导致事件发生，对用户造成损失，最终形成了用户的投诉。

通过上述事件的简单分析，我们可以发现相对于传统的网络安全、系统安全而言，来自于业务系统、业务流程方面的缺陷或不足所引起的安全问题更为严重。传统由后台推动的安全建设难以支撑当前的业务发展，并将逐步转换为业务发展来推动安全建设，由来自市场、用户对安全的诉求转变为安全保障和建设的直接动力与需求。

针对业务安全层面进行安全评估和风险控制，固然能很好地规避上述安全问题，但是在实际的操作中却困难重重。第一、行业竞争压力巨大，新业务新系统都需要更快地投入运行，吸引用户、增加行业竞争力，难以在有冗长的周期进行业务层面的安全评估和测试；第二、依据现有的业务合作模式，业务系统厂商还缺乏较为全面的安全能力，难以开展业务安全的识别与控制；第三、业务系统上线运行后，缺乏持续的安全跟踪，往往是出现安全事件以后由市场的投诉反映出来，难以防范于未然。

由于业务系统本身就是运营商的核心竞争力所在，安全问题需要受到高度关注，为了应对上述的难题，采用一系列的综合措施来降低业务安全问题将是一个必然趋势，这些措施包括：制定业务系统的入网上线的基础要求，作为一个业务系统上线必须满足的条件；引入第三方的安全咨询组织对业务系统的安全进行监理；梳理业务特性，通过人工拨测或者自动化的稽查系统在用户感知前发现异常现象，避免用户投诉；制定更为严格的安全管理制度，加大人为安全事件的惩处力度。

新业务模式的安全新诉求

2009 年是中国 3G 全面启动的第一年，也是运营商展开全业务竞争的第一年，各家运营商不仅需要面对来自于另外两家运营商的全业务竞争，更为重要的是随着 3G 的上线，移动互联网的应用和业务模式逐渐明晰，就是抓住用户。而传统的互联网、手机终端企业也开始通过终端、浏览器、门户、内容、移动互联网应用等等来扩展自己的势力范围，争夺原属于运营商的用户。当前，各大运营商都在互联网中积极的开拓新的业务，利用固有的行业优势扩展自身的势力范围，以寻找新的业务增长点。

互联网业务的安全

中国移动的 12530、飞信业务、139 互联、手机游戏，中国电信的“爱音乐 i music”等都属于典型的运营商在互联网业务方面的尝试，而且取得了不错的效果。对于这样的互联网业务来说，与运营商的传统网络安全比

较起来就显得更为错综复杂，遭遇的安全挑战也要大得多，依靠传统的安全策略并不能满足其需求。因此，大力开辟互联网业务的过程中，门户网站、网上营业厅、新互联网业务平台的安全运营就显得尤为重要，需要投入重点精力进行关注。

在这方面，搜狐、盛大、腾讯、阿里等互联网业务公司在安全防护方面就是比较成功的案例。互联网业务对他们来说就是公司生存和发展的全部，经过多年的发展，对于如何保障业务站点的安全、保持业务持续运作积累了相当丰富的经验。通常，由于安全公司偏向于传统网络安全，关注通用性的安全技术和产品的研究，难以完全满足互联网公司对安全与业务紧密结合的需求，因此大规模的互联网公司都组建了自身的安全团队，具体的安全工作方面主要保护了这么两方面：一是基础安全。主要关注网络层面、系统层面的安全问题，比如安全漏洞、安全配置，安全域划分，防火墙、扫描器、抗DDoS 等通用化的安全产品部署，此部分与传统的安全建设类似，重点是筑高安全风险的门槛。

二是业务安全。这才是互联网业务安全的关键所在，安全渗透到主营业务中，甚至以安全模块植入到具体的业务平台中。比如网游公司更为关注的是账户安全、反外挂、虚拟资产安全；门户站点更为关注内容安全，防止不良信息出现；而搜索型站点关注的重点在点击欺诈方面等。同时，互联网业务具有一个业务发展迅速的特点，相对应的安全需求也越来越高、越来越迫切，时刻都需要针对新的业务制定新的安全策略。

首先解决诸如防篡改、入侵防护、DDoS 攻击防护等基础安全问题，然后深入业务层面，针对业务特性定制安全策略或者技术，将是保障互联网业务安全运营的一条关键之路。而运营商现有的安全建设模式多是依靠安全公司提供安全服务和产品满足安全需求，而传统的安全公司更擅长提供通用型的安全服务和产品，难于提供完全贴合互联网业务特性的安全技术，因此需要重点考虑如何利用自身优势开展互联网业务特性的安全研究，或者引入业务安全领域的合作伙伴，持续互联网业务开展的整个过程，保障新兴业务的安全运营。

开放能力，还需守住安全

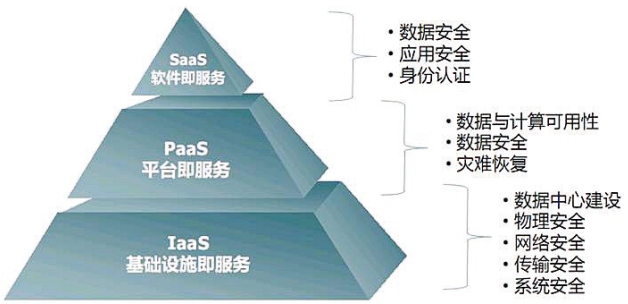
开放运营商通信能力，让用户和开发者能灵活的运用这些能力，创造出新型应用，吸引用户更多的使用运营商业务，并开辟新的收入渠道。目前，中国电信的“天翼应用工厂”已经上线运营，可以为开发者提供通信能力（主要包括短信、定位、IVR 等，以API 等方式共开发者调用），开发者开发的应用还可以通过“天翼空间”对用户进行销售。

通过为开发者和用户开放运营商的部分能力，固然可以促进创新移动互联网应用的产生，在新的竞争中扩展优势，但安全问题却是值得重点关注的内容。能力开放的平台不仅需要考虑传统的安全问题，还需要重点关注由于能力开发带来的新兴安全问题，比如开发者对能力的滥用，造成用户骚扰；用户的隐私数据泄露等问题。同时，能力的开放是否会给运营商的基础网络引入新的安全风险也值得研究。

云计算，安全将何去何从

云计算是当前的热门话题，云计算源于搜索引擎平台，也由于他的特性使其成为互联网服务的重要平台。从 Amazon、

Google 等互联网公司对云计算的成功应用来看，云计算提高了信息服务能力，具有巨大的运算和存储成本优势。当前，无论是传统的“IT 贵人”，还是“互联网新秀”公司都积极的投身于云中，那么对于运营商来说，云计算同样也充满了诱惑与机会。运营商为客户提供了丰富的应用，拥有大量的用户数据，需要海量的数据存储和处理能力，而这些都是云计算的优势所在。我们已经看到，中国移动研究院从 2007 年开始进行云计算研究（“Big Cloud”项目），搭建起基于 256 个节点的云计算平台，展开数据挖掘等方面的研究和应用开发工作。同样，我们也看到中国电信、中国联通也陆续启动了云计算相应的研究和实验。运营商不仅关注云计算为自身的应用提供舞台，也关注通过自身资源应用云计算提供增值业务，开拓新的市场。



云计算平台安全示意图

云计算并非一个全新的技术体系，而是 IT 技术的一种新的业务模式，那么原来出现的安全问题，DDoS 攻击、WEB 入侵、漏洞利用等等，云本身还会有，不会增加，也不会减少。但由于云计算的资源共享、动态分配、可伸缩的特性，也会带来新的安全问题。

第一、数据泄漏。大量的重要数据和业务应用都存储在云平台中，这些信息具有不同的服务级别、归属于不同的应用群体，那么如何保证这些信息的私密性，不被非法的泄漏和滥用。而作为云计算的运营单位，自身内部的安全管理和职责分离如何有效执行，保证云平台中数据的安全都将是云计算的安全关注焦点。

第二、潜在的商业纠纷。比如我购买了“Bmazon”的云服务，用于承载公司的业务应用和数据，但哪天我们发生纠纷、吵了架，那我的敏感数据还能安全可靠的带走吗？另一方面，由于虚拟化技术的应用，带来了存储和计算物理位置的不确定性，不同区域的法律法规完全不同，可能带来潜在的合同纠纷和法律诉讼。

第三、作恶的云？！云计算平台拥有大量的计算资源，并可以让购买者低价的获取，如果被恶意使用者购买云计算资源，用以作为发起攻击的平台，后果非常严重。换一个方向，如果黑客利用互联网资源向云中的某业务站点发起 DDoS 攻击，那么根据云计算的弹性资源特性，云计算平台会线性的增加此站点的计算能力，循环往复下去，岂不导致了恶意的资源消耗，甚至租用费用的大幅攀升？而这一块是否存在有效控制手段也是云计算需要重点考虑的安全问题。

基于云计算环境中安全问题的复杂性，云计算提供商、OWASP、ISACA、专业安全公司等都开展了广泛的安全研究，在 2009 年的 RSA 大会上成立了云安全联盟 CSA（Cloud Security Alliance，2010 年初绿盟科技成为其亚太区第一位成员）。CSA 成立后，发布了云安全指南，系统化地对云安全的建设提出指引，可以为云计算平台的安全体系建设提供有益的帮助。

由于云计算对于运营商来说具有重大的商业价值，为了使云计算能整合运营商的网络资源、用户资源、业务能力资源、信息资源等各种资源，为用户提供强大的个性化移动互联网信息服务，基于云计算的安全研究与建设也将成为运营商重点关注的内容。

合规是压力，也是动力

说起合规大家并不陌生，自“SOX 法案”以来，在美上市公司已经投入了大量的精力进行相关工作，通过法案涉及内容，满足合规要求。我们认为依据国家、行业等对风险控制的政策法规要求，推动相应组织、企业进行符合性度量和审计，一般就称为合规。

通常运营商在进行安全建设的时候，考虑的是自身业务需求，而现在逐渐多起来的安全法规、规范也给予运营商很大的压力，同时也给安全建设带来了推动力。特别是当合规要求与业务安全需求有机地融合到一起的时候，则可以通过合规的建设来迅速提升业务安全的能力。当前运营商行业的安全合规，一个是“SOX 法案”，另外一个就是“等级保护”，两者都以法规的形式督促运营商坚强内部控制，增强抵御风险的能力。

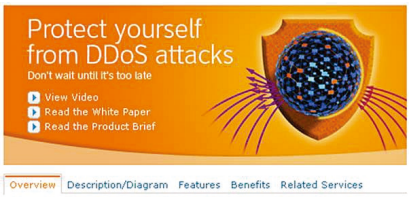
工业和信息化部（简称工信部），于 2010 年初发布了第 11 号令，即《通信网络安全防护管理办法》，自 3 月 1 日起开始实施。以“令”的规格发送出来，对运营商形成了一种合规性要求，必将逐步带动实际安全建设要求并形成持续的动力。在《通信网络安全防护管理办法》中，体现了等级保护的思想，要求针对业务系统进行定级，并进行备案、测评、检查、风险评估、差距修补等相关工作，在业务系统建立之初就需要考虑安全。

手机支付目前尚处于起步阶段，但已吸引了足够多的关注，三大运营商都已或快或慢的进行着试点推行、产业布局等工作。正是由于手机支付是属于一块新兴业务，大家还普遍缺乏安全经验，处于“无规可寻”的状态。因此可以充分的参考既有行业规范（如 PCI-DSS、ADSS 等），快速提升系统的安全能力。

提到合规检查，首先思考的就是需要大量的审查、复杂的流程、细化的表单等工作需要进行，效率很低，是否可以运用技术手段提高安全合规的效率成为大家的一个关注焦点。这方面基于 SCAP（Security Content Automation Protocol）做了一个很好的尝试，即通过将复杂的规范拆解为标准化的检查内容和检查方法，并通过自动化的工具来执行，成倍地提供效率，促进合规的落地和执行。基于运营商行业合规的特性，制定自动化的合规检查工具，对于合规的落地和执行都将具体积极的作用，具有广泛的应用前景。

安全业务，运营商的新机遇

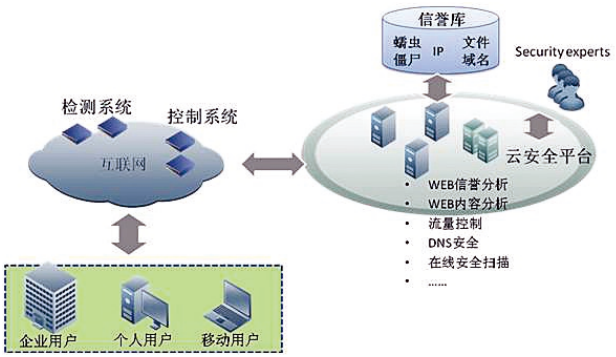
随着互联网越来越成熟，用户对于安全需求越来越多，希望便利的获取安全服务，运营商在自身网络上积累了丰富的安全经验，利用这些经验，为运营商的客户提供安全服务，既提升服务质量又开拓新业务。



Source：AT&T

在增值业务方面，国外运营商 AT&T 在提供传统接入基础类资源基础之上，还逐渐开展了很多互联网应用，包括应用管理、数据媒体应用，其中在网络安全和云计算方面是走在前列，它提供基于流量清理中心所提

供的防护业务，为集团客户、企业用户提供异常流量清洗服务。网络安全服务也已经成为英国电信 BT 综合信息服务提供的关键产品，而漏洞评估服务则是用户接受程度最高的一类安全服务。与此同时，中国电信、中国联通也在多个省份进行了安全增值业务的尝试。



云安全业务示意图

先行的运营商对安全增值业务已经推动了多年，从实际推广的效果来看，客户对 DDoS 攻击流量检测与清洗的安全增值业务接受程度较高，同时，DDoS 清洗业务以自动化流量检测和清洗工具为基础，可以完全实现自动化，对运营商运维人员的要求较低，因此开展的效果不错。那么是否还存在新的安全增值业务模式呢？是的，云安全，应用云计算模式为客户提供安全增值服务。云计算是互联网未来的发展方向，运营商可以利用大量基础资源发展云计算业务，并基于此为互联网用户、移动互联网用户提供安全预警信息服务、在线安全扫描、安全 DNS 服务、Web 安全防护服务、互联网安全信誉等，开拓广阔安全增值业务市场。

内存中的战争

研究部　于旸

摘要：本文回顾分析了过去 10 年中出现的部分漏洞攻击和防护技术。

关键词：缓冲区溢出　DEP　NX 技术　Return to LibC　Heap Spray　Flash JIT Spray

1988 年，Robert Morris 利用 Fingerd 缓冲区溢出漏洞编写的蠕虫程序肆虐互联网，数小时内感染了 6000 多台 Unix 服务器——差不多是当时整个互联网服务器总数的 10%。这是人们第一次感受到安全漏洞的巨大力量。

在此之前，关于缓冲区溢出漏洞的知识其实早已在地下世界流传多年。事实上，即使在此后很长一段时间，这些知识也一直处于半地下状态。直到 1996 年，Aleph One 在第 49 期 Phrack 杂志上的一篇《Smashing the Stack for Fun and Profit》才将这些知识公开介绍给大众。

人类花了很长时间才意识到地球不是宇宙的中心，又花了很长时间才明白太阳也不是宇宙的中心。我们对安全漏洞的认识也是渐进的。

比较早的时候，人们甚至认为堆溢出是无法利用的，所以早期的安全编程资料中甚至有推荐使用堆来代替栈以避免安全问题的说法。一开始，人们也认为缓冲区溢出攻击只能在 Unix 类操作系统上实施。因为 Windows 系统的堆栈地址不稳定，并且通常高位包含 0，无法在常见的字符串拷贝溢出中使用。然而 1998 年 Dildog 的《The Tao of Windows Buffer Overflows》，1999 年 Dark Spyrit 在第 55 期 Phrack 杂志上的《Win32 Buffer Overflows - Location, Exploitation and Prevention》先后提出了成熟的 Windows 缓冲区溢出漏洞利用技术。公元 2000 年到来的时候，世界并没有如科幻电影中描述的那样因为千年虫而崩溃，著名黑客 Kevin Mitnick 也在这一年刑满释放了。在新的千年里，计算机技术就像著名电影《星球大战》中所说的原力一样，光明面和黑暗面各自发展，两者的斗争从未停止。

我们目前使用的计算机都是基于所谓“Von Neumann 体系”。该体系的一个重要特点是：程序和数据以二进制形式不加区别地存放在存储器中，存放位置由地址确定。也就是说，计算机无法分辨存储器中某处存储的到底是程序，还是数据。

这个特点，是利用缓冲区溢出等安全漏洞的基础条件之一。因为攻击者可以简单地将自己的代码和其他数据混在一起提交给程序，并利用漏洞让计算机去执行这些代码。为了解决“冯•诺依曼体系”这一特点带来的问题，人们发明了 NX（No eXecute）技术。NX 技术的诞生其实远比我们接触到它早，但一直都是用在那些为服务器设计的 CPU 上，譬如 SPARC、DEC Alpha、IBM 的 PowerPC，甚至是英特尔的 Itanium 处理器。AMD 公司在 2003 年推出的 Athlon 64、Opteron 等 CPU 上首先使用了 NX 技术并为之命名。后来，Intel 在 2004 年初推出 Prescott 内核的 Pentium IV 处理器时也开始应用 NX 技术。虽然 Intel 将该技术称

之为 XD（eXecute Disable），但实际上和 AMD 的 NX 完全一样，只是命名的问题。

NX 技术的本质是在内存分页的属性中增加是否可执行的标志。带有 NX 技术的 X86 处理器，会将 63 号页表索引（即第 64 位）指向的位置作为 NX 位。如果 NX 位是 0，在页表内的数据就可以作为指令执行；如果是 1 则只能作为数据进行读写，不能执行。CPU 在执行代码时，会判断所执行的地址所在分页的 NX 位，如果执行到 NX 位为 1 的分页，就会抛出异常。这样，CPU 就有了分辨存储器中某处存储的到底是程序还是数据的能力。这就在一定程度上弥补了“Von Neumann 体系”在安全上带来的问题。

当然 CPU 的这一新特性也要操作系统的配合才能得到实际应用。微软在 Windows XP SP2 中开始正式支持利用 NX 技术实现 DEP（Data Execution Prevention）。在开启了 DEP 的环境下，如果利用传统方法进行漏洞攻击，当 CPU 执行到攻击者传递的代码时，会发现这片区域是用来存数据的，没有可执行的属性。攻击自然就失败了。

DEP 技术的出现，在一定程度上阻挡了对漏洞的利用，同时也促使人们去探索绕过它的办法。

早在 NX 技术还没有应用到 X86 上的时候，人们就针对它研究出了一种称作“Return to LibC”的方法。这种方法的关键之处是并不让 CPU 去执行攻击者的代码，而是让 CPU 按照特定顺序去执行系统中已经存在的代码，借助这些按照特定顺序组合的代码片断，组合成攻击者要完成的功能。这些系统中已经存在的代码当然是存放于可执行内存中分页的。这就绕过了 NX 技术的限制。利用类似“Return to LibC”的思路，很容易在 Windows 系统上实现同样的攻击。

然而要实施“Return to LibC”类的技术，有一个前提，即要调用的那些代码地址可预知。如果地址不可预知，则难以实施攻击。所以，也早在 NX 技术还没有应用到 X86 上的时候，Unix 类操作系统上就有一种用以对抗“Return to LibC”的办法 :ASLR（Address Space Layout Randomization）。即将模块加载地址和堆栈等都随机分配。微软从 Windows Vista 开始，也使用了该技术。

对于同时使用了 ASLR、DEP 等安全技术的 Windows Vista、Windows 7 等操作系统，由于 DEP 的存在，传统的攻击肯定是不行了；由于 ASLR 的存在，“Return to LibC”也很难生效。然而，攻守双方的较量并没有到此结束。

攻击一方又发现，微软 IE 浏览器支持嵌入用户编写的 .Net 模块。而这种 .Net 模块在内存中的加载地址是可以指定的，不受 ASLR 的随机化影响。而且 .Net 模块所加载的内存分页属性也是可执行的，不受 DEP 的影响。借助在页面中嵌入 .Net 模块的方法，就可以完全绕过 DEP 和 ASLR，实施攻击。微软方面也很快对此技术作出了反应：取消 IE7 和 IE8 默认对 .Net 的加载支持。因为实际上在 WEB 开发中，.Net 技术使用的并不多，所以取消这个默认支持对用户的影响并不大。

就这样，防守一方的优势算是暂时保持住了。然而，在 2010 年，攻击一方又有了新的突破。这种新技术一般称作“Flash JIT Spray”。要理解“Flash JIT Spray”，首先要回顾一下在漏洞利用技术的发展过程中，出现过的一种革命性的技术，称作“Heap Spray”。

很早以前，就有人提出可以在网页中插

入会导致大量内存分配的脚本，导致浏览该网页的用户物理内存耗尽，系统运行速度变慢。这原本是一种无聊的拒绝服务攻击手段，但很快人们意识到，借助这种技术，可以在内存中可预期的地址上制造出特定内容的数据。这一特点，使一些原本几乎不可能被利用的漏洞现在都可以利用了。譬如覆盖虚函数指针表、对象释放重利用等。一些原本能利用的漏洞，如堆栈溢出，借助“Heap Spray”，也可以大大降低利用难度，简化攻击代码的编写过程。

但是，“Heap Spray”技术也有一个严重的缺陷：通过大量分配内存，虽然可以规避 ASLR 的影响，但是分配的内存毕竟只是数据，可读写，不可执行。所以在 DEP 环境下“Heap Spray”的意义就很有限。不过，由于在 IE7 中默认不开启 DEP，所以很长一段时间里，“Heap Spray”技术在 IE 漏洞利用中非常流行。

随着默认开启 DEP 的 IE8 逐渐开始流行，支持 ASLR 的 Windows 7 慢慢开始取代 Windows XP，“Heap Spray”技术的光彩也在逐渐暗淡。

“Flash JIT Spray”技术实际上延续了“Heap Spray”的思路，通过大量分配内存来规避 ASLR 的影响，但是所分配出的内存是可执行的。

为了提高 Flash 播放器的性能，开发人员在 Flash 10 中使用了 JIT（Just In Time）技术。所谓 JIT 就是对 Flash 中的代码不像传统脚本执行方式那样逐行解释，而是先将其编译，然后直接执行生成的机器码。这样可以大大提高 Flash 的播放效率。

不过，既然要执行编译出来的机器码，那么存放机器码的这块内存自然是有可执行属性的。所以，攻击者通过巧妙地构造 Flash 中的脚本，就可以让 Flash 在内存中编译出想要的数据，而且存放在可执行分页中。这样，“Flash JIT Spray”技术就同时绕过了 DEP 和 ASLR 两种防护方式。

目前无论是 Windows 的开发商微软还是 Flash 的开发商 Adobe 暂时都还没有拿出对“Flash JIT Spray”技术的防护手段，不过肯定只是暂时的。这种攻守双方的技术较量是一场长期的拉锯战，未来双方肯定还会有更精彩的技术出现。

业务安全如何评估

行业营销中心　李国军

摘要：本文提出了业务安全评估的概念、内容，给出了评估流程和相关工具，并以短信业务的恶意订购流程进行了举例说明。同时，本文也阐明了业务安全评估与传统信息安全评估的关系。

关键词：业务安全评估　业务流程　数据流　数据处理单元　攻击路径

1. 引言

1.1 问题

在电信、金融等许多行业，IT 系统已经成为企业的重要资产和生产设施，对其业务起着承载和支撑作用。这些企业经过多年信息安全建设，在其系统内部署了大量的安全设施，并建立相应的安全管理组织和流程，但还是发生了如恶意订购、充值卡盗用、用户信息泄露等问题。

这些问题大部分都与企业的业务密切相关，且呈现不断增长的趋势。主要表现在 :1）面对日益激烈的市场竞争和多样化的用户需求，企业的业务种类不断增多，多种业务流程并存；2）承载业务的 IT 系统越来越复杂，功能越来越多，接口众多，使用了大量的新技术；3）与系统有关的角色越来越多，如最终用户、开发人员、测试人员、运维人员、代维人员等；4）一个系统承载者多个业务，业务之间存在着依赖、交叉。

面对巨大的经济诱惑，有组织的团伙犯罪逐渐增多，地下黑色产业链也逐渐形成，这些问题所隐含的风险正在不断变成现实，严重影响着企业的正常运营。

1.2 挑战

传统的安全评估是基于资产（IT 系统和信息）的，即评估资产面临的威胁、存在的脆弱性，进而分析系统存在的风险。这种评估方法不能有效的发现业务层面的安全问题，例如：恶意订购、垃圾短信、业务冒用、业务欺诈等。如何及时、有效、全面的发现这些问题及隐患，并采取针对性的控制措施，成为摆在企业面前巨大的挑战。

基于业务安全评估正是针对这种情况，提出的一种创新性的评估方法。

2. 什么是业务安全评估

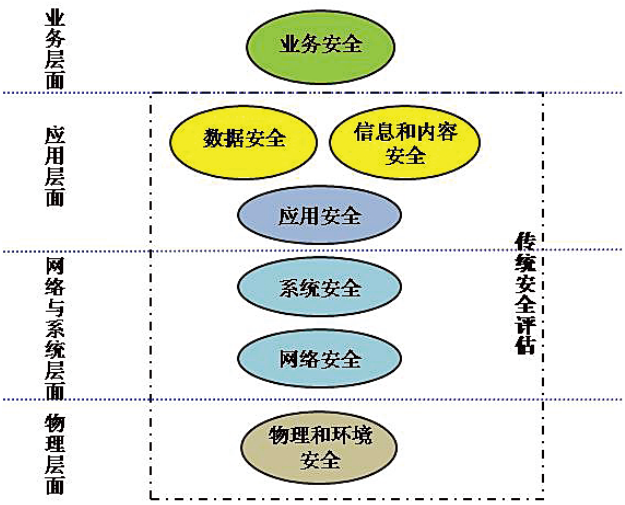
业务通常是指提供给客户的、有价值的服务。一种业务通常面向特定的使用对象、由一系列相互关联的业务处理活动组成。保障业务安全的目的可以归纳为：保证各类业务服务的合法、合规、可控提供，保障业务安全、稳定运行，并避免对客户和企业权益造成损害。

那什么是业务安全评估呢？如何评估呢？在回答这些问题之前，首先要明确业务和信息系统的关系。首先，在信息化时代，业务是由信息系统来承载和支撑的，离开了信息系统业务将不能存在或高效运行，业务对信息系统有一定的依赖关系；其次，随着业务的延伸，一种业务可能是基于多个信息系统，甚至是云计算系统，同时，一个信息系统可能承载着多个业务服务；最后，多个

信息系统因为业务需要，通过相应的服务接口而有机的组织在一起，又因为一个信息系统承载着多个业务，系统间的接口和互联关系是非常复杂的。

业务安全评估是面向业务及其承载系统的一种评估方法，是以业务为中心，以业务流程和数据流驱动的一种安全评估方法。

业务安全评估是传统安全评估的延伸和发展，包括了传统安全评估的所有内容，并侧重于评估业务层面的安全风险，即关注于业务流程、业务处理活动，关注于业务恶用、滥用、盗用、欺诈威胁和风险等。业务安全评估与传统安全评估的关系如下图所示：



业务安全评估以业务为中心，遵循业务风险导向的安全评估，其评估对象和内容也有别于传统安全评估。

3. 业务安全评估的对象和内容

业务安全评估关注业务风险，其评估范围包括：1）覆盖了业务的全生命周期，包括业务设计与实现、业务运行与管理及业务间的接口和关联关系；2）覆盖了信息系统的全生命周期，包括需求、设计、开发、测试、部署、运维、废弃等各个环节；3）覆盖了业务与信息系统承载关系，即业务在信息系统层面的数据流、数据处理活动及其关联关系；4）覆盖了业务安全保障体系的各个方面，包括监控、保护、响应、审计等。

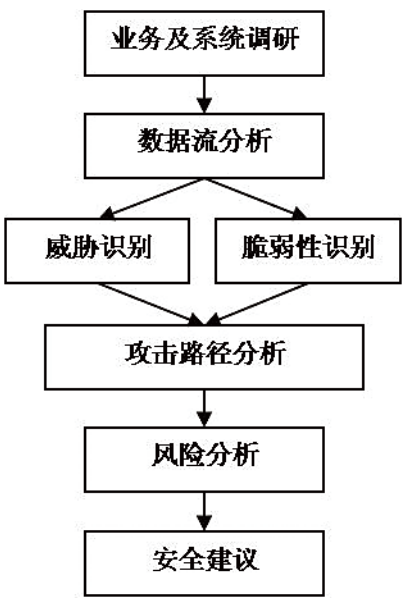
在这些评估范围内，包含了一系列的业务安全评估对象。按照业务层面可分为业务流程、数据流和数据处理活动。业务流程如 OA 系统中的发文流程、收文流程等，反映了端到端的业务逻辑，另外，与业务流程并列的管理流程也是评估的对象。数据流是业务流程在信息系统层面的映射，通常由一系列的数据处理活动单元构成，数据处理活动单元一般是进行技术评估的主要对象。按照信息系统的分层模型可分为数据、应用、系统、网络、物理及信息和内容等。这里需要强调的是：传统的安全评估侧重于数据的机密性、完整性、可用性，而对于业务安全而言，则要进一步考虑数据的可控性、可靠性。按照管控措施可分为管理和技术两个方面，管理方面包括业务流程、IT 管理流程、安全管理流程，技术方面包括扫描、监控、访问控制措施、审计日志等。

业务安全评估是一种评估方法，针对评估对象的评估内容同样是风险构成的三要素即：业务（资产的一种）、威胁、脆弱性及安全

保障措施。从评估内容上可以看出，业务安全评估几乎与传统安全评估相同，同样，其评估流程也基本相似。

4. 业务安全评估流程

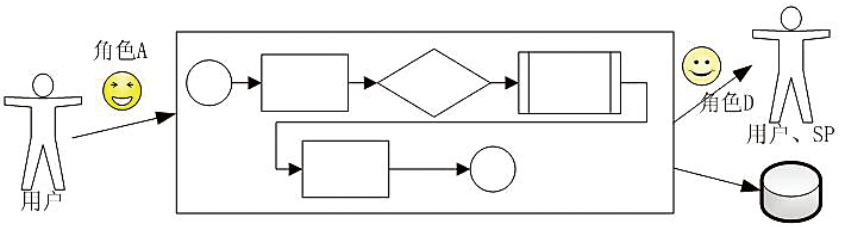
业务安全评估的难点是理清流程，系统全面地描述系统层面的数据流和数据处理活动单元，并对其进行深入的分析和评估，所以其评估流程与传统评估稍有不同。业务安全评估的流程如图所示：



4.1 业务及系统调研

1. 业务功能调研

业务对外表现为一系列的业务功能，因此应首先进行业务功能的调研。即从用户角度调研系统提供的功能，以及支撑功能实现的一系列流程。例如：对于短信业务，具有发信、收信、业务订购和取消功能，发信功能又可分为手机间发信、手机和 SP 间发信等。



例如：对于短信订购功能，有 MO 短信订购流程、WAP 订购流程等。

2. 流程梳理

通常，广义的业务流程包括了众多的业务流程、管理流程（含运维管理、安全管理），且流程间存在着复杂的关联关系，需要进行梳理和分析，以便理清业务与业务流程的对应关系。

流程通常是一个端到端的服务过程，包括用户角色、活动、数据等内容。如下图所示：

3. 明确业务与信息系统承载关系

通常一个业务可能由多个系统承载，因此需要从业务角度出发，明确相关的信息系统，确定信息系统的调研范围。

4. 信息系统调研

信息系统调研主要是明确系统的组网结构、网络结构、系统结构，以及用户、访问途径、数据等构成要素。

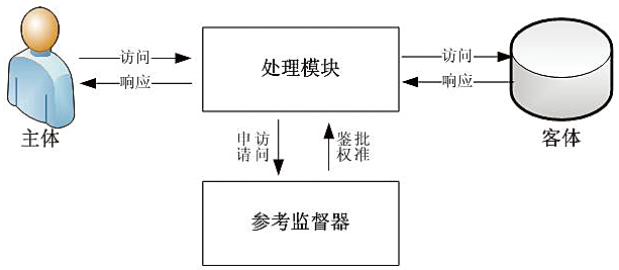
4.2 数据流分析

1. 数据流梳理

基于业务流程，借助信息系统逻辑拓扑图，描述出系统层面的业务数据流，并进行数据流的梳理，明确关键数据流。一个完成的数据流包括访问主体及角色、访问客体、访问活动

等。这些访问活动，通常称为数据处理活动。

一个数据处理活动单元通常指完成单一功能的、密切相关的若干数据处理活动，这些数据处理活动一般存在高度信任关系。一个数据处理活动单元一般可以使用主体、客体、处理模块、参考监督模块等要素进行描述，如下图所示:



另外，还需明确每个数据处理活动单元与信息系统的对应关系，这是进行后续评估的基础。

4.3 威胁识别

在进行威胁识别时，要在业务流程、数据流、数据处理活动单元等不同层面，识别和分析业务面临的威胁。在业务流程层面，主要是流程不畅、流程失控、业务欺诈，用户假冒等威胁。在数据流层面，既要考虑正常数据流面临的威胁，也要考虑隐蔽的、非法的数据流对业务构成的威胁，在数据处理活动单元层面，主要考虑用户假冒、木马攻击、数据泄漏等威胁。

当然，在进行威胁时，还应从传统威胁库出发进行威胁识别和评估。

4.4 脆弱性识别

脆弱性识别是业务评估的重点和难点。脆弱性识别主要基于业务流程、数据流、数据处理活动单元对业务逻辑、系统自身和防护情况进行评估。

1. 基于流程和数据流的评估

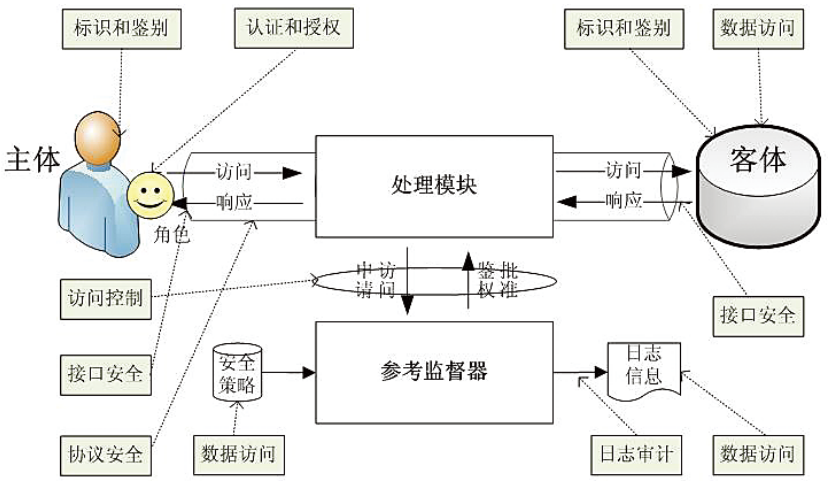
基于业务流程和数据流，使用穿行测试的方法，检查业务逻辑在正常及异常情况下执行时存在的问题。

例如：某运营商的 10 元 300M GPRS 包月业务。1）业务订购：BLWHT 到 XXXXX，回复 Y，就能成功办理万花筒业务，包含有 10 元包月 300M 的 GPRS 套餐，和一个 10 元包月叫新闻的万花筒信息业务；2）业务取消：发短信 0000 到 XXXXX，系统回复短信提示定制了：1、新闻，这个业务，回复：QX1 ，就能取消这个新闻业务，也就是万花筒业务。 取消后，系统短信回复 该业务已经被取消，24 小时内生效，下月不会再扣信息费。但是 10 元包月 300M 的 GPRS 套餐却不会被同时取消。

2. 基于业务处理活动单元的评估

基于业务处理活动单元，可从业务、应用、系统、网络及数据等不同层面，分析系统存在的脆弱性。

业务层面的安全评估主要内容如下图:



• 标识和鉴别：包括主体、客户及其安全等级的标识和关联；

• 认证和授权：包括鉴权绕过、鉴权失效、用户假冒、算法漏洞及角色授权等；

• 访问控制：包括权限边界、权限提升、权限制约（最小授权、分表分权）等；

• 协议安全：协议漏洞、算法漏洞等，例如 WAP、GPRS 等协议漏洞；

• 监控和审计：活动的监督和批准、日志记录、数据处理活动与业务的关联分析等；

• 接口安全：如 Web Service、SOAP 等。

• 数据访问：包括服务器端、客户端的数据安全，以及内容监控检查。例如服务器端的数据创建、修改、删除、访问等，客户端包括 Cookie 修改等。

• 对于应用层面，安全评估的主要内容包括：系统配置（如用户管理、安全策略设置、协议配置等等）、编码（预防 SQL Injection、跨站脚本、缓存溢出等漏洞）、输入检查、错误处理等等。

另外还有系统、网络等层面的评估。这些评估都应借鉴传统安全评估方法和实践，以提高评估的效率和质量。

4.5 攻击路径分析

在威胁、脆弱性分析完成后，需要评估威胁和脆弱性的结合，即威胁是否能够利用脆弱性，如果能够利用，则要深入分析业务被攻击的可能路径和危害。攻击路径分析的最终结果必须明确是如何对业务构成影响。

为了验证攻击路径假说是否存在及发生的可能性，可采用渗透测试的方法加以检验。

4.6 风险分析

风险分析可采用定性的方法，评估威胁造成的客户损失、法律责任、经济损失、市场品牌损失等。

4.7 安全建议

最后是根据发现的问题，给出相应的安全建议。例如：

• 漏洞修补；

• 切断攻击路径；

• 加强审计，加强震慑；

• 对业务运行情况进行实时监控等。

5. 举例

针对某运营商的短信系统。

1. 业务及系统调研

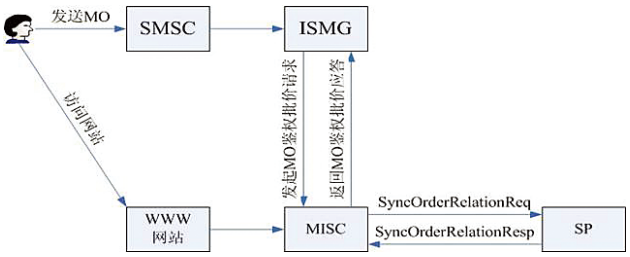
对于运营商的短信系统，其具有的业务功能有: 发信、收信、订购、退订、计费等。

对于订购功能，又可分为 MO 订购和 WAP 订购两种方式。MO 订购流程为：发送订购信息 > 服务商批价鉴权 > 生成订购关系 > 与 SP 订购关系库同步；WAP 订购流程为：访问 WAP 网站 > 提交订购信息 > 服务商批价鉴权 > 生成订购关系 > 与 SP 订购关系库同步。

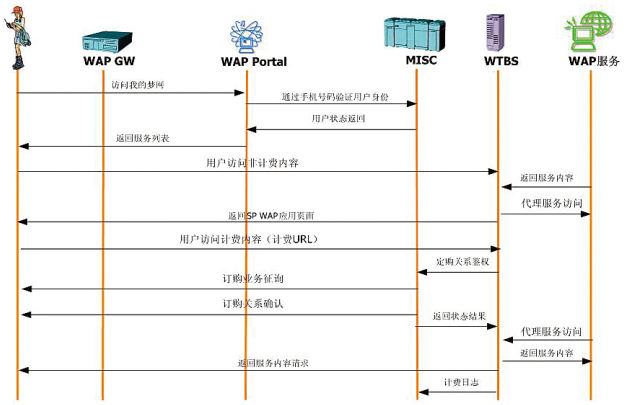
而短信功能依赖的系统有: GSM 无线网、短信中心、短信网关，以及 GPRS、WAP 网关等。

2. 数据流分析

基于系统的逻辑拓扑结构，其订购流程的数据流如下图所示:



贯穿订购数据流的数据处理活动可以采用流程图或者时序图描述，例如 WAP 订购的数据流如右图所示:



分析发现，这些数据处理活动分属于不同的系统（这是由于该数据处理活动分析粒度较粗的缘故，当然，根据需要可以进行更加细粒度的分析），信任关系较低，所以作为不同的数据处理活动单元进行后续分析。

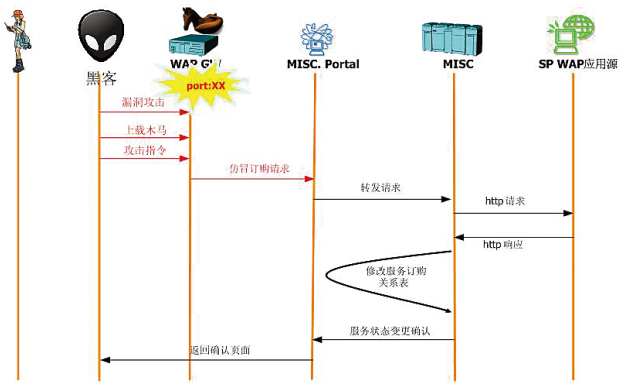
3. 威胁和脆弱性分析

订购业务的主要威胁是：恶意订购、假冒订购等。系统存在的脆弱性包括：代维方有超级用户权限、WAP 协议漏洞、终端软件控制等。

4. 攻击路径和风险分析

1）由于代维方拥有超级用户权限，其可以上载木马，假冒用户建立业务订购关系，谋取私利。

2)WAP 协议漏洞，造成外部黑客可以攻击 WAP 网关，上载木马，假冒用户建立业务订购关系，如下图所示。



3）客户手机终端被恶意植入木马，可以隐蔽地发起订购流程，并拦截二次确认信息，伪造确认响应，形成恶意订购关系。

6. 评估工具与手段

在进行业务安全评估可采用的评估工具包括:

系统漏洞扫描器

- WEB 应用扫描器
- 代码检查
- 渗透测试工具
- 当然，也需要采用顾问访谈、人工检查、工具扫描、渗透测试、文档检查、穿行测试等评估手段。

7. 结束语

业务安全评估是信息安全评估发展的一个重要方向，它针对的是企业在业务层面所面临的一些安全问题。通过业务安全评估，企业能够做到:

全面、快速、有效的发现面临的业务风险; 明确风险控制策略，制定针对性的安全控制措施；推动信息安全保障体系的改进和完善。

在进行业务安全评估时，应与传统安全评估相结合，并根据具体业务情况，对评估内容和流程进行调整和优化，以有效提高评估的质量和效率。

随着安全管理日益常态化，业务安全评估也将向业务安全监控和分析的方向发展和演变，业务安全评估也必然会加快此类产品的发展。

WEB应用评估思路与趋势

技术支持部 梁伟

摘要：信息技术与信息安全是并存的，随着各类 Web 应用的出现和相关技术的不断进步发展，Web 安全问题已经日益凸显出来。根据 IBM X-Force 的威胁分析报告显示，2008 年与 Web 相关的漏洞占全年总体披露漏洞的 54.9%，而在 09 年虽因一些原因导致这个数字有所下降，但这个数字仍达到了49%，所以 Web 应用安全仍然是近几年不能忽略的重点。

关键词：Web　安全评估　用户业务

1. 引言

随着信息技术的不断发展，终端用户正在逐步抛弃繁琐、多样的客户端软件，并急切地需要将所有客户端能无缝的融合在同一个软件之上，只需这样一个软件就能完成一切他们想要在互联网上的任何操作。

而另一方面，作为服务的提供者和运营者，也更期望能将多种多样的服务同样以一个简单、易操作的界面呈现给终端用户，从而减少管理和维护的成本、统一各类服务的接口规范。

因此，Web 应用在产生十余年后的今天，再次绽放，终端用户无需再准备各种复杂的客户端，只需通过浏览器在 Web 界面上进行简单的点击就可以完成大部分的工作，而服务提供者们也顺势将各类应用的呈现形式都转移到 Web 之上。

但是，信息技术与信息安全是并存的，随着各类 Web 应用的出现和相关技术的不断进步发展，Web 安全问题已经日益凸显出来，根据 IBM X-Force 的威胁分析报告显示，2008 年与 Web 相关的漏洞占全年总体披露漏洞的 54.9%，而在 09 年虽因一些原因导致这个数字有所下降，但这个数字仍达到了 49%（如图 1 所示），所以 Web 应用安全仍然是近几年不能忽略的重点。

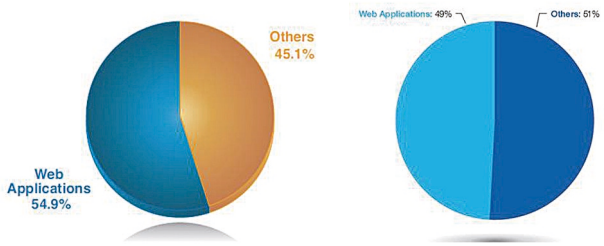


图 1　08 年（左）和 09 年（右）Web 安全漏洞占总提漏洞的百分比

2. 传统安全评估

传统安全评估主要以点到点的方式进行（如图 2 所示），尤其在传统评估中，针对 Web 应用的评估大多以渗透测试的方式来完成，这虽然能从很大程度上模拟甚至完全实现一般入侵者的入侵行为，但却难以覆盖全部 Web 应用相关的技术点，更无法从业务逻辑上对 Web 应用所承载的业务实现有效的安全测试。

因传统评估中对 Web 应用的评估手段覆盖范围小，导致报告输

出内容较为狭窄，其输出完全决定于渗透测试人员的技能和“运气”，因此很可能会出现无输出或是输出内容较少而缺少实质参考价值的情况。而且，技术人员的渗透测试往往是以技术为输入、同时以技术为输出，其输出报告内容技术性较强，对于一般用户来说，这样的报告可读性较弱，多数用户可能在读后仍不能完全理解这些技术点与其业务系统之间的关联，很多时候，甚至需要专业的开发人员相互配合的情况下才能对这份输出做到完全理解。

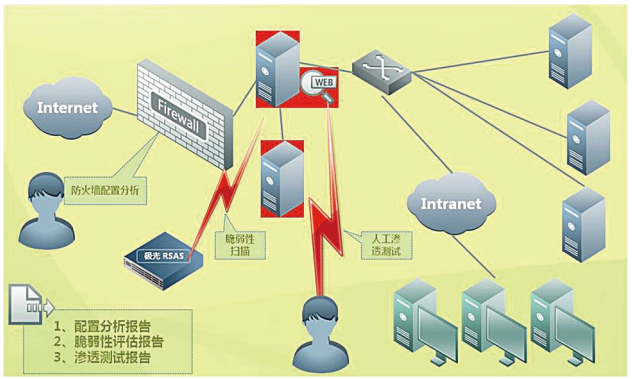


图 2 传统评估方式

3. Web 应用评估思路

在 Web 承载了重要业务应用的网络中进行安全评估时，Web 应用是必不可少的评估对象，甚至可以这样理解，整个评估对象就是以 Web 应用为核心向四周进行网状散发的一整套系统，而网线所链接到的各个系统不过是 Web 呈现的基础支撑，出于这样的考虑，我们将 Web 应用评估划分为以下五个重要过程:

1. 确定评估范围

2. 实施业务流梳理

3. 行白盒 / 黑盒测试

4. 节点风险与业务流合并

5. 结果输出

下面，将对前四个过程进行详尽的阐述。

3.1 确定评估范围

在 Web 应用为核心对象的评估过程中，承载 Web 应用的服务器自然是必备纳入评估范围之内的，这些服务器一般分为三类:

前台 Web 服务器

大多以 Apache 或 IIS 作为 Web 应用的前端，仅对部分静态页面的请求进行响应和解析，而对于动态页面的解析直接转发到中间件。

- 中间件

用于接受和处理前台转发的动态请求，如：weblogic、websphere、tomcat 等。

- 数据存储

- 用于存储数据，接受中间件的存取请求，如：Oracle、MSSQL、Sybase 等。

除这些必不可少的应用之外，不同的业务系统还会有额外的用于提供重要业务数据的存储和处理用的服务器，这些服务器一般都是与置于前端的 Web 服务器独立分开但又有所交互，在评估过程中，这些对象是不可遗漏的。

另外，还有一些服务器往往也存在于这些业务系统中，如：管

理主机、报表系统等等。

那么，到底该如何定义评估对象呢?

在这里，我们首先将对象分为两类：可信对象和非可信对象。

对于可信对象的定义是：完成全部对外或对内所提供的业务时，必不可少的服务器即为可信对象。

对于非可信对象的定义是：若缺少该服务器，可能会影响日常管理等工作，但不会造成任何业务的中断。

为什么要区分可信对象和非可信对象?

因为，对于可信对象和非可信对象的要求应该是不同的，甚至从逻辑上可能是要分离的，但在很多企业网络中并没有很好的实现和贯彻。

3.2 业务流梳理

业务流的梳理能从前期解决最终输出过程中很重要的一个问题，即：业务的拥有者往往无法理解技术测试者在说什么。

通过业务流的梳理，有以下三个目的:

1. 查找业务系统承载的全部业务

以业务办理者的视角去理解这套系统能为他提供什么。

2. 为业务办理流程的安全测试提供素材

在以业务为测试对象的过程中，业务流程的测试是经常被忽略却又十分有价值的。

3. 以业务流作为业务拥有者和技术测试者的共同语言。

业务拥有者可能对技术关注不多，而技术测试人员对业务又不了解，那么，就如同两个使用不同语言的人在进行交流，而在业务流程梳理清晰后，技术测试人员就能以业务流作为其语言向业务拥有者进行安全问题的描述。

由此看来，业务流的梳理虽看似与实际测试过程相关性不大，但却对最终测试结果起到至关重要的作用。

3.3 黑盒 / 白盒测试

无论业务系统如何复杂，仍是由各个节点组成，因此，技术测试仍然要从每个单独的节点开始，这里的安全测试包括以下几项:

1. 外部脆弱性扫描（黑盒）

外部脆弱性扫描作为黑盒测试的手段出现，其中又包括：远程扫描器扫描；远程人工渗透测试及验证。

2. 本地脆弱性评估（白盒）

本地脆弱性作为白盒测试包括：本地漏洞扫描；本地系统策略分析；本地应用配置分析；本地应用权限分析；代码安全性检测。

除对单节点的常规测试之外，还要从网络层对整体的网络安全性进行测试，包括:

1. 信任关系检查

对于点对点传输的链路，检查上下游两点所对应服务器是否具备唯一的信任关系，以防止外部恶意用户通过中间人劫持的方式进行欺骗。

2. 传输安全检查

检查数据传输过程中是否安全。

最后，据业务流的梳理结果对整体业务进行业务层面的白盒安全测试，包括:

1. 业务逻辑常规测试

在业务逻辑常规测试过程中，需尝试通过认为干预的方式是否能破坏正常的业务流程。

2. 业务逻辑劫持测试

假设正常业务逻辑为：A → B → C → D，而恶意用户为 H，则测试会尝试使用各种手段进行劫持，造成逻辑变为：H → B → C → D 或 A → H → B → C → D 等情况。

3. 业务逻辑中断测试

该测试会尝试使用各种手段导致业务逻辑中断，从而影响正常的业务办理，但这些手段中不包括拒绝服务、溢出等传统攻击手法，而仅仅是从业务逻辑层面进行，如：构造逻辑 A → H → B → C → D，而恶意用户 H 尝试中断整个逻辑过程。

业务测试过程中，可能会带有一定的风险，因此，业务测试一般采用两种手段：

1. 单节点测试

仍假设业务逻辑为：A → B → C → D，而恶意用户为 H。单节点测试不会涉及全部的 A、B、C、D 四个系统，而仅尝试 H → B 或 A → H → B 的可能性，从而减少风险。

2. 交流代替测试

在很多需要 24 小时在线的业务系统中，即使使用单节点测试也可能会带来隐患，因此，在很多情况下，与业务系统的设计、实现者进行测试方法的交流也能很好的代替实际测试过程。一般交流以业务流梳理完成为起点，测试人员提出可行的测试方案以及具体实现思路和方法，由业务系统的设计者和实现者评定测试方案是否能够实现，若能够实现，则认定系统存在问题，由实现者协助修补，这种方式的好处在于不但能规避所有风险，而且还能让设计者和实现者参与其中，更好地了解系统设计的缺陷，同时更有效地提供修补方案。

3.4 节点风险与业务流合并

在此环节，测试人员需将针对节点和针对业务流的测试进行汇总，将汇总结果进行合并，合并原则是：所有测试结果最终均以业务流作为中心。这样，就完成了以业务流为主线的测试结果。

另外，由于之前在测试过程中业务流梳理者和节点测试者两个角色可能由两个甚至多个人分担，因此，在合并汇总的过程中，还有一项重要工作：节点风险在业务流上的体现及二次测试。这个测试过程主要是结合业务流自身问题将节点上的问题再次凸显出来，从而形成真正完整的以业务流作为中心的评估结果。

4. Web 应用评估输出

评估的输出不但是评估成果的重要展现，也是评估过程及评估思路的重要体现。

在以 Web 应用承载的业务系统为主要评估对象的过程中，评估的输出除了传统的各类分析报告外，还会输出业务逻辑威胁分析报告。

业务逻辑威胁分析报告主要用于展示业务流程，并包含业务流程中所涉及到的各个节点上所存在的安全问题，同时，将这些问题与业务流自身的问题结合在一起，形成针对业务流自身安全问题的分析报告，正确的梳理出业务系统中所包含的威胁路径。

5. 后记

关于 Web 评估思路的介绍大概就到这里了。

而对于 Web 安全评估来说，这也仅仅是一个开端。Web 应用与传统的操作系统、应用软件不同 —— Web 应用并不像它们一样：即使装在全世界的机器上也仅仅是版本和语言之间的区别，每个 Web 系统都是个性化、都是与众不同的，因此，围绕 Web 应用的每一次评估工作也都是一次针对客户的定制化评估过程，所以，我们还需不断摸索以寻找更高、更理想的评估思路和方法，以达到 —专攻术业，成就所托。

网上银行安全面面观

行业技术部 徐一丁

摘要：本文就网上银行比较重要的安全问题进行了讨论，包括网上银行的三个交易环节、客户端与服务器端如何保护以及今后的发展等内容，可以作为了解网上银行背景与现状的参考材料。

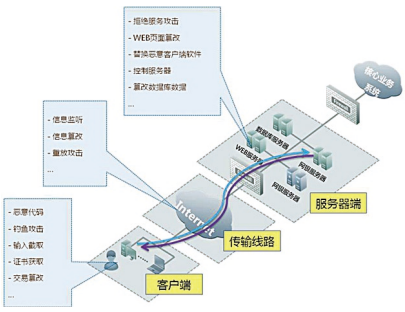
关键词：网上银行　客户端和服务器端保护　安全建议

新业务模式带来的风险

国内第一家正式运行的网上银行在1999年开通，至今已经有十余年了，这种新的业务模式从诞生之时起，针对它的攻击行为就层出不穷。用户既享受着网上银行带来的便利性，又不免担心着自己账户里资金的安全。现在，网上银行的安全性已经成为一个不可回避的严重问题。

网上银行面临的安全威胁

为了清晰地介绍网上银行的安全状况，首先简要介绍一下网上银行面临的主要威胁。



从网上银行整个业务过程来看，可以分为客户端、传输线路和服务器端三个环节，它们都面临着不同的安全威胁。如右图所示：

客户端位于网上银行用户一方，网上银行操作的各种请求在这里生成，通过B/S或C/S软件向服务器端发出；传输线路主要指Internet，是客户端与服务器端连接的必经之路；服务器端位于银行一方，接收来自用户的请求并进行处理，同时与内部的核心业务系统交互来完成操作。

下面从技术角度对这些不同环节所面临的威胁进行分析。

客户端面临的威胁是多方面的，攻击者的目的一般都是获取用户的账号、口令和个人证书等信息，冒充用户身份非法转移资金。主要威胁包括恶意代码、钓鱼攻击、输入截取、证书获取、交易篡改等；恶意代码通常是作为侵入客户端的第一个手段，包括蠕虫、病毒、恶意脚本等。钓鱼攻击是伪造网上银行交易系统，诱使投资者使用虚假系统登录，造成账号和口令的泄密；输入截取是获得用户的击键或鼠标点击记录，通常包括网上银行的账号与口令；证书获取是取得用户计算机中个人证书，以冒充用户的身份；交易篡改是较少出现但很有威胁的一种攻击，可以将用户的网上银行操作指令内容进行非法改变以实现其攻击目的。

传输线路中主要面临信息监听、篡改和重放攻击的威胁。信息监听会将交易请求在传输过程中泄露给非授权人员；信息篡改会使交易信息在传输过程中遭非授权人员篡改；重放攻击是未授权人员复制合法用户的交易请求，并多次提交。

服务器端是网上银行系统运行的中心，通常会遭受拒绝服务攻击。拒绝服务是利用海量的数据包或长连接占用服务器端的线路资源，导致正常用户不能访问；“侵入”是一类攻击的总称，攻击者利用如SQL注入、远

程溢出等手段入侵并控制服务器端，并进行页面篡改和替换客户端下载程序等后续操作。

当前攻击的主要目标是客户端

理论上，三个环节都存在威胁，而从国内网上银行的现实来看，大多数攻击行为集中在对客户端的攻击上。这是由攻击成本、攻击风险和攻击收益几个因素决定的，请见下表：

攻击对象	攻击成本	攻击风险	攻击收益	攻击者意愿
服务器端	高	高	高	少碰为妙
传输线路	中	中	低	懒得去搞，费事
客户端	低	低	中	主攻方向

首先看服务器端，这里属于“高风险、高回报”的区域，服务器端是网上银行系统运行的平台，保存着网上银行用户的资料，并向内联接银行的核心业务系统。现在的网上银行系统都十分注重安全防御，通常部署了完备的安全设备，包括防火墙、入侵检测系统、抗拒绝服务攻击系统、漏洞管理系统等等，同时还有专门的人员进行监控，一旦发现异常能够马上进行处理——可谓重兵把守，层层设防。在这种情况下，攻击服务器端需要有更高的技能、更隐蔽的手段和足够的耐心，而且这种案件被重视的程度高，一旦失手被擒，后果就非常严重，完全可能被以“破坏金融管理秩序”的罪名来判刑，量刑极重（参考广州许霆 ATM 一案）。因此，虽然攻破网上银行服务器端的获利是巨大的，但需要更多的技术与经验，而且面临着严厉的追查和沉重的刑罚，这让大多数攻击者望而生畏。

其次是传输线路，这里可以利用的攻击方法少，也缺乏有价值的获取物，因此很少被关注。Internet 是开放的区域，攻击者可以进行监听和信息篡改，但网上银行的数据包都是加密的，真实的信息截取不到；即使被破解，数据包里最多只有账号和口令，而网上银行交易必不可少的证书信息是不会在网络上进行传输的；重放攻击也涉及到很复杂的技术与流程而不易实现。

最后是用户所在的客户端，这是最容易攻击也最容易获益的一个环节。攻击者可以利用 Internet 将木马很方便地传播到成千上万的用户计算机上，通过击键记录、截屏等方式获得网上银行账号口令，同时获得软证书，这样就完全控制了用户的网上银行账户；如果用户使用的是硬件的 U-Key 来保存证书，攻击者还可以想办法篡改网上银行操作的指令，直接将钱转到自己的账户中去，攻击进行的时候，大多数网上银行用户可能毫无知觉，直到某天查看自己账户的时候才大吃一惊。

用手握住一根铁链的两端用力去扯，力量足够大时，链条会在最薄弱的一环断开。在网上银行的业务链条中，客户端就是这个最薄弱的环节。即使在安全知识已经普及的情况下，还是有很多网上银行用户的计算机

存在各种漏洞，再加上用户的安全意识差，攻击者会轻而易举地找到很多目标。风险小而获利可观，因此大部分网上银行攻击就自然地聚焦于客户端。

网上银行客户端是如何被攻击的?

攻击起来很方便，成功了就能得到钱，而且被抓住的可能性很小。这使得现在受到利益驱动的攻击行为越来越普遍。

在一台用户计算机上，主要的攻击操作是由木马自动实现的。木马可以在受害的计算机后台悄悄地完成许多任务：截取用户的击键记录、截屏以记录用户的鼠标点击动作（可以截取到软键盘上的网上银行口令）、窃取网上银行的软证书等等。攻击者的首要任务就是编写这样一个木马程序，在木马成功植入受害计算机时，能顺利地完成这些操作。

木马程序写好之后，怎么传播到别人的计算机上呢？这里有多种方式，例如侵入一个比较热门的网站，篡改其网页，在其中插入木马下载的动态语句，当有某种漏洞的计算机来打开这个网页时就会中招，把木马下载到本地并安装；再例如，通过即时通讯软件或邮件传播木马，发送这样的消息："知道最近著名的 XX 门吗？我的附件里有照片！"……"想在春节时买到平价的火车票吗？打开这个附件看看"……安全意识差的人往往会点击打开，木马就进入系统了。

在现实环境中，攻击者散播木马时不会拘泥于网上银行账号的钱，有什么值钱的东西都会盗走。用户计算机里可能有网游的高级装备、Q 币、网上银行账号、网上证券账号、网上支付账号等，这些都可以转变为实际的钱。比较完善的木马会扫描受害计算机，找出、记录这些有价值的信息，打个包发送到攻击者指定的邮箱去；也可以只是告诉攻击者这台计算机有什么东西值得注意，攻击者再从远程偷偷地人工获得这些信息。

攻击硬件 U-Key 的网上银行客户端，相对来说比较麻烦，因为理论上硬件 U-Key 中保存的用户证书是无法被攻击者取得的，但还是可以想办法去攻击。例如篡改用户的交易指令，将用户想转到账号 A 的钱转到账号 B 上去。

网上银行安全建设的要点

银行作为网上银行系统的建设和运营者，需要全面地考虑安全保护措施。近几年来国内的区域性银行纷纷上线网上银行业务，为保障网上银行业务的安全运行，在本文的分析基础上，可以考虑以下几点建议。

注意服务器端和客户端的双重保护

虽然攻击主要集中在客户端，但服务器端的保护对银行来说仍然极其重要。即使服务器端防守严密，安全监控到位，但由于高回报的驱使，还是会有少量的技术高超、经验丰富的攻击者会尝试对服务器端进行入侵，就像胆大妄为的人会去抢银行一样。客户对银行信任，才会把自己的钱存到银行，因此服务器端是绝不能被攻破的，一旦被攻击者得逞将直接威胁客户资金的安全，给商业银行带来的利益与信誉损失是无法想象的。

尤其是那些新开办网上银行业务的银行，第一次将业务系统直接接入 Internet，缺乏相关的经验，更需要在服务器端进行全面的保护。

网上银行项目前期就需考虑安全

在网上银行建设阶段就要重视安全，安全设计介入越早成本越低。很多应用系统的漏洞是在业务流程和架构设计、程序开发时

就存在的，在后期改正起来非常麻烦，甚至改正的成本要大于重新设计开发；在网上银行系统集成的设计阶段也应加入安全体系的设计，而不是系统建成后再添加安全设备，因为有些问题是存在于网络架构设计与安全域划分当中的，我们很难在网上银行系统正在运营时再去重建一次网络，来达到安全。

注意合规性，满足监管部门的相关要求

根据银监会的要求，商业银行开办网上银行，要按照 2006 年发布的《电子银行业务管理办法》的规定，依据《电子银行安全评估指引》要求的八个方面去进行评估，提交申请材料后才可以正式运行网上银行。2010 年 1 月，人民银行也发布了《网上银行系统信息安全通用规范（试行）》，要求各银行按照其中的要求去建设网上银行，这也是一个非常好的参考文档，与银监会的《评估指引》相比，人民银行的《通用规范》新增了对客户端保护的要求，能够实现较好的保护水平。

注意安全保护的适度

从综合的效益考虑，银行不必在网上银行的每一个环节上都做到完全的安全。按照风险管理的思想去降低和转移风险，把风险控制在可接受的水平，才能实现银行利益的最大化。例如，国内很多家网上银行还保留着软证书，其实这些银行都明白软证书与硬件 U-Key 证书相比不安全，相对容易被非法窃取。那为什么还要保留软证书呢？因为软证书用户体验好，更方便，在计算机上打开浏览器直接就可以登录，不怕把 U-Key 忘在公司抽屉里，也不必在使用较老的计算机时爬到桌子下面去插 U-Key。没有软证书，电子业务部门担心马上会产生客户流失，他们认为相对于客户流失，少量用户被盗后产生的赔偿损失反而是可接受的。

在银行内部，网上银行系统的使用者是电子业务部门，运维者和主要保护者是 IT 部门，两类部门应进行充分的沟通，确定一个“最合适的安全方案”，而不是“最安全的方案”。

网上银行安全今后的发展

从将来的发展来看，个人用户、银行和安全研究机构应该进行良好的配合。个人用户的安全水平和安全意识有待进一步提高，这样才能运用银行和安全公司提供的安全手段，配合整体安全体系。银行需要时刻关注用户的安全需求和安全攻防技术的进展，随时准备加强网上银行业务的安全性。安全研究机构需要对个人的用户和银行提供长期的技术支持，不断研究新的安全技术来保障这方面的安全。

除了以上和网上银行业务安全直接相关的各方外，国家和政府也需要制订合理的法律法规，在网上银行犯罪举证和法规方面进行加强。如果从网上银行攻击的取证、定罪到制裁的过程有一套很完整、很合理的法律法规去保证的话，攻击网上银行的行为人能很快被抓到，根据确凿的证据进行定罪，再进行合理的惩罚，这样对制止网上银行犯罪会有很大的震慑力。

从长远来看，建立国家级的社会信用体系会对制止网上银行犯罪有很大作用。如果网上银行攻击会导致一个人的信用分数下降，就加大了攻击者的成本和风险，严重时可能让罪犯在这个社会上难以立足，应该能从另一方面有效地制止网上银行攻击。

DDoS进入全面技术对抗时代

技术支持部　何坤

摘要：作为绿盟科技抗 DDoS 产品（又名黑洞）的工程师，笔者参与了若干国内重点 DDoS 事件处理，与 DDoS 攻击者进行了多次素未谋面的网络对抗。本文在介绍国内 DDoS 攻击发展趋势的同时，也向读者介绍 2009、2010 年各类常见 DDoS 攻击的特点以及防护策略。

关键词：DDoS 趋势 流量清洗 ADS 黑洞

在网络世界里，DDoS 是“强盗”的代名词，它是攻击效果最为明显的攻击形式，不同于其它攻击，DDoS 攻击的影响范围广、影响程度大。

DDoS 攻击已不再是黑客技术的炫耀，它更多出于经济利益或政治目的。

1. 不同时期的 DDoS

为了方便介绍，暂且将 DDoS 大致分为三个阶段，每个阶段都有其相应的特点，在这里先简要介绍一下各个阶段的特点，然后进行分析。

1.1 早期的 DDoS 攻击

早期的拒绝服务攻击以使用 DoS 工具的居多。现在只要花点时间在网上搜一下，仍然能搜罗出大量的 DoS 工具，比如阿拉丁攻击器随处可见。工具的泛滥导致了拒绝服务攻击的门槛降低，只要你想，你就可以随便 down 两个 DoS 工具随意发起攻击。

这些工具有一个特点：源 IP 虚假。也就是说，DoS 工具只管向服务器狂发包，其余什么都不管。由于源 IP 虚假，受害者也就无法溯源，反过来让攻击者肆无忌惮。

还有一些 DoS 单机工具，可以构造一些特殊的畸形报文，让服务器一触即挂，但现在各个地方服务器补丁的管理已经非常到位，网上的这种工具已经没有效果。

1.2 中期的 DDoS 攻击

上面提到，早期的 DoS 工具的特点是源 IP 虚假。而早期的抗拒绝服务设备（也叫清洗设备）就利用了这一点，只要清洗设备能够验证这个源 IP 是否真实存在，也就可以很轻松的防护住假 IP 发起的攻击。

也是在这时候，一些新名词出现了：肉鸡、傀儡、僵尸。利用木马技术，黑客可以控制住活跃在网络中的大量主机，也就是肉鸡，然后可以利用他们做很多事情，发起 DDoS 攻击就是其中之一。

使用肉鸡发起的攻击主要特点是什么呢？源 IP 是真实的。

1.3 现在的 DDoS 攻击

现在已经形成单机工具攻击、肉鸡攻击、复杂攻击并存的局面。

先谈复杂攻击，攻击之所以变得复杂，不是攻击者自己想要复杂，他也是受整个大环境的影响。因为受害者也都全是被动的，市面上已经有很多抗拒绝服务设备，经常受到 DDoS 侵扰的受害者已开始使用这类设备，与攻击者对抗。当攻击者发现过去的攻击方式没有效果，必然会寻求另外一种有效的攻击手段。

笔者在近一年来监测到很多起非常有效、非常致命的 DDoS 攻击，在这里，我们把它叫做“复杂攻击”。

比如，我们去年发现的一种 DDoS 攻击就很“特别”：源 IP 都是真实的，这些源向服务器发起的访问也是真实的，只是这些真实流量“去错”了地方。打个比方，这些源 IP 本来是要去访问 www.a.com 的，但都“莫名其妙”的来到了 www.b.com，造成的后果就是 www.b.com 的服务器负载增大，甚至无法访问。经过这次事件的处理，笔者与同事分析了这种“攻击”的特点。

1、这是攻击吗?

站在受害者 www.b.com 的角度，这属于攻击。因为 b 只有一台服务器，1 秒钟约 100 个本应到达 a 的流量就让它不堪重负，已经产生了拒绝服务的效果，所以在 b 看来，这是攻击；

那么 a 是攻击者吗? 从技术角度来说，不能断定 a 就是攻击者，完全可能有个第三者 c 通过篡改 DNS，让 a 的流量去向 b，又或者 DNS 或其他的网络环节出了故障。从我们几次与这种攻击交锋的经验来看，这种“故障”的概率未免高了一点。

2、不用抓肉鸡，人人皆“肉鸡”

过去发起 CC 攻击需要拥有大量肉鸡，而再看这种攻击，攻击者不需要自己抓肉鸡了，已经有另一种途径发起类似肉鸡发起的 CC 攻击，也许哪一天，你在访问某知名服务的时候，就意外的成为了“肉鸡”。

3、防范难度增大

这种看似攻击又不太像攻击，却能达到很强的攻击效果的行为，让很多网络维护人员防不胜防，即使防住了，想要抓到真正的幕后仍然很难。

下面介绍笔者遇到的其中一种“复杂攻击”。

2. 应对策略分析

2.1 应对早期的 DDoS 攻击

DDoS 安全防护发展了这么多年，大多现在的清洗设备都已能够直接防御早期的 DDoS 攻击，也就是虚假源 IP 攻击，而且都能“清洗”得很干净。

现在攻击者再用此类攻击的话，可能会先用小流量尝试攻击，如果受害者的攻击者服务器性能弱、带宽小，又没有任何防措施，那很快就能得手，也不用费太多精力。

当攻击者发现小流量攻击没有效果，他会意识到受害者可能有防护设备（或者是防火墙、或者是专业抗 DDoS 设备），攻击者将提升攻击流量（前提是攻击者有带宽资源）。很多人知道，防火墙从防护机制上决定了它是不具备抗 DDoS 攻击能力的，小流量还可，流量一大，被攻击的服务器瘫痪之前，防火墙可能已经垮了。这时候，被攻击用户要么提高服务器能力、带宽、改 IP; 要么使用更大性能的专业抗 DDoS 设备，因为有人已经盯上你了，你别无他法。

2.2 应对中期的 DDoS 攻击

前面提到一些攻击者开始以提升攻击流量来达到拒绝服务的效果，这是需要物质基础的，并不是很多人都有这个条件。然而全球范围内的大量肉鸡群，正好可以满足。一台肉鸡带宽有限，但上千、上万台肉鸡的力量就不可忽视，再加上肉鸡 IP 是真实的特点，防护算法差的设备就难以防范此类 DDoS 攻击。当肉鸡的攻击的流量到达清洗设备，清洗设备对肉鸡进行探测，将发现这些源 IP 是真实的，不是虚假的，此时清洗设备的第一道关卡被突破。

优秀的清洗设备，在面对真实 IP 的攻击时，其不光能够辨别源 IP 的真假，还能从应用层行为上判断这些源 IP 是否真的是要访问服务器资源，也就是所谓的 CC 防护。CC 防护算法

主要有 URL 防护、HTTP Cookie 防护、图片验证等等，防护算法越多，在对抗时能够采取的手段也就越多，攻击者就越难以突破。

2.3 应对现在的 DDoS 攻击

为了提升攻击效果，攻击者不断地创造新的攻击手段，攻击流量大小往两级分化，要么攻击流量很小（几兆流量，以小博大），要么攻击流量巨大（上 G 流量，以大欺小），发出的攻击报文经过精心构造，以期让受害者毫无还手之力。

下面再向大家介绍一些目前经常遇到的精细化攻击及防护。

1、精心挑选的动态页面

动态页面是最耗服务器资源的，当攻击者发现目标的网站中存在需要数据库查询的连接，比如“站内搜索”、“投票”…它就可以使用肉鸡资源，对这些页面进行快速查询，这些动作产生的流量不用太大，最终的结果，服务器在这类小流量的冲击下崩溃。

这种攻击的防护不是简单判断一下真假就可行的，因为肉鸡 IP 是真的。此时清洗设备可使用 CC 防护算法（肉鸡可以自动识别高复杂度的图片吗？），还可以结合连接耗尽策略（限制服务器的连接数）。

如果你没有清洗设备，那可以去掉这个动态页面，也可保障服务器的正常运行，当然也损失了部分正常用户。

2、精心构造的攻击报文

针对不同的攻击目标，攻击者将攻击报文进行不同的伪装，从报文任何一方面看上去都没有破绽。比如攻击网吧，就用与网吧正常流量非常类似的流量进行攻击；攻击网站，就用与网站正常流量非常类似的流量进行攻击，让你的防护设备无法正确识别。

这种攻击的防护对清洗设备的防护算法要求极高，清洗设备主要利用应用协议的一些细节部分进行防护，抱歉在这里还不能与大家分享，相信大家理解。

3、不按套路出牌

攻击包有时随机、有时固定、有时分片；攻击报文长度有时超长、有时超短。对于这种攻击的出现，笔者认为攻击者知道被攻击目标部署了清洗设备，而防护算法可能是存在缺陷的，他是在使用各种流量来进行试探攻击，也许你的清洗设备对这类报文就不防护了呢？

这就是考验清洗设备的算法完备性了，虽然流量清洗设备基本上没有类似病毒库的东西，但算法上必须要做到完备，什么情况都必须考虑到，否则将无法适应当前的 DDoS 新形势。

除了以上攻击，现在也开始出现由于软件 BUG 引起的 DDoS 问题，比如某著名软件引起的 DNS 断网事件。相信在网络日益紧密的大环境下，这类由软件 BUG 引起的 DDoS 情况将增多。

3．小结

道高一尺、魔高一丈？还是魔高一尺、道高一丈？

从目前的 DDoS 形势看来，一眼就能看出是攻击的情况将会越来越少，未来的 DDoS 攻击将更加隐蔽，DDoS 攻击已经不再是搞几个工具，然后狂发 SYN 包、狂发 ACK 包的时代；更多的往应用层攻击（CC 攻击）发展，新的 CC 攻击将层出不穷，让你很难发现和识别；攻击流量大小两级分化，要么以小博大，要么以大欺小；清洗设备防护算法的更新很重要，DDoS 应急响应的能力也同样重要；取证会越来越困难，想要抓住真正的攻击发起者也更难，可以推测，DDoS 将进入全面技术对抗的时代。

Flash 安全漫谈

研究部　曲富平

摘要：文章首先对 Flash 安全的重要性进行了解释；然后结合 Flash 的运行机制，对已有的多种漏洞类型进行了介绍；最后就如何提高用户使用 Flash 安全性提出了一些建议。

关键词：Flash　安全　漏洞

互联网已经在中国发展了十多年，目前已经渗透到人们日常生活的方方面面。网络安全作为互联网的一个分支，涉及每个人的切身利益，其重要性也逐渐被大家所关注。网络安全包含了很丰富的内容（安全意识、安全技术、安全管理……），本文篇幅有限，因此主要关注安全技术。

安全技术虽然有很多，但是狭义上讲，80% 的内容都与漏洞相关，包括漏洞的发现、利用、检测、预防等。从被攻击者的角度，漏洞可以分为两类：服务器端漏洞和客户端漏洞。互联网早期，服务器端漏洞所占比重较大，当时的应用以大型机 / 终端模式为主，有用的信息都存储在服务器上，因此成为早期黑客的目标；现在，服务器端软件逐渐成熟，好用的漏洞已经越来越少，而客户端软件由于个人 PC 机的发展，存放的信息越来越有价值，再加上客户端软件开发者良莠不齐，存在的问题很多，黑客们逐渐把注意力放在客户端软件上，因此，这几年客户端软件漏洞的数量和质量都呈爆发性增长。

为什么关注 Flash 安全

读者可能会问，客户端最严重的漏洞是什么？答案是 Flash 播放器，先罗列一下理由：

1.Flash 播放器的装机量世界第一。Adobe 官方网站宣称安装 Flash 插件的个人 PC 达 99% 以上，数字可靠性与否我们先不考虑，读者只需问自己一个问题，“你周围有谁的机器在网上无法观看 Flash 动画？”

2.Flash 跨平台甚至支持嵌入式系统。无论是 Windows、Linux、Unix 还是 WindowsCE 都支持 Flash 播放（只有一个例外，iPhone）。

3.Flash 不光能在浏览器（IE/Firefox/Chrome/Opera）里播放，还能嵌入到许多软件中：

- Flash 可以嵌入到 Office
- Flash 可以嵌入到 PDF

• 常见 IM 都在使用 Flash 技术，包括 QQ/MSN/ 淘宝旺旺

4. 在所有的浏览器上，Flash 的漏洞利用方法相对一致。在 IE 上利用成功的代码不用作太大修改就能在非 IE 浏览器上使用。

5.Flash 可以自己控制漏洞利用环境。即使浏览器不允许执行 JavaScript 脚本或者没有堆喷射 (Heap Spraying) 环境，Flash 仍可以利用 ActionScript 来实现堆喷射，而且这些行为在浏览器层面很难禁止 (浏览器可以禁用 JavaScript，但是只要能够播放 Flash，就无法禁止 ActionScript 的运行)。

6. 目前 Windows 的 DEP+ASLR 技术可以提高漏洞利用的门槛，最近在 BlackHatDC2010 新出的技术可以利用 Flash 来消除这种门槛。

可见，如果 Flash 存在严重漏洞，那么基本上所有接入互联网的客户机都会受到影响。虽然部分客户机上安装了防御软件，能够降低风险，也仅仅是降低 (特征类型的检测对 Flash 漏洞效果有限，主动防御的效果相对好一些)。

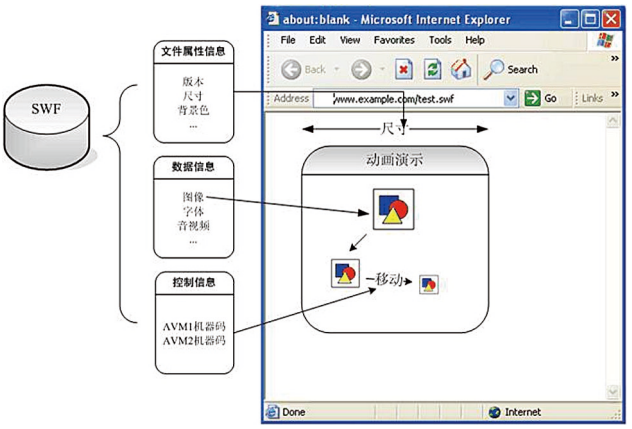
Flash 的运行机制

Flash 播放的文件以 SWF 作为扩展名, 文件主要包含三部分内容 :

• 文件属性信息。包括文件版本、动画尺寸、播放速度、默认背景色等

• 数据信息。包括播放动画所需的各种数据，如静态图像、形状描述、字体信息、视频、音频等

• 控制信息。对图像、视频、音频等数据的播放进行控制，类似



于 HTML 里的 JavaScript。实际上 Flash 使用的是与 JavaScript 兼容的 ActionScript。但是 SWF 中存储的并不是文本格式的 ActionScript，而是经过编译的在 AVM1/AVM2 虚拟机上运行的机器码。

相应的，SWF 播放的也分为四个步骤 :

1. 解析文件，确定动画的基本信息

2. 解析文件，为数据信息建立内存中的数据结构

3. 解析文件，为控制信息建立内存中的数据结构

4. 利用控制信息显示动画

Flash 的安全问题

Flash 文件格式比较丰富，因此 Flash 播放器的实现非常复杂，潜在的问题主要包括 :

文件畸形导致的安全问题

SWF 文件由文件头以及若干个标签组成：

属性标签和普通标签里会保存各种类型的数据和控制信息，而每种类型的信息都有相应的存储格式。如果播放器在处理这些标签时对内容的合法性没有充分验证，就会产生缓冲区溢出或者整数溢出。CVE-2007-0071 和 CVE-2007-6019 就属于这种类型的漏洞。Mark Dowd 在 BlackHat2008 Las Vegas 上关于 CVE-2007-0071 的稳定利用是一个很有份量的议题，涉及的标签为 DefineSceneAndFrameLabelData，格式如下：

Field	Type	Comment
Header	RECORDHEADER	Tag type = 86
SceneCount	EncodedU32	Number of scenes
Offset1	EncodedU32	Frame offset for scene 1
Name1	STRING	Name of scene 1
...	...	...
OffsetN	EncodedU32	Frame offset for scene N
NameN	STRING	Name of scene N
FrameLabelCount	EncodedU32	Number of frame labels
FrameNum1	EncodedU32	Frame number of frame label #1 (zero-based, global to symbol)
FrameLabel1	STRING	Frame label string of frame label #1
...	...	...
FrameNumN	EncodedU32	Frame number of frame label #N (zero-based, global to symbol)
FrameLabelN	STRING	Frame label string of frame label #N

漏洞很简单，SceneCount 和 FrameLabel Count 相乘的整数溢出导致内存破坏。通常的利用方法无法很好的使用该漏洞。Mark Dowd 对 Flash 的虚拟机进行了深入研究，发现了一种能在多种浏览器下稳定利用此漏洞的技术。之后的一段时间，成为了国内挂马集团最喜欢的挂马漏洞。

```
.data:00703978 FR_ NativeTableEntry <52Eh, kNativeMethod, \
.data:00703978                       ; DATA XREF: .data:00720FAC↑o
.data:00703978                       offset flash_net_FileReference_nameG, 0, 480000h>
.data:0070398C     NativeTableEntry <52Fh, kNativeMethod, \
.data:0070398C                       offset flash_net_FileReference_sizeG, 0, 480000h>
...
.data:007039F0     NativeTableEntry <531h, kNativeMethod, \
.data:007039F0                       offset flash_net_FileReference_browseM, 0, 480000h>
.data:00703A04     NativeTableEntry <534h, kNativeMethod, \
.data:00703A04                       offset flash_net_FileReference_uploadM, 0, 480000h>
```

虚拟机实现的安全问题

为了提升 ActionScript 的运行效率，Flash 引入了虚拟机机制，控制信息在虚拟机上运行，其速度比解释型代码更快。Flash8 及以前版本支持的虚拟机是 AVM1，Flash9 及以后 AVM1 和 AVM2 并存。由于虚拟机的实现非常复杂，因此也会有不少安全漏洞，通常以设计逻辑为主，利用更加容易。比较有代表性的一个漏洞是 CVE-2009-1862，与 AVM2 有关，是一个逻辑漏洞。由于 AVM2 是开源的（Adobe 贡献给了 Mozilla 基金会，项目的名字 Tamarin），因此 Adobe 有一个 bugzilla 服务器专门供用户提交软件 Bug，有位用户提交了一个可以导致 Flash AVM2 崩溃的 Bug，但 Adobe 的开发人员认为这个 Bug 并不严重，因此很长时间都没有处理。国内的某些黑客获取了触发样本，经过研究发现这个漏洞竟然可以稳定利用，之后一段时间，该漏洞又成为国内挂马集团最喜欢的挂马漏洞。

内建对象实现的安全问题

前面提到的虚拟机只是一个运行环境，还有很多逻辑需要 Flash 内部对象的支持，这有点类似于 HTML JavaScript 里的 document 对象、div 对象。AVM 支持的对象在实现上也有可能存在各种各样的问题，因此也是漏洞的多发区。CVE-2008-4401 就是 FileReference 对象在处理文件上传和下载时（即 browse 和 upload 方法），用户的确认操作可以被绕过而造成的。

与浏览器交互的安全问题

通常情况下，Flash 是以浏览器作为容器来进行播放的，因此可以与浏览器进行交互。默认情况下，Flash 可以调用 IE 的 Javascript，IE 也可以调用 Flash 的 ActionScript。如果某个网站允许用户上传 Flash，且没有对上传后的 Flash 进行任何限制，那么攻击者可以在网站上执行任意脚本、偷取用户 Cookie、在网页上挂马……这个漏洞本质上和 Flash 自身没有关系，类似于 XSS，需要在服务器端进行限制。

跨域的安全问题

浏览器设计的一个重要原则就是同源策略（Same origin policy），通俗点说，就是

同一个域名下的信息可以互相访问，而不同的域之间不能互相访问。Flash 通过 crossdomain.xml 来确定域之间的访问权限。由于实现的问题，crossdomain 的访问限制有可能被绕过，导致跨域访问，CVE-2010-0186 就是一个典型的例子。

杂项

此类型主要是前面类型漏洞的补充，通常为逻辑型漏洞，例如 ClickingJack（CVE-2008-4503）可以通过透明窗口诱骗用户点击，从而不需用户许可即可打开摄像头。感兴趣的读者可以访问 http://www.sectheory.com/clickjacking.htm

几点建议

如何才能使普通用户在浏览 Flash 的时候尽量不会“中招”呢？以下给出一些建议：

- 使用最新的 Flash 播放器插件
- 使用带有沙盒功能的浏览器，如 IE8 保护模式或者 Chrome，或者启用防御软件的浏览器沙盒功能
- 使用普通用户账号，不要使用管理员账号
- 系统盘使用 NTFS
- 不要随意打开内嵌 Flash 的未知邮件，例如 Office 文档、PDF 文件等等
- 另外，对于网站管理员来说，尽可能不要让用户上传 Flash，如果一定要有这个功能要求，至少也要：
  - 加上 allowScriptAccess 设置成 never
  - 把上传的 Flash 放到单独的域上

绿盟科技入侵防御产品荣获 NSS Labs 高级别认证

网络安全领导厂商——绿盟科技对外宣布，其入侵防御产品（NSFOCUS IPS）顺利通过 NSS Labs 的严格测试，荣获 NSS Labs Approved 认证，并且被 NSS Labs 认定为最高级别——“Recommended”。由此，绿盟科技自主研发的 IPS 产品成为国内安全厂商中惟一获得该权威机构认证的产品。

在最终的测试报告中，NSS Labs 对绿盟科技的 IPS 产品做了如下评价：“NSFOCUS IPS 的管理非常简单，直观得让人惊讶，加载有效的预定义防护策略后，它能够被快速部署到企业网络之中”、“基于 NSFOCUS IPS 行业领先的应用安全防护能力、卓越的千兆处理性能，以及杰出的总体拥有成本（Total Cost of Ownership），这款产品非常值得用户考虑。”能够获得 NSS Labs 的推荐，这意味着用户可以坚信 NSFOCUS IPS 在提供最大限度安全防护能力的同时，不会影响企业网络的正常使用。

旨在解决企业选择和管理 IPS 时所面临的问题，NSS Labs 测试报告提供的数据都源自公正、可实践的真实世界（real-world）测试过程，主要从安全有效性、处理性能、稳定性、以及易用性等方面，对 IPS 产品进行一系列近乎残酷的测试。

1、安全有效性测试：基于业内最高品质的攻击样本库，采用数千个严格保密，且覆盖 2005 年至 2009 年所有高危漏洞的攻击样本，以最严肃的态度评判 IPS 的安全有效性。

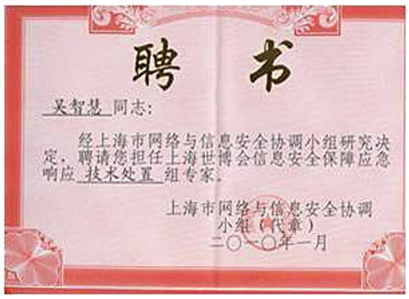
2、性能测试：real-world 测试环境，由数十种网络真实流量混合而成，模拟最真实的用户应用场景，评估 IPS 加载所有检测规则之后，在各种极端环境下的处理性能。

本次绿盟科技参与测试的 IPS 产品被 NSS Labs 最终认定为“推荐”级别。NSS Labs 对所有通过测试的 IPS 产品会给出三种不同级别的认定，分别是“推荐”（Recommended）、“中立”（Neutral）和“谨慎”（Caution）。

绿盟科技的入侵防御系统（NSFOCUS IPS）自 2005 年发布以来，已持续多年占据国内 IPS 市场领导者地位。随着公司整体国际化的进一步发展，其 IPS 产品将不断出现在世界舞台，这次 NSS 测试最高级别的认定，将有助于中国 IPS 第一品牌在全球范围内的推广，也是绿盟科技全面拓展国际市场的重要里程碑。

绿盟科技入选世博会信息安全保障应急响应支撑单位

经“上海市网络与信息安全协调小组”一致审核和评定，绿盟科技上海分公司入选“上

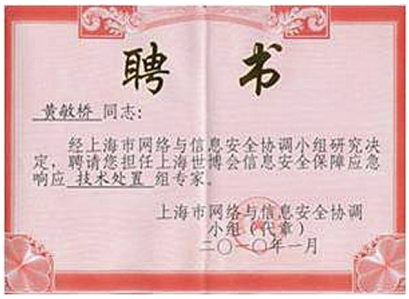

聘书

吴智慧 同志：

经上海市网络与信息安全协调小组研究决定，聘请您担任上海世博会信息安全保障应急响应 技术处置 组专家。

上海市网络与信息安全协调小组（代章）

二〇一〇年一月


聘书

黄敏桥 同志：

经上海市网络与信息安全协调小组研究决定，聘请您担任上海世博会信息安全保障应急响应 技术处置 组专家。

上海市网络与信息安全协调小组（代章）

二〇一〇年一月

海世博会信息安全保障应急响应支撑单位”，这也是世博会信息安全保障应急响应单位入选的首批成员。同时，绿盟科技上海分公司技术部的黄敏桥、吴智慧也被选为“上海世博会信息安全保障应急响应技术处置组专家”成员。

在上海世博会期间，绿盟科技将通过现场值守、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，全力为世博会核心信息系统、城市基础设施信息系统以及各重点单位信息系统提供完备的安全保障和应急响应工作。

绿盟科技作为国内信息安全企业的领导者，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。作为国内最具安全服务经验的公司，绿盟科技在应急服务方面积累了丰富的经验。绿盟科技安全事件响应小组与客户的网络安全中心、应急体系配合协作，已经共同完成了数百次安全事件的应急响应和处理，应急类型覆盖了各个层面。

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。多年来，绿盟科技为春节联欢晚会、中国东盟博览会、广交会百届盛会、十七大、第 29 届奥运会、温总理与网友在线交流、国庆 60 周年等多项重大活动提供了安全保障。

微软再爆 IE 0day 漏洞 绿盟科技第一时间提供预警及防护手段

继 2010 年 1 月 14 日微软 IE 浏览器曝出“Aurora” 0day 漏洞而引发大规模的挂马攻击后，3 月 10 日微软 IE 浏览器再次爆出严重级别的 0day 漏洞（Microsoft IE 畸形对象操作内存破坏漏洞 CVE-2010-0806），受影响的 IE 浏览器版本包括 IE7.0、IE6.0 SP1、IE6.0 等几乎所有主流版本。

由于 IE 在处理非法的对象操作时存在内存破坏漏洞，远程攻击者可能利用此漏洞通过诱使用户访问恶意网页在用户系统上执行指令，从而完全控制用户系统。此漏洞是一个 0day 漏洞，目前已经报告有利用此漏洞的攻击出现，并随着技术细节的扩散有可能被用来大规模进行挂马攻击。微软已经得知了此漏洞的存在并开始研究处理，但还未提供针对此漏洞的安全补丁。

针对此情况，绿盟科技安全专家通过快速对该漏洞进行研究，在发现该漏洞的 2

天内即已研发出该漏洞的检测规则及防护算法，并且运用于绿盟科技相关产品中：

•绿盟远程安全评估系统（RSAS）可以对该漏洞进行准确检测。（需升级至V5.0.6.22 及以后版本）

•绿盟网络入侵防护系统（NIPS）可发现并阻断针对该漏洞的攻击。（需升级至V5.6.0.106 及以后版本）

•绿盟网络入侵检测系统（NIDS）可有效检测针对该漏洞的攻击。（需升级至V5.6.0.106 及以后版本）

由于微软官方还未提供针对此漏洞的安全补丁，因此该漏洞很可能造成严重的危害。绿盟科技建议相关用户通过手动调整主机和浏览器的安全级别进行单主机的加固处理，（临时解决方法请参考绿盟科技紧急通告 Alert2010-04:http://www.nsfocus.net/index.php?act=alert&do=view&aid=110）企业级用户可及时调整企业防火墙和入侵保护产品的安全规则，以应对此漏洞带来的安全风险。对于没有部署绿盟科技相关产品的用户，可以咨询绿盟科技技术服务人员，以提供临时性解决方案。

绿盟科技获“中国企业 IT 年度优秀解决方案奖”

绿盟科技 Web 应用防护系统、低俗网站内容安全审计解决方案在由计算机世界主办的“中国企业 IT 优秀解决方案年度评选和推介活动”中荣获优秀解决方案奖。在众多的参选方案中，绿盟科技的这两款针对互联网的解决方案以其优良的方案设计、领先的产品优势以及卓越的口碑，凭借在 2009 年市场上的优异表现，获得用户的广泛赞誉。

绿盟科技 Web 应用防护系统贯穿 Web 应用生命周期，提供了整体的 Web 安全防护解决方案。该方案充分考虑了网站安全的现状，关注应用层面的防护，符合网站攻防的发展趋势；从 Web 应用生命周期出发，依照事前 - 事中 - 事后，提供了分阶段的整体防护；突显安全服务的重要支撑作用。

绿盟科技低俗网站内容审计解决方案通过采用业界领先的主动安全审计专利技术（NSFOCUS Proactive Audit）和绿盟科技云安全中心，自动化实现对海量网站的内容监测和域名管理，全面快速地发现含有不良

低俗信息的网站，及时追踪有害信息来源，有效地解决了网站内容监控的难题。

此次评选由计算机世界方案评估中心专家筛选评定，该中心成立于 2004 年 6 月，拥有广泛的专家资源，经过多年运作经验的积累，已经制定出一套完善的方案评估指标体系，具有较高的完整性、公正性和权威性。08 年绿盟科技的 IPS/SG 在一年一度的评选中荣获计算机世界年度产品奖，09 年绿

盟科技推送的解决方案也是不负众望，两款解决方案在严格的评选中最终获得评委专家的青睐。

绿盟科技第三次组团赴美参加 RSA2010 大会

一年一度的安全业盛会 RSA 大会如期而至。3 月 1 日，2010 年 RSA 大会（RSA Conference 2010）在美国加州旧金山隆重开幕，绿盟科技（展位号 :1059）再次组团赴美参会。这已是继 2008 年、2009 年两次参加 RSA 盛会后，绿盟科技第三次组团参加RSA大会。此次参会重在展示公司形象，了解国际前沿的安全动向，并和与会人员探讨未来两三年的安全发展热点和趋势。

RSA 大会是目前全球信息安全领域最具权威的年度峰会。大会吸引了来自全球的顶级信息安全企业、各行业 IT 决策者、资深安全专家以及学术界的领军人物。会议分为主题论坛、专业论坛、创新论坛、展会等多个部分。其中专业论坛涉及面极广，从加密算法数学原理的讨论，到安全合规性管理、Web 安全、移动安全方面的热点话题。据了解，网络安全、端点安全、云安全、身份识别、数据安全与网络社会安全等都将成为 2010 年 RSA 大会关注讨论的热点。

2008 年绿盟科技作为第一家国内网络安全厂商参加 RSA 展会，绿盟科技获得了大量的安全前沿信息，同时与日本、新加坡的同行建立了多纬度的合作关系。2009 年，绿盟科技通过展示具有自主知识产权的多项安全解决方案和产品，包括中国首个 Web 应用防火墙及综合 Web 安全解决方案，赢得了全世界安全行业的关注。展望今年的 RSA 大会，绿盟科技将会继续与业界同行沟通与交流，把握国际上最新的信息安全走向，密切关注国际安全发展趋势，跟踪产品技术动态，并将这些观点和技术、前沿趋势融入到绿盟科技的研发与营销体系当中，为国内的用户提供高品质的安全产品与服务，同时也将进一步拓展海外市场。在本届会议上，绿盟科技将重点推广拳头产品诸如 WAF、ADS、IPS、RSAS，以及与云安全密切相关的安全服务组件。

目前，绿盟科技通过对国际化工作的不断摸索，已经获得了美国，日本，东南亚等地的订单，建立了多家本地销售渠道和合作伙伴。绿盟科技以国际一流的产品标准、服务标准、运营标准不断提升自身能力，从而赢得了国际客户的信赖。这种全方位能力的提升，也将使绿盟科技在未来的海外业务拓展以及面向国内众多的行业客户服务中，继续取得技术领先的优势，为客户提供更为优质的安全解决方案与高水平的服务。

绿盟科技再获《通信世界》颁发的“业务安全贡献奖”

绿盟科技在《通信世界》周刊一年一度

的年终大盘点中，凭借 2009 年在运营商领域的精耕细作，再次荣膺报社授予的“业务安全贡献奖”。

作为国内具有典型代表意义的重要行业，绿盟科技始终关注电信运营商业务网络的发展，始终贴合电信运营商行业的业务特点和安全需求，持续不断地为运营商用户提供优秀的安全产品和专业的安全服务。针对运营商的安全运维需求，订制配置核查类产品，提供专业化的培训，为宽带运营商提供抗 DDoS 类的安全产品，与运营商进行广泛合作，开展 IDC 增值服务等等。

2009 年，绿盟科技持续加大与运营商的合作，与电信集团合作建设 SOC 增值平台；在 5.19 事件中快速反应，帮助运营商进行应急处理；为做好国庆安保，通过快速通畅的信息通报、专业细致的安全值守、高效及时的应急响应在国庆期间为各省运营商提供了有力的安全保障。现在，绿盟科技正积极投身于运营商的各项安全建设中，为运营商的业务网络安全事业贡献着力量，矢志成为运营商背后的安全专家。

“专攻术业，成就所托”。正是凭借着多年协助客户进行网络安全建设的经验和对电信行业的理解，绿盟科技为电信运营商及他们的最终客户提供着一系列领先的解决方案及专业的安全服务，从而得到了用户的极大信任。

绿盟科技专家入选国家等级保护建设指导专家委员会

在最近召开的国家信息安全等级保护安全建设指导专家委员会成立大会上，绿盟科技孙铁成为国家信息安全等级保护安全建设指导专家委员会成员，这是专家委员会中为数不多的企业代表之一。

专家委员会成员分别来自中国工程院、公安部、证监会、人民银行、工信部、发改委、国资委、海关总署、税务总局、审计署、国土资源部、国家电网、军队测评中心、国家测评中心等国家部委、科研院所、大型企业主管信息化建设的领导及测评中心的领导，委员会主任为沈昌祥院士、副主任是方滨兴院士。新组建的专委会将承担起指导等级保护贯彻实施和建设规划、推动等级保护行业应用与标准建立、参与相关单位等级保护整改方案评审等工作。

绿盟科技成员成为国家信息安全等级保护安全建设指导专家委员会专家，是公安部对绿盟科技技术能力的认可，也是对绿盟科技在配合国家主管部门进行等级保护工作标准制定落地、工作宣贯推进、解决方案研究推广等各项工作的认可，作为国内信息安全行业的领导企业，绿盟科技将再接再厉，充分发挥公司在政策理解和技术方面的优势，为等级保护整改工作在全国开展贡献自己的力量。

绿盟科技获得“国庆 60 周年网络与信息安全保障先进单位”

1 月 13 日，北京市政务信息安全应急处置中心在北京组织召开了北京市政务信息安全应急体系国庆六十周年信息安全保障表彰会。表彰会上，绿盟科技获得了由北京市网络与信息安全协调小组、北京市通信保障和信息安全应急指挥部、北京市经济和信息化委员会颁发的“国庆 60 周年网络与信息安全保障先进单位”奖牌。

在 2009 年 60 周年大庆期间，为更好地处置突发信息安全事件，北京市政务信息安全应急处置中心从 9 月 25 日至 10 月 8 日，安排专职值班人员进行安全职守，保证了信息安全事件的快速处置。

绿盟科技作为中心应急支撑单位，在国庆安保期间，安排专人值班、监控互联网安全状态、特别是各级政府网站安全状态，每日将值班情况发送给北京市政务信息安全应急处置中心的职守人员。通过基于云安全的互联网安全监控平台，绿盟科技可以实时监控互联网安全状况，对网站挂马情况进行实时监测。在此基础上，值班人员以互联网公开信息进行补充，提示每日互联网安全状态和短期趋势分析，供北京市信息安全测评（服务）中心与北京市政务信息安全应急处置中心参考。

此外，本次会议还针对 2010 年北京市信息安全保障工作思路和重点以及近期信息安全形势进行了交流，提出了 2010 年北京市信息安全保障工作的主要设想。会议认为，2010 年是北京市信息安全基础保障工作年，应进一步完善安全保障常态化工作，以市级应急保障队伍为重点，按照专业方向组建各级应急保障队伍，健全应急保障队伍管理机制，为进一步做好北京市信息安全保障工作提供有力的支撑，为推进建设信息安全一流的可信城市打下坚实的基础。绿盟科技作为国内安全企业的领导者，将进一步为北京市建立完善网络与信息安全领域应急预案体系做出贡献。

Web 应用系统爆严重漏洞问题
绿盟科技第一时间提供快速检测

1 月 6 日，国内广泛使用的 Web 论坛程序——Discuz！论坛系统爆出严重漏洞（Discuz！论坛 showmessage 函数远程代码执行漏洞，受影响版本为 Discuz! 7.1-7.2）。利用该漏洞攻击者可远程生成 Webshell，

从而执行系统指令。针对此情况，绿盟科技安全专家快速研究，于1月7日针对该漏洞的检测发出紧急升级包。目前通过绿盟远程安全评估系统Web应用扫描模块可以第一时间检测用户的Web应用是否存在该漏洞，并提供相应的修补建议。

由于Discuz！论坛系统是国内使用最广泛的论坛之一，并且该漏洞利用难度低，仅需要注册一个一般账号就可以利用该漏洞攻击Discuz！论坛系统，攻击者通过该漏洞与其他漏洞相结合可获得整个Web系统的控制权，甚至可通过此漏洞渗透进其内网。因此该漏洞的出现，很可能导致地下黑客产业利用该漏洞进行广泛的挂马攻击。

据绿盟科技安全专家介绍，绿盟远程安全评估系统Web应用扫描模块采用了很多业内领先的技术，如模拟点击智能爬虫技术、主动挂马检测及核心调度引擎，该产品能够提供Web应用、Web服务及支撑系统（网络层、操作系统层、数据库）等多层次全方位的安全漏洞扫描、审计、渗透测试。该系统可以应用于网站管理员进行Web上线前安全测试，上线后周期性安全评估以及企业安全管理员进行统一的风险监控与管理。

绿盟科技荣获“2009中国通信业成功解决方案评委推荐奖”

日前，绿盟科技获得了由人民邮电出版社信通传媒旗下《通信世界》、《电信技术》、《电信科学》杂志社颁发的“2009中国通信业成功解决方案评委推荐奖”，获奖项目是绿盟科技提出的“运营商门户网站安全解决方案”，该解决方案也被正式收录到2009中国通信业成功解决方案文集。

近年来，运营商门户网站所面临的Web安全形势越来越严峻，针对运营商门户网站所面临的Web安全威胁，绿盟科技针对性地提出“运营商门户网站安全解决方案”。该方案得到了评委会的高度认可，评委专家在评语中写道，门户网站安全直接影响着电信企业的企业形象和信息安全，绿盟科技提供的安全建设方案对Web应用攻击进行了详细的讲解，并对门户网站从最初的规划和开发到后期的运行维护，都分阶段地提供了防护手段。

评委专家一致认为，该方案提出了一套贯穿Web生命周期的安全防护手段，采用WAF产品实现用户与服务器之间的双向数据清洗，加强了数据的安全性，针对运营商门户网站所面临的Web安全问题，提出了贯穿Web应用生命周期的安全防护方案，解决方案具有一定的先进性，是不错的门户网站安全建设解决方案。

作为国内具有典型代表意义的重要行业，绿盟科技始终关注电信运营商业务网络的发展，凭借着多年来协助客户进行网络安全建设的经验和对电信行业的理解，绿盟科技为电信运营商及他们的最终客户提供着一系列领先的解决方案及专业的安全服务，从而获得了用户的认可和信任。

NSFOCUS 2010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. 2010-01-15 Microsoft IE 非法事件操作内存破坏漏洞

NSFOCUS ID: 14349

http://www.nsfocus.net/vulndb/14349

综述:

Microsoft IE 是微软 Windows 操作系统自带的浏览器软件。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。

危害:

攻击者可以诱使受害者打开嵌入了恶意数据的网页来触发此漏洞，从而控制受害者系统。

2. 2010-01-14 Oracle 2010 年 1 月更新修复 Oracle Database 多个安全漏洞

NSFOCUS ID: 14339

http://www.nsfocus.net/vulndb/14339

综述:

Oracle Database 是大型的商业数据库系统。通过认证的远程攻击者可以利用 Oracle 数据库的 Listener、OLAP、ApplicationExpress Application Builder、Data Pump、Spatial、Logical Standby、RDBMS 组件中的多个安全漏洞操控某些数据或读取敏感信息。

危害:

攻击者可以利用这些漏洞对系统信息进行非授权的访问。

3. 2010-01-14 Adobe Reader 和 Acrobat JpxDecode 内存破坏漏洞

NSFOCUS ID: 14341

http://www.nsfocus.net/vulndb/14341

综述：

Adobe Reader 和 Acrobat 都是非常流行的 PDF 文件阅读器。Adobe Reader 和 Acrobat 没有正确地处理 PDF 文件中 JpxDecode 编码数据流中的 Jp2c 流，在处理 JPC_MS_RGN 标记时整数符号扩展可能导致绕过边界检查，触发内存破坏。

危害：

攻击者可以诱使受害者直接或通过浏览器打开特制的 PDF 文件来触发此漏洞，从而控制受害者系统。

4. 2010-01-15 Linux Kernel fasync_helper() 函数本地权限提升漏洞

NSFOCUS ID: 14351

http://www.nsfocus.net/vulndb/14351

综述：

Linux Kernel 是开放源码操作系统 Linux 所使用的内核。Linux Kernel 在处理 FASYNC 标志集中的文件描述符时存在释放后使用错误。

危害：

本地攻击者可以利用此漏洞获得 root 权限。

5. 2010-01-07 Discuz! 论坛 showmessage 函数远程代码执行漏洞

NSFOCUS ID: 14300

http://www.nsfocus.net/vulndb/14300

综述：

Discuz! 是一款华人地区非常流行的 Web 论坛程序。Discuz! 的 showmessage 函数中 eval 中执行的参数未初始化，可以任意提交，从而可以执行任意 PHP 命令。

危害：

攻击者可以利用此漏洞控制受影响的服务器系统。

6. 2010-01-11 PHPWind 多个文件包含漏洞

NSFOCUS ID: 14317

http://www.nsfocus.net/vulndb/14317

综述：

PHPWind 是一款国内比较流行的基于 PHP 的 Web 论坛程序。PHPWind 的 api/class_base.php、apps/share/index.php、apps/groups/index.php 页面的多个本地和远程文件包含漏洞导致执行任意 PHP 代码。

危害：

攻击者可以利用此漏洞控制受影响的服务器系统。

7. 2010-01-07 Flashget IEHelper 控件远程内存破坏漏洞

NSFOCUS ID: 14305

http://www.nsfocus.net/vulndb/14305

综述：

FlashGet 是一款多线程下载程序。FlashGet 所安装的 IEHelper ActiveX 控件在处理对象的实例化时存在内存破坏问题。

危害：

攻击者可以诱使受害者打开嵌入了恶意数据的网页来触发此漏洞，从而控制受害者系统。

8. 2010-01-05 网络传送带 eDonkey 协议栈溢出漏洞

NSFOCUS ID: 14287

http://www.nsfocus.net/vulndb/14287

综述：

网络传送带是中国第一个实现 MMS、RTSP、PNM、HTTP、HTTPS、FTP、FTPS、SFTP 和 BT、电驴的下载工具。网络传送带在处理电驴 OP_LOGINREQUEST 报文时存在栈溢出漏洞。

危害：

远程攻击者可以通过向受影响系统的 ed2k 监听端口发送特制报文来触发这个溢出，从而控制受害者系统。

9. 2010-01-13 Microsoft Windows 嵌入式 OpenType 字体引擎 LZCOMP 内存破坏漏洞（MS10-001）

NSFOCUS ID: 14325

http://www.nsfocus.net/vulndb/14325

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。Microsoft Windows EOT 字体引擎解压特制 EOT 字体的方式存在内存破坏漏洞。

危害：

攻击者可以诱使受害者打开嵌入了恶意 EOT 内数据的文件来触发此漏洞，从而控制受害者系统。

10. 2010-01-11 Juniper Networks JUNOS 畸形 TCP 报文远程拒绝服务漏洞

NSFOCUS ID: 14319

http://www.nsfocus.net/vulndb/14319

综述：

JUNOS 是 Juniper 网络公司的系列边界路由器所运行的操作系统。JUNOS 在处理带有畸形 TCP 选项的 IPv。

危害：

远程攻击者可以通过向 JUNOS 发送带有畸形 TCP 选项的 IPv4 报文导致拒绝服务。

NSFOCUS 2010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. 2010-02-23 Microsoft DirectX DirectShow AVI 文件解析堆溢出漏洞（MS10-013）

NSFOCUS ID: 14520

http://www.nsfocus.net/vulndb/14520

综述:

Microsoft DirectX 是 Windows 操作系统中的一项功能，流媒体在玩游戏或观看视频时通过这个功能支持图形和声音。DirectX 的 DirectShow 组件（quartz.dll）在解析 AVI 文件中的特定类型视频流时没有正确的使用分配所用的长度字段, 导致分配了不充分的缓冲区。

危害:

攻击者可以诱使受害者打开特制的 AVI 文件触发堆溢出，从而控制受害者系统。

2. 2010-02-04 Microsoft IE 动态 OBJECT 标签信息泄露漏洞

NSFOCUS ID: 14459

http://www.nsfocus.net/vulndb/14459

综述:

Internet Explorer 是 Windows 操作系统中默认捆绑的 web 浏览器。Internet Explorer 在加载 OBJECT 标签中所指定内容时存在信息泄露漏洞。

危害:

攻击者可以利用此漏洞获取服务器信息。

3. 2010-02-23 Microsoft Windows SMB 路径名远程溢出漏洞（MS10-012）

NSFOCUS ID: 14519

http://www.nsfocus.net/vulndb/14519

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft 的 SMB 协议实现中在验证畸形 SMB 请求中的路径名字段时存在缓冲区溢出。

危害：

通过认证的用户可以通过向运行 Server 服务的系统发送特制网络消息来利用该漏洞，从而控制服务器系统或导致拒绝服务。

4. 2010-02-15 Microsoft Windows ICMPv6 路由信息远程代码执行漏洞（MS10-009）

NSFOCUS ID: 14495

http://www.nsfocus.net/vulndb/14495

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 的 TCP/IP 栈没有对特制的 ICMPv6 路由信息报文执行正确的边界检查，匿名攻击者可以通过向启用了 IPv6 功能的计算机发送特制的 ICMPv6 路由信息报文触发缓冲区溢出。

危害：

攻击者可以向服务器发送特制的 ICMPv6 路由信息报文来利用该漏洞，从而控制服务器系统。

5. 2010-02-16 Microsoft Windows CSRSS 本地权限提升漏洞（MS10-011）

NSFOCUS ID: 14499

http://www.nsfocus.net/vulndb/14499

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。当用户注销时 Windows 客户端 / 服务器运行时环境子系统（CSRSS）没有正确的终止用户进程，这可能允许本地用户以其他用户的权限执行任意代码。

危害：

本地攻击者可以利用此漏洞窃取系统敏感信息。

6. 2010-02-12 Microsoft PowerPoint TextBytesAtom 记录解析栈溢出漏洞（MS10-004）

NSFOCUS ID: 14487

http://www.nsfocus.net/vulndb/14487

综述：

Microsoft PowerPoint 是微软 Office 套件中的文档演示工具。PowerPoint 处理特制 PPT 文件中的 TextBytesAtom 记录时没有对大小参数执行边界检查，memcpy() 将文件中的用户数据拷贝到了栈上。

危害：

远程攻击者可以诱使受害者打开包含恶意内容的 PPT 文件，从而控制受害者系统。

7. 2010-02-09 Oracle 数据库不安全过程调用远程命令执行漏洞

NSFOCUS ID: 14477

http://www.nsfocus.net/vulndb/14477

综述:

Oracle 是大型的商业数据库系统。由于没有正确地限制对 DBMS_JVM_EXP_PERMS 软件包中过程的访问，远程用户可以通过 IMPORT_JVM_PERMS 过程修改 Java 策略表，导致执行任意操作系统命令。此外由于没有正确地处理传送给 DBMS_JAVA.SET_OUTPUT_TO_JAVA 过程的参数，远程用户可以以 SYS 用户权限执行任意 SQL 命令。

危害:

远程攻击者可以利用此漏洞对系统和数据库资源进行非授权的访问。

8. 2010-02-20 Firefox showModalDialog() 方法跨域脚本执行漏洞

NSFOCUS ID: 14513

http://www.nsfocus.net/vulndb/14513

综述:

Firefox 是一款流行的开源 WEB 浏览器。Firefox 的同源策略实现上存在漏洞，远程攻击者可能通过使用 showModalDialog() JavaScript 方法绕过权限限制，获取其他浏览网页的信息。

危害:

远程攻击者可以绕过浏览器安全限制，操作其它浏览的网页。

9. 2010-02-19 Adobe Reader 和 Acrobat TIFF 图像处理缓冲区溢出漏洞

NSFOCUS ID: 14512

http://www.nsfocus.net/vulndb/14512

综述:

Adobe Reader 和 Acrobat 都是非常流行的 PDF 文件阅读器。Adobe Reader 和 Acrobat 采用的开源 TIFF 图像解析库 libtiff 实现上存在缓冲区溢出漏洞。

危害:

攻击者可能利用此漏洞通过诱使用户使用 Adobe Reader 打开处理恶意 TIFF 图像文件在用户系统上执行任意指令，从而控制用户系统。

10. 2010-02-17 Cisco Security Agent 远程目录遍历漏洞

NSFOCUS ID: 14502

http://www.nsfocus.net/vulndb/14502

综述:

Cisco Security Agent (CSA) 可以为服务器和桌面计算系统提供威胁防护。Cisco Security Agent 的实现上存在目录遍历漏洞，远程已通过认证的用户可能利用此漏洞查看、下载安装了 CSA 的服务器上的任意文件。

危害:

攻击者可以利用此漏洞对服务器进行未授权的访问。

NSFOCUS 2010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> 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. 2010-03-10 Microsoft IE 畸形对象操作内存破坏漏洞

NSFOCUS ID: 14600

http://www.nsfocus.net/vulndb/14600

综述:

Internet Explorer 是 Windows 操作系统中默认捆绑的 web 浏览器。Internet Explorer 通过使用 iepeers.dll 组件提供对 Web 文件夹和打印的支持，该组件中存在释放后使用错误。

危害:

攻击者可以诱使受害者打开恶意的 HTML 文档或 Office 文件来触发此漏洞，从而控制受害者系统。

2. 2010-03-01 Microsoft IE winhlp32.exe 服务远程代码执行漏洞

NSFOCUS ID: 14551

http://www.nsfocus.net/vulndb/14551

综述:

Internet Explorer 是 Windows 操作系统中默认捆绑的 Web 浏览器。用户可以使用 VBScript 从 IE 调用 winhlp32.exe 服务，如果向该服务传送了恶意的 .HLP 文件就会导致执行任意命令。

危害:

攻击者可以诱使受害者察看提示框的帮助信息来触发此漏洞，从而控制受害者系统。

3. 2010-03-10 Apache mod_isapi 模块悬挂指针漏洞

NSFOCUS ID: 14551

http://www.nsfocus.net/vulndb/14551

综述:

Apache HTTP Server 是一款流行的 Web 服务器。如果远程用户向 Apache 服务器的 mod_isapi 模块发送了特制的请求之后又发送了重置报文，就可能导致从内存中卸载目标 ISAPI 模块。但函

数指针仍在内存中，在引用已发布的 ISAPI 函数时仍可调用，这就造成了悬挂指针（野指针）问题。

危害：

远程攻击者可以通过向 Apache 服务器提交恶意请求来触发此漏洞，从而控制服务器系统。

4. 2010-03-10 Microsoft Excel XLSX 文件解析远程代码执行漏洞（MS10-017）

NSFOCUS ID: 14603

http://www.nsfocus.net/vulndb/14603

综述：

Excel 是微软 Office 套件中的电子表格工具。XLSX 文件是组成新的开放 XML 文档相关内容的 ZIP 档案文件。在解压 XLSX 文件中的某些 XML 元素时由于没有验证 ZIP 头，可能会导致执行未初始化的内存。

危害：

攻击者可以诱使受害者打开恶意的 .XLS 文件来触发此漏洞，从而控制受害者系统。

5. 2010-03-10 Microsoft Excel DbOrParamQry 对象解析内存破坏漏洞（MS10-017）

NSFOCUS ID: 14602

http://www.nsfocus.net/vulndb/14602

综述：

Excel 是微软 Office 套件中的电子表格工具。Excel 在解析包含有畸形 DbOrParamQry 记录的 .XLS 文件时存在内存破坏漏洞。

危害：

攻击者可以诱使受害者打开恶意的 .XLS 文件来来触发此漏洞，从而控制受害者系统。

6. 2010-03-02 IBM Informix Dynamic Server librpc.dll 库远程栈溢出漏洞

NSFOCUS ID: 14553

http://www.nsfocus.net/vulndb/14553

综述：

IBM Informix Dynamic Server 为企业提供运行业务所需的任务关键型数据基础设施。Informix Dynamic Server 中 ISM Portmapper 服务 (portmap.exe) 所使用的 RPC 协议解析库 librpc.dll 中存在栈溢出漏洞。

危害：

远程攻击者可以通过向默认的 TCP 36890 端口提交恶意请求触发这个溢出，从而控制服务器系统。

7. 2010-03-11 IBM Lotus Notes 远程栈溢出漏洞

NSFOCUS ID: 14617

http://www.nsfocus.net/vulndb/14617

综述：

Lotus Notes 是由 IBM 开发的集成邮件、日历、即时消息、浏览器和业务协作应用，可用作 Lotus Domino 服务器应用的桌面客户端。Lotus Notes 在处理发往服务器的请求时存在栈缓冲区溢出。

危害：

远程攻击者可以通过向 Lotus Notes 服务器提交恶意请求触发栈溢出，从而控制服务器系统。

8. 2010-03-19 Google Chrome 4.1.249.1036 版本修复多个安全漏洞

NSFOCUS ID: 14650

http://www.nsfocus.net/vulndb/14650

综述：

Google Chrome 是 Google 发布的开源 WEB 浏览器 Chrome 的 4.1.249.1036 版本更新修复了多个安全漏洞，包括一些竞争条件、整数溢出错误、指针错误和绕过下载警告对话框或同源策略限制。

危害：

攻击者可以诱使受害者打开恶意的 Web 页面来触发此漏洞，从而控制受害者系统。

9. 2010-03-14 MicroWorld eScan 杀毒软件远程命令注入漏洞

NSFOCUS ID: 14630

http://www.nsfocus.net/vulndb/14630

综述：

eScan 是综合的杀毒和内容安全解决方案。Linux 平台的 eScan 杀毒软件没有正确地过滤提交给 forgotpassword.php 页面的 uname 参数便在命令行中使用。

危害：

远程攻击者可以通过向服务器提交恶意请求在服务器上执行任意命令，从而控制服务器系统。

10. 2010-03-03 Helix Player 编码 URI 解析缓冲区溢出漏洞

NSFOCUS ID: 14567

http://www.nsfocus.net/vulndb/14567

综述：

RealPlayer 是一款非常流行的媒体播放器，支持多种格式；HelixPlayer 是其开源版本。Helix Player 的 common/util/hxurl.cpp 和 player/hxclientkit/src/CHXClientSink.cpp 文件中的 Unescape 函数在反转义特殊编码的 URL 时存在缓冲区溢出漏洞。该函数假设“%”字符后总是跟随有至少两个额外的 16 进制字符，如果仅跟随了一个字符的话就无法正确的检测到 URL 字符串的末尾，一直处理内存内容，直至找到第一个 “\0'”。这可能会导致越界读写缓冲区。

危害：

攻击者可以诱使受害者打开恶意的 URL 来触发此漏洞，从而控制受害者系统。

巨人背后的专家

- 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，为军工、政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是倍受信赖的专家。

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