安全+
SECURITY
2010/07 总第009
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

初探ICT供应链完整性

从Gumblar谈网页挂马

从攻击规避检测技术看IPS的安全有效性

智能电网的几类运行特征与安全防护要点研究

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

2010/07 总第 009

Nsmagazine@nsfocus.com

安全+ SECURITY+

目录 CONTENTS

从Gumblar谈网页挂马

国际拓展部　郭宇

摘要：本文从 Gumblar 事件入手，分析了国外区域市场对于安全事件的不同反应，包括用户、安全服务商（MSSP）和安全厂商，并就此事件背后的原因作了剖析。重点针对 Web 安全和网页挂马的恶意行为分析。

关键词：Gumblar　Web 安全　网页挂马

一、Gumblar 生平

Gumblar 最早被安全界认知是由于其利用 Adobe Flash/PDF 的漏洞传播恶意软件，不同的安全厂商将 Gumblar 认定为不同的恶意行为，如 Botnet、Downloader 和 Trojan。实际上，Gumblar 是一系列攻击行为的统称（自动化的恶意软件传播系统），包括网站入侵、植入恶意代码、攻击客户端等等，主要恶意行为是窃取客户端 FTP 密码和重定向用户搜索结果。

在 2009 年 5 月第一次被发现后，Gumblar 几乎席卷了整个互联网，业界认为这是一次比 Conficker 更严重的安全事件。

我们以日本为例，对 Gumblar 事件进行分析。

在日本，大量的动漫网站首先遭到攻击，表现为网页被植入了恶意代码，随后很多网站也先后被攻击并植入类似的恶意代码。事后分析发现，动漫网站大多采用包括 wordpress 在内的开源程序，而开源程序本身及其第三方插件都存在着大量的安全漏洞，Gumblar 自动化地通过漏洞特征寻找有漏洞的网站并完成随后的网页恶意代码植入，通常恶意代码经过加密并指向其他恶意软件托管站点。

浏览者在访问包含恶意代码的网站时，如果攻击成功，恶意软件会被下载并安装到浏览者的主机上，恶意程序会自动寻找本地的 FTP 账号，并利用 FTP 账号自动感染下一个网站，快速地进行传播，具体流程可参见图 1 Gumblar 传播示意图。

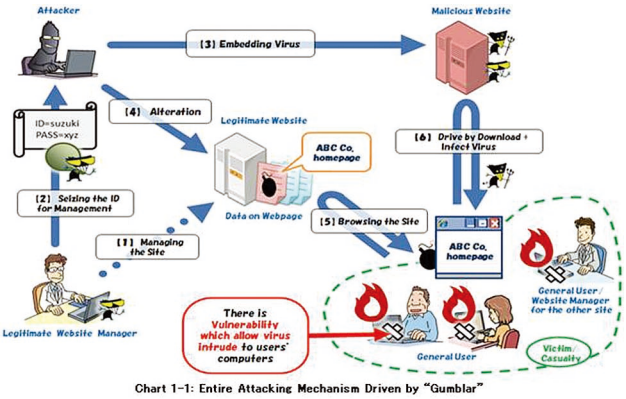


图 1 Gumblar 传播示意图

随着 Adobe 发布 Flash 和 PDF 相关补丁，Gumblar 的影响在逐渐减弱。但是在 2009 年 11 月份，Gumblar 变种再次席卷日本互联网，众多知名网站纷纷遭遇攻击，网页中被植入了恶意代码，其中包括:

- 日本本田网站;
- 东日本旅客铁路网站;
- 日本民主党东京网站;
- 日本著名便利店 Lawson 网站;
- 日本某著名博客提供商。

根据网站的 FTP 日志判断，部分攻击仍然通过 FTP 上传进行，另外一些则是典型的群注方式，通过指定特征在互联网上扫描发起攻击。

对捕获的恶意样本分析发现，此次 Gumblar 变种仍然采用基于浏览器相关的漏洞进行传播，甚至一些几年前的漏洞还在被使用，微软 2009 年安全报告中描述了更新服务的使用情况：世界各个区域内有很多 Windows 用户没有启用 Windows 更新服务，因此其系统中可能存在安全漏洞，有些甚至是几年前的漏洞。

二、日本市场 Gumblar 事件反应

Gumblar 变种攻击事件出现后，在日本国内造成了巨大的反响，中小企业认为像本田这样的世界 500 强的网站都会遭受 Gumblar 攻击，那么中小企业的安全性则更加无法保证，互联网行业更是如临大敌，在各大网站上都能看到 Gumblar 防护专栏。

日本的安全提供商敏感地捕获到了这一需求并转换为商机，于是在日本市场上出现了很夸张的一幕：几乎所有的安全厂商、系统集成商和安全服务提供商都推出了针对 Gumblar 的解决方案，包括以下几类:

- 网站安全扫描服务;
- 网页防篡改服务;
- 网站恶意代码监控服务。

通过之前对 Gumblar 原理的介绍，这些单一的安全服务对自动化攻击系统是无法起到根本作用的，同时这也说明三方面的问题:

1. 日本本土安全厂商核心技术积累不足

图 2 绿盟网站安全监测服务

目前日本主流的技术和安全厂商大多来自欧美，比如 Symantec, McAfee, Panda 等，本土安全厂商偏少并且安全核心技术积累不足，所以甚至有些厂商采用变更管理的方式进行网页防篡改监控，而完全不顾可能带来的高误报率。

2. 日本客户对于网站安全非常重视

日本市场目前信息化程度很高，电子商务在其中占的比例很高，因此各类客户对电子商务的关键因素网站的安全问题非常重视。当然这里也有法律法规的部分原因，比如日本目前的《个人隐私保护法》也要求对客户的信息进行保密等等。

3. 日本安全服务商市场反应迅速

当市场上出现了安全事件时，安全提供商迅速地对安全事件进行宣传和包装，制造出新的商业机会，从而制造出新的利润增长区。

通过和日本安全服务代理商的深入接触，他们对于绿盟网站安全监测服务非常感兴趣，认为我们在挂马监检测和 Web 扫描技术上处于国际领先地位，希望能和我们在网站安全方面展开深入的合作。

三、其他区域网页挂马分析

微软公司的一份安全报告显示，恶意站点数量有逐年上升的趋势，从图 3 我们可以看到，域名后缀 .CN 的网站中恶意网站比率高达 0.79%，也就是说每 125 个 .CN 网站中就有一个是恶意网站，其他域名如日本 (.JP)、新加坡 (.SG) 的恶意网站比例低于中国，但绝对数量仍然较多。

网站被挂马的原因多种多样，Gumblar 主要利用 Web 应用程序的漏洞进行攻击，那么是否还存在其他安全漏洞呢，我们先来看一个 Nginx 安全漏洞。

TLD	Associated Country/Region	Percent of Sites
.JP	Japan	0.10%
.SG	Singapore	0.38%
.CN	China	0.79%

图 3 世界顶级域名恶意站点比例 (按区域分)

Nginx 是一款开源的 Web Server 软件 , 世界著名的网络公司 netcraft 的数据显示，截至 2010 年 4 月份，Nginx 的全球市场份额大约是 4.70%, 紧随 Apache 和 Microsoft IIS 之后, 排名世界第三位。

表 1 全球网站 Web Server 市场份额

Developer	March 2010	Percent	April 2010	Percent	Change
Apache	666,003	67.00%	664,232	66.82%	-0.18
Microsoft	170,023	17.10%	168,829	16.98%	-0.12
nginx	44,489	4.48%	46,698	4.70%	0.22
Google	20,544	2.07%	20,913	2.10%	0.04

2010 年 5 月份爆出的 Nginx 的 0day 漏洞闹得是沸沸扬扬，由于利用方式简单粗暴，对使用 Nginx 作为 Web Server 的网站几乎是一击必杀。由于世界上数万台 Web 服务器使用 Nginx，这期间很多网站遭受攻击，并被植入恶意代码。

从下图中我们可以看到，安全威胁可能来自 OS、Web Server、Web App 或者是其他相关的应用等等。Nginx 漏洞是网站的 Web Server 层面出现问题，从而被攻击者所利用。

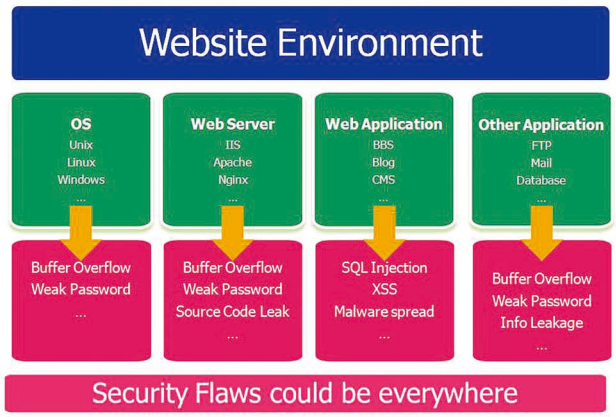


图 4 网站安全结构图

Web 攻击和网页挂马由于其背后利益驱动巨大，在很长时间内还将是网络安全的一个重要领域，绿盟科技也会对这方面持续跟进，增强与国内外安全组织 / 厂商的合作，为更好地保护用户信息安全做出自己应有的贡献。

参考文献:

http://www.ipa.go.jp/security/english/virus/press/201001/E_PR201001.html

http://www.securelist.com/en/blog/208187897/The_Gumblar_system

http://news.netcraft.com/archives/category/web-server-survey/

高校网站如何保安全

行业营销中心　孙铁　行业技术部　何财发

摘要：随着高校网站承载业务的增加，针对高校网站的各类 Web 特定应用攻击也是层出不穷。由于这些攻击手段具有个性化和不通用的特点，传统的技术手段如防火墙、入侵检测等已不能有效地防范和检测网站特定的威胁和攻击，高校网站面临的安全形势异常严峻。为了保证高校网站安全持续稳定地提供服务，绿盟科技凭借其强大的技术优势，建立了全面的保障体系。本文站在应用安全的角度，从检测与发现 - 风险预警、防护与阻击 - 风险防护、运维监控 - 风险管理、事后响应 - 应急支持体系、安全恢复 - 风险处理、溯源取证 - 积极主动等几个维度介绍了绿盟科技全面、主动的高校网站安全保障方案。

关键词：高校网站　安全保障　网站监控　追踪溯源

一、高校网站安全现状

随着高校信息化建设的逐步深入，各高校教务工作对信息系统依赖的程度越来越高。作为高校窗口的高校网站，所面向的用户群也越来越广泛，所承载的功能也越来越全面，不单是面向校内，同时面向社会也提供了诸多服务。高校网站已从一个简单的信息发布、展示平台，逐步转变为汇集了招生就业、远程教育、成果共享、招标采购等功能的综合性业务平台。高校网站已积聚了教育信息化建设中大量的信息资源，成为高校成熟的业务展示和应用平台。

但不得不承认，在大力进行高校网站业务建设的同时，各高校在系统安全保障的建设上出现了严重缺失，网站挂马、网页篡改、DDoS 攻击等攻击事件呈逐年上升的趋势，以即将开始的高招为例，2010 年高考前夕，5 月 14 日一天之内，全国 128 所高校网站被集体挂马，其中不乏重点大学，这一数字已经超过 2009 年全年挂马数，近几年修改考试成绩、骗取认证证书等事件屡有发生，高校网站已经逐渐成为黑客关注的重点目标，高校网站的安全保障工作已经迫在眉睫。

二、高校网站面临的典型安全威胁

用卡尔•萨根“魔鬼出没的世界”这句话来形容高校网站目前所处的恶劣安全环境是再合适不过了。针对高校网站所承载的各类应用的特点，目前比较典型的攻击总结如下:

跨站脚本

跨站脚本漏洞的特点在于对存在漏洞的网站本身并不构成威胁，但会使网站成为攻击者攻击第三方的媒介。

跨站脚本的危害：攻击者可以利用 XSS 漏洞借助存在漏洞的 Web 网站转发攻击其他浏览相关网页的用户，窃取用户浏览会话中诸如用户名和口令（可能包含在 Cookie 里）的敏感信息，通过插入挂马代码对用户执行挂马攻击。

信息泄漏

信息泄漏是攻击者通过应用系统部署时没有将注释去掉、应用系统部署时没有正确地配置服务器程序等方式获得应用系统某些敏感信息的攻击技巧，通常是利用程序员遗留在代码中的注释或者服务

器程序的错误信息。

信息泄露的危害：远程攻击者可以利用漏洞获得敏感信息，有利于攻击者进一步的攻击。

SQL 注入

SQL 注入是攻击者通过输入恶意的请求直接操作数据库服务器的攻击技巧。SQL 注入是应用系统中最常见、同时也是危害最大的一类弱点。导致 SQL 注入的基本原因是由于应用程序对用户的输入没有进行安全性检查，从而使得用户可以自行输入 SQL 查询语句，对数据库中的信息进行浏览、查询、更新。基于 SQL 注入的攻击方法多种多样，而且有很多变形，这也是传统工具难以发现和定位的。

SQL 注入的危害：利用 SQL 注入漏洞可以构成对 Web 服务器的直接攻击，还可能用于网页挂马，导致机密数据泄漏，如电子商务网站的客户信息、服务器被控制；后台数据库执行非授权的查询、修改、删除、泄露认证相关的敏感信息，导致攻击者控制 Web 应用，网站数据的恶意破坏。

越权攻击

越权攻击是由于应用系统对权限没有严格识别，导致用户文件权限过滤不严格而导致的攻击。

DDoS 攻击

DDoS（Distributed Denial of Service）攻击则是一种可以造成大规模破坏的黑客武器，它通过制造伪造的流量，使得被攻击的服务器、网络链路或是网络设备（如防火墙、路由器等）负载过高，从而最终导致系统崩溃，无法提供正常的服务。

随着各种业务对 Internet 依赖程度的日益加强，DDoS 攻击所带来的损失也愈加严重。包括运营商、企业及政府机构的各种用户时刻都受到了 DDoS 攻击的威胁，而未来更加强大的攻击工具的出现，为日后发动数量更多、破坏力更强的 DDoS 攻击带来可能。

三、高校网站整体安全保障

围绕高校网站所承载的业务特点以及面临的典型威胁，绿盟科技凭借自身强大的产品和技术优势，在对最新安全形势深入研究的基础上，推出了高校网站安全保障解决方案。该方案的特点是:

- 以高校网站面临的威胁风险作为设计的核心

以高校网站所面临的风险为核心，从风险预警、风险防护、风险处理、应急保障、风险管理、积极主动等方面实现高校网站安全风险全流程控制。

- 全面

绿盟科技高校网站安全保障方案的另一个特点是全面：着眼点是高校网站全生命周期的安全保障，涵盖了网站运行的各个阶段，而不仅仅单纯从检测、防护等角度考虑 。

- 被动防御与主动溯源相结合

以往的方案是从被动防护的角度来设计的，而绿盟科技凭借其技术实力，在有效检测和防护的同时，也从主动的角度，增强了对网站安全事件追踪溯源的能力。

方案主要由以下几个方面组成:

检测与发现—风险预警

目前对网站新漏洞、网页被挂马等状况，绝大多数网站建设和运维者并不能及时察觉。可在前阶段分析的基础上，围绕具体业务类别采

用针对性比较强的 Web 安全自动化检测工具，定期或不定期地对网站安全状态进行检测和评估，不但可以提高对安全隐患及现有安全问题准确、深层次的预警发现，而且自动检查工具的使用也可以降低维护管理和人力成本。

高校网站安全问题的检测与发现设计可分为预警检测和事后检测两个方面。预警检测目的是利用现有的安全技术，提供一种准确、实用、可行的预警手段，注重防患于未然；事后检测是对发生问题的网页进行问题定位、影响评估。

通过对 Web 服务器的多种项目 (包括潜在的危险文件 /CGI，以及多个服务器版本上的特定问题等) 进行全面的测试，还可以对 Web 服务器、应用服务器、数据库服务器的配置检查，确保服务器的配置正确，对后台数据库进行安全基线审计，对一些常见的 Web 攻击，如参数注入、跨站脚本、目录遍历攻击 (directory traversal) 、身份验证页上的弱口令长度等进行技术层面的验证，有效地防止网页篡改、网页挂马等安全事件的发生。

对于有特殊需求的用户，还设计了灵活的编辑接口，对 Web 扫描的策略进行增加或者编辑，满足特定的要求。

防护与阻击—风险防护

除了采用信息系统传统的防护技术对网站的基础设施进行必要的防护外，针对 Web 应用攻击还应采用专门的机制，对来自 Web 应用程序客户端的各类请求进行内容检测和验证，提供细粒度应用层 DDoS 攻击防护功能，确保其安全性与合法性，对非法的请求予以实时阻断，有效防止 HTTP 及 HTTPS 应用下各类安全威胁，如 SQL 注入、XSS、跨站伪造 (CSRF)、cookie 篡改以及应用层 DDoS 等，有效应对网页篡改、网页挂马、敏感信息泄露等安全问题，充分保障高校网站各类 Web 应用的高可用性和可靠性。

对各类网站站点进行有效防护，降低攻击的影响，确保业务系统的连续性和可用性，降低网站安全风险，维护网站公信度。对其进行有效检测、防护。

其主要的功能如下:

• 网页篡改在线防护

按照网页篡改事件发生的时序，提供事中防护以及事后补偿的在线防护解决方案。事中，实时过滤 HTTP 请求中混杂的网页篡改攻击流量 (如 SQL 注入、XSS 等)。事后，自动监控网站所有需保护页面的完整性，检测到网页被篡改，第一时间对管理员进行短信告警，对外仍显示篡改前的正常页面，用户可正常访问网站。

• 网页挂马在线防护

网页挂马是一种相对比较隐蔽的网页篡改方式，本质上这种方式也破坏了网页的完整性。网页挂马的攻击目标为各类网站的最终用户，网站作为传播网页木马的 “傀儡帮凶”，严重影响了网站的公信度。

当用户请求访问某一个页面时，会对服务器侧响应的网页内容进行在线检测，判断是否被植入恶意代码，并对恶意代码进行自动过滤。

• 敏感信息泄漏防护

自定义非法敏感关键字，EB 站点可能包含一些不在正常网站数据目录树内的 URL 链接，提供细粒度的 URL ACL，防止对这些链接的非授权访问。对其进行自动过滤，防止非法内容发布为公众浏览，识别并更正 Web 应用错误的业务流程，识别并防护敏感数据泄漏，满足合规与审计要求。

• 智能应用层 DDoS 攻击防护

防护各类带宽及资源耗尽型拒绝服务攻

击，如对 SYN Flood 这种常见攻击行为能够有效识别，并实时对攻击流量进行阻断，确保了 Web 业务的可用性及连续性。

• OWASP Top 10

超越传统 IPS 设备基于静态规则的防护机制，NSFOCUS WAF 有效结合了静态规则与基于用户行为识别的动态防御机制，应对 OWASP Top10 中的 Web 应用安全问题，对恶意应用流量进行双向清洗，保护网站免于攻击。

安全恢复—风险处理

如果高校网站出现安全问题，必须在最短时间内、在不影响正常业务应用的前提下进行网站问题的恢复和解决，国内外发生的一些重大案例都表明对网站进行监控并在必要时提供恢复措施是非常必要的。

网站实时监控与自动恢复技术解决了 WWW 服务器网页文件被破坏后的自动恢复问题，它的保护对象是网站的文件或目录（也可以扩展到其他的文件和目录），从而保证它们的内容、属主、时间等属性不被非法修改；被保护对象不被非法删除；没有文件或目录被非法添加到被保护目录中。这项技术采用的方法是实时对网页文件的内容进行一致性检查，一旦发现有上述的非法情况发生，就使用备份进行自动恢复并及时报警和记录日志。

运维监控—风险管理

除了通过各类技术设备实现高校网站的检测、防护、恢复等方面的安全保障外，绿盟科技还推出了基于绿盟科技云安全平台的托管式服务模式“绿盟网站安全监测服务”，该平台主要解决网站运维阶段的安全预警和监控，为客户站点提供 7*24 小时不间断网站安全实时监控，帮助客户随时掌控 Web 应用的安全状况，在网站出现风险情况后在第一时间通过邮件、短信方式通知用户。

用户无需购买、安装或维护任何软、硬件就可以在几个小时内将监测服务投入运行。网站安全监测服务几乎不会对现有网络结构和 IT 资源产生任何影响，对于不希望在自身网络环境中部署安全设备、预算有限、安全重点集中在某一段时间如高招这样的用户群体，采用该类服务可最大限度地保障网站运维阶段的安全问题监控。

主要包括以下几方面的内容: 远程网站漏洞扫描、远程网页木马监测、网页敏感内容监测、网站平稳度检测、网页篡改监测。

溯源取证—积极主动

在安全形势日益严重的今天，以往对针对高校网站的攻击行为仅采用防护和阻击的方法已经远远不够了，在现有的保障体系上一定要保证对攻击源、攻击路径、攻击行为有足够的回溯能力，保证对恶意攻击行为的威慑和取证，为必要时通过法律手段维护高校权益打下良好基础。绿盟科技网站保障方案提供了对攻击行为的深入分析，对攻击现场进行还原，并对典型攻击行为具备路径回溯能力，实现对严重危害高校网站的安全事件的场景还原、攻击溯源和信息取证。

实践表明：通过对高校网站进行预警检测、安全防护、安全恢复、运维监控、追踪溯源等环节的安全建设，并在运维阶段加强信息安全管理，可有效保障高校网站的信息安全，满足国家、行业主管机构的监管要求；保证重大事件（高考、招生）期间的网站安全；维护高校的形象和声誉；提高高校网站的安全运维效率。

云安全服务：电信运营商新利润增长点

行业营销中心　田民

摘要 互联网应用的迅猛发展丰富和方便了人们的生产生活，客观上也为黑客提供了充分施展拳脚的广阔空间。不断变化和演进的攻击手段，使得传统的企业安全防护体系面临着前所未有的严峻挑战。随着云计算在各个领域的成功落地，基于云计算的安全服务已经从概念阶段过渡到了完善和推广阶段。以 AT&T 和 NTT 为代表的传统运营商，面向其企业用户推出的云安全服务，虽然在技术实现和业务模式上存在不同，但是无疑为其他电信运营商开展与时俱进的安全增值业务提供了很好的参考案例。

关键词：云计算　云安全服务　电信运营商　增值业务

无处不在的“云”

在不久的将来，如果有人问：“云”在哪里？答案一定是，无所不在。

越来越丰富的市场数据正在打消人们对于“云”概念的怀疑，越来越多成功的部署案例表明云计算不再是漂浮在头顶上空的一团虚无缥缈的水气。

在 IDC 公司 2009 年上半年的一次市场调查中显示，现阶段约 11% 的被调查企业已经采用了诸如云计算平台或云服务的商业化云方案，同时约有 41% 的被调查企业正在对云方案评估或正在进行云方案的试用。云计算被广泛应用于企业运营管理、数据存储，以及日常桌面办公等诸多方面，类似于 Saleforce 以及 Google App 等基于云的应用正在逐渐取代传统的应用模式，融入到人们实际的生活和工作中。

人们在云计算“元年”之后盘算着 2010 年乃至今后若干年云计算该如何蓬勃发展的同时，基于云计算的安全服务（Cloud-based Security Service）逐渐浮出水面，越来越多的企业用户成为云安全服务的受益者。提供云安全的服务提供商，最初主要是一些专业的安全厂商。近两年，提供公众服务的电信运营商也从关注到采纳，依托强大的电信网络资源和营销优势，推出了面向其企业用户的一系列基于云计算的安全增值业务。

发展和演变

“Bad guys go where the money is.” – 安全角度上的互联网万有引力定律。

随着互联网应用的迅猛发展，基于 Web 的应用变得异常的丰富。“HTTP is the next TCP”突出地表现为用户对浏览器的依赖性到达了不可割舍的程度。越来越多的应用系统从 C/S 架构迁移到 B/S 架构，在线办公、线上游戏、网上交易以及即时通信成为趋势。互联网提供了前所未有和无以伦比的便利，并最终紧密地融入到人们的日常生产生活之中。

积累了巨大财富的互联网最终造就了越来越多的互联网富翁，其

中，也包括黑客。

黑客的财富始终伴随着互联网用户的不断增加和互联网应用的不断发展而与日俱增。丰富的互联网应用客观上为黑客提供了充分施展拳脚的广阔空间，攻击手段也不断变化和演进。首先，黑客攻击的目的越来越向应用破坏和信息窃取演变。无论是提供网站服务的服务器端资源还是作为访问者一方的用户端资源，都有可能成为入侵者攻击的目标。其次，攻击者使用的攻击方式也变得越发复杂和五花八门，利用 Web 网站和互联网应用软件（如 IM 等）进行网站挂马、网络钓鱼以及散布恶意软件等各种攻击手段不断涌现。最后，新的安全威胁，单纯从数量上来说越来越多，扩散速度也越来越快。根据国家计算机病毒应急处理中心病毒样本库的统计，2009 年新增病毒样本 299 万个，是 2008 年新增病毒数的 3.2 倍。2009 年发现新增木马 246 万多个，是 2008 年新增木马的 5.5 倍。安全威胁的演进给最终用户带来前所未有的安全威胁。

安全威胁的发展和演变对安全防护手段提出了更高的要求。从功能相对单一的防火墙到多层次多功能的 UTM 设备，再到专门用于 Web 防护的 WAF 产品；从单纯提供流量监控的 IDS 系统到兼具监控和控制的 IPS 系统；从基于 Flow 的流量检测到基于数据包深度包分析 DPI 系统；安全产品的不断推陈出新以及针对不同场景和应用的细分，为防护者提供了丰富多样的部署设备。

防护的挑战

真正困惑企业用户的，与其说是越来越多的安全攻击手段和越来越快的病毒木马扩散速度，不如说是如何在众多的安全产品中选择适当的产品以及部署适当的防护设备。

攻防正日益演变为一场残酷的面对面博弈。就像一对拳击选手，攻击的一方想方设法要么通过组合拳令对手防不胜防，要么提高出拳速度，给予对手出其不意的打击；而作为防守的一方，不仅要利用双拳和必要的躲闪构建起纵深化稳固的防护工事，同时也必须要有先见之明，在攻击者出拳的一刹那甚至出拳之前就要预见对方的拳法和打击点，做出必要的反应。

遗憾的是，在很多情况下，黑客和企业用户间的拳击比赛并不是一场公平而对称的对抗。

首先，不能不承认很多黑客具备了专业的技能和“职业”的精神。不管原动力是对经济利益的追逐，还是对“翻墙”感受的渴望（前者的成分往往大于后者），单纯从攻防技能角度上讲，在很多成功的入侵案例中，攻击的一方具有比较明显的技术优势。除了技术因素之外，与人相关的还有一个更深层面的意识问题。一个企业是否具有专业或专职的安全管理人员，以及安全管理人员自身是否具有充分的安全意识，都是决定企业能否有效防御黑客攻击的重要甚至决定性因素。

其次，部署在企业用户现场的安全防护产品，设备的更新和升级能否跟得上攻击者攻击手段变化的步伐是一个巨大的问号。现阶段安全防护产品仍然普遍依赖于传统的样本采集、分析、特征码生成和分发机制。恶意代码样本数量的爆发式增长，直接导致传统上依赖于特征库的防护体系不堪重负。基于特征和签名识别的静态检测方式已经远远不能满足对现阶段迅速发展和变化的攻击手段的有效防护。此外，如果安全防护设备对流经的每个数据包都进行深层次的扫描，很

可能由于自身处理性能的瓶颈而最先挂掉。以广泛部署在企业边界的 UTM 设备为例，其特征库的更新是否及时将直接影响到该设备的防护效果。此外，可以想象，开启全部安全防护策略对于 UTM 设备本身就是一个噩梦。

由此可见，人员和设备都是影响甚至制约企业能否有效防护安全威胁的重要因素。那么，如何才能规避或者缓解因人员和设备的原因对防护造成的不利影响，或者更直接地说，有什么方法可能帮助企业更好地应对不断变化和快速发展的攻击手段呢? 至少有一点是可以明确的，防护手段必须跟上攻击手段的不断发展和变化，做到敌变我变，与时俱进，“以不变应万变”的静态防护思路已经不能满足现阶段安全防护的要求。

防护的演进

如果云计算是一场深刻的技术革命的话，那么云安全服务（Cloud-based Security Service）更像是一种多种因素下促成的防护体系以及商业模式的演进。

正像云计算不是偶然，而是人类文明在计算发展过程中，与互联网技术相结合后步入的一个崭新且必经的阶段一样，基于云计算的安全服务同样是互联网应用、安全威胁与安全防护三方面因素不断发展、不断演进和相互作用的一个必然结果。

什么是云安全? 简单来说，就是把云计算的理念应用到安全的规划、建设和交付中去。众所周知，云计算最大的优势在于最大程度上将处于不同物理位置的各种资源逻辑地连接在一起，形成统一的资源 / 信息池。分布式计算、资源共享和动态伸缩性是云计算的最主要的三个特点。云安全从交付的方式上来讲，与其他云计算的交付方式类似，很大程度上是以（计量）服务的方式提供给最终用户。云安全体系看起来更像是一个保持稳定而自我循环状态和新陈代谢的生态系统，可以很好地解决在安全防护过程中由于人和设备因素所面临的挑战。

首先，对于企业负责安全管理的人员来说，他所需要做的就是保证部署在企业中的安全防护设备与云安全中心之间的网络连通性，或者干脆把全部的网络流量重定向到云安全中心里，依托部署在云安全中心里的安全设备对流量进行全面检查和过滤。对于一些特定的应用，如企业门户 / 办公网站，企业的安全管理员可以通过简单的鼠标操作，购买云安全服务提供商提供远程扫描服务，对其门户网站进行随时的评估。

其次，在云安全体系中，安全设备不再是相对独立的一个个“安全孤岛“，而是一个完整的安全监控和防护体系之下的一个个传感器和安全闸门。分布于不同地域的安全终端节点，既是安全防护策略的执行者，也担当了对最新攻击行为的采集和反馈工作。它们及时采集到未知的安全攻击行为和恶意代码，通过安全专家的分析和研究，将研究成果以更新检测和防护策略的形式下发到终端节点。通过在终端节点中植入 lightweight 的信誉库，随时保持与中央信誉库的同步更新，保证对最新攻击行为的感知和防护。云安全体系下防护策略的更新不再是以季度、月或周来进行，而是随时随地的完成。

运营商的机遇

在 everything-over-browser 的趋势下，云安全服务为电信运营

商将安全变支撑，为盈利提供了崭新的思路和难得的机遇。

互联网的蓬勃发展，客观上加速了运营商从单一的“管道”提供商向综合服务提供商转变的进程，与互联网结合的数据业务成为运营商的核心业务和最主要的利润增长点。在云计算方面，国外运营商在几年前就以增值服务的方式推出了基于云的存储和企业管理（如 CRM）服务。

有意思的是，国外运营商以云安全服务的方式提供安全增值业务，似乎不比其他云计算服务晚多少。事实上，国外运营商早在 2007 年就开始尝试采用“云”的方式为其用户提供安全保护服务。例如 AT&T 公司，从 2007 年开始与 ScanSafe 公司合作，推出基于 SaaS 模式的云安全服务。采用 AT&T 云安全服务的企业，其上网流量被重定向到部署在 AT&T 数据中心里的 ScanSafe 平台上。ScanSafe 平台系统对用户的上网流量进行检查，保证用户访问的网站和诸如电子邮件等的应用是安全的。而在今年初刚刚发布云安全增值业务的 NTT Com. 则采用了与 AT&T 不同的服务内容和模式，NTT 推出的云安全服务——Biz Security Vulnerability Management，向其企业用户提供远程脆弱性（漏洞）评估的服务。

为什么最终用户会采用云安全服务呢？NTT 给出的答案是，吸引企业用户订购云安全服务的三个主要原因分别是快速、简单、和便宜。其中，省钱（cheaper）是吸引企业用户的首要因素。根据 IDC 的调查，超过 50% 的云计算客户选择“云”是因为“云”相对于传统部署要便宜。用户不用购买太多的软硬件设备就可以实现相应的业务防护需求。其次，省事（simpler）也是打动客户的一个关键因素。与繁琐的设备上架、软件配置、设备升级、维护和扩容相比，云安全服务往往只需要企业安全管理员点击几下鼠标就可以完成安全防护的部署。最后，省时（faster）不仅仅体现在快速部署即获得充分和全面安全防护上，及时发现系统安全隐患并在黑客利用这些隐患之前就堵上漏洞更是极大降低了事后恢复的时间成本。

对于电信运营商来说，提供云安全服务能够为运营商自己带来哪些收益和价值呢？同样有三点。第一，便于运营商更近地接触到客户，特别是新客户。云安全服务是基于互联网的，原则上是不区分网内客户与网外客户的，换句话说，A 运营商完全可以通过云安全服务将 B 运营商的客户纳入其安全增值业务覆盖范围之中。第二，降低业务交付过程中的开销。对于电信运营商来说，基于互联网的云安全服务的交付成本是很低的，互联网可达的地方就是云安全服务可交付的所在。第三，依托差异化服务寻求更多的利润增长点。云安全服务是一个依托互联网开展的增值数据业务，在 everything-over-browser 的趋势下，为电信运营商将安全变支撑，为盈利提供了崭新的思路和难得的机遇。

顾虑、风险与规避

云安全服务不是一个单纯的服务项目，而是一整套解决方案。

任何事物都有好的方面和存在风险的另一方面，云安全服务亦然。IDC 的资料表明，成本和价格因素并不足以影响用户最终通过采购云安全服务的决策。如何安全地获取云安全服务以及如何保证来自“云”的安

全能够满足其全部的防护要求，同样是用户决策过程中非常关注的方面。

对于电信运营商来说，同样面临两个非常现实的问题。第一个问题，如何与客户签订适当而合理的 SLA 协议？这与客户的担心是类似的。电信运营商往往与第三方安全厂商合作推出云安全服务，运营商提供的是一个运营平台而不是安全防护技术和安全设备，安全防护的效果甚至安全设备的稳定性都是运营过程中运营商需要面对的风险；第二个问题，如何规避前向收费价格战？这不仅仅是一个商业模式的问题。无论采用哪一种收费模式（pay per use 或 pay per month），都存在一个前向收费的挑战——用户更倾向于价格便宜的服务。如何说服用户购买一个更好而不是更便宜的服务，是电信运营商必须仔细思考的。

对于打消用户在获取云安全服务过程中有可能造成数据泄露的顾虑，NTT 采取的手段是依托 VPN 来实现用户到云安全服务中心间的数据交互。用户的安全管理人员对云安全服务中心的所有访问都是通过加密隧道来完成的，可以保证访问过程中数据的保密性。而对于最终用户和电信运营商都关心的 SLA 问题，Gartner 给出的建议是电信运营商在选择云安全厂商的时候就要对这个潜在的合作伙伴进行必要的评估，好的合作伙伴和好的安全产品 / 技术是云安全增值业务成功最基本的条件。

最后一个风险，可能也是电信运营商最关注的前向收费价格战风险。这是一个运营商必须要面对的问题，即如何在日益残酷的竞争中处于主动和领先地位。对此，IDC 和 Gartner 均给出了相同的回答——云安全服务不是一个单纯的服务项目，而是一整套解决方案。无论是在用户的客户端部署云安全终端设备，还是把用户的流量定向到自己的云安全中心里来，或者通过跨互联网远程扫描的方式进行脆弱性核查，相应的专家咨询、系统加固、现场取证以及事件追查都可以作为供企业选择的配套服务选项。

云安全服务，和其他数据业务一样，“the cheaper , the better”的逻辑并不完全适用。一套丰富而完整的云安全解决方案本身就是确保电信运营商云安全增值业务收益的最大保证。

智能电网的几类运行特征与安全防护要点研究

行业营销中心　张书嘉

摘要：本文旨在依据我国智能电网的运营特点与安全所需—规避那些制约着生产输配进程、对公服务信誉、以及电网 IT 系统资产稳健运行的隐患因素，设想并构建一种适度化防护及完善测量／控制能力的安全模式，进而巩固电网的运行水平和专责运维绩效。

关键词：智能电网　智能调度　智能表计　风险控制

引言

智能电网的关键使命和运营战略依赖于信息技术的推动，创新型的运营模式将衍生更多的业务应用和互动环节，而 IT 设施成为电网设备→用户 / 站点间双向交互机制的重要基础。本文研究基于智能电网几类业务类型中的上下游应用节点，测量可能隐含的安全薄弱环节并藉此引申出适用性的防护控制方案和优化设想。如下章节中的细节陈述和关键提议都将尊重于智能电网运营体制与安全性的必然联系；同时“支持诸如双向能量计量、分布式并网调度等中长期电网业务”的需求扩展。

本课题可适用于如下的电网业务单元:

业务模式	业务单元／区间
智能表计／集抄	包含载波集中器→表计 / 负控终端→子站端系统→主站及营销中心系统群组
智能调度	包含 SPDnet、110kv 以上变电站、主配网五级调度 / 集控中心、县调接入、并网电厂
智能变电站	包含 SPDnet、110kv 以上变电站、主配网五级调度 / 集控中心、县调接入、并网电厂
未来战略扩展	包含营配一体化体系中各级 IT 相关节点、分布式并网调度中的虚拟电厂接入节点等

本课题的核心论点即重点解答如下的疑问:

- 基于智能电网的几类业务模式，如何定位防护环节并构建合理的上下游安全策略?
- 面向各级／各类的智能电网业务单元，如何有效地测量安全水平，并差异化的控制风险?
- 如何提升专责式的运维绩效，同时强化垂直的集约化监管与考核能力?
- 面向不断发展的智能电网，如何构建中长期的安全机制，以测量和支撑未来新的业务模式?

REQUIREMENT：智能电网的业务特性与安全环节

本小节意在简述智能电网几类业务模式的特点特性，以及其中可能隐含的安全薄弱环节；分析“解决这些隐患的策略和所需条件”是本小节的论述要点。

重点解答如下的疑问:

- 关于智能变电站、调度系统、表计业务节点以及过程中隐含的薄弱环节有哪些?
- 可能的危害，以及解决它们所需的条件是什么?

1、智能表计／集抄的业务特点、安全薄弱环节与防范条件

智能表计在传统集抄的基础上提供了更细粒度的负荷控制与计量管理模式，一方面优化了最终用户的用电管理，同时也为区域配电扩容、能量控制和智能家电业务提供了决策支持依据。在智能表计的体系中，业务过程相关于智能电表端→载波集中器→表计 / 负控终端→子站端系统→主站及营销中心系统群组；在这一链条中，集中器和负控终端将直接参与 IT 自动化过程，并引用标准的通信规约兼 TCP/IP 协议，其本地汇集的数据以及直至主站的上行链路均存在明显的双向安全隐患。

隐患与危害:

- 举例：透过窃取表计数据来推测军械工厂的产能和产期，并模拟指令上报虚假负荷和转发能量数据，伪装校验，将一方面导致生产事故，一方面威胁国家安全；
- 集中器面向下游终端建立电力载波通信，面向上游系统建立标准的规约或 TCP/IP 通信；临时存储于本地的由采集器上传的数据内容可能被恶意窃取和修改；
- 载波集中器的上行链路存在非法会话劫持的可能，一方面可窃取和还原上报至主站的数据封装，一方面可以恶意修改它们。包括由主站下发的操作信令；
- 未经审核的负控终端将存在非法接入的可能，通过模拟应用行为即可传播伪造信令和建立非法数据分析。

需求与条件:

- 需要为集中器和负控终端提供更有效的文件系统级保密存储机制，以支持任意数据类型的快速保密，且不破坏其数据结构；
- 需要建立双向的链路级保密机制，以确保数据流在通信介质中的机密性和完整性；
- 需要在集中器与主站之间建立端对端的接入认证机制，以确保只有合法的终端允许参与到智能表计业务中；
- 上述的一切需要集中的策略管理和状态监控。

2、智能变电站的局部业务特点、安全薄弱环节与防范条件

数字化变电站的核心除了光电互感和部分智能一次技术以外，最关键的当属 IEC61850 规约通信与鉴于此基础的数据接口规范；依据此规约的业务过程相关于本站内的变电站层、间隔层和过程层，以及面向主站端的上行纵向链路；在这一链条中，全部自动化系统将基于 IEC61850，其脆弱的协议结构和缺少异常报文识别能力的应用系统可能导致业务安全隐患；而新上线的 D5000 以及即将下线纵向保护装置也可能导致子站缺少有效的边界安全机制。

隐患与危害:

- 举例：建立非法的 TCP/IP 通信以传播恶意代码导致应用缓冲溢出，或构造 61850 协议炸弹并伪造开关／刀闸设备的信令，将一方面导致生产事故，一方面威胁国计民生设施的安全；近似中间人式的攻击也将难以追溯记录；
- 已投运的 61850 站点均以明文方式建立报文传输；破坏者无需点表，即可轻易读懂开关、刀闸等各类变电站逻辑节点信息；
- 缺少能够过滤异构通信的边界关守，使更多基于 TCP/IP 等通用协议的攻击会威胁到站内系统；

• 缺少针对入站流量的深度检测，将导致非法的 61850 数据结构／逻辑炸弹可能破坏站内自动化系统;

• 新上线的 D5000 将逐渐终结纵向加密装置的历史意义，这可能导致多数智能化子站缺少了专有的安全保护机制，而传统的防火墙设备难以为变电站通信提供保护。

需求与条件:

• 变电站的边界关守需要提供解析 61850 和 TCP/IP 通信，并在此基础上提供深度的威胁监测（病毒、蠕虫、挂马、已知 / 未知攻击类型、缓冲区溢出操作等）、威胁阻断甚至主动处置的机制;

变电站的边界关守需要支持 IEC61850 规约的完整性校验，支持非法的 61850 协议数据结构（逻辑炸弹）识别，以确保合法的 61850 通信被路由;

• 变电站的边界关守不可影响智能电网应用系统的正常业务逻辑，不可为电网系统的运维人员附加额外工作负担;

• 需要提供扩展支持，例如扩展通信规约的结构语义、安全监测的威胁类型与特征等。

3、智能调度体系的局部业务特点、安全薄弱环节与防范条件。

智能调度体系所包含的关键意义是对调度中心、变电站、厂站和一次系统的数字化管理，进而保障电力输配和优化电网运行效率；在这一链条中，全部系统节点应在调度中心的管控范围，其中的薄弱环节在于县调接入的低安全性，以及并网电厂与远端站点内的脆弱的系统运维水平等；可能导致更多的威胁来源来自于此，成为入侵主站的攻击途径。

隐患与危害:

• 举例：长期处于低保护状态、缺少运维支持的县调或远端厂站系统，其难以合理的具备安全运维能力和专业人员；未经巩固的站内系统和通信节点可能成为入侵者的攻击途径，进而伪造信令窃取数据，或伪装身份进入主站；将一方面导致生产事故，一方面威胁国计民生设施的安全。

• 县调和厂站的接入仍以 2006 年的安全标准为参考，成为进入 SPDnet 的最大安全隐患；无论应对安全检查或是保障运行安全，传统机制已经不足以应对风险。

• 不易快速响应，面对突发威胁时，难以迅速调整全网安全水平；面对敏感时期时，难以迅速提高各地站点的运维水平。

需求与条件:

• 需要为各类 IT 节点或应用系统逐个制订入网安全基准，以确保符合基准安全水平的 IT 设施被应用于智能调度体系;

• 以调度中心和安全专责为核心，能够适时监控所辖的站点、各类 IT 应用系统和网管工作站的安全运行水平，提供加固指导和操作票，弥补厂站内 IT 运维人员的缺乏;

• 依据电网系统安全运行相关的政策标准／法规，为所辖站点内所有 IT 装置／系统独立制订安全合规策略，并提供符合各类政策法规的立据声明;

• 形成面向县调、并网电厂、远端站点、第三方系统的安全接入标准;

• 上述的一切需要集中的策略管理和适时监控。

SOLUTION：基线式的测量、控制、决策支持

上述的“3”个方面显示了智能电网个别

运营环节可能隐含的风险隐患，它概括了电网系统愈加丰富而开放的业务模式下，对于专有化保护、细粒度控制以及集约化内控的期望。本小节旨在延续上一章节，分析“有效识别和控制这些隐患所需的策略和方案”是本小节的论述要点。

即意在解答如下的疑问:

- 如何面向调度系统、智能变电站、表计业务建立专有化风险控制方案?
- 方案的技术实现过程，以及实际的应用情景是什么?

1 课题定位与适用范围

本小节将来自于三类电网业务的安全需求分解为三个研究课题，以独立说明它们的技术研究路线和适用范围。

课题一:

课题名称	《智能表计的末端节点接入控制、源数据保护与主站集控管理》
研究路线	应用于智能表计业务过程内，面向数字化子站和终端设备（集中器／负控终端设备）提供专有化的接入认证、链路保护与本地源数据保密机制;
适用范围	集团营销中心、省级营销中心、参与表计业务的数字化子站与终端设备、智能电网办;

课题二:

课题名称	《智能变电站的 61850 规约通信关守与会话风险控制》
研究路线	应用于兼容 IEC61850 的智能电网设施内，建立保证 61850 出入站会话安全的深层次威胁监测与阻断机制；以解析变电站间的通信语义为依据，形成专有化的防护机制。
适用范围	国调、省／地级调度中心（或集控中心）、兼容 IEC61850 通信的数字化子站;

课题三:

课题名称	《智能调度体系内 IT 装置／系统的入网安全水平测量与集约化监管》
研究路线	应用于智能调度体系内，承担各类 IT 装置与系统的入网安全基准认证、差距分析与安全水平监控；藉此完善对于县调、并网电厂与远端站点的接入控制与持续监管。
适用范围	国调、省／地级调度中心（或集控中心）、智能电网办;

2 过程与实现:

本小节将来自于三类电网业务的安全需求分解为三个研究课题，独立说明它们的技术实现原理和交付成果。

课题一:

课题名称	《智能表计的末端节点接入控制、源数据保护与主站集控管理》
内容摘要	应用于智能表计业务过程内，面向数字化子站和终端设备（集中器／负控终端设备）提供专有化的接入认证、链路保护与本地源数据保密机制。
实践思路	1) 以主站／营销中心为核心，梳理智能表计的上下游站点的数据交互关系；制订接入控制标准与链路保护标准; 2) 依据子站或终端系统接口规范，研发分别应用于载波集中器、负控终端设备的上行接入认证与链路通道保密模块，该模块提供基于本站／本终端的身份鉴别，以及建立合法通信通道所需的密钥凭据；使子站端与终端设备能够在接入表计网络时提供合法身份，并确保上行传输的机密性与完整性; 3) 依据子站或终端系统接口规范，研发分别应用于载波集中器、负控终端设备的文件系 统级保密模块；该模块提供文件系统级的静态数据保密措施，以及建立透明加密所需的密钥凭据; 使临时存储于集中器／负控终端系统中的任意数据类型得到保护，同时确保一方面不变更原有数据结构、一方面与本地应用程序接口无关; 4) 将上述功能模块发布到子站端／终端设备中，通过正常模式导入安装; 由于其依据子站或终端系统接口规范研发，具备专有性，无需二次改造；与现有应用程序无关，对表计业务的正常运行不构成影响; 5) 由此，由载波采集器上传的数据封装将被临时存储于集中器／负控终端本地，由安全的文件系统提供透明加密措施；汇总后的数据上传时需要提供证明当前设备合法身份的凭据，并以此建立与主站端的通道加密；这一链条确保了计量数据进入 TCP/IP 网络直至主站端的过程可信性。
交付成果	1) 形成兼容于集中器／负控终端的安全文件系统模块、接入控制模块; 2) 形成应用于主站的集中策略管理与监控中心; 3) 形成标准化的产品耦合接口、策略模板; 4) 形成长期的辅助决策支持与改进服务。

课题二:

课题名称	《智能变电站的 61850 规约通信关守与会话风险控制》
内容摘要	61850 专用安全关守：基于 IEC61850 通信规约的语义解析与威胁识别，它将有效的过滤智能电网上下游通信，并结合业务特点采取风险控制措施。
实践思路	1）对“厂站与调度中心、调度中心间、厂站间”的 IE61850 会话模式进行梳理，并制订会话特征与策略模板; 2）在现有的 TCP/IP 通信基础上开发 IEC61850 规约的驱动层，使其对 61850 通信 header 和内容中隐含的威胁特征进行解析识别; 3）编制符合 IEC61850 规约会话特征的威胁核查机制和特征库; 4）修订传统的威胁过滤与访问控制模块，使其加入针对性 61850 会话特征和威胁特征的仲裁模板; 5）以关守形式部署于主站或子站网络出口，统一针对全部通信会话／信令流量进行审核，合并判断 61850 通信和 TCP/IP 通信的安全性；并有选择的采取监测、被动阻断、主动阻断的仲裁机制；最大限度避免影响应用系统的正常业务逻辑。
交付成果	1）形成兼容 IEC61850 与 TCP/IP 的安全关守装置; 2）形成标准化的产品耦合接口、电力数据通信规约模板、策略模板; 3）形成长期的辅助决策支持与改进服务。

课题三:

课题名称	《智能调度体系内 IT 装置／系统的入网安全水平测量与集约化监管》
内容摘要	智能调度系统的基线式安全监管中心，承担各类 IT 装置与系统的入网安全基准认证、差距分析与安全水平监控；完善县调、并网电厂与远端站点的接入控制与持续监管。
实践思路	1) 第一阶段，定义目标与制订安全基线: 测量智能调度 “各类信息系统” 所需的理想化安全运行目标与当前水平的差距，同时结合本地保障要求、业务特点和政策法规等因素，制订适用于本地的合理安全基线标准; 2) 第二阶段, 试行与配平基线: 新的安全水平(基线) 是面向各级各类电网系统分别定制的“差异化的安全策略”, 是作为“保持调度自动化系统稳健运行的一组最佳运行指标”；各级／各类系统依据各自的基线标准被适度巩固的过程称之为 “配平”，这一过程将确保这些系统均达到 “预定的理想安全水平”; 3) 第三阶段，监控与维护基线：监控基线的应用情况将确保各系统 “仍然保持于一个理想的安全运行水平”；确保各类信息系统在运行周期中被针对性保护和持续保护，然而，当出现最新的威胁／漏洞、或敏感时期的特殊政策要求时，以及新系统的实用化运行或技改情况时，可适时针对当前基线水平进行审核和微调。藉此建立有针对性的持续改进闭环。 4) 第四阶段，将基线运行标准实现自动化，使该工具能够自动化的针对各类系统提供测评和监控，并能够适时提供保护策略和配置方案，简化运维压力；同时亦能够针对即将入网的各类 IT 系统／装置提供入网安全测评服务，为符合安全要求的系统颁布认证，为低于基线标准的系统提供安全整改或配置加固建议; 5) 第五阶段，当面临外部安全检查时，该工具能够适时审核各级／各类系统对于指定政策或标准的符合性，以提供补足建议和配置方案，并能够针对各类检查标准提供符合性立据声明，以确保当前系统符合指定要求; 6) 同时可制订县调、并网电厂、远端站点的测评模板，使该工具能够以调度中心为核心节点，控制所辖厂站的入网接入标准；监控它们的恒定安全运行水平，定期核查与督导，并对其运行水平／运维水平提供评价；敏感时期亦可迅速地强行提升各级系统的安全水平，快速处置新的薄弱环节。
交付成果	1) 形成面向各级／各类自动化系统／装置的技术核查标准与指标; 2) 形成自动化的基线式管理工具; 3) 形成标准化的产品耦合接口与策略模板; 4) 形成长期的辅助决策支持服务。

3 应用的场景:

本小节进一步解析上述三个研究课题，以独立说明它们的实际应用情景。

课题一:

课题名称	《智能表计的末端节点接入控制、源数据保护与主站集控管理》
应用情景	1) 由载波采集器汇总电表端计量与负荷数据，基于电力载波安全的上传至子站端集中器; 2) 数据封装将被临时存储于集中器／负控终端本地，由安全的文件系统提供透明的加密措施；以确保它们难以被窃取和解读; 3) 进一步汇总后的数据需要上传至主站，此时需要提供证明当前设备合法身份的校验凭据，以确保仅合法设备可以建立上行通信; 4) 确认接入设备合法性后，由当前设备提交密钥并与主站端协商建立私有的保密通道，以此确保与主站端通信链路的机密性和完整性; 5) 这一链条确保了表计数据进入 TCP/IP 网络直至主站端的过程可信性。

课题二:

课题名称	《智能变电站的 61850 规约通信关守与会话风险控制》
应用情景	1) 兼容 IEC61850 的通信关守部署于主站与子站的流量汇集点，面向应用逻辑提供透明的协议层 + 内容层监测能力; 2) 当入站流量到达关守适配器时，它将首先判断该流量是否为一个合法的 61850 会话，其中包含是否封装合法的规约 header 以及是否携带有效的 61850 载荷; 3) 在第二阶段仲裁过程中，关守将针对 61850 报文的内容进行解析审核，其包含判断报文实际内容中是否携带病毒、木马、蠕虫以及某种攻击性特征；同时对 61850 报文内的数据结构进行审核，以确保不具备逻辑炸弹或威胁应用的特征; 4) 在仲裁过程中匹配出的任何违规报文都将依规则阻断或丢弃，仅合法流量允许入站; 5) 同时当关守旁路部署时，将体现一个 61850 流量威胁告警装置的作用，用于适时监测违规流量，发出威胁预警。

课题一:

课题名称	《智能表计的末端节点接入控制、源数据保护与主站集控管理》
可行性与受益	1) 本课题的相关技术采用轻量级方式实现，应用中立技术，电力单位可自主掌握; 2) 本课题深入于实际业务，杜绝了潜藏的安全隐患，避免了智能表计数据被恶意窃取和利用的风险，通过轻量级的方式建立了终端 -> 子站 -> 主站的过程可信性; 3) 智能表计的各安全模块均保持与应用程序的无关性，在部署和运行过程中对于实际业务无影响; 4) 智能表计的各安全模块基于电力系统标准而研发，具备较强的专有性，能够与电力系统有效耦合，并支持更多的功能扩展; 5) 本课题同时适用于智能电网的未来战略，例如在双向能量计量、智能家庭用电业务中均能够提供安全性支撑; 6) 创新价值：目前国内外尚没有针对智能表计业务过程的有效保护，且这一系列风险隐患尚未受到关切，本课题提供了深入实际业务的专有性风险控制方案，并针对全部表计过程的安全性进行逐一控制；具备形成国内外创新成果的良好条件。

课题二:

课题三:

课题名称	《智能调度体系内 IT 装置／系统的入网安全水平测量与集约化监管》
应用情景	1) 基线工具预置本调度中心所辖各级各类系统的核查／测评标准，并对这些系统提供周期性的安全水平监控，以判断其是否正处于理想的安全运行水平，当低于此标准时，基线工具提供适度配平的整改方案，以协助本地／远程运维人员针对目标系统进行适度巩固；被核查的系统可以包含：变电站层和间隔层的信息系统，网络设备（含 61850 交换设备）、智能设备、网管工作站等; 2) 能够结合行政手段，依据各级各类系统的运维要求建立 KPI 评价指标，当此项功能应用于县调接入、并网电厂时，将能够进一步强化调度中心的集控性监管能力; 3) 同时可提供入网 IT 系统／装置的安全水平评测，能够对即将入网的 IT 系统／装置进行安全性核查，以判断其是否具备一定的安全运行能力，以及其自身所携带的安全功能是否发挥作用；从而决定该系统是否有能力运行在理想的安全水平上，在低于基线检查指标时，基线工具在输出认证的同时也将提供系统整改要求或配置加固方案。

BENEFIT: **综合收益与可行性**

课题名称	《智能变电站的 61850 规约通信关守与会话风险控制》
可行性 与收益	1) 应用无关性：61850 关守作用于主站或子站的流量汇集点，针对出入站流量进行内容级审核以及透明仲裁，无应用接口耦合，对现有应用逻辑不造成影响; 2) 通信规约的兼容性；能够同时将 IEC61850 流量与 TCP/IP 流量合并处置，必要时可兼容 IEC60870 通信，可以综合判断各种协议流量或合并协议流量的安全性; 3)D5000 的互补：61850 关守将弥补 D5000 上线后的子站安全性不足，其将有效的为子站通信提供更加完备的访问控制能力，以满足 D5000 体系对于上下游通信的安全性要求; 4) 细粒度的安全审核与灵活的仲裁机制: 能够进行内容级安全审核, 包含针对病毒、蠕虫、木马、多数主 / 被动攻击行为等并可选择的通过静态规则阻断、主动阻断、丢弃等模式仲裁流量; 5) 未来可扩展：未来可以适时依据电网行业标准或特殊需求而改进，包含规约语义、特征库升级、仲裁模式的改进等; 6) 兼容 IEC61850 的通信安全关守采用轻量级方式实现，应用中立技术，电力单位可自主掌握; 7) 创新价值：同时兼容智能电网 IEC61850 和 TCP/IP 通信，并提供合并仲裁的技术尚没有应用，本课题提供了一种轻量级的更具创新性和实践性的思路。

课题三:

课题名称	《智能调度体系内 IT 装置／系统的入网安全水平测量与集约化监管》
可行性 与收益	1) 基线式的管理模式采用轻量级方式实现，应用中立技术，电力单位可自主掌握; 2) 可完全契合现行的电网业务特点、政策标准与制度体系、专责管理模式等条件; 3) 基线管理模式是契合于本地实际情况的标准化产物，可持续履行，持续改进; 4) 基线管理模式旨在维护适度安全建设，因其是基于业务的测量、基于差距的补偿；可避免重复投入、重复建设; 5) 基线工具可协助调度单位面向 IT 系统厂商提供入网安全水平评测和认证服务，使更安全和稳定的 IT 系统能够应用于智能电网中; 6) 基线管理模式可促进安全保障体系与评价考核体系融合；可作用于智能电网的安全集控与合规；可面向调度中心、集控中心、厂站提供安全水平的集约监管; 7) 创新价值：“基线式安全”使所有信息系统的安全水平、运维绩效都成为可测量的、可考核的、可改进的；其质变的思想可应用于调度单位和智能电网中，可藉此形成创新性成果。

POSTSCRIPT:

本文依据智能电网的几类业务特征，分析其中可能隐含的安全隐患，并建立深入业务的创新课题研究；意在面向智能电网的不同运营实体提供保障。上述的三个课题成果同时预留对未来电网业务的扩展支持，诸如双向能量计量、智能家庭用电、分布式发电与虚拟电厂等业务环境下的安全性要求。

绿盟科技具备专属的能源行业研究团队，并长期致力于电网业务特点的研究与成果创新；进而能够深入业务，密切契合电力单位的业务保障目标，提供行业化的安全解决方案和产品；协助电网单位建立理想的安全运行水平与运维水平。

把脉信息系统安全审计

产品管理中心　蒲新宇

摘要：本文介绍了信息系统安全审计（Information System Security Audit, ISSA）的定义、发展历史和趋势，并阐述了信息系统安全审计的主要应用领域、技术手段和发展趋势。

关键词：安全审计　发展历史　审计技术　趋势

随着信息化水平的快速提高和信息安全建设的逐渐深入，如何有效加强内控管理、信息系统安全风险控制，满足政策合规的要求，成为企事业单位面临的普遍问题。作为问题的主要解决技术手段之一——信息系统安全审计，正逐渐成为国内信息系统安全建设热点。

一、信息系统审计定义与发展历史

信息系统审计 (Information System Audit, ISA) 是通过收集和分析审计证据，对信息系统是否能够保护资产的安全、数据的完整、运营效率等方面做出判断的过程。

信息系统审计是计算机技术与数据处理电算化发展的结果。数据处理电算化对信息系统审计产生了重大影响，计算机在数据处理中的运用形成了电子数据处理系统，它产生于 20 世纪 50 年代。因此，信息系统审计的概念产生可追溯到 20 世纪 60 年代。信息系统审计的发展历史可以分为三个阶段:

1960 年 -1970 年，信息系统审计概念形成阶段

20 世纪 60 年代，信息系统审计最早称为计算机审计，是随着计算机在财务会计领域的应用而产生。早期的计算机应用比较简单，计算机审计业务主要关注对被审计单位电子数据的取得、分析、计算等数据处理业务。1960 年初，IBM 出版了《Audit Encounters Electronic Data Processing》，该书首次提出了电子数据环境下的内部审计规则和组织方法。60 年代中期，美国国防部海军审计局引进了通用审计软件包。1968 年美国 EDPAA 协会（执业会计师协会）发表《电子数据处理系统与审计》，详细探讨了审计与电子数据处理系统的关系，并提出若干计算机辅助审计电子数据处理系统的方法。

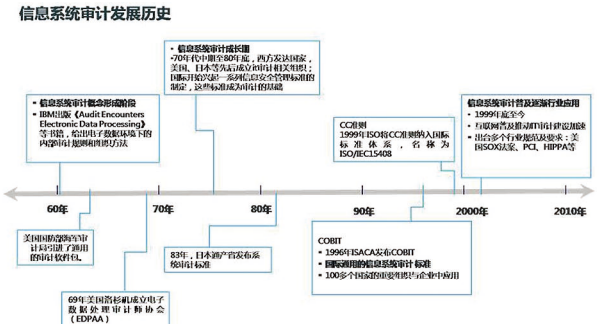


图 1　信息系统审计发展历史

1970 年 -1999 年，信息系统审计成长阶段

70 年代中期至 80 年代，美国、日本等先后成立计算机审计相关组织；国际开始兴起一系列信息安全管理标准的制定。1983 年，日本通产省发布《系统审计标准》，开始培训信息系统审计人员。1984 年美国 EDPAA 协会(执业会计师协会)发布一套 EDP 控制标准-《EDP 控制目的》。

1996 年，ISACA 协会发布了 COBIT（Control Objectives for Information and related Technology）标准，是国际上公认的安全与信息技术管理和控制的权威标准，也是国际通用的信息系统审计标准，已在 100 多个国家的重要组织和企业中应用。

1999 年 - 至今，信息系统审计普及和行业应用阶段

2001 年至今，美国安然事件及由此引发的一系列美国著名大公司在公司治理和财务管理力方面的问题，促使美国陆续出台了多个具有较强影响力的行业法案，如：2002 年美国出台 Sarbanes-Oxley 法案（萨班斯—奥克斯利法案），其中第 404 条款要求企业在财务报告方面加强内控，企业的 CEO 和 CFO 必须对本企业的内控系统的有效性发表诚信声明。因此，IT 信息系统同样需要加强控制以达到 SOX 法案的合规要求； 2005 年针对 IT 信息系统的 SOX 合规审计成为全球 CIO 最关注的事。目前，西方发达国家的信息系统审计应用已较为普遍，并发展到了较高的水平。

二、信息系统安全审计定义与发展

信息系统安全审计是信息系统审计全过程的组成部分，主要依据标准包括 COBIT、CC、ITIL 等信息安全管理标准。信息系统安全审计是评判一个信息系统是否真正安全的重要标准之一。通过安全审计收集、分析、评估安全信息、掌握安全状态，制定安全策略，确保整个安全体系的完备性、合理性和适用性，才能将系统调整到“最安全”和“最低风险”的状态。安全审计已成为企业内控、信息系统安全风险控制等不可或缺的关键手段，也是威慑、打击内部计算机犯罪的重要手段。

在国际通用的 CC 准则（即 ISO/IEC15408-2:1999《信息技术安全性评估准则》）中对信息系统安全审计（ISSA：Information System Security Audit）给出了明确定义：信息系统安全审计主要指对与安全有关的活动的相关信息进行识别、记录、存储和分析；审计记录的结果用于检查网络上发生了哪些与安全有关的活动，谁（哪个用户）对这个活动负责；主要功能包括：安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件选择、安全审计事件存储等。

这是国际 CC 准则给出的一个比较抽象的概念。通俗来讲，信息安全审计就是信息网络中的“监控摄像头”。通过运用各种技术手段，洞察网络信息系统中的活动，全面监测信息系统中的各种会话和事件，记录分析各种网络可疑行为、违规操作、敏感信息，帮助定位安全事件源头和追查取证，防范和发现计算机网络犯罪活动，为信息系统安全策略制定、风险内控提供有力的数据支撑。

（一）国内信息系统安全审计发展历史

与国外相比，中国的信息系统安全审计起步较晚，相关审计技

术、规范和制度等都有待进一步完善。随着我国信息化水平快速提高，信息系统安全审计正逐渐成为国内信息系统安全建设热点之一。我国的信息系统安全审计发展可分为两个阶段:

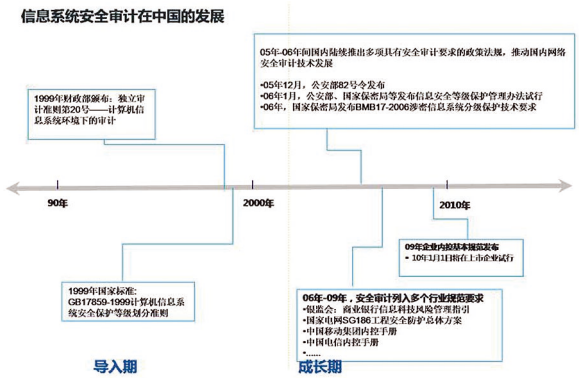


图 2 信息安全审计在中国的发展

1999 年 -2004 年 信息系统安全审计导入期

1999 年财政部颁布了《独立审计准则第 20 号 - 计算机信息系统环境下的审计》，部分内容借鉴了国外研究成果。这是国内第一次明确提出对计算信息系统审计的要求。

同年，国家质量技术监督局颁布《GB17859-1999 计算机信息系统安全保护等级划分准则》，该准则是建立计算机信息系统安全保护等级制度，实施安全保护等级管理的重要基础性标准，其中明确要求计算机信息系统创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏 。

2005 年 -2009 年 信息系统安全审计的快速成长期

互联网在国内迅速普及应用，推动国内信息系统安全审计进入快速发展阶段。国家相关部门、金融行业、能源行业、运营商均陆续推出多项针对信息系统风险管理政策法规，推动国内信息系统安全审计快速发展。

2005 年 12 月，公安部颁布 82 号令《互联网安全保护技术措施规定》，其中明确要求“互联网服务提供者和连接到互联网上的企事业单位必须记录、跟踪网络运行状态、记录网络安全事件等安全审计功能，并应当具有至少保存六十天记录备份的功能。”

2006 年，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合制定并发布了《信息安全等级保护管理办法（试行）》，该办法明确要求信息系统运营使用单位在开展等级保护工作中要按照或者参照国家、行业技术标准进行系统定级、建设、整改、测评等工作。《信息系统安全等级保护基本要求》是信息安全等级保护标准体系中重要的基础性标准之一。该要求针对不同安全保护等级信息系统的基本安全审计能力均有明确要求，如: 需要对用户行为、安全事件等进行记录，对形成的记录能够统计、分析、并生成报表。2006 年，国家保密局发布 BMB17-2006 号文件《涉密信息系统分级保护技术要求》，文件要求相关涉密单位信息系统，根据不同涉密级别，采取相关审计措施。如:

- 必须制定明确的系统安全审计策略;
- 确定的审计事件范围应对安全事件的事后追查提供足够的信息;
- 审计记录包括服务器、涉密重要用户终端、安全保密设备、用户、用户权限修改以及用户操作等。

2006 年 -2009 年，安全审计被列入多个行业信息系统安全建设要求

随着政府、金融、电信、能源等行业信息化的发展，信息科技的作用已经从业务支持逐步走向与业务的融合，成为各行业稳健运营和发展的支柱，为加强信息系统风险管理，各行业陆续发布了行业性信息系统管理规范和要求。

2008 年 6 月，财政部、证监会、银监会、保监会及审计署委联合发布了《企业内部控制基本规范》，该规范被称为中国的"SOX 法案"，是我国在审计领域的重大改革举措，该规范将首先在上市企业中实行。如何把 IT 内控与企业内控管理统一起来，是《企业内部控制基本规范》的一个关键点，信息安全审计则将成为企业 IT 内控、安全风险管理的不可或缺的技术手段。该规范将促使国内企业加强 IT 内控建设，从而推动安全审计市场的发展，但其中非常关键的一点就是安全审计技术如何有效地与规范结合，满足企业合规审计要求。

2009 年 3 月，银监会为加强商业银行信息科技风险管理，发布了《商业银行信息科技风险管理指引》，该指引中重点阐述了信息系统风险管理和内外部审计要求，特别是要求审计贯穿信息科技活动的整个过程之中。另外，在《国家电网 SG186 工程防护总体方案》、《中国移动集团内控手册》、《中国电信集团内控手册》等行业要求中也均明确要求采取信息系统风险内控和审计技术手段。

目前，随着信息安全建设的深入，安全审计已成为国内信息安全建设的重要技术手段。总体来看，由于信息系统发展水平和业务需求的不同，各行业对安全审计的具体关注点存在一定差异，但均是基于政策合规、自身安全建设要求，如：政府主要关注如何满足"信息系统安全等级保护"等政策要求的合规安全审计；电信运营商则基于自身信息系统风险内控需求进行安全审计建设。

（二）信息系统安全审计技术分析

目前，国内信息系统安全审计有下述几类主流审计技术：网络安全审计、数据库安全审计、业务运维安全审计和日志审计。

下表列出了信息系统中的主要审计对象与安全审计技术的对应关系：

审计对象 \ 审计技术		网络安全审计	数据库审计	业务运维审计	日志审计
终端用户	监测上网行为	√			
	监测业务操作	√（非加密）		√（加密）	
网络设备	收集网络设备日志				√
	监测网络设备访问操作	√（非加密）		√（加密）	
服务器	监测服务器网络访问操作	√（非加密）		√（加密）	
	收集服务器系统日志				√
数据库	监测数据库访问操作		√		
	数据库安全漏洞审计		√		
	收集数据库日志				√
业务应用系统	监测各种应用系统访问操作	√		√	
	收集系统日志				√

下面分别针对国内主流安全审计应用进行说明。

1. 网络安全审计

网络安全审计是目前国内应用最广泛的安全审计技术，主要应用于企事业单位的网络行为审计和内容的审计，已广泛应用于政府、

电信运营商、能源、金融等行业。

网络安全审计系统大多通过旁路镜像或分光方式，采集网络数据进行分析、识别，实时动态监测网络行为、通信内容和网络流量，全面记录网络系统中的各种会话和事件，发现和捕获各种违规行为和内容，实现对网络安全事件的跟踪和事后追查取证。

技术特点：

- 网络安全审计系统不会影响网络信息系统自身运行与性能；
- 对各种网络行为，如网站访问、邮件、远程终端访问、即时通讯、论坛、在线视频、P2P 下载、网络游戏等，提供全面的行为监控，方便事后追查取证；
- 对网站访问、邮件、文件上传下载、论坛发帖、非加密运维操作等进行内容监测。

2. 数据库安全审计

随着信息系统业务不断发展，数据库系统应用范围越来越广，如企业的账务数据、贸易记录、工程数据等均需要利用大量的数据库资源。由于数据库的作用和影响越来越大，企业数据库信息安全面临严峻挑战，近年来不断发生的企业数据库的重要敏感数据的被窃取、篡改问题，已引起企业的高度重视，成为迫切需要解决的问题。

数据库安全审计系统主要通过旁路或分光方式，对网络数据的采集、分析、识别，实时监控记录数据库各种账户（如超级管理员、临时账帐户等）的数据库操作行为，发现各种非法、违规操作，降低数据库安全风险，帮助企业保护数据库资产安全。

技术特点:

数据库安全审计不会影响数据库系统自身运行与性能；

- 支持同时审计多种数据库及跨多种数据库平台操作，覆盖主流数据库类型，ORACLE、MS SQL SERVER、SYBASE、DB2 等
- 数据库安全审计可支持对多种 SQL(Structured Query Language) 语言的审计；包括 DQL- 数据查询语言 (SELECT)、DML—数据操纵语言 (DELETE，UPDATE，INSERT)、DDL—数据定义语言 (CREATE，ALTER，DROP，DECLARE)、DCL—数据控制语言 (GRANT，REVOKE，COMMIT，ROLLBACK)；
- 支持实时审计用户对数据库系统的操作，如: 登录、注销、插入、删除、执行存储过程、用户自定义操作等，支持分析、提取 SQL 语句中绑定变量，并可完全监测还原 SQL 操作语句包括源 IP 地址、目的 IP 地址、访问时间、MAC 地址、数据库用户名、客户端类型、数据库操作类型、数据库表名、字段名等。

3. 业务运维安全审计

目前，企事业单位日趋复杂的 IT 业务系统与不同背景业务运维用户的行为给信息系统安全带来较大风险，如：多个运维人员使用同一账号维护一台设备，导致权责不清；账号繁多，管理不便；账号权限分配粒度粗，无法实现更细粒度的命令控制；缺少对加密、图形操作协议的审计手段，存在风险隐患，导致事后无法查找来源。

业务运维安全审计系统在逻辑上将运维操作终端用户和目标设备隔开，终端用户必须通过该审计系统才能访问目标设备，从而实现对运维操作的统一接入管理，对 SSH、SFTP、RDP 等加密、图形操作协议的内容审计，满足企业运维管理和风险内控需要，帮助

企业定位安全事件源头和追查取证。

技术特点:

• 建立统一的运维管理平台，集中管理运维账号和集中授权。

• 实现传统网络安全审计无法实现的对运维加密、图形操作协议的审计，如: SSH、RDP、X-WINDOW、VNC 、SFTP 等运维协议。

4. 日志审计

日志安全审计主要通过对网络设备、安全设备、应用系统、操作系统的集中日志采集、集中存储和关联分析，发现信息系统的安全事件，同时当遇到特殊安全事件和系统故障时，确保日志存在和不被篡改，帮助用户定位追查取证。

技术特点：

• 可全面地集中采集各种网络设备、安全设备、操作系统、业务系统的日志信息；

• 针对收集的日志，通过集中存储、标准化、查询、分析，可帮助发现潜在安全问题和事后追查取证，并输出合规报告。

三、信息系统安全审计发展趋势

随着国内企业信息系统风险内控制度日益完善，信息系统安全审计将呈现满足政策合规审计、企业内控管理和数据风险控制需求的特点。

政策合规审计

安全审计技术将更加紧密与“信息系统安全等级保护”、“企业信息内部控制基本规范”等政策要求相结合，依据 CC、ITIL 、COBIT 等标准，提供更符合企事业单位信息系统风险内控和政策合规管理要求的安全审计功能，如：业务运维安全审计、数据库安全审计等；同时需要输出细粒度的合规审计报告，如：符合信息系统安全等级保护要求的安全审计报告、企业信息系统风险内控审计报告等，帮助用户提升审计力度，降低人工审计工作量，有效控制信息安全风险。

基于账号的网络安全审计

网络安全审计技术将逐步与身份认证管理技术结合，实现基于账号的网络安全审计，相比传统的基于 IP、MAC 地址等用户身份的审计判定手段，将能够更加准确的定位到人，全面提升审计对象身份的可靠性。

专业的数据库安全审计

数据库已成为广大企业的数据核心资产，其重要性毋庸置疑，近年来在各行业中频繁发生企业数据库的重要敏感数据被篡改牟利、泄密事件，已经引起各方面的广泛高度重视。数据库安全审计技术作为数据库安全的重要监测手段，将越来越受到政府、金融、电信等用户重视。为了进一步提高数据库安全审计的完整性和准确性，须追根溯源，从源头抓起，需要安全厂商与数据库厂商加强技术合作，共同推动完善数据库安全审计技术。

参考书籍:

ISO/IEC15408-2:1999《信息技术安全性评估准则》

《计算机信息系统控制与审计》张金城著

实践数据业务系统安全域划分

行业技术部　程文静

摘要：本文针对中国移动制定的《中国移动数据业务系统集中化安全防护技术要求》进行了简要解读，同时，基于绿盟科技多年的研究和经验积累，提出了数据业务系统安全域划分的具体的实施流程和项目实践。

关键词：中国移动　数据业务　安全域　实施流程　项目实践

引言

中国移动在 2010 年 2 月正式发布了《中国移动数据业务系统集中化安全防护技术要求》（以下简称“技术要求”），要求明确了以省网为单位统一规划数据业务系统组网，实施安全域划分和边界整合的基本原则，并进一步提出了数据业务系统安全防护的基本要求。

绿盟科技最早在 2006 年就开始对数据业务安全域进行课题研究，并逐渐形成系统化的安全域方法论和工程指导。本文从标准解读、实施流程、项目实践等几个方面提出绿盟科技在数据业务系统的安全域划分、边界整合以及安全防护工作的理解和讨论，希望能够为数据业务安全域划分工作的开展提供参考和借鉴，促进数据业务系统安全防护水平的提高。

一、《技术要求》简要解读

（一）内容简介

《技术要求》主要从技术层面规范了以下 3 个方面内容:

- 数据业务系统安全域划分;
- 数据业务系统边界整合;
- 数据业务系统的安全防护。

《技术要求》所指数据业务系统为采用 IT 设备完成主要业务功能且和互联网存在接口的总部和各省自维护业务系统，如 WAP 网关、彩信、短信网关、彩铃系统、MISC、通用下载平台等，不包括通信网，如 CMNet、IP 专网、GPRS 等。

《技术要求》作为中国移动通信有限公司、各省公司在数据业务系统规划、开发、建设以及维护各阶段组网和实施安全防护工作的依据，支撑实现网络与信息安全工作“同步规划、同步建设、同步运行”。

（二）数据业务系统安全域划分

数据业务系统的安全域划分，它明确了根据各数据业务系统之间的威胁等级、保护等级，划分安全域的基本原则、域间互联的基本要求。

《技术要求》明确指出安全域划分的 4 条原则：业务保障原则、结构简化原则、等级保护原则、以及生命周期原则。

《技术要求》依据数据业务系统组网的基本架构提出了安全域划

分方法，数据业务系统可划分为以下 4 类主要的安全区域：核心生产区、内部互联接口区、互联网接口区和核心交换区。如下图所示。

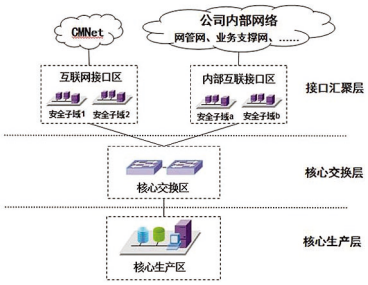


图 1 数据业务系统安全域划分示意图

需要特别指出的是数据业务系统安全域划分不设置单独用来放置终端的安全域。由于终端的风险较高，除超级终端外，其它各类终端应通过以省为单位部署的网络安全管控平台接入业务系统进行维护。

（三）数据业务系统边界整合

数据业务系统边界整合，它明确了数据业务系统边界整合的基本原则，分别阐述了具备多个传输出口和单一传输出口情况下边界整合的具体要求。

《技术要求》确定数据业务系统边界整合范围的基本原则是：应至少以相同物理位置的数据业务系统为基本单位设置集中防护节点，对节点内系统进行整体安全域划分和边界整合。在具备传输条件的情况下，可以进一步整合不同集中防护节点的互联网出口。

《技术要求》确定集中防护节点内部的边界整合的基本方法是将各系统的相同类型安全域整合形成大的安全域，集中设置和防护互联网出口和内部互联出口。在整合后的内部互联接口区内设置“内部安全服务区”子域，集中部署本安全域内的安全防护设备。

同时，《技术要求》确定在具备传输条件的前提下，将现有集中防护节点的互联网出口整合至互备的一个或几个接口，实现多个集中防护节点共享一个互联网传输出口。

（四）数据业务系统的安全防护

数据业务系统的安全保护，它在安全域划分和边界整合的基础上，进一步明确了域间互联的安全要求以及各类基础安全技术防护手段的部署原则。

《技术要求》明确指出数据业务系统安全防护的 3 项原则：集中防护、分等级防护和纵深防护。

《技术要求》明确提出数据业务系统 6 类安全域边界互联防护要求：数据业务系统之间互联、数据业务系统与支撑系统互联、数据业务系统与互联网互联、数据业务系统与第三方系统互联、维护终端和数据业务系统互联、数据业务系统内部不同安全区域之间互联。

《技术要求》明确指出在在安全域划分和边界整合基础上，数据业务系统自身在业务流程（逻辑）、软件代码、功能和配置等 4 个方面应满足相应的安全要求；并进行防火墙、入侵检测、防病毒、异常流量检测和过滤、网络安全管控平台等 5 类通用的基础安全技术防护手段的部署。

二、安全域划分的实施流程

绿盟科技数据业务系统安全域划分的实施过程主要包括：安全现状调研、安全域划分及防护方案设计、以及安全域建设与实施，这里介绍的是主要流程，另外比如实施前的工具准备、人员准备等以及实施前的双方对实施范围的确认等一般流程，都没有纳入到其中。

（一）安全现状调研

1、网络调研

网络调研的目的：识别网络系统的物理

环境、网络拓扑结构和硬件设备的部署情况，在此基础上明确信息系统的外部和内部边界，即确定网络优化的对象和范围。

需要提醒的是，在网络调研中，IP 地址分配的调研非常重要，应该是不可少的。

网络调研的输出：《系统网络拓扑图》。

2、资产调查

资产调查的目的：识别信息系统内部所有类别的网络设备、主机服务器及操作系统、应用系统、数据、各类终端等具体资产。

在资产调研中，要包括对安全设备的调研，除了防火墙 IDS，还有补丁分发服务器、日志收集、病毒库同步等内容。

资产调查的输出：《系统资产调查表》。

3、业务系统调研

业务系统调研的目的：识别信息系统的业务种类和特性，即了解具体信息系统处理的有多少种业务应用，这些业务应用各自的业务内容、业务流程、业务用户和管理用户等，从中明确网络系统的业务特性，有助于根据业务特征和安全需求制定安全策略。

业务调研的作用实际上是帮助我们了解业务系统的网络架构，确定每个 IT 网元的具体工作任务。

业务系统调研的输出：《业务系统调研报告》。

（二）安全域划分及防护方案设计

1、安全域划分

安全域划分的目的：根据网络拓扑及业务系统现状，在信息系统内部划分安全域，并对安全域及其形成边界进行定义。

它是依据《技术要求》对具体数据业务系统进行安全域的划分，确定核心生产区、内部互联接口区、互联网接口区和核心交换区，以及可能的安全子域，并对安全域、安全子域及其它们形成的边界进行定义。

安全域划分的输出：《业务系统安全域划分方案》。

2、安全需求确认

安全需求确认的目的：依据安全域划分方案，明确业务系统安全改造的安全需求。

安全需求确认的输出：《业务系统安全需求分析》。

3、安全改造方案设计

安全改造方案设计的目的：依据业务系统安全需求分析，明确信息系统的安全改造方案，包括边界整合方案、系统自身安全、安全产品部署、安全监控等安全技术性方案。

安全需求分析，应该不是单个业务系统的安全需求，而是要通盘考虑整个省公司的安全方向以及现有安全策略的完善。

安全改造方案设计的输出：《业务系统安全改造方案》。

（三）安全域建设与实施

1、网络安全改造

网络安全改造的目的：根据确定的《业务系统安全改造方案》实施网络改造，包括边界整合以及边界访问策略优化，保证系统清晰的安全域划分结构。

网络安全改造的输出：《业务系统网络安全改造实施报告》。

2、安全产品采购与实施

安全产品采购与实施的目的：根据确定的《业务系统安全改造方案》

采购安全产品并进行根据预期部署方案进行实施，确保满足安全域防护需求。

安全产品采购与实施的输出：《业务系统安全产品实施报告》。

3、安全服务实施

安全服务实施的目的：根据确定的《业务系统安全改造方案》采购安全加固服务并进行实施，确保满足安全域防护需求。

安全服务实施的目的输出：《业务系统安全服务实施报告》。

三、安全域方案的设计实践

按照上一章描述的实施流程，上述的 3 个阶段是一个相对完整的安全域划分项目的过程，但具体到某个项目中，通常用户更加关注的是第二个阶段的内容，即“安全域划分及防护方案设计”是如何实现的。对于第三个阶段的内容，由于改造的涉及面很广，周期会比较长，用户方通常会需要一个中期规划来实现，所以用户通常要求咨询方在第二个阶段的方案设计中提出一些建设性的建议。

针对这个情况，在中国移动某省公司的安全域项目中，依据用户需求——“针对数据业务系统网络现状，制定合适的数据业务系统安全域整合方案，在安全域整合的基础上实现集中安全防护、共享相关安全产品，并为后期改造实施提出可行的建议”，本节将主要介绍绿盟科技在此项目中的设计实践。

绿盟科技在经过安全现状调研阶段之后，了解到的基本信息有：某省公司的数据业务系统全部集中在省公司，范围包括：《技术要求》中定义的全部数据业务系统，以及增值业务系统，这些业务系统分布在 3 个不同地点的数据业务机房，某类数据业务系统分布在 3 个不同机房但具备传输条件。

依据了解到的情况，绿盟科技在具体设计实践中，是按照各业务系统分别进行安全域划分、对多个业务系统安全域进行整合、以局点为单位进行安全域的整合这样的一个顺序进行的方案设计。

（一）各业务系统安全域划分方案

梳理各数据业务系统业务数据流以及管理数据流，按照《技术要求》中的要求，分别对各数据业务系统进行安全域划分和边界识别，并在此基础上实现各项安全防护要求，包括添加安全防护设备和调整安全防护策略。

（二）多业务系统安全域整合方案

在对各数据业务系统完成安全域划分和边界识别的基础上，结合中国移动某省公司网络现状，对多个数据业务系统进行安全域整合，以实现集中防护，共享相关安全防护设备。

这里的多个数据业务系统主要是两类：一类是已具备传输条件的短信系统为核心的相关数据业务系统；一类是已建成的独立组网和集中组网这两种模式的 30 多个增值业务系统。

（三）以局点为单位安全域整合方案

在多业务系统安全域边界整合的基础上，分别对 3 个局点进行多数据业务系统 CMNET 和 MDCN 网络边界整合，按照《技术要求》将部署相关安全产品，以实现集中监控、集中防护、统一安全运维接口等。

参考文献

1.《中国移动数据业务系统集中化安全防护技术要求》，2010.2

2.《电信网和互联网安全防护管理指南》（YD/T 1728-2008）

3.《中国移动安全域管理办法》（网通 [2008] 272 号）

电信基础网络安全探析

行业技术部　刘炅

摘要：本文通过对电信基础网络发展的介绍，以及对移动互联网的架构和安全威胁的分析，来揭示电信基础网络的安全问题。对于电信基础网络的 DDoS 攻击问题，文章从控制源头、有效检测和攻击防护三个技术层面提出了解决的方法，同时对于 DNS 的安全提出了安全防护体系。

关键词：电信基础网络　移动互联网　僵尸网络　流量分析　流量清洗　DNS

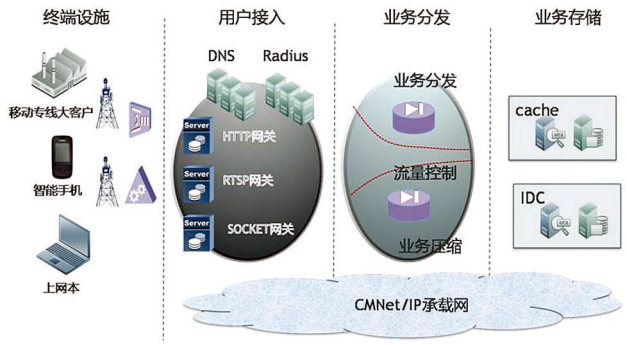
电信的基础网络即承载电信业务的核心网络和相关的支撑网络，包括传输网、交换网、信令网、移动网、互联网和智能网等一系列网络系统。在工信部等级保护规范中，电信基础网络被划分为十一个专业的电信网络系统。本文所介绍的基础网络安全，主要是指以互联网和 IP 承载网为主的 IP 化网络系统的安全问题。随着 NGN 软交换的应用，核心网向 IMS 的演进，都说明 IP 化是电信网发展的趋势，这也使我们越来越关注 IP 网络的安全问题。电信基础网络的安全问题，无论从其对社会影响的广度和深度、还是对运营商企业本身的影响而言，无疑都非常巨大，这也给运营商网络运维人员和网络安全厂商以更大的责任。

在 IP 化的网络中我们往往更关心互联网的安全。互联网是一张公开网络，上面承载各种各样丰富的应用，更容易受到各方面的攻击；同时互联网也和专业网络有很多的接口，如果互联网出现安全问题，也会使专业网络受到影响。比如，中国移动的 IP 承载网是承载移动语音业务的主要平台，在设计之初就考虑了如何把互联网业务在 IP 承载网的一个 MPLS VPN 中承载，而直到现在互联网业务也没有割接到 IP 承载网上，其主要原因就是无法量化判断互联网会对语音网络产生多大的影响。中国电信的 IPTV 网络也面临同样的问题，IPTV 网络几乎都是专网，和城域网都是分别部署的，这也是为了保证媒体网络的质量。

虽然互联网上安全威胁比较多，但其网络应用却发展迅猛，互联网的形态已经不仅仅是传统的有线宽带网，不仅仅是 ADSL 的拨号接入或小区宽带的接入，而随着无线城市的发展，3G 业务的开通而产生了新的接入方式和新型的业务形态。“移动互联网”的概念应运而生，它不是移动网和互联网简单的叠加，而是一种新型的业务模式的产生。它的发展有三个特点：首先是终端在趋向于融合。特别是随着具有操作系统的智能手机的问世，手机跟互联网越来越趋向于融合。今后的智能手机在互联网访问方面会越来越便捷、应用也会越来越丰富；第二是网络 IP 化。由于整个移动通信网络逐步向 IP 不断演进，这跟现有的互联网结构也越来越呈现出一种融合趋势。如上面我们提到的核心网、交换网的 IP 化，以及接入基站的 IP 化，使得网络部署、业务的更新越来越灵活快捷；第三是内容和应用趋向于一致。目前互联网的大部分应用在手机上都能得以实现，同时手机又进一步促进了互联网新业务形式的诞生。比如手机支付，就

是依托移动互联网的新型业务形态，它的产生也会改变我们的生活方式。根据“移动互联网”发展的三个特点，使我们从终端、到承载网络、再到业务三个层面上审视安全问题，以保证对互联网安全研究的领先性。

“移动互联网”网络基础架构如下图所示:



图中移动互联网架构包括了终端设施、用户接入、业务分发和业务存储四个部分。

终端设施包括了智能手机、上网本和基站等终端设备和接入设备，其中手机终端安全是目前最受关注的安全领域之一。

用户接入部分由核心网的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。这一区域的解析和验证设备是安全防护的重点，另外如 WAP 网关、RSTP 网关等也是最容易受到安全威胁的。

业务分发部分是承载网络，我们重点考虑流量分析和 DDoS 流量攻击的安全问题，它起到对流量的分发和控制作用。

业务存储部分包括了 IDC 业务和数据的存储业务，其中一部分业务是用户托管业务，一部分业务是运营商自有业务。在这里我们更关注业务的可用性和信息的保密性。

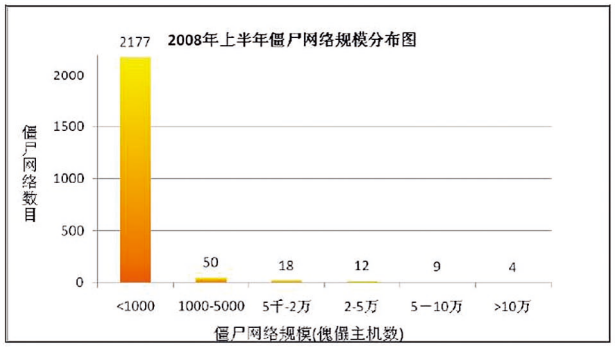
根据上文的分析，我们了解了基础网络的架构和面临的严重威胁，这表明基础互联网的安全威胁不容乐观，互联网世界总不是太平的。由于基础网络的安全直接影响到国家安全，美国等发达国家也把基础网络安全提到了很高的高度。美国总统奥巴马公布的网络安全评估报告，认为来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。美国近年来日益重视网络安全，把确保网络安全列为国家安全战略最重要的组成部分之一，采取了一系列旨在加强网络基础设施保密安全方面的政策措施。尽管如此，奥巴马公布的网络安全报告依然认为，美国主要建立在互联网基础上的数字基础设施目前并不安全，现状“不可接受”。

美国是世界上第一个引入网络战概念的国家，也是第一个将其应用于战争的国家。美国还建立和发展了新的军种——网军。网络战争已经不是一个耸人听闻的名词，而是真正出现在了我们的现实时生活中。俄罗斯近年来，由于国家利益和政治信仰方面的问题已经对其周边国家发起了多起网络攻击事件，包括对爱沙尼亚、格鲁吉亚、吉尔吉斯坦等国发起的 DDoS 攻击，都导致了这些国家基于互联网的政府、金融等网络业务中断。网络战争会对一个国家的基础网络的防护能力提出严峻的考验。

根据基础网络的安全威胁，如何进行防护，我们从控制源头、有效检测和攻击防护三个层面进行分析。

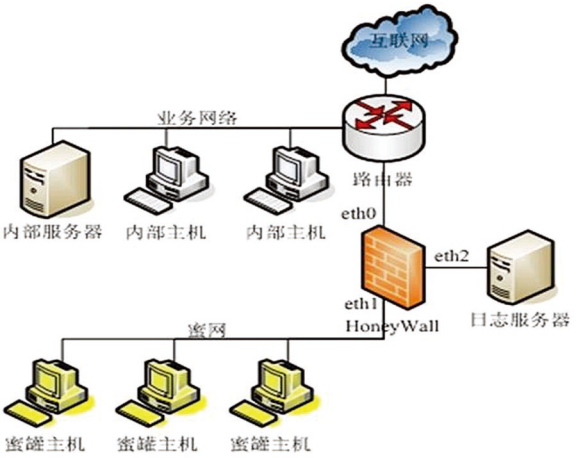
控制源头

僵尸网络是 DDoS 攻击的主要源头之一，它是被控制的大量主机的集合。如何能发现和控制僵尸网络，是国家监管部门和运营商的一个重要职责。下图是 08 年上半年僵尸网络规模分布图：



从僵尸网络的规模来看，虽然目前绝大多数的主机数目在 1000 台以内，但僵尸网络的专业性更强。它能够更有针对性地进行 DDoS 攻击、传播垃圾邮件等，所以危害性更强。近几年流行的僵尸程序如 Storm、Waledec、Conficker 等，他们好像还没引爆的定时炸弹，随时都有可能进行定向爆炸。

如何检测和控制僵尸网络，目前通用的是蜜网技术。蜜网实质上是一种以高交互型的蜜罐为核心的整合多种附属功能的网络攻击诱骗技术。

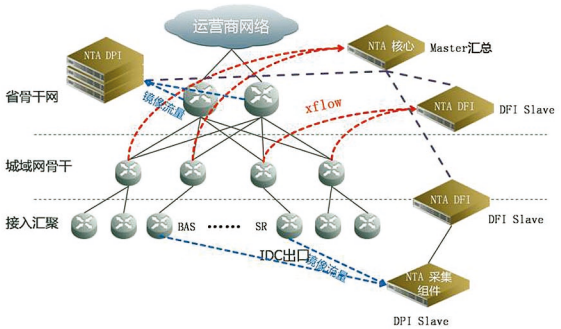


蜜网可以监控、诱捕、定位网络中的僵尸主机，部署在运营商网络中可以发现本网络中现存的僵尸主机数目，起到预警和控制的作用。目前在许多运营商网络和电信监管部门都部署了绿盟科技的蜜网设备，对监测全国的僵尸网络起到了极其重要的作用。

有效检测

对于基础网络的流量监测也是基础网络安全重要的组成部分。目前流量检测技术有两个流派：DPI 和 DFI。DPI 即深度数据包检测，其特点是捕获数据包，并对数据包进行 3-7 层的分析。由于运营商网络带宽都比较大，DPI 设备的部署是通过分光或者串联部署在骨干网或者城域网的出口处。应用层的数据包检测，可以了解到传送数据的每一个细节，对于应用层的攻击、病毒的检测、内容的监控都有非常好的效果。DFI 即深度流检测，利用的是 Netflow 技术，对数据的流量进行统计分析。Netflow 技术是路由交换的一个标准

协议，它通过在路由器上进行采样，从而对流经路由器的流量进行统计分析，对于流量流向的分析和异常流量的检测非常准确。在运营商网络里采用这种技术，大大降低了对分析处理设备的性能要求，也使设备的部署简单方便。绿盟科技在流量分析技术中，没有简单使用某一种检测技术，而是把这两种技术有机地结合在一起，通过分级分层的部署，以及流量宏观统计及微观解析的方法，把流量中的安全问题分析处理。下图即是 DPI+DFI 统一部署和分析的示意图。

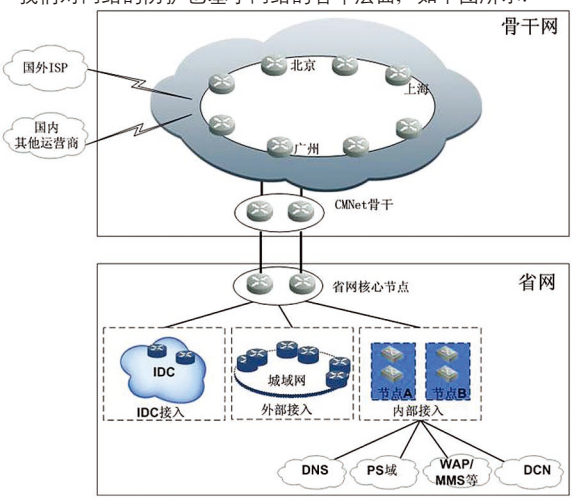


攻击防护

当 DDoS 攻击发生时，如何能够有效地进行防护，这是运营商基础网络需要解决的问题。大流量的 DDoS 如果发生，被攻击的用户通常是无力防护的。租用的带宽已经被堵塞，采用什么样的安全设备和安全技术都无济于事。用户只能求助于运营商，而运营商在基础网络里的防护攻击的手段和能力就显得异常重要。

目前我们了解到的 DDoS 攻击的目标和对象，遍布于运营商提供的所有服务。有对 IDC 托管主机的攻击、对于宽带接入用户（如网吧）的攻击、对于基础网络设施 DNS 的攻击、对于网上营业厅的攻击、对于移动数据业务的攻击等等。

我们对网络的防护也基于网络的各个层面，如下图所示：



骨干网层面：通常有和国际互联网的互联节点，也有国内运营商间的互联节点，同时骨干网也连接着全国各省级节点，所以防护尤为重要。从骨干网层面考虑，希望能有一个“干净”的骨干网络，同时流量的防护能够全网整体协作。骨干网防护能把国际上的“网络战争”，运营商间的跨网攻击，和省际间的相互攻击都进行屏蔽。我们的部署原则和防护策略就是就源清洗和粗粒度大流量清洗。中国电信在骨干网层面率先进行了尝试，在全国十三个节点进行了部署，初步形成了统一的骨干网防护体系。中国移动也在积极筹备骨干网的防护，特别是对国际节点的防护，和 DPI 检测产品结合，给出了全新的防护思路。

省网 / 城域网层面：这个层面主要是对 IDC 和城域网专线用户的保护，它主要保护着重要的用户，所以防护的质量直接关系到用户的体验和满意度。在城域网我们还可以开展增值的业务，把流量清洗作为一项基础的安全服务提供给我们的用户。很多省级运营商都在 IDC 和城域网提供了此类的服务，给企业带来了很好的收益。

应用层面：对于运营商提供的许多基础业务都是暴露在互联网上的，比如上面提到的网厅门户网站、WAP 网关、彩信业务，甚至 DNS 解析服务，都对网络的稳定运行有更高的要求。分不同的业务单独进行部署，单独进行访问策略的配置，在这里我们更强调精细化的流量分析检测和更精确的防护策略。

基于上文所述三个层面的防护策略，我们的基础网络能够更加强健，犹如身披多层铠甲的勇士，足以抵御各种各样的威胁。

对于基础网络，DNS 是我们不能不提的一个重点领域。09 年发生的 “519” 事件，使得国家电信监管部门对于 DNS 的防护空前重视。2009 年，工信部安全大检查中把 DNS 的检查定为重要的检查项目，同时发布了 DNS 的安全防护规范，作为工信部等级保护规范文件中的一项重要规范。

2010 年初，工信部 14 号文《关于开展通信网络单元安全防护定级备案调整工作的通知》，把互联网中的域名解析体系统的安全等级最高设置为 4 级，这也是电信网络中惟一的 4 级系统。

2010 年 2 月，工信部对于 DNS 的安全专门发布了《关于加强互联网域名系统安全保障工作的通知》即 53 号文，强调 DNS 的安全性，并在安全技术、定级保障、监控日志、应急响应等方面做了具体的要求，可见 DNS 对于电信基础网络的重要性。

如上图所示，绿盟科技针对于 DNS 安全，建立一整套安全建设体系。在网络方面，从物理安全、网络安全、主机安全、和应用级数据安全角度进行分析；在运维保障方面，从安全评估、安全防护、安全运维角度进行分析，这样就形成一个矩阵式的防护体系。从技术到管理、从产品到服务、从预防到应急，从物理安全到应用安全形成一系列的防护方法和措施，使得这个体系不仅能够真正解决 DNS 的安全问题，也完全符合工信部刚刚下发的 DNS 安全建设要求，能够帮助运营商把 DNS 的安全工作切实落地。

电信基础网络的安全，关系到我们每一个人的日常生活，关系到运营商企业的经济命脉，更关系到国家的信息化安全战略，作为一个专业的安全公司，绿盟科技有责任来为基础网络的安全奉献出自己的力量。

一种简化网站安全管理工作的手段

产品管理中心　李晨

摘要：目前，由 Web 应用而引发的黑客攻击热潮极大地困扰着网站提供者，给企业形象、信息网络甚至核心业务造成严重的破坏。不同的站点面临着共同的威胁，但是站点自身的资源状况却千差万别，如何在最小的资源投入下，采取尽可能完善的安全手段，则是中小企业站点管理员所需要重点思考的问题。“绿盟网站安全监测服务”通过不间断的远程监测，为客户网站提供安全性检查、安全事件监测、实时响应和安全趋势分析服务，使其成为用户网站安全体系的最好补充。

关键词：Web 应用安全　漏洞扫描　实时监测　托管式安全服务

随着 Web 应用的日益广泛及其蕴藏价值的不断提升，黑客的攻击热潮也不断上涨，网站内容被篡改、页面被植入木马、DDoS 攻击造成业务中断、网站机密信息被窃取等安全事件时有发生，这些都极大地困扰着网站提供者，给企业形象、信息网络甚至核心业务造成严重的破坏。

据 CNCERT/CC 的统计数据显示，2009 年全年，中国大陆有 4.2 万个网站被黑客篡改 [1]。在微软 2009 年 7 月至 12 月的安全统计报告中，以 .cn（中国）结尾的挂马站点比例将近 1%，远远超过由 Bing 跟踪的平均 0.24% 的网站包含一个恶意页面的比例 [2]。

对于一些大型的门户网站、电子商务网站等，自身的业务就依靠于网站进行运营，因此大多数大型站点都建立了严格的安全管理与保障体系。可是对于地市级政府、中小金融机构、中小企业以及一些教育机构的互联网站点，由于人力、物力、财力的限制，难以建立完善的网站安全保护体系，安全保障力度有限，导致频频发生站点被篡改、被挂马等安全事件，严重地损害了相关机构、企业的对外形象，甚至受到了上级监管部门的问责。在资源有限的情况下，如何提高网站的整体安全水平，提升安全效能，是这些站点安全管理员的一个重大挑战。

若能够主动地发现网站的风险漏洞，实时监测网站的安全状况，发现问题后及时采取修补措施，则可以降低影响和减少损失。绿盟科技基于多年对 Web 应用安全的研究与积累，针对目前中小机构、企业缺乏有效的网站安全监测手段，推出“网站安全程监测服务”。该项服务通过不间断的远程监测，为客户网站提供安全检查、安全事件监测、实时响应和安全趋势分析服务，在最小的资源投入下，获取最高的安全效能。

“绿盟网站安全监测服务”是一款托管式服务。该项服务基于绿盟科技“云安全”平台，由绿盟安全监测专家团队远程为客户提供。当监测到用户网站遇到风险状况后，绿盟安全专家会在第一时间确认并通知用户，同时提供专业的解决方案建议。绿盟安全监测团队会定期为客户出具周期性的网站安全监测报告，让用户掌握网站

的风险状况及安全趋势。整个监测过程对用户透明，用户无需安装任何硬件或软件，无需改变目前的网络部署状况，就能将网站管理人员从繁重的日常安全维护工作中解放出来，降低投入和管理成本，并获得对行业和政府法规的遵从情况。

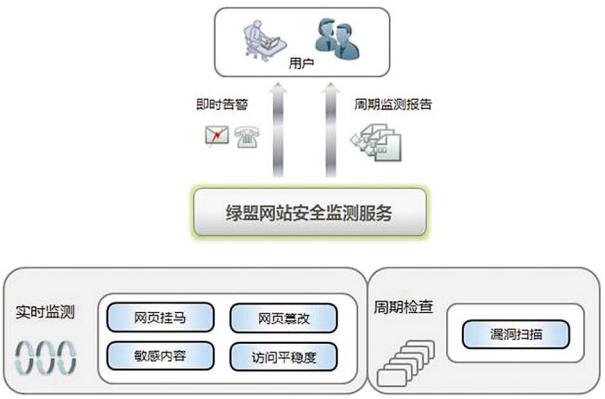


图 1　绿盟网站安全监测服务内容

该服务产品主要包括以下几方面的内容:

远程网站漏洞扫描

网站的风险漏洞是站点被攻击的根源，通过定期对被服务站点进行远程漏洞扫描服务，用户无需采购任何 Web 应用扫描产品，即可获得网站的漏洞情况，以及修补建议。而站点管理员只需及时依据修补建议并进行漏洞修复，就可以为打造一个坚固站点打好基础。

远程网页挂马监测

永远没有 100% 的安全。由于 0day 漏洞的存在，以及一些应用配置的疏忽，网站永远存在被挂马的风险，这就要求能够实时的对站点进行监测，一旦发现安全问题能第一时间知晓，并进行处理。绿盟科技“云安全”平台不间断从目标站点主动爬取页面，采用业内领先的智能木马检测技术，可高效、准确识别网站页面中的恶意代码，使网站管理员能够第一时间得知自己网站的安全状态，避免由于网站被挂马给访问者带来的安全隐患。

网页篡改监测

通过不间断从目标站点主动获取页面，为监测页面形成基准，由后台系统自动的对比每次页面的恶意变化情况，同时配合监测人员的分析。一旦目标站点发生页面被篡改情况，第一时间通知用户，避免页面篡改给站点造成声誉影响。

网页敏感内容监测

网站管理员所关注的安全角度不仅仅是风险漏洞、网页挂马和页面篡改。对于站点中的论坛、blog 中的低俗内容、敏感词汇也是站点管理员的一大烦心事。“云安全”监测平台在实时获取目标站点的页面后，后台系统自动地对页面内容解析、语义分析，监测页面内容是否含有用户所关注的敏感内容及信息泄露的情况，从而降低法律风险。

网站平稳度检测

“绿盟网站安全监测服务”还为站点管理员设计了一项贴心功能。

即模拟访问者对服务站点的页面访问效率进行动态监视，跟踪访问平稳度的动态变化情况，并根据访问效率突变的严重程度及时发出报警信号。

与传统的安全评估、值守服务相比，绿盟科技基于“云安全”平台的网站安全监测服务具有更为鲜明的特点:

一是监测能力强，可提供不间断的风险监测能力。众所周知，网站挂马、页面篡改都是实时性很强的安全事件，而不定期的评估检查并不能帮助用户实时发现这些安全事件。而采用云平台，能够为客户提供7×24小时不间断的风险监测能力，及时发现风险并通知用户，降低或避免用户损失。

二是托管式安全服务。由绿盟科技专家团队协助用户解决一切安全问题，就如同一个私人的网站安全管家。通过可靠的、免操作式交付模型提供出色的网站安全监测服务，用户无需过多投入管理精力。实时监测、预警通告、分析报告等，每一步过程都由值得信赖的安全专家来帮助用户完成。

三是透明化。使用此托管服务直接让绿盟科技安全专家发现并解决问题，无需改变现有网络结构和管理体系，服务的部署快捷方便，让用户运维轻松自在。

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

参考文献:

【1】2009 年中国互联网网络安全报告，CNCERT/CC，2009

【2】Microsoft_Security_Intelligence_Report_volume_8，Microsoft ，2009

初探ICT供应链完整性

首席战略官　赵粮

摘要：本文简要总结回顾了信息通信技术（ICT）供应链完整性的研究背景，分析了围绕着 ICT 供应链完整性的相关概念，并对后续的研究方向和方法进行了展望。

关键词：ICT　供应链　完整性　安全

一、关于 ICT 供应链

1、什么是供应链安全？

供应链安全并不是一个新词汇，在业界媒体和学术期刊中已有相当的覆盖。随着经济全球化的逐渐深入，供应链的长度和复杂度、地理分布都大幅增长。在货物生产过程和运输过程中造成的盗窃、丢失、伪造、损坏、以及恐怖袭击等带来的损失对商业和经济的影响越来越大 [CTPAT]。在此背景下，政府权威机构和业界发起了一系列的安全增强活动。例如，由美国国土安全部海关与边境保护局（CBP）推动，与进口商、物流业及制造厂商合作的“海关 - 商贸反恐怖联盟”C-TPAT（Customs-Trade Partnership Against Terrorism）成为新时代供应链安全管理的一个具有代表性的项目。该项目是在“9·11”事件发生后所倡议成立的一个自愿性计划，于 2002 年 4 月 16 日正式施行。 CBP 希望通过此项目能与相关业界合作建立供应链安全管理系统，以确保供应链从起点到终点的运输安全，安全讯息及货物状况的流通，从而阻止恐怖分子的渗入 [DHS]。

2、ICT 的供应链有什么不同

相对于 IT 和电信来说，信息通信技术（ICT）是个相对较新的词，虽然关于其定义，也有一些争论，读者可以参见维基百科，也可自行使用百度或 Google 搜索相关结果。

在转型的时代主题下，电信运营商也开始频频使用 ICT 来概括电信业务的新边界。新的用法语义上全然不同，最先使用 ICT 的电信公司是英国电信。在英国电信网站上有一段描述性的解释：“ICT- Information Communication Technology, The ‘C’ now added to the traditional ‘IT’ reflects the worldwide convergence of computing and telecommunications. ICT has made possible instant exchange of information, regardless of distance.”大意是“C”加入到“IT”中反映全世界计算和电信的融合，ICT 促成了超越空间的快速信息交换。从字面意义上看，反映的是 IT 服务和电信服务之间边界消失过程中扩张和衍生的产物。

相对于传统领域的供应链，ICT 系统通常是采购 + 开发 + 集成模式，其最终用户感知到的安全很大程度上取决于采购、开发和集成等这些中间环节，涉及到更多的外包方、集成商、以及其它第三方等，这些供应商的安全素养、流程和产品质量的重要性愈发地凸显出来。

简要来说，ICT 的供应链包括:

- 使用的设备通常包括硬件、软件等众多组件;
- 项目涉及到全球很多地区的供应商、生产厂、集成商、运输服务商等;
- ICT 业界主要依靠采购成熟的商业组件和设备，对供应链的依赖性更强;
- 设备之间有很多通信功能等关联关系;
- 设备的功能和质量很难被完全的测试、测量和直观的展示出来;
- 等等。

这些独特性给 ICT 的供应链带来了很多新的威胁挑战。如图 1 所示，从软件工程过程中出现的软件缺陷，到供应商内部的恶意人员，到可能的商业间谍甚至国家网络战等各种各样的威胁方，针对目标的供应链的攻击成为攻击其 ICT 系统的一个重要路径。

这些新的威胁挑战促成了在传统供应链安全之外对 ICT 供应链的完整性的重视和投入。

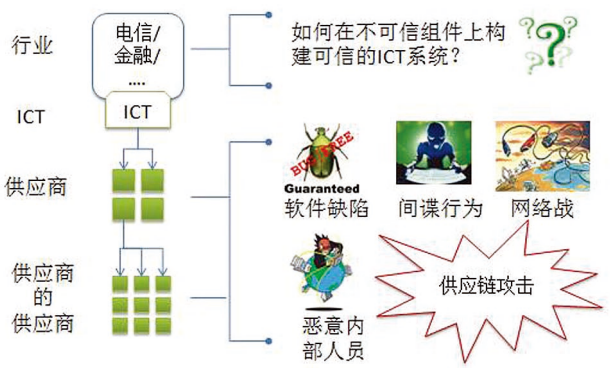


图 1 ICT 供应链面临的安全威胁

二、关于安全和完整性

这个标题看似有些多余。机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）是信息安全的三个重要属性，如图 2 所示的 CIA 铁三角是信息安全标准内容。在有些场合下，真实性（Authenticity）、不可否认（Non-Reputation）、可纠责性（Accountability）、可靠性（Reliability）等也会成为信息安全的属性[ISO27000]。

图 2 机密性、完整性和可用性是信息安全的三个属性

但是，值得我们注意的是，安全和完整性之间的结构关系在不同的领域并不总是如此。例如，保障（Assurance）、可靠性、质量等概念在有些场合成为比“安全”更高的概念，安全成为其概念下的一个属性。ENISA 在其名为“当前和未来网络技术研究的优先级”报告

中较为详细地阐述了 ICT 供应链完整性领域的研究状况，报告中借鉴了 SAFECode 的软件保障概念模型 [SAFECode]，如图 3 所示。

图 3 SAFECode 关于软件保障、完整性、真实性和安全性的概念模型

其中，安全性、完整性、真实性成为属于软件保障概念下并列的属性，共同定义了总体的软件保障概念。我们来看看该模型中如何定义这几个概念。

安全：安全威胁在软件的设计、开发和测试中被解决。这就要求同时关注质量（例如不存在缓冲区溢出漏洞）和功能（例如数据库中的护照号码必须加密）。

完整性：完整性是指分包、创建和交付软件的流程中包含增强关于软件按照供应商意图运行的信心的控制措施。

这个完整性定义中的关键信息点是“软件按照供应商意图的方式运行”。与此相对照，在信息安全的概念范畴中，完整性的定义通常是

- 完整性是指保护资产的准确性和完备性 [ISO27000];
- 完整性是指数据不会被非授权的改变 [Wiki]。

从上述不同的定义中可以看出，在供应链完整性中的定义是一个范围非常大的概念，偏重于“动态开发过程”和“供应的流动环节”，强调客观上的功能和运行方式满足商业目标。而信息安全的“完整性”则强调“非授权”对“资产”带来的“改变”。相对来说，“资产”是已经拥有的，其在描述未来的、开发中的软硬件产品的“功能”和“运行方式”时显得有些力不从心。

从这个对照分析上，我们看到了在 ICT 供应链这个领域中“完整性”概念的内涵和必要性。

三、面临的挑战和对策

从前述背景的讨论中我们看到，全球化、大量的离岸外包以及 ICT 技术的特殊性带来了 ICT 供应链的特殊性。这些特殊性要求我们研究开发针对性的技术和方案来解决其面临的各种各样的挑战。这些挑战体现在以下几方面 [ENISA]:

- 全球化分布的供应链体系在人员、流程和技术等各个方面巨大的复杂度;
- 业界在 ICT 供应链完整性方面缺少通用的指导原则;
- 缺少测量 ICT 系统的信心水平、验证其完整性的工具、流程和控制措施;
- 最终用户用以验证 ICT 产品服务的方法论和技术不够有效，缺少评估方法和工具;

• 缺少广泛可用的工具、技术和流程来检测或者消灭 ICT 系统中的伪造和篡改;

• 缺少协同一致的方法能够从采购一直到运行使用所有环节中保证 ICT 产品的完整性;

• 缺少通用的商业模式来推动跨 ICT 各个细分领域完整性要求的“和谐化”。

在上述挑战之外，我们还必须意识到各个不同地区、不同行业对于 ICT 供应链完整性的要求可能会不同，不同大小规模的企业组织对完整性的要求也有所不同。解决上述挑战，需要大量的国际间、跨行业的协作沟通和开发，需要业界和学术界的积极投入，寻找切实可行、能够广为接受的方案途径。今年 3 月份，东西方研究所 EWI 在达拉斯举办的第一届国际网络安全峰会对 ICT 供应链完整性进行了非常有益的探索 [Sbin]，这些探索包括:

• 定义不同等级的保障和认证要求（Assurance Profile），以适应不同行业和规模的 ICT 系统;

• 着手建立对各种 ICT 组件和设备的认证机制。通用准则 CC 是一个不错的参考体系，但是需要进一步的开发和调优，来适应新时代 ICT 系统的环境;

• 开发较低成本、切实可行的 ICT 组件和设备的测试工具和流程。能够从需求设计、开发环境、代码、二进制代码、逻辑功能等各种层次角度来进行测试和验证;

• 开发能够通过功能分离（Segregation Of Duties）来实现整体 ICT 系统的“容错”能力的标准架构;

• 等等。

4 结束语

本文讨论了信息通信技术（ICT）供应链面临的威胁和挑战，分析了在供应链语境中“完整性”的含义及其必要性，并简要总结推荐了业界、学术界、政府机构的需要共同努力的方向。可以预计，其中每一项任务都将需要付出长期的努力，需要业界和学术界、政府机构等投入大量的资源才能完成，但是无疑其意义也是巨大的。

参考文献

[CTPAT] http://www.aiou.edu/banews/062005/01062005.doc

[DHS] Strategy To Enhance International Supply Chain Security, http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf

[ENISA] Priorities for Research on Current and Emerging Network Technologies, http://www.enisa.europa.eu/act/it/library/deliverables/procent/at_download/fullReport

[ISO27000] ISO/IEC 27000

[SAFECode] The Software Supply Chain Integrity Framework, http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf

[Sbin] http://sbin.cn/blog/2010/05/06/ewi-worldwide-cybersecurity-summit-supplier-chain-security/

[Wiki] http://en.wikipedia.org/wiki/Information_security

从攻击规避检测技术看IPS的安全有效性

开发中心　刘水生　产品管理中心　陈星霖

摘要：攻击规避技术是众多蓄意隐性攻击中应用范围最广、最有效的一类技术。当攻击者发现被攻击目标正受到 IPS 等产品保护时，攻击者往往会根据攻击目标的协议特性或漏洞，对攻击方式或攻击内容进行精心调整，进而逃避 IPS 等产品的检测。本文主要从“安全有效性”角度，以攻击规避流量检测为例，描述 IPS 产品所面临的挑战，以及相应的解决思路。

关键词：TCP/IP 协议规避　RPC 协议规避　URL 混淆　FTP 规避攻击

引言

根据业内知名市场咨询机构 IDC 的最新报告显示，国内网络入侵防护市场已形成了群雄割据的局面，仅进入 IDC 市场报告统计名录的企业就有 14 家之多。众说纷纭的入侵防护产品技术让人难辨良莠，孰优孰劣，市场需要一把可以适度评价的标尺。

“安全、高速、易于部署”，这是国际著名安全产品测评机构——NSS Labs 在评价一款 IPS 产品时，认为其应该具备的三种能力。也就是说，NSS Labs 的专家们在建议企业客户选择 IPS 时，虽然要充分考虑产品的性能、部署能力及 TCO（Total Cost of Ownership，总体拥有成本）等各项指标，但仍将安全有效性指标排在首位。

本文主要从“安全有效性”角度，以攻击规避流量检测为例，描述 IPS 产品所面临的挑战，以及相应的解决思路。

一、从攻击规避检测技术看 IPS 的安全有效性

众所周知，为了提高产品的攻击检测效率，IPS 一般采用特征检测、异常检测和关联分析等多种技术手段，以降低产品的误报率和漏报率。特征检测技术主要用于识别和定位各类已知威胁，异常检测方法则通常集成针对协议、应用和统计数据的异常检测技术，能够保护企业信息系统免受未知攻击的侵害，包括新的蠕虫、蓄意的隐性攻击、新环境下的攻击变种，以及 DDoS 攻击流量。

攻击规避技术是众多蓄意隐性攻击中应用范围最广、最有效的一类技术。当攻击者发现被攻击目标正受到 IPS 等产品保护时，攻击者往往会根据攻击目标的协议特性或漏洞，对攻击方式或攻击内容进行精心调整，进而逃避 IPS 等产品的检测。

应用了规避技术的网络攻击，会给企业带来不容忽视的安全威胁，如果不能对其进行正常、有效的处理，这类攻击会使得 IPS 产品形同虚设，将用户的网络资源暴露于攻击者面前，从而降低用户网络环境的安全性，增加用户资产遭受损失的风险。

二、常见的攻击规避技术分析

攻击规避一般也叫做攻击逃逸。攻击者通过对攻击数据包的精心定制和伪造，企图

绕开 IPS 此类产品的检测。目前比较流行的攻击规避技术包括：数据包分片、数据流分隔、RPC 分片、URL 混淆，以及攻击负载的多态和混淆等。下面将针对几种主流的协议和应用逃避技术，分别进行较为详细的介绍和分析。

（一）TCP/IP 协议规避技术

TCP/IP 协议的抗规避处理难点主要集中在 TCP 协议上。TCP 协议是端到端的复杂流式可靠传输协议，它的序列号、窗口，以及重传等保障可靠传输的机制，会给 IPS 的检测带来很大困难，IPS 只能被动地跟踪通信双方的数据及状态变化，通过实时的数据流重组以进行检测。

IPS 必须内置 TCP 状态跟踪及流汇聚机制，以确保对 TCP 会话的持续跟踪和分析。然而在数据传输过程中，一旦出现数据包顺序错乱，报文丢失或重传等问题，很多 IPS 的检测机制就会失效，一些规避攻击恰恰利用这个缺陷，得以绕开 IPS 的检测。

归结起来，针对 TCP/IP 协议的规避技术，主要包括如下几种实现方式:

- 通过重传机制发送干扰数据包(TTL、校验和、窗口大小、序列号、标志位、时间戳等异常的数据包）和正常数据包，在正常数据包中嵌入攻击负载，终端的 TCP/IP 协议栈会丢弃干扰数据包，并将载有攻击的正常数据汇聚起来提交给应用程序。
- 通过利用 TCP 协议的序列号或 IP 协议的片偏移机制，对数据包进行细小划分，并打乱发送顺序（逆序，乱序)。
- 利用攻击目标的协议栈特性，将数据以前重叠或后重叠的方式发送，例如下图所示，Windows 会倾向于先到的数据流分段，而 Solaris 倾向于后到的数据流分段。

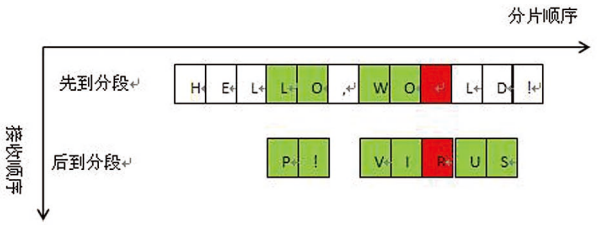


图 1 数据报文分片重叠结构示例

在 VISTA 中如上所示的数据会被汇聚为 “HELLO,WORLD！”，而在 Solaris 系统中会被汇聚为 “HELP!,VIRUS!”，这就要求 IPS 产品不仅能够实现一个完整的 TCP/IP 协议栈，还要能够根据保护目标的类型进行重组策略的调整。

TCP/IP 协议的规避技术，早在 1998 年发表的论文《Insertion, Evasion, and Denial of Service：Eluding Network Intrusion Detection》中就已经被详细的描述。然而，目前大多数的 IPS 产品仍未具备完善的数据重组能力，这给入侵成功创造了很大空间。

（二）RPC 协议规避技术

MS-RPC 和 Sun/ONC RPC 都允许应用程序以分片的方式发送请求，这些分片在 RPC 服务器内会被重新组装成完整请求形式。攻击者通过将不同程度的 RPC 碎片和不同的 TCP 传输机制进行组合后，可以构造出多种的规避方式。例如：在单 TCP 数据包中发送所有分片，在不同 TCP 数据包内发送不同范围的分片（如每个 TCP 数据包只携带一个 RPC 分片）等。

以 MS08-059 为例，Host Integration Server 的 RPC 接口所暴露的一些方式，允许未经认证的攻击者在服务器上执行任意程序。RPC opcodes 1 和 6 都允许攻击者调用 CreateProcess() 函数并向其传送命令行，这可能导致完全入侵服务器。利用这个漏洞，攻击者可以发送如下所示的请求，来提升权限:

CMD/c net user admin admin /ADD

为逃避检测 IPS 对这种异常权限提升行为的检测，攻击者可以对 RPC 请求进行分片处理，下图是在单 TCP 数据段内进行分片后的效果:

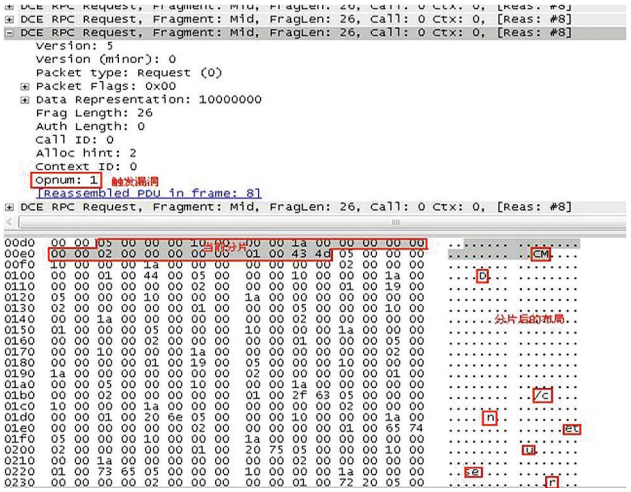


图 2 RPC 分片结构示例

由于特征信息被 “打散”，传统的基于包特征匹配的方式很难处理这种规避，要检测该攻击需要依据 DCERPC 协议对 RPC 分片进行重组。可见，IPS 不仅需要能够对底层协议进行精确解析，还需要有非常细粒度的应用层协议处理能力。

（三）URL 混淆

URL 混淆通常被攻击者用以逃避 IPS 产品的 URL 过滤机制，这类规避方式主要包括如下几种:

- 采用转义符 “%” 将字符用 16 进制表示;
- 采用转义符 “%u” 将字符用 UNICODE 方式表示;
- 随机插入 “//”，“/./” 和 “\” 字符;
- 随机变换大小写;
- 用 tab 符（0x09 或 0x0b）或回车符（0x0d）做分隔符;
- 加入干扰字符串。

以 CVE-1999-0070 为例，该漏洞产生原因是 NCSA HTTPd 和早期的 Apache Web Server 自带了一个名为 “test-cgi” 的 Shell CGI 脚本，通常位于 “/cgi-bin” 目录，用于测试 Web 服务的配置是否已经可以正常地使用 CGI 脚本。test-cgi 脚本的实现上存在输入验证漏洞，远程攻击者可能利用此漏洞遍历主机的目录，查看目录下的内容，因此检测该攻击的特征码一般包含 “cgi-bin/test-cgi” 这个字符串，该攻击概念验证（PoC）如下:

GET /cgi_bin/test-cgi?/* HTTP/1.1

对该 PoC 的 URL 进行混淆后可以得到如图 3 所示的 URL 格式:

不幸的是这些混淆后的形式都是 Web 服务器可接受的，显然要避免这种攻击的漏报，IPS 就不能在原始 URL 中进行特征匹配操作，而应先对 URL 进行恢复和整理后再进行规则检测等操作。

a) GET /egi-%62%69%6e/t%65st%2d%63%67%69?/* HTTP/1.1↵

b) GET /egi-bIN/tEst-egI?/* HTTP/1.1↵

c) GET (CR)/egi-bin/test-egi?/*.HTTP/1.1 (CR 表示回车符)↵

d) GET /./egi-bin/./test-egi?/* HTTP/1.1↵

e) GET /egi-bin|test-egi?/*.HTTP/1.1↵

f) GET
/%20HTTP/1.1%0d%0aAccept%3a%203%0xLEt9y6xIro/../../egi-bin/test-egi?/*
HTTP/1.1↵

.

8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr
hIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUj
xJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LC
dr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIP
UjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJy
LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8LCxJyUjhIPdr8
/egi-bin/test-egi?/* HTTP/1.1↵

图 3 URL 请求混淆示例

（四）FTP 规避攻击

为逃避 IPS 产品对 FTP 攻击的识别与拦截，攻击者通常在 FTP 命令中随机添加一定数量的干扰字符（空格符、Telnet 非文本控制符等），这些干扰字符在 FTP 服务器的处理过程中往往会被过滤掉。

假设攻击者向 FTP 服务器发送如下命令:

CWD/test1/test2/test3/test4/test5/test6

向其添加干扰字符后我们得到如图 4 所示的 FTP 请求:

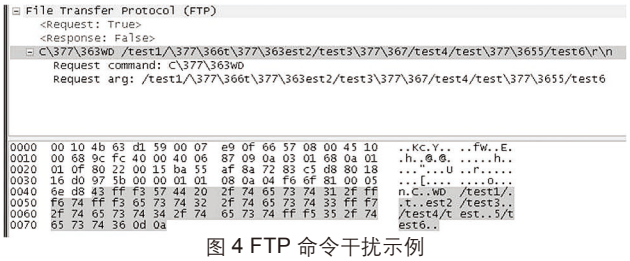


图 4 FTP 命令干扰示例

假设参数中包含“test2”的 CWD 请求会触发 FTP 服务器的某一漏洞，IPS 需要先于 FTP 服务器正确识别 CWD 请求命令，并过滤请求参数中是否存在“test2”这个特征，如果 IPS 不能在正确解析 FTP 协议的同时，准确地滤除干扰字符，它最终看到的将是“t\xff\xf3est2”进而导致漏报发生。

三、攻击规避技术的应对思路和策略

攻击规避技术往往利用系统的协议处理缺陷，绕开正常的检测机制，使得真正的攻击流量能够渗入企业内网，其危害之大，防范之难，正被用户越来越关注。用户在选择一款优秀的 IPS 产品时，已经把攻击规避的检测能力，作为一种必备的产品技术要求进行评估。然而，攻击规避技术应用广泛，种类繁多，而且变种、更新速度较快，要想有效地防范这类攻击，将面临三大挑战:

首先，IPS 产品需要对相关的网络协议有清晰的理解，具备细粒度协议解析机制和异常处理能力。各种规避技术都遵从相应的协议规范，导致规避攻击成功的原因主要是 IPS 的协议解码引擎过于简单甚至存在疏漏。

其次，安全厂商需要及时跟进各类攻击规避技术的发展动向。当出现新型的攻击规避技术时，能够及时透析其原理并制定有效的应对方案。

最后，IPS 产品应该具备良好的扩展能力。一般而言，产品协议解析层面的结构变化会对整个系统带来较大的影响，牵一发而动全身。具备良好扩展能力的引擎架构，可以降低抗攻击规避模块的维护成本，缩短应急响应时间。

攻击规避技术对于 IPS 的应用带来了巨大的挑战，为了有效应对此类威胁，IPS 产品在设计和开发攻击检测引擎的时候，必须考虑以下几方面的因素:

- 具备细粒度协议解析机制和完备的协议异常控制结构，第一时间对非法协议数据及时处理，杜绝安全隐患的蔓延;
- 配置高效的 IP 数据包重组策略，能过同时处理多种模式的分片数据包;
- 过滤协议异常数据的同时，积极修正、恢复正确的协议数据，最大限度地保障解码过程的完整性;
- 兼顾性能最优化，降低规避处理过程对引擎性能带来的影响;
- 尽量控制可能引入的风险，确保系统的稳定性不受影响。

为了验证 IPS 产品对于攻击规避手段的抵御能力，NSS Labs 的安全专家们在“安全有效性”专项测试中，采用了五个测试项目，对 IPS 的攻击规避检测能力，进行了全面（覆盖 IP、TCP、HTTP、DCERPC、SUNRPC 等多种协议）且严格的测试。

基于强大且完善的协议解析引擎，以及多年以来在入侵检测 / 防护领域的深厚技术积淀，绿盟网络入侵防护系统（NSFOCUS NIPS）在 NSS Labs 的“规避测试”项目中获得 100% 的通过率，并最终得到 NSS Labs 在全球范围内的鼎力推荐。在此之前，仅有两家国际顶尖安全厂商的 IPS 产品获此殊荣。

Description	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasion	TOTAL
NIPS-1200	✓	✓	✓	✓	✓	✓

图 5 NSFOCUS NIPS 攻击规避检测能力（引自 NSS Labs 测试报告）

四、结束语

应用了规避技术的蓄意隐性攻击，只是 IPS 面临的众多挑战之一，作为一款优秀的 IPS 产品，必须具备各类已知和未知风险的识别和控制能力，以确保产品的安全有效性，这也是 IPS 发展、演变历程中必须遵循的一项基本原则，惟有精确识别各类攻击，并及时做出响应，才有可能最大限度发挥 IPS 的功效，保障企业信息系统的安全。

手机安全面面观

研究部　刘业欣

摘要：随着智能手机的蓬勃发展，手机能做的事情也越来越多，而手机自身的安全性也越来越凸现出来。本质上说，手机安全和 PC 终端安全原理上一致，但手机上的安全也有其自身的特点。

关键词：智能手机　强制签名　3G　物联网

引言

2009 年在加拿大温哥华举办的 CanSecWest 安全会议上，Pwn2Own 黑客大赛第一次把手机作为攻击目标，但当年没有任何斩获。 2010 年的 Pwn2Own 大赛终于传来了好消息，卢森堡大学的 Ralf Philipp Weinman 和 Zynamics 公司的 Vincenzo Iozzo 合作成功攻破了 iPhone 3GS(iPhone OS 3.1.3)。他们只利用 Safari 浏览器访问特定的 Web 页面，就得到了执行任意代码机会（这种攻击方式就是目前常见的网页挂马攻击方式）。

随着智能手机的蓬勃发展，手机能做的事情也越来越多，而手机自身的安全性也越来越凸现出来。本质上说，手机安全和 PC 终端安全原理上一致，但手机上的安全也有其自身的特点。

一、智能手机的主要操作系统及其安全机制

所谓智能手机 (Smartphone)，是指像 PC 一样，具有独立的操作系统，可以由用户自行安装软件、游戏等第三方服务商提供的程序，通过此类程序来不断对手机的功能进行扩充，并可以通过移动通讯网络来实现无线网络接入的这样一类手机的总称。

智能手机最早可以追溯到 1992 年 IBM 设计的一款概念性的智能手机 “Simon”。智能手机真正出现则是在 1996 年 Nokia 推出的 Nokia 9000。Nokia 9000 的操作系统是 GEOS（基于 DOS 开发），CPU 为 x86 架构，支持 MMC 扩展卡。由于智能手机不具备像 PC 一样的标准，经过十几年的发展，现在其功能已越来越强大，其产品也是花样繁多，数不胜数。从现在主流的智能手机来看，其 CPU 都采用 ARM 架构，其上的操作系统被几大智能手机操作系统来统治。下面我们就来按照当前市场占有率排名依次分析一下主流的智能手机操作系统:

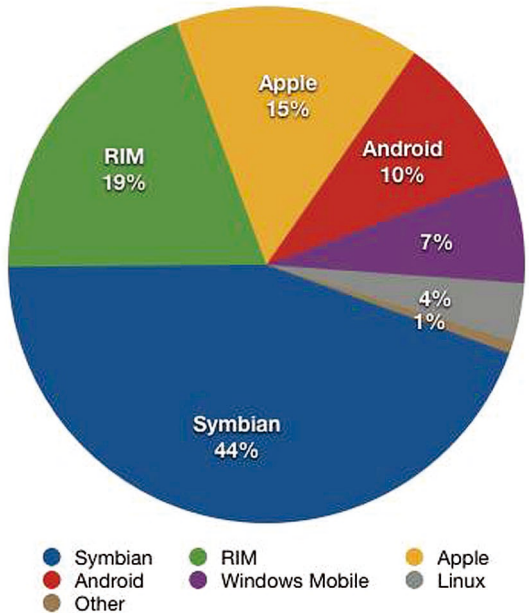


图 1 智能手机操作系统 2010 年 1 季度全球市场占有率分布图

表 1 智能手机操作系统 2010 年 1 季度全球市场占有率统计数据

Worldwide Smartphone Sales to End Users by Operating System in 1Q10 (Thousands of Units)

Company	1Q10 Units	1Q10 Market Share (%)	1Q09 Units	1Q09 Market Share (%)
Symbian	24,069.8	44.3	17,825.3	48.8
Research In Motion	10,552.6	19.4	7,533.6	20.6
iPhone OS	8,359.7	15.4	3,848.1	10.5
Android	5,214.7	9.6	575.3	1.6
Microsoft Windows Mobile	3,706.0	6.8	3,738.7	10.2
Linux	1,993.9	3.7	2,540.5	7.0
Other OSs	404.8	0.7	445.9	1.2
Total	**54,301.4**	**100.0**	**36,507.4**	**100.0**

Source: Gartner (May 2010)

Symbian OS

Symbian OS 依靠以诺基亚为首的多个手机大厂的支持，一直都是智能手机市场的老大。Symbian OS 前身叫做 “EPOC”，到 6.0 版本的时候正式改名为 “Symbian OS”，目前最新版已经是 9.5 版本，并且已经被 Nokia 收购，开放了部分版本的源代码。当前的 Symbian OS 内核是微内核设计，具有抢占式多任务和内存保护机制。由于 Symbian OS 中存在多种不同的用户接口（UI），Symbian OS 又可分为 UIQ、S30、S40、S60、S80、S90、MOAP(S) 等等多种平台。Symbian OS 9 之前的版本可以说是没有任何安全机制，因此其上的恶意软件比较泛滥。从 Symbian OS 9.1(S60 v3) 开始引入了平台安全（Platform Security）机制，即用数字签名技术来进行 “能力”（也就是权限）限制，从此 Symbian OS 安全性才得以大大提高。目前 Symbian OS 对应用程序的能力可以细分为 20 项。

只需要通过签名获得的能力 6 项:

- LocalServices: 用于通过 USB、红外和蓝牙发送或接收消息;
- ReadUserData: 准许读取用户数据。系统服务器和应用引擎可以自由地对他们的数据施加这一限制;
- WriteUserData: 准许写入用户数据。系统服务器和应用引擎可以自由地对他们的数据施加这一限制;
- UserEnvironment: 准许访问用户及其附近环境的实时保密信息;
- NetworkServices: 用于使用移动网络，例如：拨打电话或发送文本消息;

• Location: 准许访问手机的位置信息。

需要通过签名和声明书（Declarative Statement）获得的能力 7 项:

• PowerMgmt: 准许在系统中中断任何进程或者转换机器状态（关掉设备）;

• ProtServ: 准许服务器应用可以用一个受保护的名字进行注册，受保护的名字以“!”开头;

• SwEvent: 准许生成或者捕获键盘以及笔输入事件;

• SurroundingsDD: 准许访问提供外围设备输入信息的逻辑设备驱动;

• ReadDeviceData: 准许读取系统设备驱动数据;

• WriteDeviceData: 准许写入系统设备驱动数据;

• TustedUI: 区分正常应用和可信应用的用户接口。

需要通过“Symbian 能力请求”认证才能获得的能力 5 项:

• MultimediaDD: 准许对所有多媒体设备驱动（声音、摄像头等）的访问;

• NetworkControl: 准许修改或者访问网络协议控制;

• CommDD: 准许访问通信设备驱动;

• DiskAdmin: 准许进行硬盘管理操作，例如格式化驱动器;

• AllFiles: 准许系统中的所有文件可见，而且还可对在 /private 下的文件进行写操作。

只有设备制造商才能获得的能力 2 项:

• DRM: 准许访问 DRM 保护的内容;

• TCB: 准许在终端中访问 /sys 以及 /resource 目录。

签名又大致分三种:

• Symbian 收费证书签名

即用 Symbian 手机操作系统官方颁发的收费证书签名。通过了 Symbian 安全认证的软件才会获得 Symbian 的证书，这个认证是需要收费的，而且每更新一次版本可能还得重新认证。该类软件有较高的安全级别，在手机上能正常安装、运行，且能实现软件提供的所有功能。

• 作者使用公共免费证书签名

软件作者在发布软件的时候就使用公共免费证书对软件进行了签名。这类软件可以在手机上安装运行（可能会遇到安全性警告, 可跳过）。但因为公共免费证书权限较低，故不能实现那些“被特别限制”了的功能。

• 用户签名 (使用开发证书)

严格来说，这个应该是属于“开发者签名”。因为 Symbian 为软件开发者提供一种“开发证书”，原意本来是让软件开发者做软件测试用的。这个“开发证书”是与作为测试用的机器的 IMEI 码挂钩的。使用这种证书签名的软件只能在该 IMEI 码对应的机器上使用，不能用于别的机器。开发证书自颁发日起有效期为三年。

不幸的是，虽然 Symbian OS 9.x 具有了强制签名机制，但仍然被人找到了漏洞可以突破这个限制。针对 S60 的最新固件版本的签名破解程序已经出现，破解之后强制签名机制将不再有效。现在还不清楚恶意软件能不能用这个破解方法进行传播，即使不能被直接利用，由于很多人为了不受限制，进行了这种破解操作，导致系统本身失去了安全性，也就给恶意软件的入侵带来了机会。Symbian 平台是 Symbian OS 的后续产品，采用 Symbian^N 的版本记号，Symbian^1 就是 S60 v5，Symbian^2 是基于 S60 v5.1

进行开发。Symbian 平台的版本规划如下:

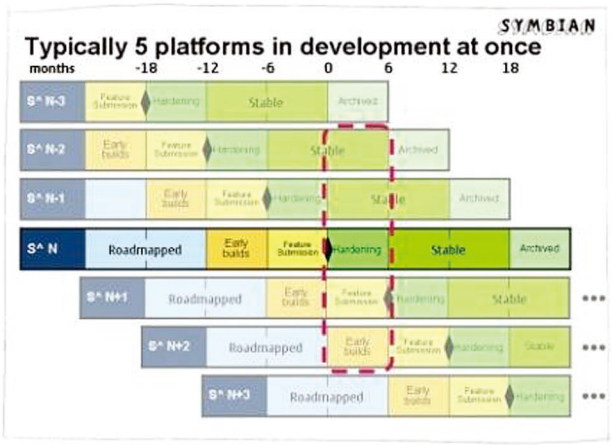


图 2 Symbian 平台开发规划图

以半年为间隔，各个版本将先后依次经历各个开发阶段，稳定后发布上市，其后生命周期为一年。因此，同时在开发过程中的系统将达到 5 个版本:

- S^N 处在 “Harden” 稳定性增强阶段;
- 两款早期系统 S^N-1 和 S^N-2 处在稳定阶段，是提供给厂商使用的主流系统;
- S^N+1 处在丰富功能阶段，开发者可以提供新的功能特性;
- S^N+2 处在早期版本测试阶段。

BlackBerry OS

BlackBerry OS 是 RIM 公司专有的手机操作系统，具有多任务能力和强大的基于 RIM 自己服务端的 PushMail 功能，为公司环境提供了端到端的企业无线解决方案。2010 年 4 月，RIM 公司发布了 BlackBerry OS 6.0。BlackBerry OS 安全机制也是通过强制签名来进行权限划分。虽然 BlackBerry OS 自身出过一些安全漏洞，但都不严重，又由于 BlackBerry OS 是个相对封闭的系统，因此 BlackBerry OS 到在现其安全机制也没有被破解，安全性和稳定性显得尤为突出。

iPhone OS

iPhone OS 是苹果公司基于 Mac OS X 开发的 iPhone 专用操作系统。其提供的多点触摸方式给手机带来了新的体验。iPhone OS 的安全机制也是强制签名机制，只有 “App Store” 上的应用软件才能安装运行。2010 年 6 月，苹果公司发布了 iPhone OS 4，并且改名为 iOS 4。随着 iPhone 市场的火爆，iPhone OS 的市场占有率迅速超过了 Windows Mobile，目前排在智能手机操作系统的第三位，并且到 2010 年底很有可能超过 BlackBerry OS 再晋升一位。如同 Symbian OS、iPhone OS 也被人找到了可以突破限制的漏洞，俗称 “越狱”（Jailbreaking）。而且在 2010 年的 Pwn2Own 大赛，攻击者利用真正的远程可利用漏洞成功地对当时最新版本的 iPhone OS 进行了攻击。

Android

Android 是基于修改的 Linux 内核，并结合关键应用程序和 Java 中间件技术而形成的开放源代码的智能手机操作系统。Android 系统最初由 Android 公司开发，后来 Android 公司在 2005 年 7 月

被 Google 公司收购。2007 年 11 月，包括 Google 在内的多家移动产品和运营公司共同成立了开放手机联盟 (Open Handset Alliance)，Android 也成为开放手机联盟旗下惟一的移动操作系统平台。2010 年 5 月，开放手机联盟推出了 Android 2.2。由于 Android 得到了大部分移动厂商的支持，并且完全开放，是最有前途超越 Symbian OS 的智能手机操作系统。Android 安全机制没有采用强制第三方签名机制，只要自签名的程序就可以正常运行了，因此这种签名机制形同虚设。

Windows Mobile

Windows Mobile 是微软公司基于 Windows CE 开发的手机操作系统。由于微软提供了强大的 Windows CE 的开发环境，使得开发 Windows CE 上的软件与 Windows 上的软件过程基本类似，再加上系统也支持 .NET，因此有众多的软件开发者和开发商为其开发应用软件，使得 Windows Mobile 上的软件资源非常丰富。2010 年 2 月，Windows Mobile 6.5.3 在索尼爱立信的 Aspen 手机正式发布。Windows Mobile 提供的安全机制也非常全面，与 Symbian OS 的安全机制有所差别，并不是只依靠签名来决定其拥有的能力，而是通过三级权限来进行划分，每一级别权限的能力依靠安全策略来配置。而且签名机制并非强制，可以在安全策略中关闭。于是在目前大多数的 Windows Mobile 的产品中，都没有启用强制签名机制。这样也就给恶意软件敞开了大门。之所以采取这样的配置，应该是考虑到大量未签名的应用软件的存在，如果采用强制签名会导致非常多的麻烦。虽然 Windows Mobile 出厂时候未做严格的安全配置，但实际上用户可以通过自行修改注册表的方式来进行严格的安全限制。Windows Phone 7 是微软公司革命性的手机操作系统，虽然仍然基于 Windows CE 的内核，但是架构与之前的 Windows Mobile 完全不兼容，不能直接运行 Windows Mobile 的应用程序。Windows Phone 7 仍在开发中，安全特性未知。

Linux

由于 Linux 操作系统是一个开放源代码的操作系统，因此基于 Linux 的手机操作系统种类繁多，很多大的手机厂商都有自己的 Linux 手机操作系统。值得一提的是，开放手机联盟的 Android、Palm 的 WebOS、诺基亚的 Maemo、英特尔的 Moblin 也都是基于 Linux。当然基于 Linux 的手机操作系统的安全机制也完全具备 Linux 的安全机制，不过 Linux 操作系统本身是不具备强制签名功能的。

Palm OS

Palm OS 是 Palm 公司为 PDA 开发的嵌入式操作系统，后来也应用到手机，成为了手机操作系统。在 Palm OS 5.0 之前的版本并不支持 ARM 芯片，到 Palm OS 5.0 才开始支持 ARM。后来由于 ACCESS 公司收购了 Palm OS，Palm OS 被改名为 Garnet OS。一直到最新的 Garnet OS 5.5 版本，Garnet OS 仍然不支持多任务，是一个单任务的操作系统。不过 Palm OS 由于历史悠久和大量的 PDA 产品，也具有丰富的应用软件资源。Palm OS 的安全机制与 Symbian OS 9 以前的版本类似，没有任何安全机制。

WebOS

WebOS 是 Palm 公司在抛弃老的 Palm OS 之后，基于 Linux 新开发的手机操作系统，为了保证兼容性，WebOS 提供了虚拟机来运行 Palm OS 5。WebOS 的界面完全依赖于包括 HTML5、JavaScript、CSS 等等 Web 应用技术。随着 Palm 公司被惠普公司收购，WebOS 很可能被用于惠普公司的平板电脑上。

Bada

Bada 是三星公司 2009 年 11 月推出的一款手机操作系统。严格来说，Bada 本身不是一个完整的操作系统，而且也不依赖于某个操作系统，Bada 既可以运行在 Linux 内核上，也可以运行在实时操作系统上。

MeeGo

MeeGo 是英特尔和诺基亚公司联手在 2010 年 2 月推出的一款开放源代码的手机操作系统。MeeGo 的目标是把原有诺基亚的 Maemo 和英特尔的 Moblin 合并成一个产品。MeeGo 同样是基于 Linux 内核，同时支持 ARM 和 x86 两种 CPU。

二、智能手机提供的主要服务及其安全问题

智能手机的强大就在于它提供了各种丰富多彩的应用，手机上网、手机炒股、手机钱包、手机支付、移动商务、地图导航随着 3G 的发展也会逐渐普及开来。支撑这些应用是智能手机提供的底层服务。某些服务可以说是智能手机相对于 PC 而独有的，因此这些服务的安全问题也是比较独特的。下面列举的主要是与安全相关的一些手机服务，比如手机拍照、GPS、收音 / 电视等等其他的功能就不再说明了。

无线通讯 (Radio)

Radio 提供了手机最基本的无线通话功能，也就是通常所说的“手机信号”。手机无线通讯从上个世纪八十年代 1G 时代的模拟信号发展到上世纪九十年代，TDMA(GSM) 和 CDMA 为代表的数字信号 2G 时代来临。2.5G(GPRS,CDMA 1x) 时代则把单纯的语音和短信服务扩展到数据传输和彩信服务。3G 时代更是把数据传输的带宽提到了更高的水平，为提供更复杂网络应用奠定了基础。目前手机无线通讯正在向可达百兆带宽的 4G 时代发展。

在 1G 时代，手机的模拟信号为了达到语音效果的清晰，几乎没有任何安全性可言，没有鉴权且语音数据没有加密，极其容易被并机盗打和监听。到了数字信号的 2G 时代，手机信号才考虑安全问题。以 GSM 为例，增加了专门用于鉴权和加密的 SIM 卡 (Subscriber Identity Module 即用户身份识别模块)。SIM 卡实际是一个智能卡，不但可以存储数据，还可以参与运算。虽然 GSM 考虑了手机信号传输的安全性，但是由于历史原因，其采用了较弱的鉴权和加密算法，使得可以在较短的时间内破解不可读的鉴权密钥 (KI)，有了这个鉴权密钥在加上一些可读的用户识别号 (如 IMSI 和 PIN)，就可以实现 SIM 卡的复制，从而实现盗打。目前 SIM 卡的复制技术已经不再是个秘密，已经被很多不法分子所利用。GSM 手机信号也是可以被窃听的，商业监听设备已经出现，但价格昂贵 (主动式至少 7 万美元，被动式要 100 万美元)。不过在 08 年 BlackHat DC 的会议上 David Hulton 发布了他们对 GSM 攻击的研究成果，基于低成

本的设备来捕获 GSM 数据并可以做到 30 分钟内解密数据。当然这些攻击只针对的是 GSM 中比较老的加密算法，采用新的加密算法就可提高 GSM 的安全性，大大降低被盗打或被窃听的可能性。除了针对 GSM 加密算法的攻击，还可以针对 GSM 协议上的漏洞来进行攻击。主动式监听设备就利用中间人的方式来欺骗被攻击方。CDMA 相对 GSM 来说要更安全，CDMA 1x 曾经是美国军方使用的保密通讯协议。

手机无线通讯除了数据层面的攻击之外，还可以对其采用物理攻击方法。手机信号由于是无线信号，容易被干扰或被屏蔽。

短信 (SMS)

短信是最早与手机语音服务同时出现的手机功能。由于短信格式简单而且还有字数限制，出现安全漏洞的可能性较低，早期的手机中都没有被发现什么漏洞。随着智能手机的出现，再加上漏洞挖掘技术的发展，在 2009 年 BlackHat USA 大会上，Collin Mulliner 和 Charlie Miller 发现了可以导致 iPhone 和 Android 系统崩溃的漏洞，这个漏洞与短信处理相关，但并非真正意义上的通过发送短信就可以远程利用的漏洞。

彩信 (MMS)

彩信是以 2.5G 提供的数据传输服务为基础的短信扩展业务，可以理解为手机网内专有 Email 系统。由于彩信的格式相对于短信而言较为复杂，并且带有音视频功能，因此彩信上出现安全漏洞的可能性就很大了。比如 2008 年有人发现可以通过彩信来攻击国产的 MTK 手机系统。其实就是彩信包含一个后缀为 imy 的音频文件附件，里面可以包括了震动、闪亮、关闭屏幕等代码，当某些有快捷功能和铃声自编功能芯片的手机在接收后，要么执行，要么因无法执行而发生故障，就产生了所谓“死机”现象。Symbian 的 S60 系统在 2008 年底也被人发现了一个彩信漏洞，当收到的彩信中邮件地址超过 32 个字符时，系统彩信和短信的接收功能就会失效，无法再接受新的彩信和短信。当然上面的漏洞还无法被利用执行任意代码，但以后很可能会发现更好用的漏洞，尤其是音视频文件格式方面的漏洞。另外还要提一下利用彩信加欺骗的手法来传播的恶意软件。恶意软件把程序或者安装包伪装成其他的文件，如图片或视频等等来欺骗用户点击并运行或者安装，从而达到传播的目的。虽然这不算是彩信自身的漏洞，但是还是要防范这种欺骗性质的攻击方式。

邮件 (Email)

手机上的邮件功能依赖于手机的访问 Internet 的能力，与 PC 上的邮件功能没有任何区别。邮件的安全漏洞也与 PC 上邮件系统的安全漏洞类似，更可能的是出现文件格式上漏洞。

WAP

WAP(Wireless Application Protocol) 全称是无线应用协议，专门为类似手机这样的移动设备设计的类似 IP/TCP 的系统。WAP 协议主要考虑到掌上无线设备带宽小、传输可靠性、屏幕小等等局限性而设计了一整套专有协议，通过 WAP 网关也可以访问到 Internet。是 2009 年 Sony Ericsson 的手机被曝在处理畸形 WAP Push 消息（可以通过短信或 UDP 发送）的时候，会导致系统重启。不过随着

无线技术的发展，WAP 最终会被淘汰。

无线局域网 (Wi-Fi)

Wi-Fi 给手机提供了廉价和快速的上网功能。但是从 Wi-Fi 技术本身的安全性来说有很大的安全隐患。其最早的 WEP 接入技术已经被攻破（在较短的时间内就可以非法接入并监听其他人的 Wi-Fi 信号），WPA 的安全性也受到威胁，目前非常安全的接入技术只有 WPA2 和 WAPI。不过更好的解决方案是开放 Wi-Fi 的接入，通过应用层的安全机制，比如 VPN 或 SSL 来保证安全性。手机上的 Wi-Fi 还可能出现的问题是 Wi-Fi 协议栈的完全漏洞。

蓝牙 (Bluetooth)

蓝牙是为了满足短距离的小设备的连接需要而设计，比 Wi-Fi 更早的应用于手机设备上。由于蓝牙协议栈提供了非常多的功能，而且协议设计比较独特，因此历史上蓝牙出现过的漏洞非常多，包含协议本身的、加密算法的、协议栈实现的等等方面的漏洞。甚至在 2004 年还出现过 S60 系统上可以通过蓝牙设备来传播的病毒。因此在非特定需要的时候建议要关闭蓝牙功能。

PDA

PDA(Personal Digital Assistant) 就是个人数字助理，在早期的手机上 PDA 的功能并不强大，随着智能手机的普及，人们已经不需要专门的 PDA 设备，PDA 所有的功能都集成到智能手机中，并且功能更强。PDA 的安全问题一个是各种应用软件的安全漏洞，另外一个最重要的是个人信息的泄漏。为了方便，更多的个人信息会保存在手机中，保护个人信息不被泄露则是 PDA 功能最需要解决的问题。

3G

3G 概念本来属于 Radio 的一部分，单独一个标题是要突出 3G 可能带来的安全问题。2G 时代手机的带宽不足，很多网络应用无法开展。到了 3G 时代，一个手机的网络带宽甚至要比 PC 的网络带宽还要大，大部分的网络应用都可以在手机上实现，比如前面提到的手机上网、手机炒股、手机钱包、手机支付、移动商务、地图导航等等应用。由于应用繁多，产生的安全漏洞的可能性就会大增，但其中包含一些敏感应用又对手机的安全性有极高的要求。这一对不可调和的矛盾会更加突出手机安全在 3G 时代的重要性。被动地检测恶意软件目前在桌面系统上已经遇到瓶颈，只有安全的手机操作系统才能不会重蹈桌面系统的覆辙。

三、手机上主要的安全威胁和防范

第一部分介绍的智能手机的安全问题，大部分还只是一个潜在的安全问题。无论是智能手机还是非智能手机目前都面临下面几种实际的安全威胁。

恶意软件

恶意软件包含病毒、木马等等，与 PC 系统上的恶意软件类型没有任何区别。当然恶意软件的威胁主要还是针对智能手机和部分支持 Java 扩展的非智能手机。目前手机上的恶意软件的传播途径主要有:

1. 独立软件包：一般通过欺骗方式，引诱手机用户安装其恶意软件。不过这种方式比较容易被用户发现。

2. 捆绑在其他应用软件安装包中：这种方式隐蔽性强，也最常

见。由于用户想免费使用某些收费的商业软件，大多都要安装来自非官方制作的安装包，因此很容易被人利用来捆绑恶意软件。

3. 捆绑在手机系统的 ROM 文件中：这种方式隐蔽性最强，而且除了重新刷 ROM 之外，恶意软件很难被清除。

为了防范恶意软件的侵袭，现代的手机操作系统都具备了强制签名功能，也就是只有官方认可的（即签名过的）安装包或程序才能在手机上安装和运行。因此当使用支持强制签名机制的手机操作系统时，要启用强制签名机制，不要禁用或者破解强制签名机制。当使用不具备强制签名机制的手机时，手机上的应用软件要用官方网站上的安装包进行安装，不要安装破解的软件。谨慎对待个人刷机行为，即使要刷机，也要刷官方提供的 ROM 文件。安装手机上的反病毒软件也是一个不错的选择。

垃圾信息

垃圾信息的威胁是属于正常应用带来的安全威胁。垃圾信息包含垃圾短信、垃圾彩信和垃圾邮件。垃圾信息最常见的就是诈骗短信，利用“广撒网，多捕鱼”的原理，利用人们的各种心理来骗取用户的钱财。安装手机短信防火墙软件可以有效摆脱垃圾短信的骚扰。当然只有提高人们的防骗意识，才能有效的避免垃圾信息带来的损失。

话费吸费

话费吸费一般是通过恶意软件在用户不知情的情况下来拨打 SP 电话或者发送 SP 短信用以获取用户话费。常见的话费吸费行为出现在山寨机中。山寨机厂商把有具有话费吸费功能的软件内置到手机的系统中，通过获取用户的话费来弥补山寨机低廉价格带来的损失，进而获取更多的利润。因此不要被山寨机低廉的价格所吸引，赔本的买卖谁都不愿意去做，其背后可能隐藏着不可告人的陷阱。

手机卡复制

上一章里已经介绍了手机卡复制的原理，理论上是可以对手机卡进行复制的。如果能够获取电信运营商手机卡数据库中的信息，那么采用什么加密算法都阻止不了手机卡被复制。如果抛开这个非技术因素，要复制某个手机卡，必须要拿到这个卡或者利用无线窃听（有距离限制）来进行。因此虽然手机卡的复制是可行的，但是市面上大多号称能复制手机卡，甚至只需要号码就能复制手机卡的绝大多数都是骗子，需要手机用户对此有所警惕。

手机信号无线窃听

上一章里已经做了分析，这属于手机信号通讯协议设计的问题。因此理论上无法阻止窃听行为。但是无线窃听手机信号，前提是必须在一个基站的覆盖范围内才能实现。远距离的窃听是不可能的。还需要强调一点，不要与“手机窃听器”混淆了。手机窃听器是利用手机的语音功能来做一个窃听器，窃听的主要是手机周围环境的声音。而手机信号无线窃听是通过捕获手机无线信号来对手机通话进行窃听。手机窃听器可以做到远距离窃听，而手机信号无线窃听的距离是有限制的。

对于上述威胁可能产生的危害如下:

- 系统破坏

通过恶意软件就可以让智能手机系统被破坏，导致用户数据的丢失，甚至手机无法正常使用。

- 信息泄露

通过恶意软件或手机信号无线窃听，就可以偷取用户的通讯录、照片、视频、短信和语音等等信息，造成用户隐私的泄漏。

- 金钱损失

通过话费吸费、诈骗短信或电话、复制手机卡盗打电话等方式，都可以导致用户的话费或者其他金钱的损失。尤其是诈骗短信或电话可导致用户大量金钱的损失。

- 成为攻击他人的工具或跳板

利用恶意软件和 3G 网络，就可以实现类似 PC 系统上“肉机”，黑客可以利用用户的手机来攻击其他的网络目标。

四、手机安全漏洞的现状与展望

目前与漏洞相关的手机安全技术仍然处于初级阶段，其中包含手机系统的漏洞挖掘和漏洞利用两大技术。手机系统的漏洞挖掘技术与 PC 系统上的漏洞挖掘技术基本类似，主要都是通过 Fuzzing 测试技术来进行，方法相对简单，工具也相对成熟。手机系统的漏洞利用技术虽然本质上也与 PC 系统上的漏洞利用技术相同，但实际可操作的技术则公开的很少，较为简单而通用的技术还没有出现。由于主流智能手机操作系统大都采用了比较先进的安全模型，被攻击的可能性大大降低了。回到本文开始介绍的对 iPhone OS 的攻击，攻击者利用”return-into-libc”（也称“Return-Oriented Programming”，即面向返回编程）技术成功获取了 iPhone 的短信数据库里的内容，包括删除后的短信内容。他们还声称同样的攻击手段也可以获取 iPhone 里的联系人、邮件数据库、照片等等内容。但本次攻击没能突破 iPhone 的沙盒，更没有拿到 root 权限，只是利用名为“mobile”的普通用户偷取了 iPhone 里个人相关的信息，因此不能用它来绕过 iPhone 的代码签名机制，也不能对 iPhone 系统产生严重的破坏。通用的 ROP（面向返回编程）技术不但可以绕过 Windows 的 DEP 技术，还可以在手机系统上畅行无阻，是漏洞利用技术研究的方向。

目前还有一个趋势，就是智能家电和物联网的发展。同样属于嵌入式设备的智能手机上的操作系统很可能也会被应用到智能家电当中。随着智能嵌入式设备的发展与普及，其数量规模必然要超过 PC 机的规模，一旦出现严重的漏洞，后果将不堪设想。因此手机操作系统虽然在设计上更安全，但出现严重漏洞的危害性却极大。

参考文献

1)http://en.wikipedia.org/wiki/Smartphone

2)http://en.wikipedia.org/wiki/Symbian_OS

3)http://en.wikipedia.org/wiki/IPhone_OS

4)http://en.wikipedia.org/wiki/Android_(operating_system)

5)http://en.wikipedia.org/wiki/BlackBerry_OS

6)http://en.wikipedia.org/wiki/Windows_Mobile

7)http://en.wikipedia.org/wiki/Palm_OS

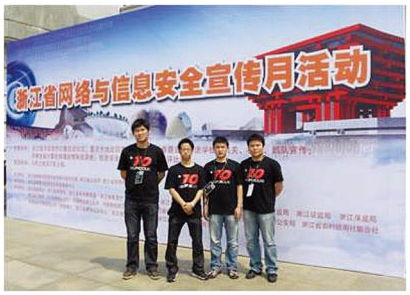
8)http://en.wikipedia.org/wiki/WebOS

9)http://en.wikipedia.org/wiki/Bada_(operating_system)

10)http://en.wikipedia.org/wiki/MeeGo

11)http://blog.symbian.org/2009/03/12/introducing-the-release-plan/

绿盟科技助力浙江省公众信息网络安全普及教育



6月上旬，由浙江省网络与信息安全协调小组办公室、省公安厅、省经济和信息化委员会主办，以“保世博盛会、建平安网络”为主题的浙江省网络与信息安全宣传月活动在杭州启动。绿盟科技作为专业的网络与信息安全支撑单位为公众提供了现场咨询服务。

本次活动，绿盟科技为广大市民带来了漫画式宣传资料，以通俗易懂的方式向民众传达了信息网络安全风险与防范常识、文明守法上网和文明依法办网的行为准则。

针对广大市民网络安全知识缺乏专业化基础、网络安全防范意识薄弱等现象，绿盟科技的安全技术人员，事先做了大量的准备工作，他们将诸如计算机登录要设置密码、离开座位要及时锁屏、使用U盘要关闭自动播放、重要文件要加密备份等等信息安全小常识融入到漫画中，并喷绘成大幅面的易拉宝展示，吸引了众多市民。很多市民都主动上前向绿盟科技的技术人员请教日常网络安全防范的知识，同时也有一些业内人士前来咨询网络安全产品及相关的解决方案。

绿盟科技作为中国网络安全领域的领导企业，不仅作为“世博安全保障单位”保障通信基础设施安全，也希望通过传播信息安全知识，在信息安全知识普及方面尽自己的一份力量，承担作为企业公民的社会责任。

绿盟科技第三次出席新加坡国际通信与信息技术展会

6月15日-18日，绿盟科技与中关村国家自主创新示范区联合参展第21届新加坡国际通信与信息技术展会（Communic Asia 2010）。继前两届Communic Asia的成功亮相后，绿盟科技在此次展会中展出了其自主研发的抗拒绝服务系统（ADS）、Web应用防火墙（WAF）、入侵防护系统（NIPS）、远程安全评估系统（RSAS），以及基于“云计算”的网站安全监测服务等产品与解决方案。此次参展将进一步加速绿盟科技在东南亚市场的国际化进程。

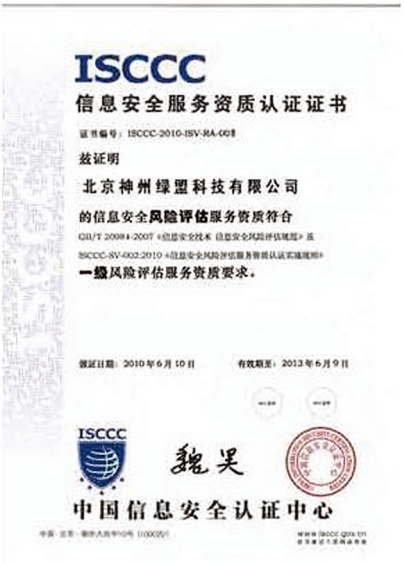
展会上，作为我国信息安全行业最早开始国际化战略的企业之一，绿盟科技与东南亚市场用户进行了积极有效的沟通，在展示公司安全产品及解决方案的基础上，绿盟科技也与周边国家及地区的业内同行进行了广泛交流与沟通，为进一步开拓东南亚市场做好了准备。

近年来，绿盟科技频繁出席RSA Conference、IST、ITSEC、CommunicAsia等国际权威信息安全展会，凭借领先的产品技术，绿盟远程安全评估系统（RSAS）与绿盟网络入侵防护系统（NIPS）先后通过了West coast Labs、NSS Labs等国际权威产品认证。目前，绿盟科技已经在美国、日本以及东南亚市场取得了业务的突破，随着绿盟科技国际化步伐的持续加速，国际市场将进一步感受来自中国网络安全公司的实力。

绿盟科技获首批信息安全风险评估服务资质证书

6月10日，绿盟科技获得中国信息安全认证中心颁发的国内首批信息安全风险评估服务一级资质认证证书。这是我国首次在信息安全风险评估领域开展服务资质认证工作。

信息安全风险评估是从风险管理角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性。对突发安全事件发生所造成的危害程度进行


ISCCC
信息安全服务资质认证证书
证书编号：ISCCC-2010-ISV-RA-008
兹证明
北京神州绿盟科技有限公司
的信息安全风险评估服务资质符合
CB/T 20984-2007《信息安全技术 信息安全风险评估规范》及
ISCCC-SV-002-2010《信息安全风险评估服务资质认证实施规则》
一级风险评估服务资质要求。
证书日期：2010年6月10日　　有效期至：2013年6月9日
ISCCC
魏吴
中国信息安全认证中心

评估，并且提出有针对性的抵御威胁的防护对策和整改措施，其防范和化解信息安全风险的有效性得到了世界各国的高度认可。目前，风险评估已成为各类信息安全服务中需求最为普遍的基础性服务之一。

此次获得该风险评估服务一级认证，一方面表明绿盟科技风险评估服务综合能力已获得国家权威认定，具备了良好的技术能力、组织管理能力和服务过程能力；另一方面，绿盟科技自成立以来，多次承担政府、金融证券、移动通信行业和企业级的重大课题研究，参与了信息安全风险评估规范及相关标准的制定工作，已经形成了一整套规范、严谨的信息安全风险评估服务体系，这些经验都将对我国信息安全保障体系建设发挥重要作用。

绿盟科技解惑政府行业：如何防范信息安全风险

随着信息化的推进，信息安全问题愈演愈烈。尤其对政府及公用事业单位而言，网页被篡改、业务被攻击、机密数据被窃取、内网被入侵等各种安全风险都会给政府及公用事业单位造成非常恶劣的影响，政府及公用事业单位的安全风险管理迫在眉睫。

针对此情况，在近日上海与广州两地举办的“政府及公用事业单位信息安全论坛”活动中，绿盟科技行业营销中心孙铁应邀就政府行业如何防范信息安全风险进行了答疑解惑。孙铁以“基于风险管理的Web应用安全保障”为主题，从“风险的内涵”、“Web应用面临的风险”、“Web应用安全保障”三个方面与到会的听众进行了交流，并就听众的问题进行了现场答疑。

政府网站如何防范信息安全风险，孙铁从检测与发现 ---- 风险预警; 防护与阻击 ---- 风险防护；运维监控 ---- 风险管理；事后响应 --- 应急支持体系；安全恢复 ---- 风险处理；溯源取证 --- 积极主动等六个维度详细讲解了绿盟科技的 Web 应用整体保障思路，从风险预警、风险防护、风险处理、风险管理等几方面具体阐述如何做到最大限度降低政府网站风险。

此次上海与广州两地的活动吸引了来自各政府及公用事业单位信息中心的主管和 IT 管理者共计 400 多人。会上，绿盟科技凭借在政府行业安全风险管理所做出的成绩，还荣获由中国电子信息产业发展研究院颁发的 “2010 年政府及公共事业单位突出贡献企业奖”。

绿盟科技等级保护整改经验助力铁路信息化

随着铁路行业的迅猛发展，铁路信息化建设如火如荼。近些年，电话订票、网上订票、客票升级、高速铁路建设等业务对于信息安全的需求越来越大，铁路行业如何保障信息安全，如何做好等级保护，成为铁路信息化建设中重要的一环。

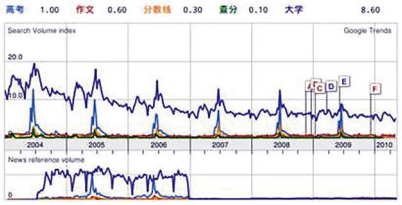
绿盟科技作为国内网络信息安全领域的领导者，长期从事等级保护实践工作，协助各行业用户开展等级保护咨询、建设、整改等工作，同时作为各地测评机构、检查机构的技术支撑队伍，积极参与了各行业、各地测评中心的体系建设，在这个过程中积累了丰富的实践经验。作为等级保护专家委员会的专家成员，绿盟科技应邀参加 “2010 铁路信息化建设技术论坛”。在会上，绿盟科技以《等级保护整改实践经验分享》为主题，与现场的听众进行了沟通和交流。

绿盟科技重点阐述了当前等级保护的市场状况以及近几年在等级保护工作中获得的经验，并在此基础上结合具体案例提出对铁路行业等级保护的一些设想和建议。绿盟科技指出，“如何保证等级保护工作有效实施，达到既节约成本、又能有效保障相应等级信息系统的目标，流程是至关重要的。等级保护工作落地不仅仅是一个技术问题，同时也是一个流程管理问题。”

经过长期的等级保护工作实践，目前绿盟科技已经探索出一套使等级保护政策切实落地的方法，完成多家单位等级保护安全体系设计、系统整改。正是基于这些成功的实践取得的经验，绿盟科技荣获 “铁路信息化建设优秀方案奖”。

绿盟科技高校网站安全解决方案保障高考网络安全

随着高考和大学生毕业离校时间的临近，各类教育、招聘类的网站，尤其是各大专业院校的网站倍受学生和家长们的关注。根据 Google Trends 的统计，在此期间，各类与高考相关的关键词搜索量将达到全年的顶峰，其中“高考”、“查分”这样的关键词的搜索量甚至能够达到平时搜索量的 10 倍左右。



除了高校网站以外，各类分数查询网站、各地考试管理中心网站、各地学校网站都有可能面临攻击者的攻击。这些网站除了在高考前后访问量剧增会吸引攻击者实施攻击以外，往往也会因为高考分数查询速度太慢、篡改考试成绩、甚至考生发泄情绪等各种原因而被黑。在过去的几年中，由于这些原因而导致网站被攻击的事件也屡见报端。

针对这一现象，绿盟科技推出保障高校网站安全解决方案，该解决方案从事前预警 --- 网站安全监测服务；到事中防护 --- 部署专业防护设备；再到事后响应 --- 应急支持体系三个维度全方位保障高校网站安全，事前预警阶段通过绿盟科技网站安全监测服务支撑体系提供的 7*24 小时不间断的安全监测服务，进行网页木马监测、页面篡改监测、敏感内容监测、页面平稳度监测以及周期性的应用漏洞扫描，从第一阶段就做好安全的监控服务。同时，绿盟科技安全专家也建议各院校要做好网站服务器安全检查，并重点对涉及高考招生相关的内外网信息系统进行安全防护和加固，避免因网络安全问题影响正常的招生工作；也建议广大学生、家长在访问互联网网站时一定要安装有效的防病毒软件，并且使用安全的浏览器访问网站。

绿盟科技成功承办“2010 信息安全高级论坛”

5 月 12 日，由中关村科技园区管理委员会 (以下简称中关村管委会)、中国计算机学会计算机安全专业委员会 (以下简称计算机安全专委会) 共同主办，绿盟科技承办的“2010 信息安全高级论坛”在京召开。

本次会议以“中国信息安全企业的国际化”为主题，吸引了来自公安部、工信部、中国科学院、中关村管委会、国内信息安全企业等单位的 100 多位代表参加。工信部软件与服务业司司长陈伟、中关村管委会副主任周云帆、绿盟科技总裁沈继业出席大会并致辞，中科院信息安全国家重点实验室教授赵战生、翟起滨，绿盟科技副总裁吴云坤以及其他安全企业的代表在会上做了精彩的演讲。论坛由计算机安全专委会常务副主任严明主持。

绿盟科技副总裁吴云坤做了主题为《从 RSA2010 看国际》的精彩演讲，与现场嘉宾一同分享了绿盟科技海外市场开拓的经

验，并阐述了国际信息安全市场的发展趋势和机遇。对于业界热议的“云计算”安全威胁与保护问题，吴云坤认为，“帮助建立用户的信心、消除用户的顾虑是云计算安全的重要目标”。为此，他向与会嘉宾列举了云计算安全所面临的七大安全风险，并给出了云计算安全的七点建议。

通过本次“2010 信息安全高级论坛”，信息安全主管部门领导、业界专家学者以及企业代表纷纷表达了对于我国民族信息安全企业参与国际市场竞争的看法与建议。工信部软件与服务司司长陈伟表示，“信息安全技术创新是我国信息安全产业发展的重要支撑，我国信息安全企业需要努力提高技术水平，积极把握产业发展趋势，优化产业结构，打造具有国际竞争力的信息安全企业”。中关村管委会副主任周云帆也表示，“中关村管委会将与国家信息安全主管部门、企业、高校展开广泛合作，依托更多核心技术创新，推动我国信息安全企业不断发展壮大”。

论坛的访谈环节中，绿盟科技、天融信、启明星辰等六家参加了 RSA2010 信息安全展会的企业代表一同登台，畅谈我国民族信息安全企业国际化的挑战与机遇，并就共同关心的问题进行了热烈讨论。本次会议，我国信息安全企业共同分享了彼此在国际市场的开拓现状，也为企业与主管部门、企业与专家、企业与企业间沟通提供了良好的平台。

绿盟科技再获 2010 年通信安全卫士奖

4 月 22 日，绿盟科技应邀出席“2010 通信网络与信息安全高层论坛”并再获 2010 年通信安全卫士奖。会上，绿盟科技首席战略官赵粮博士以“云计算安全威胁和保护要点”为主题，和与会人士分享了绿盟科技对于云计算和云安全的理解。

赵粮博士指出，云计算为运营商带来充满想象的蓝海，云计算作为一个新生事物，它给我们的实际工作、实际业务带来了非常深远的影响，不仅仅是在运营流程、采购流程，甚至业务研发方面都提供了新的思路。所以我们一方面要大力保护云计算，另一方面也可以借力云计算推出新业务。赵粮博士在分析云计算面临的主要威胁的同时，也讲述了绿盟科技在云安全方面的一些进展。作为云安全联盟 CSA（Cloud Security Alliance）亚太地区第一家企业成员，赵粮

博士还牵头成立了云安全联盟大中华区分会，希望有更多感兴趣的业内同仁以及上下游的厂商加入进来，共同探讨与分享对于云安全的理解、促进与云安全有关的标准规范的开发与落地。

在当今的信息经济时代，数据爆炸对 ICT 产业的发展构成了极大挑战，而云计算因其强大的数据处理和资源共享能力成为各界关注的焦点，同时，云计算也带来了新的安全问题。会上，绿盟科技行业技术顾问唐洪玉与工信部、中国电信网络安全领域的相关专家以及网络安全厂商，围绕云安全的热点问题展开了进一步的讨论。

作为中国网络安全领域的领导企业，绿盟科技于 08 年 10 月推出了自己的云安全计划，09 年 12 月，绿盟科技成为云安全联盟 CSA 亚太地区第一家企业成员，并积极支

持了赵粮博士主持的云安全指南中文版工作小组的翻译工作。未来，绿盟科技还将在更深入的领域研究和参与云安全，持续增加在云安全相关领域的技术和资源投入。

绿盟科技获“2010 年度中国信息安全优秀服务奖”

4 月 21 日，绿盟科技应邀出席由中国电子信息产业发展研究院主办的“第十一届中国信息安全大会”。面对来自国家信息安全主管部门领导、业界资深专家与学者、以及企事业单位信息中心主管，绿盟科技产品市场经理李晨针对业界所广泛关注的“云安全”应用做了精彩演讲，获得了与会嘉宾的热烈掌声。同时，绿盟科技赢得“2010 年度中国信息安全优秀服务奖”。

作为我国一年一度的信息安全产业盛会，本届信息安全大会以“融合安全，风险识别”为主题，向听众全面展现了我国信息安全产业发展所面临的挑战与机遇。针对互联网快速发展所带来的网站挂马、网页遭篡改以及网络钓鱼等诸多难题，绿盟科技推出了一项基于“云安全”的网站安全监测服务，对目

标站点的可用性及安全性进行 7×24 实时监测。在演讲环节，绿盟科技产品市场经理李晨以《洞察网站风险，简化安全管理》为主题，进一步为用户阐述了绿盟科技网站安全防护解决方案为用户提供的服务与价值。

多年来，绿盟科技一直关注应用层的安全研究。针对 Web 应用，从“漏洞扫描”、“配置管理”、“威胁防护”到“实时监测”，已经形成了全方位的 Web 应用安全解决方案，真正实现为客户的网站安全保驾护航。

此次荣获“2010 年度中国信息安全优秀服务奖”，时值绿盟科技成立十周年之际，这一奖项是业界对绿盟科技信息安全服务的肯定和鼓励。伴随绿盟科技自主创新步伐的加快，以及云安全解决方案的不断完善，绿盟科技将给用户的 Web 安全带来更多更有效的安全产品与服务，为用户的全面信息安全保驾护航。

绿盟网站安全监测服务布局 Web 安全

针对目前大多数网站没有独立和专业的安全运维团队，难以发现网站的风险漏洞及安全隐患，无法第一时间知晓所遭受的安全威胁等现状，绿盟科技推出了一项专门针对网站安全的托管式服务——绿盟网站安全监测服务。该服务能通过远程方式对目标站点的可用性及安全性进行 7×24 实时监测。

对网站所有者来说，“绿盟网站安全监测服务”是一项第三方托管式服务，该服务由绿盟科技安全监测专家团队远程为客户提供。当监测到用户网站遇到风险状况后，绿盟科技安全专家会在第一时间确认并通知用户，同时提供专业的解决方案建议。绿盟科技安全监测团队会定期为客户出具周期性的

网站安全监测报告，让用户掌握网站的风险状况及安全趋势。用户无需安装任何硬件或软件，无需改变目前的网络部署状况，就能将网站管理人员从繁重的日常安全维护工作中解放出来，降低投入和管理成本。

该服务产品主要包括以下几方面的内容：网页木马监测、页面篡改监测、敏感内容监测、页面平稳度监测以及周期性的应用漏洞扫描。与传统的安全评估服务相比，绿盟网站安全监测服务具有更为鲜明的特点:

一是基于绿盟科技云安全平台，提供不间断的风险监测能力。众所周知，网站挂马、页面篡改都是实时性很强的安全事件，而不定期的评估扫描并不能帮助用户实时发现这些安全事件。而绿盟安全监测服务能够为客户提供 7×24 小时不间断的风险监测能力，及时发现风险并通知用户，降低或避免用户损失。

二是托管式安全服务。由绿盟科技专家团队协助用户解决一切问题，就如同一个私人的网站安全管家。通过可靠的、免操作式 “SaaS” 交付模型提供出色的网站安全监测服务，用户无需过多投入管理精力。实时监测、预警通告、分析报告等每一步过程都由值得信赖的安全专家来帮助用户完成。

三是透明化。使用此托管服务直接让绿盟科技安全专家发现并解决问题，无需改变现有网络结构和管理体系，服务的部署快捷方便，让用户运维轻松自在。

作为国内信息安全的领导厂商，绿盟科技一直关注应用层安全的研究，针对 Web 应用，已经形成了从 “漏洞扫描”、“配置管理”、“威胁防护” 到 “实时监测”，全方位的 Web 应用安全解决方案布局，真正实现了为客户的网站安全保驾护航。

NSFOCUS 2010年4月之十大安全漏洞

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

1. 2010-04-19 Oracle 2010 年 4 月更新修复多个 Oracle Database 安全漏洞

NSFOCUS ID: 14842

http://www.nsfocus.net/vulndb/14842

综述:

Oracle 是大型的商业数据库系统。

Oracle 数据库的 Oracle Internet Directory、Core RDBMS、XML DB、Change DataCapture 和 Audit 组件中存在多个安全漏洞，通过认证的远程用户可以通过 LDAP 或 OracleNet 协议来利用这些漏洞访问或操控数据库中的某些数据。

危害:

远程攻击者可以利用这些漏洞对数据库进行非授权的访问。

2. 2010-04-14 Microsoft Windows 媒体单播服务远程栈溢出漏洞（MS10-025）

NSFOCUS ID: 14808

http://www.nsfocus.net/vulndb/14808

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 媒体单播服务（nsum.exe）处理 MMS TRANSPORT_INFO 报文的方式存在栈溢出漏洞。

危害:

远程攻击者可以通过向运行可选 Windows Media Services 组件（非默认安装）的 Windows 2000 Server SP4 系统发送畸形报文触发这个溢出，从而控制服务器系统。

3. 2010-04-16 Apple Type Services 服务嵌入式字体解析远程代码执行漏洞

NSFOCUS ID: 14838

http://www.nsfocus.net/vulndb/14838

综述：

Mac OS X 是苹果家族机器所使用的操作系统。Mac OS X 系统中所使用的 Apple Type Services 服务中存在索引错误。libFontParser.dylib 库的 TType1ParsingContext::SpecialEncoding() 方式在解析 PDF 文档的字体轮廓时，如果用户指定了大于 0x400 的偏移就会触发堆破坏。

危害：

攻击者可以诱使受害者打开包含恶意内容的 PDF 文档来利用此漏洞，从而控制受害者系统。

4. 2010-04-16 Adobe APSB10-09 更新修复多个安全漏洞

NSFOCUS ID: 14835

http://www.nsfocus.net/vulndb/14835

综述：

Adobe Acrobat/Adobe Reader 是非常流行的 PDF 文件阅读器。APSB10-09 更新修复了 Adobe Reader 和 Acrobat 中的多个安全漏洞，包括多个堆溢出、内存破坏问题。

危害：

攻击者可以诱使受害者打开包含恶意内容的 PDF 文档来利用此漏洞，从而控制受害者系统。

5. 2010-04-16 Helix Server 多个缓冲区溢出漏洞

NSFOCUS ID: 14834

http://www.nsfocus.net/vulndb/14834

综述：

Helix Server 是一款支持多格式、跨平台的流媒体服务器软件。Helix Server 的 NTLM 认证实现在处理无效的 base64 编码字符串时存在堆溢出，所捆绑的 AgentX++ 中 AgentX::receive_agentx 函数存在栈溢出和整数溢出漏洞。

危害：

远程攻击者可以通过向服务器提交恶意的请求来触发这些溢出，从而控制服务器系统。

6. 2010-04-14 Microsoft Windows MP3 音频解码器栈溢出漏洞（MS10-026）

NSFOCUS ID: 14809

http://www.nsfocus.net/vulndb/14809

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 中所使用的 MP3 编码解码器处理 AVI 媒体文件的方式中存在栈溢出漏洞。

危害：

攻击者可以诱使受害者打开包含 MP3 音频流的特制的 AVI 文件来利用此漏洞，从而控制受害者系统。

7. 2010-04-06 Microsoft IE 未初始化内存远程代码执行漏洞（MS10-018）

NSFOCUS ID: 14744

http://www.nsfocus.net/vulndb/14744

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 web 浏览器。Internet Explorer 访问尚未正确初始化或已被删除的对象的方式中存在多个远程执行代码漏洞。

危害：

攻击者可以诱使受害者打开包含恶意内容的网页来利用此漏洞，从而控制受害者系统。

8. 2010-04-07 Discuz! 论坛个人签名持久性跨站脚本漏洞

NSFOCUS ID: 14759

http://www.nsfocus.net/vulndb/14759

综述：

Discuz! 是一款华人地区非常流行的 Web 论坛程序。Discuz! 个人中心里的“个人签名”没有对恶意代码进行检测，在 Discuz! 及 img 代码禁用的情况下仍可写入恶意代码，Discuz! 会保存并执行该代码，导致持久性跨站脚本。

危害：

攻击者可以利用此漏洞向 Discuz! 论坛页面注入恶意代码，盗取受害者的用户信息或进行恶意操作。

9. 2010-04-07 Firefox 浏览器引擎多个内存破坏漏洞

NSFOCUS ID: 14748

http://www.nsfocus.net/vulndb/14748

综述：

Firefox 是一款流行的开源 WEB 浏览器。Firefox 浏览器引擎的多个函数在处理超长输入参数时存在多个内存破坏漏洞。

危害：

攻击者可以诱使受害者打开包含恶意内容的网页来利用此漏洞，从而控制受害者系统。

10. 2010-04-02 Foxit Reader 执行内嵌可执行程序漏洞

NSFOCUS ID: 14737

http://www.nsfocus.net/vulndb/14737

综述：

Foxit Reader 是一款小型的 PDF 文档查看器和打印程序。出于安全考虑 Foxit Reader、Adobe Reader 等阅读器不允许执行 PDF 文档中内嵌的可执行程序（如二进制程序和脚本），但攻击者可以使用特殊技术绕过这种安全机制启动命令（/Launch /Action），最终执行内嵌的可执行程序。Foxit Reader 不会给出任何提示。

危害：

攻击者可以诱使受害者打开包含恶意内容的 PDF 文档来利用此漏洞，从而控制受害者系统。

NSFOCUS 2010年5月之十大安全漏洞

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

1. 2010-05-10 QQ 旋风下载链接处理缓冲区溢出漏洞

NSFOCUS ID: 14974

http://www.nsfocus.net/vulndb/14974

综述:

QQ 旋风是腾讯公司 08 年底推出的新一代互联网下载工具。QQ 旋风在处理下载链接时存在栈缓冲区溢出漏洞。

危害:

远程攻击者可以通过诱使用户访问恶意网页来触发这个漏洞，从而控制用户系统。

2. 2010-05-21 nginx 文件路径处理远程命令执行漏洞

NSFOCUS ID: 15077

http://www.nsfocus.net/vulndb/15077

综述:

nginx 是多平台的 HTTP 服务器和邮件代理服务器。nginx 可以被配置为以 CGI 的方式支持 PHP 的运行，nginx 在处理 PHP 脚本文件路径的解析时存在问题。如果网站允许上传文件，而且上传文件路径可得到，远程攻击者可以利用此漏洞上传包含恶意代码的文件并得到执行，实现以 Web 进程权限执行任意命令。

危害:

远程攻击者可能利用此漏洞控制服务器系统。

3. 2010-05-24 多家厂商 rpc.pcnfsd 服务整数溢出漏洞

NSFOCUS ID: 15091

http://www.nsfocus.net/vulndb/15091

综述:

rpc.pcnfsd 是一个在网络上提供认证和打印服务的 RPC 守护进程，运行在大量 Unix 类操作系统上。多个厂商的 Unix 系统中所使用的 rpc.pcnfsd 服务在处理 RPC 请求时存在整数溢出漏洞。

危害:

远程攻击者可以通过发送特制的 rpc 请求来触发此漏洞，从而

控制服务器系统。

4. 2010-05-13 HP OpenView 网络节点管理器 getnnmdata.exe MaxAge 参数远程栈溢出漏洞

NSFOCUS ID: 15010

http://www.nsfocus.net/vulndb/15010

综述:

HP OpenView 网络节点管理器（OV NNM）是 HP 公司开发和维护的网络管理系统软件，具有强大的网络节点管理功能。OV NNM 中所使用的 getnnmdata.exe 服务进程中存在栈溢出漏洞。如果使用无效的 MaxAge 参数请求了这个 CGI 的话，就会调用 sprintf() 记录错误，未经检查就把无效的 MaxAge 参数拷贝到了固定长度的栈缓冲区。

危害:

远程攻击者通过提交超长的 HTTP POST 请求触发此漏洞，从而控制服务器系统。

5. 2010-05-13 MySQL COM_FIELD_LIST 命令远程溢出漏洞

NSFOCUS ID: 15005

http://www.nsfocus.net/vulndb/15005

综述:

MySQL 是一款使用非常广泛的开放源代码关系数据库系统，拥有各种平台的运行版本。MySQL 在处理超长表格名称参数时存在缓冲区溢出漏洞。

危害:

远程攻击者可以通过向服务器提交包含有超长表格名称参数的 COM_FIELD_LIST 命令触发此漏洞，从而控制服务器系统。

6. 2010-05-12 Microsoft Visual Basic for Applications 文本解析栈溢出溢出漏洞（MS10-031）

NSFOCUS ID: 15001

http://www.nsfocus.net/vulndb/15001

综述:

Microsoft Visual Basic for Applications（VBA）是用于开发客户端桌面所包装的应用程序并集成到现有数据和系统的开发技术。在搜索支持 VBA 的文档（如 Office 文档）中的 ActiveX 控件时 VBA 所使用的 VBE6.dll 库中的文本解析代码存在单字节栈溢出漏洞。

危害:

远程攻击者可以通过诱使用户打开特制的文件来触发这个漏洞，从而控制用户系统。

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

NSFOCUS ID: 15002

http://www.nsfocus.net/vulndb/15002

综述:

Outlook Express 和 Windows Mail 都是 Windows 操作系统中默认捆绑的邮件和新闻组客户端。Outlook Express 和 Windows Mail 客户端所使用的通用库验证特制邮件响应的方式存在整数溢出漏洞。

危害：

如果用户受骗使用 POP3 和 IMAP 邮件协议连接到了恶意的服务器并收到了畸形的 STAT 响应就会触发这个溢出，可能导致在用户系统上执行任意代码。

8. 2010-05-13 Adobe Shockwave Player 嵌入式字体解析堆溢出漏洞

NSFOCUS ID: 15017

http://www.nsfocus.net/vulndb/15017

综述：

Adobe Shockwave Player 是专门播放使用 Director Shockwave Studio 制作的网页的外挂软件。Shockwave 处理文件中嵌入式字体时存在堆溢出漏洞。

危害：

远程攻击者可以通过诱使用户访问恶意网页来触发这个漏洞，从而控制用户系统。

9. 2010-05-10 Apple Safari window.parent.close() 远程代码执行漏洞

NSFOCUS ID: 14982

http://www.nsfocus.net/vulndb/14982

综述：

Safari 是苹果家族机器操作系统中默认捆绑的 WEB 浏览器。Safari 在处理父窗口时存在错误，可能导致以无效的指针调用 window.parent.close() 函数。

危害：

用户受骗访问了恶意网页并关闭了弹出窗口时就可以触发这个漏洞，导致执行任意代码。

10. 2010-05-05 Samba mount.cifs 工具符号链接攻击本地权限提升漏洞

NSFOCUS ID: 14946

http://www.nsfocus.net/vulndb/14946

综述：

Samba 是一套实现 SMB（Server Messages Block）协议、跨平台进行文件共享和打印共享服务的程序。Samba 的 mount.cifs 工具中的 client/mount.cifs.c 文件存在安全漏洞，本地用户可以通过对加载点目录文件执行符号链接攻击导致在任意加载点上加载 CIFS 共享，获得权限提升。

危害：

本地攻击者可以利用此漏洞对服务器资源进行非授权的访问。

NSFOCUS 2010年6月之十大安全漏洞

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

1. 2010-06-11 Windows 帮助和支持中心绕过白名单限制漏洞

NSFOCUS ID: 15211

http://www.nsfocus.net/vulndb/15211

综述 :

Windows 是微软发布的非常流行的操作系统。Windows 中默认提供了帮助和支持中心以访问在线文档，可通过 hcp:// 形式的 URL 直接访问帮助文档。在通过注册的协议处理器调用 hcp://URL 时，会向帮助中心应用传送命令行参数 /fromhcp，这个标记将帮助中心切换到受限制的模式，仅允许白名单中的帮助文档和参数。但这个白名单实现并不安全，可能被绕过。

危害 :

攻击者可以诱使受害者查看特制的 hcp:// 帮助链接来利用此漏洞，从而控制受害者系统。

2. 2010-06-08 Adobe Flash Player AVM2 newfunction() 函数远程代码执行漏洞

NSFOCUS ID: 15193

http://www.nsfocus.net/vulndb/15193

综述 :

Flash Player 是一款非常流行的 FLASH 播放器。Flash 9 及之后版本中的 AVM2 将 ActionScript Bytecode（ABC）用作输入，并实时编译到处理器特定的指令中。由于 AVM2 在处理 newfunction() 调用时错误地计算了指针位置且之后使用该指针获得对象引用，这可能导致执行内存中受控的数据。

危害 :

攻击者可以诱使受害者察看特制的 swf 文件来利用此漏洞，从而控制受害者系统。

3. 2010-06-17 Samba SMB1 报文链接远程内存破坏漏洞

NSFOCUS ID: 15245

http://www.nsfocus.net/vulndb/15245

综述：

Samba 是一套实现 SMB（Server Messages Block）协议、跨平台进行文件共享和打印共享服务的程序。Samba 的 process.c 文件中 chain_reply 函数处理链接 SMB1 报文时没有正确地验证客户端所提供的输入字段，存在内存破坏漏洞。

危害：

远程攻击者可以向 Samba 服务器发送特制的 SMB 报文来利用此漏洞，从而控制服务器系统。

4. 2010-06-12 Excel DBQueryExt 记录 ADO 对象解析远程代码执行漏洞（MS10-038）

NSFOCUS ID: 15224

http://www.nsfocus.net/vulndb/15224

综述：

Excel 是微软 Office 套件中的电子表格工具。Excel 在解析电子表格中的 DBQueryExt 记录时没有正确地检查其中的 ADO 字段，可能导致调用用户所控制的指针。

危害：

攻击者可以诱使受害者打开特制的 Excel 文档来利用此漏洞，从而控制受害者系统。

5. 2010-06-11 Excel RTD 记录解析栈溢出漏洞（MS10-038）

NSFOCUS ID: 15216

http://www.nsfocus.net/vulndb/15216

综述：

Excel 是微软 Office 套件中的电子表格工具。Excel 在解析电子表格中的畸形 RTD（recType 0x813）记录时存在栈溢出漏洞。

危害：

攻击者可以诱使受害者打开特制的 Excel 文档来利用此漏洞，从而控制受害者系统。

6. 2010-06-10 Microsoft Office COM 对象验证远程代码执行漏洞（MS10-036）

NSFOCUS ID: 15203

http://www.nsfocus.net/vulndb/15203

综述：

Microsoft Office 是非常流行的办公软件套件。Office 中的组件在实例化对象时没有充分地验证 COM 对象，存在代码执行漏洞。

危害：

攻击者可以诱使受害者打开特制的 Office 文档来利用此漏洞，从而控制受害者系统。

7. 2010-06-10 Microsoft IE 未初始化内存远程代码执行漏洞（MS10-035）

NSFOCUS ID: 15208

http://www.nsfocus.net/vulndb/15208

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 web 浏览器。Internet Explorer 访问尚未正确初始化对象的方式中存在一个远程执行代码漏洞。

危害：

攻击者可以诱使受害者打开特制的网页来利用此漏洞，从而控制受害者系统。

8. 2010-06-21 PHP SplObjectStorage 解序列化程序远程安全漏洞

NSFOCUS ID: 15257

http://www.nsfocus.net/vulndb/15257

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 SplObjectStorage 解序列化程序中存在安全漏洞。如果对不可信任的数据使用了 PHP unserialize() 函数的话，攻击者就可以在服务器上导致信息泄露或执行任意代码。

危害：

远程攻击者可以向 PHP 提交特制的数据来利用此漏洞，从而控制服务器系统。

9. 2010-06-12 HP OpenView 网络节点管理器 ovutil.dll 模块远程栈溢出漏洞

NSFOCUS ID: 15225

http://www.nsfocus.net/vulndb/15225

综述：

HP OpenView 网络节点管理器（OV NNM）是 HP 公司开发和维护的网络管理系统软件，具有强大的网络节点管理功能。OV NNM 中由 ovwebsnmpsrv.exe 进程所加载的 ovutil.dll 模块中存在栈溢出漏洞。超长的变量会导致 sprintf 溢出静态的缓冲区。

危害：

远程攻击者可以向 OV NNM 发送包含超长变量的 HTTP 请求来利用此漏洞，从而控制服务器系统。

10. 2010-06-11 Microsoft IIS 认证令牌处理远程代码执行漏洞（MS10-040）

NSFOCUS ID: 15212

http://www.nsfocus.net/vulndb/15212

综述：

Microsoft Internet 信息服务（IIS）是 Microsoft Windows 自带的一个网络信息服务器，其中包含 HTTP 服务功能。IIS Web 服务器在解析从客户端所接收到了认证信息时没有正确地分配内存，存在远程代码执行漏洞。

危害：

远程攻击者可以向 IIS 服务器发送特制的认证报文来利用此漏洞，从而控制服务器系统。

巨人背后的专家

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

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

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

NSFOCUS

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com