安全+
SECURITY
2010/12 总第011
与安全人士分享技术心得 Share technique experience with security professionals

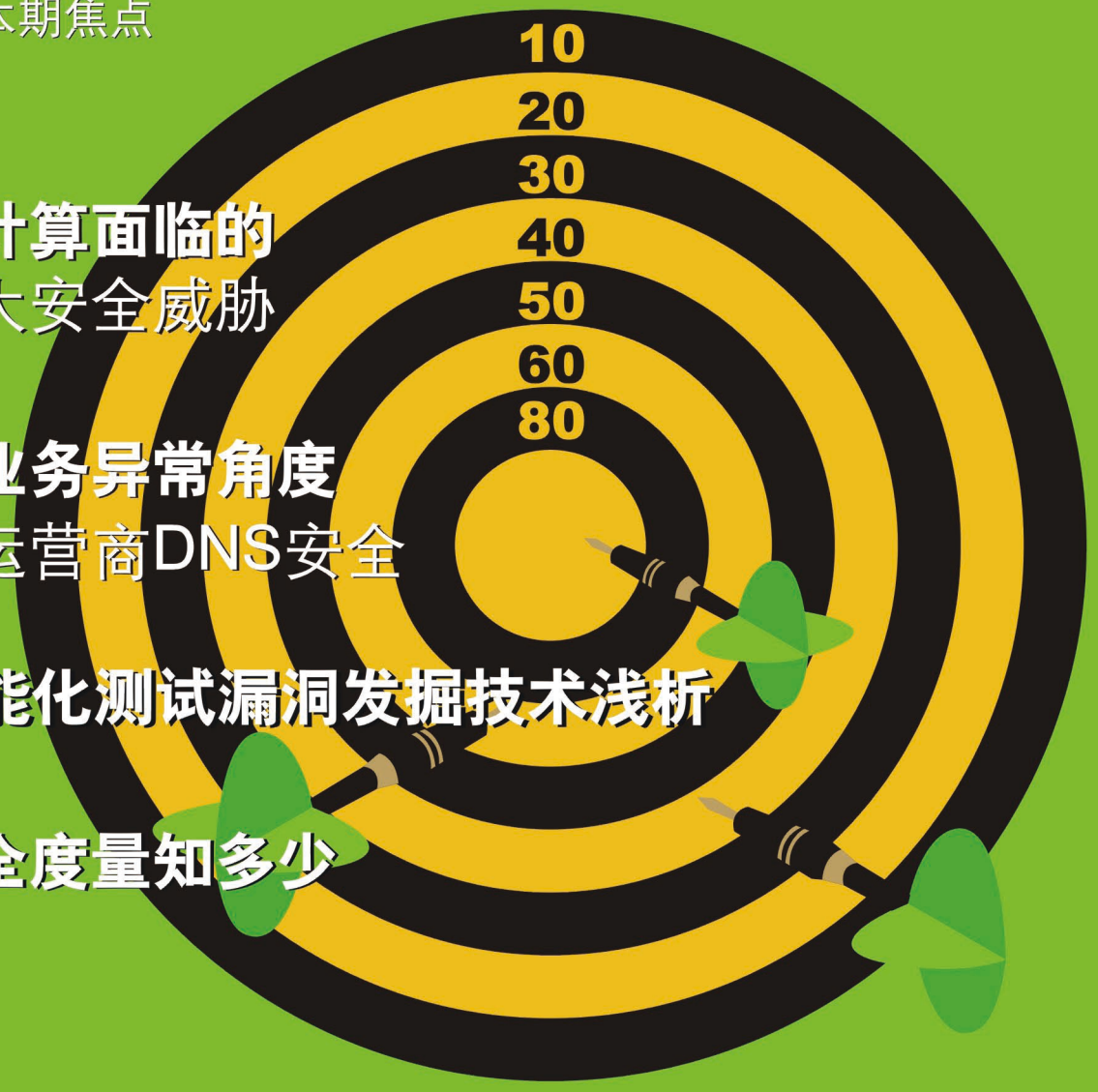
★ 本期焦点

云计算面临的七大安全威胁

从业务异常角度谈运营商DNS安全

智能化测试漏洞发掘技术浅析

安全度量知多少



NSFOCUS

本期看点 HEADLINES

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

Nsmagazine@nsfocus.com

2010/12 总第 011

安全+ SECURITY+

© 2010 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，
一概不得以任何形式、方法转载或使用。本刊保留所有版权。

SECURITY+ 是绿盟科技的注册商标。

需要获取更多信息，请访问WWW.NSFOCUS.COM

目录 CONTENTS

从业务异常角度谈运营商DNS安全

行业营销中心　唐洪玉

摘要：DNS 是十分重要的 Internet 基础设施，对互联网服务至关重要。保障 DNS 业务安全，对于运营商而言迫在眉睫。本文阐述了 DNS 业务的异常定义、异常分析、异常处理，从业务异常的角度给出了 DNS 业务安全防护的思路。

关键词：DNS　业务异常　防护体系　DDoS　缓存投毒

域名系统（DNS：Domain Name System）作为互联网基础设施，在互联网服务中占据着越来越重要的地位，对于运营商而言，保障域名系统的安全运行，对于维护互联网安全、提升客户感知、增加客户粘度具有非常重要的意义。

近期，互联网领域频繁发生 DDoS 攻击、缓存投毒、域名篡改等导致互联网断网或者重要应用无法访问等 DNS 安全事件。对运营商而言，进行 DNS 业务监控、保障 DNS 平稳运行，实现业务安全，是亟待需要解决的问题。

一、DNS 业务异常定义

1.1 DNS 系统的重要性

DNS 是 Internet 的一项核心服务，是十分重要的 Internet 基础设施，是 Internet 的基石，是互联网的起点和入口，更是全球互联网通信的基础，基于 Internet 的各种 Web 服务、Email 服务、路由服务都依赖或者间接依赖 DNS。

DNS 的作用相当于互联网的中枢神经系统，域名系统的故障会导致互联网陷入瘫痪。域名系统就像是“空气”，平时我们感觉不到它的存在，但是一旦出现问题，对互联网而言，其影响可能是“致命”的，而且损失巨大：例如“5.19 断网事件”，据有关人士估计，电信运营商损失约为 1.2 亿元，游戏运营商损失 1 亿元，网吧经营者损失约为 1000 万元。

1.2 DNS 系统面临的主要攻击及安全事件

目前，DNS 面临的安全攻击主要可以分为四类：拒绝服务类攻击、数据篡改类攻击、隐私类攻击、其他类攻击，下文将分别进行简要介绍：

(1) 拒绝服务类攻击：包括针对 DNS 的拒绝服务类攻击（如伪造源 IP DNS 攻击、DNS 畸形包 DoS 攻击、DNS Query Flood、随机域名 DNS Query Flood、UDP Flood、TCP(SYN、ACK、Connection) Flood 等等）、利用 DNS 的拒绝服务类攻击（反射攻击、放大攻击）、流量异常类拒绝服务攻击、缓冲区溢出类拒绝服务攻击等；

(2) 数据篡改类攻击：包括缓存中毒（或 DNS 欺骗）（Cache Poisoning or DNS Spoofing）、域名劫持（Domain Name Hijacking）、中间人攻击（Man in the Middle Attack）等;

(3) 隐私类攻击：如缓存窥探（Cache Snooping）等;

(4) 其他类：如 Fast Flux 网络等。

在互联网领域，发生的由 DDoS 攻击、缓存投毒、域名篡改等导致的 DNS 安全事件，层出不穷，例如:

• 2009 年，5.19 断网事件。

• 2009 年 10 月 12 日，瑞典当地时间 21 点 45 分，由于在日常维护中不正确的软件升级，顶级域名 .se 出现故障，导致整个瑞典互联网几乎完全瘫痪，所有的 .se 网站都无法访问。

• 2009 年 10 月 21 日，Yammer 由于 DNS 配置错误而经历了长时间的瘫痪。

• 2010 年 1 月 12 日，百度域名被篡改事件。

• 2010 年 2 月 8 日，印度最大的软件开发商塔塔 (Tata) 咨询服务公司网站遭黑客攻击，经证实攻击手段为 DNS 劫持。

• 2010 年 3 月 9 日，澳大利亚游戏网站 Ubisoft 遭受 DDoS 攻击。

• 2010 年 3 月 24 日，维基百科 Wikimedia 的 DNS 在做服务切换时发生配置错误，致使欧洲用户数小时无法访问维基百科网站。

• 2010 年 3 月 26 日，国外著名 VoIP 提供商 Line2 的域名系统遭受 DDoS 攻击。

• 2010 年 6 月 2 日，Netscape 网景公司的 DNS 服务遭受攻击并致瘫痪。

• 2010 年 8 月 7 日，国际知名 DNS 服务提供者 DNS Made Easy 遭受 DDoS 攻击，造成 1.5 小时的服务宕机。

1.3 安全问题引发的 DNS 业务异常

DNS 的安全问题通常会引起 DNS 的业务异常，使 DNS 系统不能提供正常的域名解析服务。那么，DNS 的业务异常是什么？又包括哪些异常呢？

DNS 业务异常，是指 DNS 系统不能为用户提供正常的解析服务，主要可以分为三种情况：服务可用性异常、解析结果异常、其他异常，以下将分别进行阐述说明:

1. 服务可用性异常

(1) 服务中断：DNS 系统由于主机软硬件故障、操作系统故障、BIND 等 DNS 服务系统软件故障、不明攻击等原因导致 DNS 系统宕机，不能提供服务。

(2) 服务时延大：DNS 系统由于遭受攻击、系统负荷过大等原因，导致 DNS 服务虽然可以提供，但是解析时延过大，即递归服务器域名解析响应时间大于或远大于 1500ms。

注：根据行标 YD/T 2052-2009《域名系统安全防护要求》，对 DNS 系统解析响应时间要求为：按月统计，95% 的权威服务器域名解析响应时间 <50Oms，95% 的递归服务器域名解析响应时间 <1500ms。

2. 解析结果异常

DNS 系统可以提供服务，但是由于遭受投毒、劫持、中间人攻击等原因导致所提供的域名解析结果是错误的。

3. 其他异常

根据 DNS 系统维护人员的维护经验，结合系统运行的主要性能指标等数据，判断 DNS 系统是否存在异常。

序号	异常分类		异常现象描述	造成该异常的可能原因
1	服务可用性异常	服务中断	服务中断，不能继续为用户提供服务	1）主机软硬件故障导致的系统宕机　2）BIND 崩溃　3）网络中断 4）DDoS 攻击：DDoS 反射攻击、伪造源 IP DNS 攻击、DNS 畸形包 DoS 攻击、DNS Query Flood、随机域名 DNS Query Flood、UDP Flood、TCP(SYN、ACK、Connection) Flood
2		服务时延大	响应时间过大，超过相关标准要求	1）系统负荷过高　2）遭受 DDoS 等攻击　3）网络链路故障
3			系统负荷过高	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值
4			解析成功率异常	1）遭受攻击　2）超出设定阈值
5			QPS 过载	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值
6			一定时间段内请求总量激增	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值
7			单个 IP 单位时间内的请求量过高	1）超出系统设计容　2）遭受 DDoS 等攻击　3）超出设定的阈值
8			某个域名单位时间内的请求量过高	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值
9			迭代应答 QPS 激增	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值阈值
10			迭代查询 QPS 激增	1）超出系统设计容量　2）遭受 DDoS 等攻击　3）超出设定的阈值阈值
11			非本地 IP 查询请求	系统未对查询用户的源 IP 做相应的限定
12	解析结果异常		解析错误	1）遭受投毒攻击　2）权威域名被篡改　3）中间人攻击
13	DNS 其他异常		BIND 存在漏洞	未及时打补丁
14			域名查询长度异常	未对域名查询长度进行限定
15			域名查询内容异常	为对查询内容进行限定

二、DNS 业务异常分析

基于前文对 DNS 业务异常的定义，下面来对其分类、现象、原因等进行详细的分析，为进一步的异常处理、安全防护提供基础和依据，详见上表。

三、DNS 业务异常处理

3.1 异常处理措施

前文对 DNS 业务异常的现象、原因等进行了分析，那么面对这些异常，如何应对呢？接下来，我们来寻求相应的应对方法和措施，进行业务异常的处理和应对。

一般而言，异常处理措施包括两个方面：一是提高系统的健壮性，增强攻击难度，减小异常出现的可能性；二是一旦攻击成功，异常出现，则应该降低损失，减小影响。同样，对于 DNS 业务异常的处理措施，也包括两大类：增强攻击难度、降低业务损失。

1. 增强攻击难度类措施

增强攻击难度类措施，主要包括业务监测、攻击防护、域名控制、安全基线管理，分别阐述如下:

(1) 业务监测：对 DNS 的业务状态进行实时监测，及时发现异常，主要监控指标包括查询量（总请求量、解析成功量 / 率、解析失败量 / 率、Nxdomain 率）、QPS、解析成功率、解析时延、根域查询分布率、Cache 命中率、TOPN 排名等等。

(2) 攻击防护：对常见的 DNS 攻击进行防护，主要包括 DDoS 攻击和缓存投毒攻击等。其中, DDoS 攻击又包括 DDoS 反射攻击、伪造源 IP DNS 攻击、DNS 畸形包 DoS 攻击、DNS Query Flood、随机域名 DNS Query Flood、UDP Flood、TCP(SYN、ACK、Connection) Flood 等。

(3) 域名控制：以域名为对象，进行限速等控制，如设定 QPS 阈值、设定单个 IP 单位时间内的请求量、设定某个域名单位时间内的请求量、限制非本地 IP 查询请求等。

(4) 安全基线管理：建立 DNS 系统安全基线，定期进行漏洞扫描、配置核查等工作，使 DNS 系统的整体安全状况处于既定水准。

2. 降低业务损失类措施

降低业务损失类措施，主要包括重点域名保护和域名容灾，分别阐述如下:

(1) 重点域名保护：对重点域名进行锁定，定期拨测，以防投毒、权威域名篡改等攻击成功后，依然可以提供正确的解析服务。

(2) 域名容灾：进行域名容灾备份，当 DNS 系统服务中断时，依然可以为用户提供正常的域名解析服务。

3.2 DNS 业务整体安全

一个完备的 DNS 系统保障体系，应该包括四个部分（策略体系、管理体系、技术体系、运作体系）、四个层次（物理安全、网络安全、主机安全、应用及数据安全）和三个阶段（安全评估、安全防护、安全运维），它们共同构成一个有机的整体，协同作用，使 DNS 系统可以提供高可靠性、高可用性、高连续性的 DNS 服务。

此外，从时间纬度，分成安全评估、安全防护、安全运维三个阶段，来看如何对 DNS 的业务进行全面整体的防护，如右图所示:

在安全评估阶段，从网络、主机、应用、数据、管理等层面，对 DNS 系统进行全面的安全评估，提出风险处置计划，可以采取的具体技术措施包漏洞扫描、配置核查等。

	安全评估	安全防护			安全运维
		保护	检测	响应	
内容	从网络、主机、应用、数据、管理等层面，对DNS系统进行全面的安全评估，提出风险处置计划	对DNS系统进行全面的实时安全防护，使其“不瘫、不错、可视”：（1）有效抵御DDoS、缓存投毒等攻击；（2）针对性的域名控制；（3）监控可视化。			从安全角度，完善DNS系统运维工作，达到DNS安全基线管理目标
技术措施	• 漏洞扫描 • 安全配置核查	• 攻击防护 • 域名控制	• 业务异常检测 • 域名控制	• 域名容灾 • 域名控制 • 攻击防护	• 业务可视化监控 • 安全配置核查 • 漏洞扫描
服务	• 安全评估服务 • 渗透测试	• 安全加固 • 安全值守	• 系统监控	• 安全事件处理 • 应急响应	• 安全值守 • 应急响应 • 事件追溯

DNS 安全整体防护思路

在安全防护阶段，对 DNS 系统进行全面的实时安全防护，使其达到“不瘫、不错、可视”的目标，即有效抵御各类攻击、域名控制、可视化业务监控，可以采用的具体技术措施包括攻击防护、域名控制、业务监测、域名容灾、重点域名保护等。

在安全运维阶段，主要是从安全角度，完善 DNS 系统运维工作，依托技术从管理上保障 DNS 业务的正常运行，达到 DNS 安全基线管理目标，采取具体的技术措施包括业务可视化监控、漏洞扫描、配置核查等。

本文从“异常”的角度，阐述了 DNS 业务的异常定义、异常分析、异常处理，进而给出了 DNS 安全整体防护的解决思路，希望可以给运营商一个有益的借鉴。

出招金融行业IT风险管理

行业技术部　徐一丁

摘要：本文简要介绍了当前银行、证券、保险三大子行业中 IT 风险管理和信息安全的状况，包括标准规范、行业机构的安全需求和今后的发展等内容。

关键词：银行　证券　保险　IT 风险管理　信息安全

金融行业相关标准规范的建设

从 2008 年开始，国内金融机构的 IT 风险管理与信息安全建设逐步进入了高峰。

银行业以《商业银行信息科技风险管理指引》为主线，已经从 2006 年开始了 IT 风险管理，2009 年借《指引》迎来更新的机会，又开始了新一轮检查，今后将把 IT 风险管理长期做下去。根据监管部门要求，各银行业金融机构要将信息科技规划纳入总体发展战略，将信息科技风险纳入全面风险管理，切实加强信息科技治理、内控机制和合规建设，建立和完善信息科技管理决策监督和激励约束机制，切实提高信息科技创新能力和治理水平。

证券期货业在奥运前后大力推进各类行业标准法规的建设，从 2008 年开始以《证券期货经营机构信息技术治理工作指引（试行）》（包含 IT 安全和风险控制）为主线，结合《证券公司分类监管规定》，以证券公司为主要监管群体进行 IT 风险和信息安全的管理工作。对具体工作的标准规范有《集中交易系统安全管理指引》、《证券公司网上证券信息系统技术指引》等。

保险业在 2006 年开展了全行业范围的“保险信息系统安全检查”，在这之后，主要以内部网络安全通告的形式，对一些近期内发生频度较高的事件进行提示，要求各保险机构注意防范，同时也非常重视保险公司的灾备系统建设。2010 年 1 月保监会发布了《保险公司信息化工作管理指引》，其中包含了对信息安全建设的要求，加强信息系统风险管理，确保信息系统安全、稳定运行，不过还没有出台专门的信息安全相关标准或规范。

一些大型保险集团公司在 IT 安全建设方面明显领先于同业机构。如以 ITIL 为纲领建立 IT 治理与建设的框架，加强业务能力、服务能力和资源能力的管理，将 IT 风险等包括进去，集团内成立专门的信息科技公司来负责各成员公司的 IT 相关工作，形成了一套很完善且行之有效的体系。

金融机构 IT 风险管理与信息安全需求

金融机构进行 IT 风险和信息安全建设的两个基本驱动力是“满足合规”和“保障安全”。如果两个目标只留下一个，那就是安全保障，合规要求是监管部门为了行业整体的 IT 风险得到控制而要求大家都达到的基线，还是会从 IT 风险管理的角度提出要求。

对金融机构来说，IT 风险管理的两个核心目标是“数据安全”和“业务持续”。数据安全是指金融机构业务经营相关的重要数据（尤其是客户数据）的保密性、完整性和可用性；业务持续是指根据金融机构的自身业务需求，将相关资源组织整合来保证业务按预期正常运行，其中 IT 系统是非常重要的资源。

银行和证券公司是业务高度 IT 化的企业，对业务持续的要求极高，其核心系统宕机哪怕几分钟，都可能面临难以估量的损失。证券公司作为投资者的“代理人”，通过自己在交易所的席位将投资者股票买、卖的请求投入市场，是投资者与股市操作联系的唯一纽带，一旦这个纽带在股价瞬息万变的开市期间断裂，投资者无法及时操作造成的损失无法估量；而银行是各类金融活动的支付、结算中心，如果在高峰期停止运作，会造成企业没法划拨货款、用户没法交水电费、在线支付和网上商城停业等等情况，其中后果最严重的可能是证券交易保证金的第三方存管业务，不能提供这项业务，股票的买卖同样无法进行，这与证券公司面临同样的压力。

银行和证券公司非常重视 IT 系统对业务持续性的支撑，因为这方面环节多、风险点多、后备资源难以完备，从业内有影响的事件来看，业务中断事件也高于数据安全事件。而且银行和证券公司业务系统中断后会有立即的影响，并随着时间推移迅速扩大，现场处理的压力巨大。即使问题能够得到解决，机构的信誉与企业评价也将大受影响，并面临监管部门的严厉措施。而数据安全方面面临的威胁相对较少，出了事件也较容易控制。

而保险公司风险管理的要求与银行、证券公司有很大不同，更多的集中在数据安全而不是业务持续上。如果把银行和证券公司的业务持续和数据安全的关注度大致分为“64 开”（甚至是“73 开”），那么保险大概是“28 开”，这是由于保险公司对 IT 系统业务持续的要求不高。目前国内保险产品的销售，无论人寿健康、财产、意外等险种，都需要经验丰富的业务人员根据客户需求定制，存在一个较长的沟通与明确过程，客户火急火燎地要在一天之内搞定合同的情况不多。因此保险业务对交易的实时性没有很高的要求，今天下单与明天下单没什么区别，这种情况是不太可能在证券公司出现的。

此消彼长，数据安全在保险公司的 IT 风险管理和信息安全中就占据了主要位置。如 2009 年 12 月，泰康人寿保险公司副总裁王道南先生在谈到金融保险行业信息安全就重点强调了数据安全:

“我们的客户信息是最重要的资产，一个客户的信息可能占不到 1KB，可能两千万的客户一张 U 盘就带走了，2000 年的时候我到日本的第一生命公司拜访，它是日本最大的保险公司，比我们大很多。我去拜访的时候，他们所有的员工在电脑里是不能使用 U 盘的，对外发一个 E-Mail 直属上司会拿到一个 Copy 的。比如他们的电脑坏了也很简单，拿一台新的电脑跟你换，把你坏的拿走，全公司 4 万多台的电脑，因为它是标准化的，没有从外面来新的系统，发的 E-mail 全部存在网络里你也带不走。当时非常压抑，为什么做到这么严格，他们讲一个例子我印象非常深刻，日本的一个县市政府里面的一个实习生用一个 U 盘把市里面 21 万个市民的资料全部带走，卖给了一家名单公司只卖了 30 万日元，当这件事情发现以后法院判决市政府要向每一位市民赔偿 1.5 万日币，

但是这样市政府就快破产了，如果是企业就了不得了，我们泰康有将近 2000 万的客户，到时候不知道能不能赔出来。”

这种情况也导致了保险业整体对 IT 风险管理的要求有别于兄弟行业。

金融行业 IT 风险管理和信息安全发展

金融 IT 风险管理和信息安全是业界非常关注的课题，业内机构和专业公司都在不断地实践与探索，但仍然对此工作的发展存在着不同看法。我们谨提出两个值得重点关注的关键性问题，供大家参考:

将 IT 风险纳入金融机构整体风险管理体系

金融机构是经营风险的，无论从业务特点还是监管部门的要求看，IT 风险管理都应是银行整体风险管理工作中的一部分，而且将占据越来越重要的位置。根据巴塞尔协议，银行操作风险是指由于银行内部流程、人员和系统不适当或者失效，而造成银行直接或者间接损失风险，包括法律和监管风险。从流程上说，银行的 IT 属于内部流程，因而 IT 风险归为操作风险。IT 风险层层地纳入 IT 风险 - 操作风险 - 保险公司大风险管理的体系当中去。

银监会相关领导已经在 2011 年 10 月举行的中国银行业信息科技风险管理年会上正式提出此思路，要求“各银行业金融机构要将信息科技规划纳入总体发展战略，将信息科技风险纳入全面风险管理”，预计证券期货业和保险业也将明确这一思路。

重视网上金融系统的安全建设

互联网和今后的无线互联网，必将成为金融业务最倚重的平台之一。

国内网上金融业务开展如火如荼。据中国金融认证中心（CFCA）介绍，2009 年我国网上银行市场交易金额已超过 400 万亿元，而 2011 年预测将达到 1100 万亿元；证券公司的网上交易量已经占有其总交易量的 60%~90%，成为主要业务收入来源；发展相对较慢的网上保险也已经开始制造声势，一些有实力的保险业机构借助网上平台强力推动某些标准险种，如车险的销售，其发展前景可以参考网上保险很发达的美国：部分险种的网上交易额已占到 30% ~ 50% 市场份额。

网上金融向广大用户开启了方便之门，也第一次将金融机构的业务系统与互联网这个“危险的漩涡”直接相连，使网上金融面临前所未有的安全考验。“连接到互联网了，我们将面临什么攻击？应如何应对？”这已经成为新建网银系统时，IT 安全负责人问的最多的问题。

网上金融系统需要应对来自任意地点的攻击，而且攻击者众多、手法更新速度很快。互联网中的地下黑金产业链已经是业内共知的事实，相对以前为了泄愤或炫耀而去攻击网站的“江湖行为”，现在默默地攻击和获利是攻击者更愿意做的事：“搞定一个网上金融系统，就可以得到钱”，这给了地下产业者最强的驱动力。

因此，相对以前封闭的业务系统，网上金融系统将面临更多的威胁，更为攻击者威胁内部系统提供了可能的途径。金融机构需要从网络安全域、系统加强和应用保护等各个层面设计安全防护措施来达到安全目标。我们将在下一期绿盟科技技术刊物中以网上银行系统为例，详细介绍网上金融系统的安全防护体系。

业务系统安全基线的研究及应用

行业营销中心　田民

摘要：安全基线是一个业务系统的最小安全保证，即该业务系统最基本需要满足的安全要求。在运营商领域，安全基线的应用范围非常广泛，主要包括新业务系统的上线安全检查、第三方入网安全检查、合规性安全检查（上级检查）、日常运维检查 / 评估等。通过对目标系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险，并通过对历史数据的分析获得业务系统安全状态和变化趋势。

关键词：SCAP　安全基线　安全合规检查　入网安全检查　日常运维安全评估

一．安全基线的技术背景

FISMA 的全称是 The Federal Information Security Management Act，联邦信息安全管理法案，是由美国国家标准和技术研究所 (NIST) 牵头制定。FISMA 把责任分配到各种各样的机构上来确保联邦政府的信息系统和数据安全。FISMA 的推出使得一直忽视计算机安全的联邦政府开始关注计算机安全。

FISMA（The Federal Information Security Management Act）提出了一个包含八个步骤的信息安全生命周期模型，这个模型的执行过程涉及面非常广泛且全面，但实施、落地的难度也非常大。如图 1.1 所示，FISMA 规范落地的过程好像从高空到地面，真正实施起来非常复杂。

为了实现 FISMA 法案的落地，由 NIST 牵头针对其中的技术安全问题提出了一套自动化的计划称为 ISAP（information security automation program）来促进 FISMA 的执行，ISAP 出来后延伸出 SCAP 框架（security content automation protocol），SCAP 框架

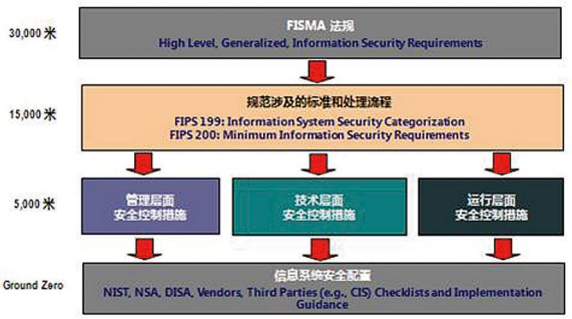


图 1.1　FISMA 法案的落地

由 CVE、CCE、CPE、XCCDF、OVAL、CVSS 等 6 个支撑标准构成。这 6 个支撑标准需要检查的内容、检查的方式由 NVD 和 NCP 来提供，由此 SCAP 框架就实现了标准化和自动化安全检查，及形成了一套针对系统的安全检查基线。

SCAP 及安全基线的最重要成果和成功案例当属 FDCC（Federal Desktop Core Configuration，联邦桌面的核心配置）项目，FDCC 是在美国政府支持下建立的桌面系统（Windows XP、Windows

vista 等）相关安全基线要求规范，并通过自动化的工具进行检查。FDCC 基于 NVD、NCP 等内容进行基线安全核查。NVD（National Vulnerability Database，国家漏洞数据库）为自动化漏洞管理、安全评估和合规性检查提供数据支撑，包含安全核查名单、与安全相关的软件漏洞、配置错误以及量化影响等。NVD 针对数据库中的漏洞等提出了一整套核查名单（Checklist），划归到 NCP（National Checklist Program）计划中。简言之 FDCC 体现了两个方面的特性:

(1) 标准化：在 NVD、NCP 的基础上，构建了一套针对桌面系统的安全基线（检查项），这些检查项由安全漏洞、安全配置等有关检查内容构成，为标准化的技术安全操作提供了框架。

(2) 自动化和工具化：通过自动化的工具来执行，为自动化的技术安全操作提供支持。

如图 1.2 所示，为 NVD 和 NCP 的逻辑关系图:

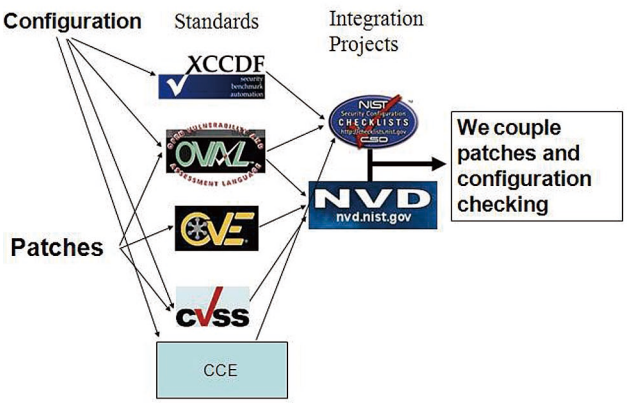


图 1.2 NVD 和 NCP 示意图

综上，安全基线的重要理论基础之一就是美国的 NVD 以及 SCAP 体系。安全基线在运营商行业的业务系统中具有广泛的应用价值，比如某运营商的 WAP 系统在各省级公司中的业务应用环境、网络连接情况、内部组网结构、内部系统构成等都存在很大的相似性，因此这就为构建一套运营商自身业务系统的“SCAP”计划提供了基础。

二．安全基线的定义

安全基线是一个业务系统的最小安全保证，即该业务系统最基本需要满足的安全要求，构造业务系统安全基线是系统安全工程的首要步骤，同时也是进行安全评估、发现和解决业务系统安全问题的先决条件。

2.1 安全基线的框架

在充分考虑行业的现状和行业最佳实践，并参考了运营商下发的相关安全政策文件，继承和吸收了国家等级保护、风险评估的经验成果等基础上，构建出基于业务系统的安全基线模型（如图 2.1 所示）。

安全基线模型以业务系统为核心，自上而下分为需求、分类和实现三层架构:

(1) 第一层是安全需求，这个层面中主要是根据不同业务系统的特性，定义不同安全防护的要求，是一个比较宏观的要求，体现在业务系统在账号权限、访问控制、安全审计以及状态监控方面的要求;

(2) 第二层是模块分类，将上一层（即安全需求层）的诸多要求

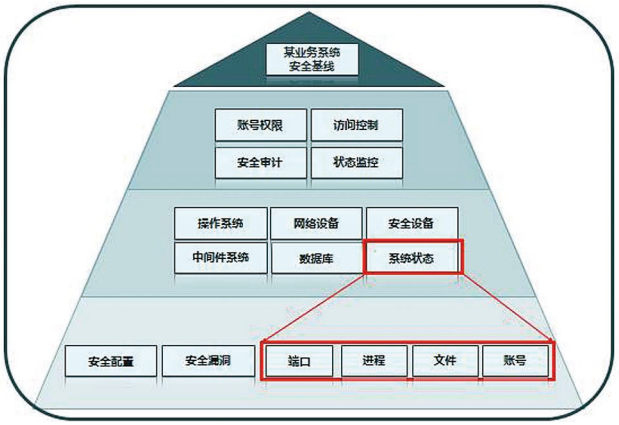


图 2.1 基线安全模型

分解为相对应的应用系统、数据库、操作系统、网络设备、安全设备等不同的设备和系统模块，这些模块针对安全需求定义的安全防护要求细化为不同模块应该具备的要求。

(3) 第三层是基线规范层，将第二层根据业务系统的特性进一步分解，如将对操作系统的要求分解为对具体的 Windows、Solaris 等操作系统模块的要求，将对网络设备的要求分解为华为路由器、Cisco 路由器等系统模块的要求，以及对业务状态的监控要求分解为端口、进程、文件和账号状态的监控要求。这些模块中又具体的把第二层的安全防护要求细化到可执行和实现的要求，称为 Windows 安全基线、华为路由器安全基线、系统状态基线等。以系统状态为例，系统状态安全基线体现了对业务系统运行和工作中的实际状态的监控要求，如开放了哪些端口和进程、对重要文件变化的监控以及系统账号变化的监控等。

2.2 安全基线的内容

从具体的内容角度上讲，我们将安全基线的内容分为三个方面:

(1) 系统存在的安全漏洞;

(2) 系统配置的脆弱性;

(3) 系统状态的监控。

业务系统的安全基线由以上三方面必须满足的最小要求组成。具体组成如图 2.2 所示:

具体来说，安全基线三个组成部分的内容分别为:

(1) 安全漏洞：漏洞通常是由于软件或协议等系统自身存在缺陷引起的安全风险，一般包括了登录漏洞、拒绝服务漏洞、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。漏洞信息一般基于相应的国际标准，如 CVE（Common Vulnerabilities & Exposures)。

(2) 安全配置：通常都是由于人为操作的疏忽造成，主要包括了账号、口令、授权、日志、IP 通信等方面内容，反映了系统自身的安全脆弱性。

(3) 系统状态：包含系统端口状态、进程、账号以及重要文件变化的监控等。这些内容反映了业务系统当前所处环境的安全状况，有助于我们了解业务系统运行的动态情况。由于系统状态基线随着业务应用不同而不同，必须和具体的业务应用相关联。

业务系统的安全基线建立起来后，可以形成针对不同系统的详细漏洞要求、配置要求和状态要求的检查项（Checklist)，为标准化和自动化的技术安全操作提供可操作和可执行的标准。

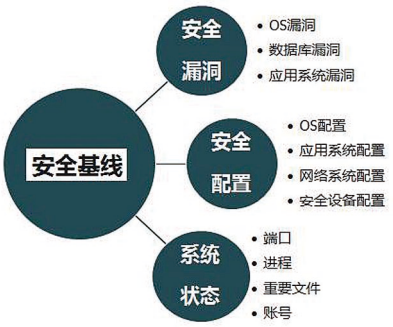


图 2.2 安全基线的组成

三．安全基线与业务系统的结合

从上文中可见，安全基线体现了业务系统最基本的安全需求，从漏洞、安全配置和系统状态三个方面。需要注意的是，安全基线并不是单纯网络层、系统层或应用层的概念，必须与具体的业务应用结合，体现具体业务系统安全状况。换个角度讲，一定程度上体现了业务系统的安全状态。

以 WAP 系统为例。WAP 系统中的关键业务应用主机，从类型上划分，主要包括 WAP 网关服务器、数据库服务器和报表服务器等，除此之外，还包括路由器、交换机、防火墙等网络设备。这些关键服务器和网络设备的安全基线既包括通用 / 标准的网络、系统和应用层面的要求，也可以从业务运行息息相关的业务层面的变化（如端口的变化、进程的变化、账号和文件的变化等）发现安全威胁的端倪。

3.1 安全基线的建立

如上文所述，安全基线包括三个部分：

(1）安全漏洞基线；

(2）安全配置基线；

(3）系统状态基线。

其中，安全漏洞基线建立的时候，首先需要满足和符合安全规范要求，并且考虑漏洞修补技术原因，限定资产出现漏洞的范围，此范围作为资产在安全漏洞方面的最低标准，即漏洞基线。一般使用漏洞白名单作为漏洞基线的标准实现。而安全配置基线是指为满足一点的安全规范要求，资产安全配置必需达到的标准，一般通过检查各安全配置参数是否符合标准来度量。

在安全基线与业务系统相结合过程中，最重要也是最关键的内容体现在系统安全状态的基线要求上。系统安全状态是指特定资产上包含的进程白名单、端口白名单、账号白名单、重要文件列表等的集合，作为安全检查的度量维度，称作状态基线。其中进程白名单对于特定类型资产，根据其服务或应用属性，限定该资产允许运行的进程集合；端口白名单是对于特定类型资产，根据其服务或应用属性，限定该资产允许开放的端口集合。端口通常和进程有关联关系；账号白名单是指对于特定资产，根据其资产应用属性，使用人范围等情况，限定该资产上所创建的系统登录账号、应用服务登录账号的集合；重要文件列表是指对于特定类型的资产，根据其系统、服务属性，通常一些重要文件经过配置后不经允许的更改为非法操作，重要文件列表是为保护和监视这些重要文件改动情况建立的文件快照列表。其他与业务系统安全状态相关的因素还有一些，这里不再一一赘述。

3.2 安全基线的动态变更

安全基线也不是一成不变的。在应用安全基线进行评估和检查工作时，可以预见的难题可能在于，由于各个业务系统、各个设备由于业务应用和功能实现的不同，安全要求也不同；同一设备随着应用的改变，安全

要求也随之改变。因此每次使用同一安全基线进行检查，就会重复出现一些已经确认过的风险，而一些新出现的风险却又未加进检查范围内。比如升级或扩容等工作都有可能引入新的安全风险。

我们在建立安全基线并进行安全评估后，系统管理员、安全人员对评估结果进行确认，如果有需要忽略或新增的项目，就调整并保存到基线数据库中，这个基线就是初始基线。在之后日常的检查和评估工作中，生成的新的评估 / 检查结果与初始安全基线可能存在偏差。这时候管理员或安全人员需要对评估结果进行确认。如果有需要忽略或新增的项目，就保存到基线库形成新的基线；如果没有任何基线项目需要变更，则延用当前基线。如此循环，使用来参照的安全基线能够随着系统变化而动态变化。

四 . 安全基线在业务系统中的应用

业务系统的安全基线建立起来后，可以形成针对不同系统的详细 checklist 要求，为标准化的技术安全操作提供了框架和标准。其应用范围非常广泛。

运营商可以在以下三个场景中应用业务安全基线，分别为:

(1) 场景 1：入网管理部门使用安全检查工具对入网设备进行入网安全检查。在本场景中，安全基线检查工具适用于对新入网设备的安全检查，主要体现生产向运维交付的验收过程。运维按照行业或企业安全规范，对新入网的设备进行安全合规检查和验收；

(2) 场景 2：运维人员使用安全检查工具进行系统日常运行维护。在本场景中，安全基线检查工具适用于运维人员对所维护的业务系统进行日常安全维护和检查，监管网络资产运行安全状态，发现网络安全变化趋势，用以制定安全加固方案和计划；

(3) 场景 3：上级部门使用安全检查工具对所属部门进行安全检查。在本场景中，安全基线检查工具适用于上级安全检查部门按照行业或企业统一的安全规范，对下级部门安全管理工作是否符合要求，展开安全检查、监督工作。

以场景 1 为例，我们已经知道，安全基线是一个业务系统的最小安全保证，是业务系统最基本需要满足的安全要求，因此一个业务系统入网上线前必须要满足安全基线的要求，否则即认为是不安全的，不符合入网要求的。这个安全基线就是建设部门向运维部门交付系统所必需要通过的安全检查，也是上线前必须要跨越的一个门槛。在交付过程中，一旦与安全基线有任何不符合现象，需要建设部门进行整改，直到完全满足安全基线的要求为止。

这个时候，可能会存在业务与安全的矛盾，也就是说，到底是首先保证业务上线，还是首先考虑安全的问题。其实答案早已不言自明，大量安全事件证明，在业务系统上线时不进行严格的安全把关，而发生安全事件之后再投入人力物力发现和修复安全问题，不管是在技术难度上，还是修复成本上都是较上线前即进行全面的安全检查要高昂很多。

参考资料

[1]. NIST，National Institute of Standards and Technology. http://www.nist.gov.

[2].NVD，National Vulnerability Database. http://nvd.nist.gov .

[3].SANS, http://www.sans.org/ .

探析网络安全态势感知

行业营销中心　李文法　孙铁 / 产品管理中心　王卫东

摘要：本文从网络安全态势感知所要解决的问题为切入点，详细介绍了网络安全态势感知基本概念、模型和体系框架。并从网络安全态势要素提取、态势理解 / 评估、态势预测等方面，阐述了网络安全态势感知的主要技术及其发展情况。最后指出网络安全态势感知面临的一些问题和未来研究方向。

关键词：网络安全　态势感知　态势评估　态势预测

一、引言

随着计算机和通信技术的不断发展，网络正朝着大规模、高度分布式的方向发展，同时针对网络和计算机系统的入侵攻击行为也朝着规模化、分布化、复杂化等方向演化，各种网络安全技术相继出现和发展，如防火墙技术、入侵检测技术、入侵防护技术、可信计算技术以及对整个系统不安全因素的扫描、检测和报警、防治等等，但这些技术仅限于对某一方面安全数据的采集处理，无法实现对全局网络安全状况的准确监控，而网络安全态势感知技术能够实时地监测网络安全状态，获得更精确的安全威胁行为描述和更全面、及时的网络安全状态估计，并试图在攻击发生或造成严重后果之前，对攻击发生的数量及时空特性进行预测，预先采取相应的防御措施来加强网络的安全。网络安全态势感知技术的研究是网络安全领域必然要经历的下一个发展阶段，该项研究的开展对于提高我国网络系统的应急响应能力、缓解网络攻击所造成的危害、发现潜在恶意的入侵行为、提高系统的反击能力等具有十分重要的意义。

二、基本概念、模型和体系框架

2.1 网络安全态势感知的基本概念

网络态势是什么？这是一个在研究过程中需要首先明确的概念。网络态势是由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和未来变化趋势。值得注意的是，态势强调环境、动态性以及实体间的关系，是一种状态、一种趋势，是一个整体和全局的概念，任何单一的情况或状态都不能称之为态势。

网络安全态势感知（Network Security Situation Awareness，NSSA）是指在大规模网络环境中，对能够引起网络态势发生变化的安全要素，进行获取、理解、评估、显示以及预测未来的发展趋势，并不拘泥于单一的安全要素。开展这项研究旨在对网络态势状况进行实时监控，对潜在的、恶意的网络行为变得无法控制之前，进行识别、防御、响应以及预警，给出相应的应对策略，将态势感知的成熟理论和技术应用于网络安全管理，在急剧动态变化的复杂网络环境中，高

效组织各种安全信息，将已有的表示网络局部特征的指标综合化，使其能够表示网络安全的宏观、整体状态，从而加强管理员对网络安全的理解能力，为高层指挥人员提供决策支持。

2.2 网络安全态势感知模型

网络安全态势感知模型是开展网络安全态势感知研究的前提和基础。在深入分析国内外相关研究的基础上，结合对其他领域态势感知典型模型的分析—JDL 功能模型和 Endsely 的态势感知认知模型，给出网络安全态势感知概念模型。该模型主要分为 3 层，依次为网络安全态势提取、态势理解 / 评估以及态势预测。如图 1 所示:

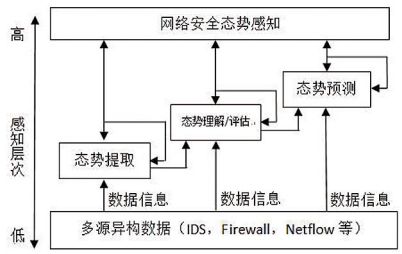


图 1 网络安全态势感知模型

- **网络安全态势提取层**。

态势要素是指构成网络安全态势的诸多因素，包括网络系统中存在的病毒入侵、黑客攻击行为、设备异常、系统资源使用情况、系统中存在的漏洞情况等。态势要素提取是网络安全态势感知的基础，没有合理准确的态势信息，就有可能生成错误的态势图。该层主要采用已有成熟技术从海量数据信息中提取态势信息，构造出安全态势的一般表示，并转化为统一易理解的格式，为网络安全态势理解 / 评估做准备。

- **网络安全态势理解 / 评估层**。

态势理解 / 评估是网络安全态势感知的核心，是对当前安全态势的一个动态理解过程，也是态势感知过程中最为复杂的部分。需要对历史态势要素信息与实时态势要素信息进行动态地融合处理，识别出态势信息中的安全事件，确定它们之间的关联关系，生成相应的分析报告和安全态势图，来反映整个网络的安全态势状况。

- **网络安全态势预测层**。

态势预测是最高级别的态势感知，态势预测依据历史网络安全态势信息和当前网络安全态势信息的状态和其动态性，对未来一定时期内网络安全态势进行预测 (即已知 T+1，T+2，…，T+n 时刻的网络安全态势，预测 T+(n+1) 时刻的网络安全态势)，使决策者能够据此掌握更高层的网络安全态势，为制定合理准确的决策提供依据。

2.3 网络安全态势感知体系框架

在网络安全态势感知相关理论和实践工作基础上，依据国家相关标准规范，研究网络安全态势感知的定性与定量方法，构建网络安全态势感知体系框架。在图 1 所示的网络安全态势感知模型的基础上，结合数据融合和层次化分析的思想，给出如图 2 所示的网络安全态势感知体系框架。

网络安全态势感知体系框架的设计，以安全态势感知流程为主线，突出要素提取、理解 / 评估、预测三个关键节点，以安全事件的识别和威胁传播网络的建立为牵引，以基于隐 Markov 模型的态势评估技术、基于 Markov 博弈模型的态势评估技术、基于对数分析的态势评估技术、基于时间序列分析的态势预测技术为支撑，最终实现网络安全态势感知的评估和预测目标。

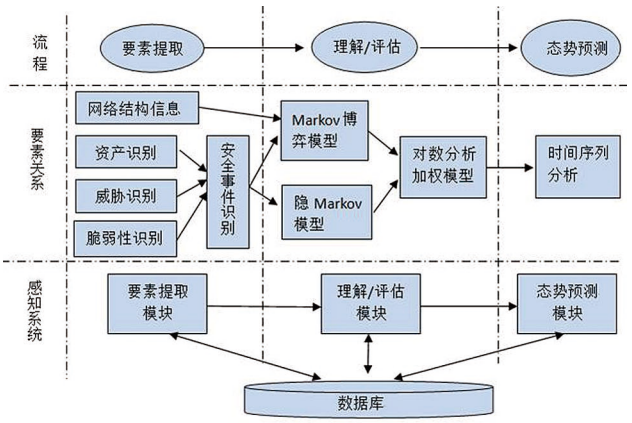


图 2 网络安全态势感知体系框架

三、网络安全态势感知的主要技术

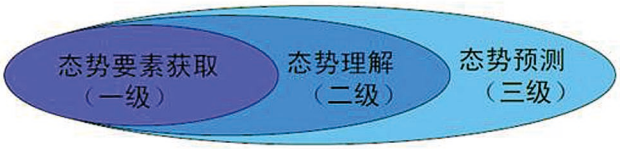


图 3 网络安全态势感知过程

网络安全态势感知是全面综合推理的过程。如图 3 所示，主要分为网络安全态势要素提取、网络安全态势理解 / 评估、网络安全态势预测三个子过程，所处理的对象是正在发生的、以前发生现在进行的网络安全事件和活动，重点关注网络安全域的行为模式。其产生的理想结果，应能反映当前真实的网络安全态势，并提供事件、活动的预测，为最优决策和网络安全管理的优化提供依据。下面从网络安全态势要素提取、网络安全态势理解 / 评估、网络安全态势预测三个方面对相关技术进行介绍。

3.1 网络安全态势要素提取技术

网络安全态势要素提取，是指从大规模网络安全状态数据源中，抽取影响网络安全态势基本元素的过程，它是网络安全态势评估和预测的基础，其提取结果对于整个态势评估和预测有着重要的影响，如果态势提取无法实现，那么整个网络安全态势评估和预测将成为无源之水，无本之木。整个网络安全态势感知系统中，安全事件的预处理与态势要素的提取，处于网络安全态势感知底层。系统从安全设备中获取到日志数据后，通过采用一定的数据格式进行统一，并对数据进行约减、合并，即将日志数据中与网络安全态势感知无关的噪声数据去除，合并重复的记录。网络安全态势的要素提取不仅提高了数据的质量，也进一步加快了安全态势分析的速度。

目前针对该项技术的研究尚属起步阶段，相关研究文献比较少。但在特征提取、分类分析、聚类分析等方面前期已经开展了一些工作。郭山清等提出了一种针对入侵检测结果的实时规则在线生成方法，在定义局部支持度、全局可信度的基础上，设计了规则生成算法，直接产生仅与当前发生的攻击相关的规则集。为了使分类方法适合网络入侵检测系统在线、实时的特点，田大新等根据自适应谐振理论提出了基于联想和竞争学习的动态分类算法。梁百川采用事件提取和分群技术实现态势要素的提取算法，但未实现该算法，马云等进一

步实现了事件提取和分群技术。Srihari 针对态势感知的信息提取问题，提出了一种基于概念的信息提取技术，用于解决军事战场中的态势要素提取问题。

目前在网络安全态势要素提取方面的研究还很不成熟，相关解决方法和实现模型较少，因此亟需寻找出一种实时高效的网络安全态势要素提取技术，用于实现攻防环境中安全要素的提取。

3.2 网络安全态势理解 / 评估技术

网络安全态势理解 / 评估主要是综合评估网络安全状态，即利用网络安全属性的历史记录和运行状况等，为用户提供一个准确的网络安全状态评判和网络安全的发展趋势，使网络管理者能够有目标的进行决策和防护准备。可以将神经网络、模糊推理等方法引入到网络安全态势评估中，进行合理的规则推理，得到合理的判断结果。依据网络安全态势评估所处理的数据源不同，可分为基于脆弱信息和基于运行信息的态势评估技术。前者是指系统设计配置状况 (包括服务设置系统中存在的漏洞)、资产价值等，侧重于对信息系统因固有漏洞等内在因素所带来的安全风险评估；后者是指系统所受攻击的状况, 主要来自于 IDS 报警、Firewall 日志、系统日志、网络流量信息等，更加关注诸如入侵攻击行为等外界因素所造成的安全态势威胁评估。

针对基于系统配置信息的安全风险评估，由原来的单机评估逐渐转向现在的以分域信息系统为重点的风险评估。Ritchey 等提出了一种网络脆弱点的模型检测方法，用于分析解决网络脆弱点的自动检测问题。陈秀真等提出了一种基于模糊信息融合的网络安全漏洞评估方法，结合漏洞扫描器的扫描结果及系统实际运行历史数据的统计结果，通过模糊查询即可得到评估结果。针对系统运行信息的安全态势威胁评估工作，主要停留在单个入侵攻击事件对系统所造成威胁的评估之上，而没有很好地考虑融合多源异构传感器的综合信息来评估整个网络的全局安全态势。Sabata 等提出了一种基于多证据融合的网络安全态势评估方法，通过对高层语义的推理来检测和识别攻击，从而有效地减轻决策者的认知负担。Gorodetsky 等提出了一种动态实时的态势评估方法，并实现了一个态势评估原型系统用于异常检测，但是未能解决多异步数据的 “老化” 问题。

在网络安全态势理解 / 评估领域，国内外研究人员和机构借鉴军事战场态势评估的成功理论和实践经验，进行了一些探索性的研究，已经取得了一定的研究成果，但实际应用系统未见报道。基于脆弱信息的态势评估技术和基于运行信息的态势评估技术，这两种评估技术各有侧重，并且最终反馈给决策者的安全态势信息、角度也各不一样。

3.3 网络安全态势预测技术

网络安全态势感知是指在大规模网络环境中，对能够引起网络安全态势发生变化的安全要素进行提取、理解、显示并预测未来发展趋势。其中，预测未来发展趋势是网络安全态势感知的一个重要组成部分。网络在不同时刻的安全态势彼此相关，安全态势的变化有一定的内部规律，这种规律可以预测网络在将来时刻的安全态势，从而可以有预见性地指导管理员进行安全策略的配置，来实现动态的安全性管理，预防大规模网络安全事件的发生。常见的用来预测网络安全态势的技术主要有人工神经元网络预测技术、

时间序列预测技术、灰色预测技术等。目前开展网络安全态势预测研究，主要有两条研究思路，一是先预测单个入侵攻击事件，再结合每种攻击的威胁程度，计算出相应的下一时刻或多个时刻的态势值，这种方法在确定每种攻击威胁程度时依赖主观经验；二是采用非线性时间序列预测方法，依据历史安全态势规律预测未来某一时刻或某一时间段内的安全态势。

针对单个入侵攻击事件或复合攻击的网络安全态势预测，所采用的方法主要有模糊神经网络、统计学习、数据融合、知识发现、贝叶斯推理、因果网络等。BAO Xuhua 等提出了一种基于入侵意图的攻击检测和预测算法，该算法采用扩展的有向图来表示攻击类别及其逻辑关系，按照后向匹配和缺项匹配的方式对报警进行关联，根据已关联攻击链的累计权值和攻击逻辑图中各分支的权值计算其可能性，可以在一定程度上预测即将发生的攻击。彭学娜等提出了一种融合网络安全信息的安全事件分析与预测模型，该模型能够对来自以 IDS 为主的多种安全部件和关键主机日志系统的网络安全信息进行校验、聚集和关联，并结合目标网络安全策略，对目标网络的安全状况进行准确评估，对基于特定攻击场景的可能攻击做出预测。任伟等初步探讨了一种基于神经网络的网络安全态势预测方法，通过大量实验和训练来建立网络安全态势预测神经网络模型，用于态势预测，这种方法存在数据量大和基函数选择难问题。

网络安全态势预测是网络安全领域一个新的研究热点，是预防大规模网络入侵攻击的前提和基础。而目前该领域的研究尚属起步阶段，尽管针对单个入侵攻击事件的预测研究已经开展了一些工作，其中有些方法能在一定程度上预测即将发生的单个入侵攻击事件或者部分复合入侵攻击行为，但都无法实现对整个网络的全局安全态势预测。

四、存在问题和未来研究方向

网络安全态势感知研究虽然已经受到了国防专项研究、国家 863、国家 973、国家自然科学基金、工业和信息化部 242 信息安全计划等国家计划的高度重视，国内学者也进行了一些研究，但目前尚属起步阶段，依然存在很多挑战性的问题：跨组织、跨机构的数据获取，还需要人们认识的提高和政策法规的支持；网络安全态势是一个综合概念，涉及到的因素有很多，而目前研究往往针对各自不同的应用给出不同的指标来刻画这些因素，缺乏统一的网络安全态势指标体系；复杂网络行为具有动态性、非线性、随机性等特性，很难用确定性的模型对其进行分析，所以需要建立一个实际可行的复杂网络行为模型用于网络安全态势感知。前期研究工作主要围绕定性评估和静态预测模型研究，已经无法适应动态多变的大规模网络环境需求，缺乏面向网络信息系统的网络安全态势量化评估和动态预测模型。对网络安全态势感知技术需要进一步地深入研究，可以从以下几个方面进行研究:

(1) 建立一套有效完备的网络安全态势评价指标体系。

(2) 构建一个实际可行的复杂网络行为模型。

(3) 研究网络安全态势量化评估分析模型。

(4) 研究基于复杂网络行为建模与模拟

的网络安全态势预测技术。

(5) 研究基于云计算、物联网等新技术的网络安全态势感知技术。

五、结束语

本文介绍了网络安全态势感知的基本概念、模型和体系框架，从要素提取、态势理解 / 评估、态势预测技术三个方面，研究分析了网络安全态势感知的主要技术及其发展情况，同时，就网络安全态势感知领域存在的问题和未来发展方向进行了探讨和概括总结。随着信息技术的不断发展和网络环境的变化，网络安全态势感知还有许多问题有待研究，但是网络安全态势感知技术必将会成为网络安全技术新的热点和发展趋势。

参考文献

1、Srihari R K. Situation awareness through concept-based information extraction. http://www.dawnbreaker.com/vas05/docs/Cymfony-Brief.pdf,2008.

2、Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities. Proceedings of the IEEE Symp. On Security and Privacy. 2000.

3、Sabata B, Ornes C. Multisource evidence fusion for cyber-situation assessment. Proceedings of SPIE, the International Society for Optical Engineering, 2006.

4、Gorodetsky V, Karsaeyv O, Samoilov V. On-line update of situation assessment: a generic approach. International Journal of Knowledge-Based & Intelligent Engineering Systems. 2005,9(4).

5、Bao X H, Dai Y X, Feng P H, etal. A detection and forecast algorithm for multistep attack based on intrusion intention. Journal of Software. 2005,16(12).

6、Liu N, Wang D G, Huang X M, et-al.Research on Network Security Situation Awareness Technology based on Artificial Immunity System. Proceedings of the IEEE International Forum on Information Technology and Applications. 2009.

7、赖积保 . 基于异构传感器的网络安全态势感知若干关键技术研究 . 哈尔滨工程大学 .2009.

8、张勇 . 网络安全态势感知模型研究与系统实现 . 中国科学技术大学 .2010.

9、郭山清，谢立，曾英佩．入侵检测在线规则生成模型．计算机学报．2006，29(9).

10、田大新，刘衍珩，李宾等．基于动态分类算法的人侵检测系统．吉林大学学报 (信息科学版)．2006，24(2).

11、梁百川．态势估计技术及其算法研究．航天电子对抗．2004，(1).

12、马云，王宝树，李伟生．数据融合中的态势觉察技术．计算机工程．2004，30(1).

13、陈秀真，郑庆华，管晓宏等．基于模糊信息融合的漏洞评估方法．小型微型计算机系统．2004，25(8).

14、彭雪娜，赵宏．一个融合网络安全信息的安全事件分析与预测模型．东北大学学报 (自然科学版)．2005，26(3).

15、任伟，蒋兴浩，孙锬锋．基于 RBF 神经网络的网络安全态势预测方法．计算机工程与应用．2006，42(31).

云计算面临的七大安全威胁

首席战略官　赵粮

摘要：本文总结了云计算面临的七大安全威胁，分析了每种威胁的业务场景和威胁方式，并推荐了可行的防御对策。同时对云计算安全的下一步研究方向进行了展望。

关键词：云计算　安全　威胁　虚拟化

一、云计算的特征

云计算已经得到了政府和各个行业信息技术管理层的高度重视。虽然对云计算的定义和特征、应用等存在各种不同的看法和流派，较为公认的一个云计算描述是美国技术和标准研究院的五个关键特征:[1][2]

C1: 按需的自服务

不同于传统网络服务或普通 IT 服务的一个鲜明特征，就是云计算服务是不用人工干预的自助服务，例如服务开通、配置变更、缴费、取消等。

C2: 宽带接入

该特征要求云计算服务主要通过网络提供，并且应该涵盖大多数的客户端，例如各种电脑、上网本、智能手机等。

C3: 虚拟池化的资源

该特征来源于云计算服务的多客户性质。在同一套物理资源之上，给多个客户提供服务，需要将原来孤立的、个体的物理资源通过虚拟化，映射成为虚拟的、功能模块化的、面向多用户服务的资源池。并由系统统一的、动态的、按需的再分配给各个客户。由此而来的另外一个结果就是客户不再关心、也基本上无法知道自己的某个服务在某个时刻运行在哪个物理位置的物理硬件之上。这些资源包括 CPU 计算能力、内存、存储、流程进程过程、网络带宽、虚拟机、备份数据、维护人员等等。

C4: 快速弹性架构

这个特征被认为是云计算带来的最大好处之一。用户不再为系统扩容跟不上用户需求预测而苦恼，也不用为短期项目完工后闲置的 IT 资源而担心。系统规模扩大、减小，对于云计算服务的用户来说，变成了鼠标点击事件，就好像云里的服务和虚拟资源是无限的、召之即来、挥之即去的。

C5: 可测量的服务

这里强调的是“服务”，它应该是可以测量的、有明确价格和收费政策的。在使用过程中，各种服务（例如存储、带宽、活动用户账号、各种计算资源等）的使用、监视、控制等对于服务提供者和用户都是透明的。

目前，IT 业界从传统的软硬件业务模式正在明显地转向服务模式，从网络信息安全的角度看，这个转变带来的影响是深远的。对新计算方式安全威胁的顾虑非常普遍。按照 IDC 2008 年 8 月份的调查结果[3]，在人们对按需 - 云计算 (Cloud/On-Demand) 的担心问题排序中，安全问题高居第一，下面依次是性能、可用性、集成问题、可定制能力等。其它多个咨询机构和权威组织的调查

结果也都反映了类似的担心。

二、安全威胁

帮助人们解决对云计算安全威胁担心的第一步就是正确的识别安全威胁，然后研究开发出正确的威胁消减方案。作为当前业界最为活跃的云计算安全专业组织 – 云安全联盟 CSA 在 2010 年 3 月份发表了自己的研究成果 – 云计算的七大威胁，获得了广泛的引用和认可。

- Threat #1: Abuse and Nefarious Use of Cloud Computing

  云计算的滥用、恶用、拒绝服务攻击

- Threat #2: Insecure Interfaces and APIs

  不安全的接口和 API

- Threat #3: Malicious Insiders

  恶意的内部员工

- Threat #4: Shared Technology Issues

  共享技术产生的问题

- Threat #5: Data Loss or Leakage

  数据泄漏

- Threat #6: Account or Service Hijacking

  账号和服务劫持

- Threat #7: Unknown Risk Profile

  未知的风险场景

接下来，我们分别较为详细地分析每个安全威胁的场景和可行的对策。

2.1 云计算的滥用、恶用、拒绝服务攻击

首先，云计算以宽带网络和 Web 方式提供服务，其可用性方面将会受到挑战，针对云计算服务的拒绝服务攻击需要云计算服务提供商认真调查、采取相应的专门保护措施[4]。其次，云计算快速弹性的特征要求服务提供商自身必须具备非常强大的网络和服务器资源来支撑，按需自服务的特征又对业务开通和服务变更等环节提出了灵活性的要求。这两个特征结合在一起，使得云计算服务很容易成为滥用、恶意使用服务的温床。在 2010 年 Defcon 大会上，David Bryan 公开演示了如何在 Amazon 的 EC2 云计算服务平台上以 6 美元的成本对目标网站发起致命的拒绝服务攻击[5]。利用云计算服务来破解密码、搭建僵尸网络等恶意使用案例也屡有报道。

可行对策: 加强抗拒绝服务攻击的能力。在云计算服务的设计阶段加强安全考量，对可能的安全威胁建立场景用例，并在业务逻辑设计过程中予以专门防护；严格设计首次注册和验证过程，实施信用卡欺诈行为监控和协调，监控公共黑名单，查看你自己的网络是否被列为垃圾邮件和恶意软件来源而被阻止；针对来自网络的投诉和监管机构的问询快速响应。

2.2 不安全的接口和 API

资源和能力开放是云计算时代的一个重要业务变革方向，作为技术层面的实现，云计算服务商需要提供大量的网络接口和 API

来整合上下游、发展业务伙伴、甚至直接提供业务。

但是，从业界的安全实践来看，开发过程的安全测试、运行过程中的渗透测试等，不管从测试工具还是测试方法等，针对网络接口和 API 都还不够成熟，这些通常工作于后台相对安全环境的功能被开放出来后，带来了额外的安全入侵入口。

可行对策: 加强接口和 API 在功能设计、开发、测试、上线等覆盖生命周期过程的安全实践，广泛采用加密、认证、访问控制、审计等安全措施以及更加全面的安全测试用例。

2.3 恶意的内部员工

按照业界的传统认知，超过半数的安全事件源于内部人员。Verizon Business 最新的数据泄漏调查报告（DBIR 2010）显示，48% 的数据泄漏是由于恶意的内部人士所为。云计算服务，作为某种程度上的外包业务，工作上有权限、有能力接触并处理用户数据的范围进一步扩大，用户自己的内部人士、供应商员工、云计算服务商的管理维护人员、云计算服务商的供应商员工等。这种访问范围的扩大，增加了恶意的“内部员工”滥用数据和服务、甚至实施犯罪的可能性。

可行对策: 从管理、合同、技术等几个角度同时入手。管理上加强安全意识教育，各个业务流程上落实相关的安全控制，由人力和法务部门明确雇员的法律责任，在违反安全规定造成安全事故时有权送交司法机关；对供应商的管理环节上必须对网络安全有专门的条款和核查措施，对供应商出现安全滥用和违反合同、甚至犯罪的情况制定明确的惩罚措施；在技术上广泛加密、认证、访问控制、入侵检测、审计等安全控制。

2.4 共享技术产生的问题

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

可行对策: 在云计算中心设计伊始，就针对客户的不同业务需求，设计可以支持不同安全等级、不同硬件分享策略的硬件分区和防御策略，并且在运行阶段，具有监控是否有未经授权的修改和违规活动的技术能力。

2.5 数据泄漏

事实上，数据泄漏是云计算、尤其是公共“云”最为广泛的担忧之一。组织的管理层和 IT 决策人需要仔细评估云计算提供商对数据的保护能力。很多威胁场景都可能会导致云中的数据的丢失和泄漏。云中关键数据的高密度聚合，对潜在的攻击者带来了极大地诱惑力。

密钥的管理也是一个挑战。密钥的丢失会导致事实上的数据毁坏。密钥的国度分享又会消弱加密的效果。另外，由于同宿主机上其它客户的法律取证要求，也可能会导致不必要的数据外泄和损失。

可行对策 从设计到运行，对数据的传输、处理和存储等各环节，提高加密和核查能力。定义良好、组织得当的密钥生成、存储、管理和销毁策略非常重要。在合同中明确规定云提供商的数据备份、恢复、销毁等各个环节的数据安全控制。

2.6 账号和服务劫持

传统的服务和会话劫持已经广为人知。云计算给账号和服务“劫持”又增添了不少

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

可行对策: 清楚理解云服务提供商的安全策略和 SLA，禁止用户和服务之间共享账号信息，及交互式的用户账号和后台服务使用的账号必须区分管理；使用强大的双因子认证技术；主动检查是否有未经授权的活动。

2.7 未知的风险场景

云计算服务商和用户之间存在很大的信息不对称性。一方面，用户选择外包自己的 IT 计算和服务到云提供商，就是为了解放和优化自己的资源，所以没有必要也没有足够的资源去全面洞察“云”中的所有细节；另一方面，云计算提供商出于商业机密和安全考虑，并不情愿分享所有的关键信息，即使是和安全直接相关的。这种情形下，云计算的用户必然需要处理大量的未知安全风险[6]。

实际上，这些“Unknown Unknowns”，也就是说那些未知漏洞们，是云中真正的危险，而软件版本、安全实践、代码更新、漏洞情况、入侵企图、安全设计等都是可以帮助评估自身所面临的安全风险的重要因素。

可行对策: 认清自身的安全现状，向云计算提供商要求最大程度的信息透明，了解它们如何配置系统，如何及时为托管的软件打补丁等等。正确地处理安全的模糊性在未来依然会是一个长期的挑战。

三、下一步

清醒透彻地调查安全威胁、有针对性地设计相应的安全控制和方案是云计算时代安全驾云的重要举措[7]。从实践上看，云计算提供商和用户都还不具备很好的、可视化的展现安全威胁、安全控制和安全效果的手段。云安全提供商正在抗拒绝服务攻击、安全配置和漏洞管理、应用安全生命周期管理、身份认证、访问控制、数据加密、电子证据发现和审计等多个细分领域，努力缩小与计算技术在发展上的差距。与此同时，安全的度量和可视化正在成为云计算时代最为重要的安全技术之一。

参考文献

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

[2] Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26, http://csrc.nist.gov/groups/SNS/cloud-computin-g/cloud-computing-v26.ppt

[3]Biggest Cloud Challenge: Security, http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security/

[4] DDoS: A Threat You Can't Afford to Ignore, Forrester whitepaper, http://whitepapers.zdnet.com/abstract.aspx?docid=1155831

[5] David Bryan, https://www.defcon.org/images/defcon-18/dc-18-presentations/Bryan-Anderson/DEFCON-18-Bryan-Anderson-Cloud-Computing.pdf

[6] http://chenxiwang.wordpress.com/2009/11/24/follow-up-cloud-security/

[7] Kim-Kwang Raymond Choo, Cloud computing: Challenges and future directions, 2010

全面系统化的终端准入控制

产品管理中心　刘敏

摘要：随着终端管理需求的日益迫切，以及终端管理类系统的大规模部署，终端准入控制已不再是一个陌生的领域，在什么时间、什么位置依据什么条件检查试图接入内部网络的终端，进而根据检查结果采取什么措施，已是各行业用户在部署终端管理类系统时首先需要深入思考的一系列问题。本文将从终端准入控制的概念、目标、手段、效果等多个角度深入剖析，为用户选择终端准入控制解决方案提供参考。

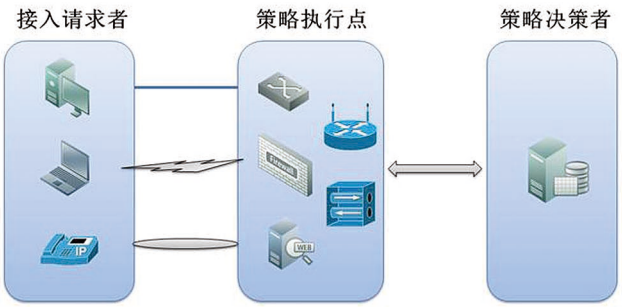
关键词：终端　准入　接入　NAC　网络

何为终端准入控制

随着终端管理需求的日益迫切，终端管理类系统的大规模部署，终端准入控制已经逐渐成为终端管理的标准功能之一，大家对其概念已经不再陌生。简单地说，就是一套整合的软件系统，基于“你是谁”、“你安全吗”或者“你合规吗”来执行准入控制策略。

终端准入控制体系的架构，分成三个组件。接入请求部分：请求接入内部网络的终端和用户，就终端设备而言可能是终端计算机、来访的电脑笔记本、或者通过 VPN 接入的家用电脑等；策略执行部分：终端准入控制策略的执行部分，可以形象地理解为“关卡”，可能是交换机、网关设备、VPN 服务器、终端自身等设备；策略决策部分：对请求接入的终端是否符合安全策略进行判断、并给出结论的部分，可能包含身份认证服务器、策略管理服务器等。

三组件之间的关系可以用下图表示：



终端准入控制的目标

终端准入控制的目标可以比作现实生活中的安全检查，检查本身并不是目标，真正的目标是通过检查确保“进入的是安全的、不安全的是不允许进入的”。我们把终端准入控制的目标细分成两个子

目标:

自动修复、阻止违规接入

终端准入控制的首要目标是检查终端是否符合准入安全策略的要求，符合则允许接入，不符合则阻止其接入。同时对于确实因为工作需要接入的终端，阻止其接入只是一种手段，最终的目标是通过自动修复使其符合策略要求，能够接入。

定期检查、确保持续遵从

对于已经通过检查接入内部网络的终端，要进行定期检查，确保其持续遵从。一旦检查未通过，则同样执行自动修复，直到符合策略要求为止。

这一过程如下面的模型图所示:

图 1.1 终端准入控制步骤

终端准入检查的标准

执行终端准入控制检查时，何为“符合”策略要求，涉及到终端准入检查的依据或标准。目前，尚未看到全行业统一的具体标准，下面就我们的实施经验提供一些参考:

依据之一：终端是否安装了客户端软件

终端是否安装了客户端软件，与其说是检查依据，更不如说是执行后续检查的前提条件，或者说是整个终端管理系统（包括终端准入控制）部署的基础。因为对尚未安装客户端软件的终端执行安全状况的检查，从理论上来说难以精准，更没有办法执行一系列的终端管理任务。因此，首要的检查依据就是终端是否安装了客户端软件，安装了则认为检查通过，否则检查不通过。

依据之二：终端安全状况是否符合要求

终端系统的安全状况是否符合要求，是终端准入控制的核心依据之一。整个终端准入控制的核心任务之一，就是确保接入到内部网络的每个终端都是健康的、未潜藏威胁的、未感染病毒的。安全状况的评估因素主要包含操作系统补丁安装情况和反病毒软件病毒库更新情况，及时安装操作系统补丁包、并更新反病毒软件的病毒库，则认为检查通过，否则检查不通过。其他的评估因素可根据自身的实际需求或者贴近业务的需求而提出，例如终端是否违规使用外部设备、是否运行了不安全或影响正常办公的应用程序等等，均可通过终端准入控制的手段阻止其接入，直到停止违规行为为止。

依据之三：终端用户身份是否通过认证

一台试图接入内部网络的终端，一般来讲涉及两个对象：终端系统和终端用户。因此在对终端系统安全状况进行检查的同时，还要确保终端用户身份的合规性。对终端用户身份进行认证，一方面防止外来人员随意接入，另一方面防止普通用户伺机到其他终端上进行越权接入和访问。

终端准入控制的方式

终端准入控制的方式，就是终端准入控制的执行点，可以分为以下几类:

IEEE 802.1X 认证

与接入层交换机进行联动，对试图通过交换机接入内部网络的终端进行认证，当且仅当认证成功时才会转发该终端的数据包。关于 IEEE802.1X 认证的技术原理已有很多公开资料，这里不再详述。IEEE 802.1X 认证的方式，相对而言控制的效果更彻底，但对环境要求较高。

网关准入

与位于出入口的网关设备进行联动，对试图跨网关访问网络资源的终端进行认证，当且仅当认证成功时才允许其跨网关访问，否则阻止访问并对 HTTP 请求进行重定向。其原理主要是通过终端管理服务器或者安装在终端的客户端软件，定期向网关汇报各终端的检查结果，借此网关设备掌握了各个终端是否符合安全策略的总体情况，并能够得到定期更新。当有终端跨网关访问网络资源时，网关设备只要把该终端的 IP 与情况表格中的 IP 进行匹配、确定准入检查结果、执行相应措施即可。网关准入的方式，因为能够为终端用户提示足够的信息，所以用户体验很好。

应用准入

与应用服务器进行联动，对试图访问应用服务器的终端进行认证，当且仅当认证成功时才允许其访问，否则拒绝访问并对 HTTP 请求进行重定向。应用准入的原理与网关准入的原理基本相似，但应用服务器主要是从终端管理服务器获取终端的合规情况，而不是从安装在终端的客户端获取。应用服务器可以是 Web 服务器、邮件服务器、DHCP 服务器、DNS 服务器等。应用准入与网关准入可以很好地形成互补，前者在内部关键的应用服务器上设置检查点，后者在网络出入口处设置检查点，对终端的内、外部访问形成封堵，同时都能够为终端用户提示足够的信息，带来非常好的用户体验。

主机准入

直接利用安装在终端的客户端程序，检查终端是否符合准入安全策略，检查通过则无须做额外动作，检查不通过则利用客户端程序自带的网络拦截功能，阻断终端的网络访问，但允许其访问必要的修复服务器，直到检查通过。该方式的前提和条件是终端上已经部署了客户端程序，否则无从谈起。

ARP 准入

最后，我们了解一下少数厂商采取的 ARP 准入，主要过程可以分为以下几个步骤:利用 ARP 包探测新上线 IP；判断该 IP 是否符合准入安全策略要求；不符合时发起多个方向的 ARP 欺骗包以最大程度地阻止该 IP 的网络通讯。

终端准入控制的效果

下面针对上述几种终端准入控制的方式，进行一个综合的评价和对比:

	执行点	检查要素			优点	缺点
		终端是否安装了客户端软件	终端安全状况是否符合要求	终端用户身份是否通过认证		
802.1X	接入层交换机	√	√	√	a. 在距离终端最近的地方执行准入，且认证不成功时等效于没插网线，因此控制力度强； b. 已有标准协议。	a. 接入层交换机须支持 802.1X 认证； b. 交换机下接 HUB 或傻瓜式交换机时，要求执行准入的交换机支持基于 MAC 的认证，对交换机有较高要求。
网关准入	网关设备	√	√	√	a. 配置简单； b. 能够重定向，用户体验好。	当且仅当终端发起跨网关的访问时才能执行准入，存在漏洞。
应用准入	应用服务器	√	√	√	a. 兼容各种应用服务器，适应性强； b. 能够重定向，用户体验好。	当且仅当终端访问应用服务器时才能执行准入，存在漏洞。
主机准入	终端自身	×	√	√	在终端系统内部执行准入，控制力度强。	需要终端上事先已安装客户端软件。
ARP 准入	子网内的某一特定终端主机	√	×	×	适用于任何 IP 网络，对网络环境要求低。	a.ARP 协议本身的特性决定了 IP 发现可能有漏报； b. 通过 ARP 欺骗阻断网络访问，效果不稳定，特别是当终端安装有 ARP 防火墙或手工插入 ARP 静态表项时，控制力度非常弱； c.ARP 欺骗包本身可能对网络的正常运行带来负面影响，占用带宽。

六、总结

本文从终端准入控制的概念讲起，深入浅出地带领大家对其目标、标准、方式和效果逐一作了分析。其中，准入控制的方式也即准入控制的执行点在很大程度上决定了控制的效果和力度，因此在实施终端准入控制时执行点部署在什么位置是关键。希望本文能为您更加全面、理性地选择终端准入控制解决方案提供一些参考。

一种基于信誉的威胁分析方法

行业营销中心　卢小海

摘要：随着互联网变得日益重要，恶意攻击者的攻击目标和手法不断变化，对传统检测和防护方案提出新的挑战，需要引入新的机制来减低广义的信息交易成本。而如何通过重复博弈理论，改善信息不对等情况下对未来的预期，是降低交易成本并鼓励建立并维护信誉的关键。该文通过引入多定义维度、多行为场景和多评估参与者，提出一种基于信誉的威胁分析方法。该方法实现了根据信誉对场景和行为的适应性和传播性，降低风险分析中误报率和漏报率的计算模型。

关键词：信誉　威胁分析　网络安全

根据 CNNIC 统计[1]，中国网民规模 2010 年已达到 3.84 亿人以上，普及率达到 28.9%；随之而来的是针对互联网应用的攻击手法日新月异，地下产业链日趋完整，已形成完整的恶意攻击研究、销售和分发体系。

从攻击者角度来看，网页挂马、钓鱼和欺诈等新兴攻击手法层出不穷；恶意代码和站点变化也越来越快，平均存活时间仅以天甚至小时计；而这些动态攻击行为往往又难以通过静态规则进行描述。

从防护者角度来看，传统基于样本收集、分析和特征分发的防护模型，受限于收集渠道、分析速度和特征分发方式，很难确保在足够小的时间窗口内做出快速反应；对日益增加的应用层流量处理能力需求也很难持续提供改善。

针对当前现状和问题，本文提出一种基于评价目标 (Agent) 信誉的威胁分析方法。与传统基于单次行为的检测思路不同，我们不把评价目标的行为看作一次独立事件，而是根据其发生的上下文及应用场景，结合其历史行为与未来预期，综合判断其威胁等级，进而根据不同威胁等级采用不同防护策略。

这种威胁分析方法，可以很大程度上减少基于行为检测过程中，对可疑灰色行为的误判或漏判，并通过增加攻击者成本的方式，鼓励评价目标积累信誉，并避免防护者一味被动跟随攻击者四处救火。

本文第一节介绍广义信誉体系，以及业内对信誉系统的相关研究和使用情况；第二节定义威胁分析方法中的信誉体系、分析方法和计算模型；第三节以网页动态行为分析的场景为例，讨论如何通过此威胁分析方法提高检测效率；第四节对本文观点进行总结，并介绍在信誉传播性和威胁影响面评估方面的后续研究思路。

一、背景

为了降低交易成本，广义信誉体系已经在经济生活中长期存在并被广泛使用。类似思想也被用于改善电子商务、P2P 网络和垃圾邮件检测等领域。

1.1 广义信誉体系

在经济学及相关学科中，交易成本 (Transaction cost) 是指在完成一次商品交换时产生的直接和间接成本。这个成本的构成[2]，除了在完成交易之前搜寻和信息自身成本、以及交易时议价和决策成本之外，还包括事后的监督和违约成本。

上述交易成本的产生根源，来自于交易本身的三项特征[3]：交易商品的专属性 (Asset specificity)、交易的不确定性 (Uncertainty) 和交易的频率 (Frequency)。

如果将一系列交易作为各自独立的事件来衡量，总体成本的增长将与交易事件的数量成正比。因为每次独立的交易，都可能因为信息不对称，而趋向于非合作博弈[4]下的纳什均衡 (Nash equilibrium)，导致交易成本的持续线性叠加。

根据博弈论 (Game theory) 的思想，在信息不对称的情况下，降低不确定性的最可行方式之一，就是通过重复博弈 (Repeated game) 改善交易参与的各方对未来的预期[5]，进而降低单次交易的成本，避免交易成本随频率线性增长。

而这里重复博弈的基础，是根据可观测的交易历史，鼓励交易参与者尝试建立并维护良好的信誉 (Reputation)，并有可能为长远利益牺牲短期利益，进而选择不同的均衡策略。

在现实生活中，类似的广义信誉体系已经广泛存在并被应用，例如公司品牌形象、朋友间口碑、信用卡使用记录等等。

1.2 信誉系统

在计算机科学领域中，类似的降低交易成本的思路也被广泛使用于诸如 Amazon、eBay 等电子商务系统[6]，P2P 信息网络[7] 和垃圾邮件检测[8] 等多个领域。

而在信誉系统的评估方法上，也有很多不同的思路。

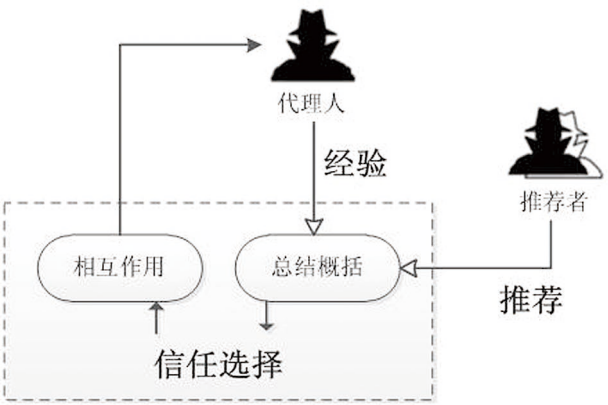


图 1 Abdul-Rahman 和 Hailes 的信誉模型

Abdul-Rahman 和 Hailes 的模型[9] 中，根据信誉信息来源将信任 (trust) 区分为直接 (direct) 信任和推荐者 (recommender) 信任，

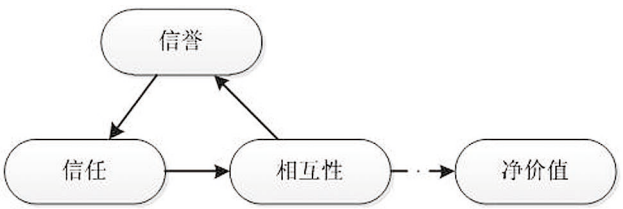


图 2 Mui、Mohtashemi 和 Halberstadt 的信誉模型

并在特定的上下文 (context) 中进行评估。直接信任分为四级，推荐者信任则根据场景作为信誉 (reputation) 来源被转化为信任。

Mui、Mohtashemi 和 Halberstadt 的模型[10]中，则将信誉和信任作为两个不同概念。将信誉定义为根据目标在历史行为的目的基础上获得的一种感知，而信任则是根据历史行为获得的对未来行为的预期，而这两者通过行为中的相互性 (Reciprocity) 互相影响。

1.3 问题与改进思路

作为通用信誉评价体系，这两种评估方法能够很好的解决了电子商务等场景下的信誉评级需求，但对于威胁评估来说过于简单。

首先，这些方法都只是简单的将信誉和信任，作为一个独立变量进行考虑，变化和影响只发生在同一维度。在威胁评估中，定义一个评价目标信誉的往往是一系列多维度因素。

其次，这些方法将信任简单定义为，两个评价目标之间固定场景的关系。在威胁评估中，需要根据不同应用场景，定义不同的向量集来评估信任，还需要考虑多级信任传递的影响。

最后，这些方法仅考虑一对一的简化情况。在威胁评估中，需要对一个完整场景中所有参与者，根据其共同对评价目标的预期，来进行最终评估。

考虑到以上三个主要问题，本文尝试从三个方面进行改进，引入多维度定义信誉和风险评估因素，针对多场景设定行为预期与权重，汇集场景中多参与者的评价与反馈。

二、定义

为解决这些问题，本文将应用威胁分析的信誉体系，定义为针对一组评价目标的信誉积累和信任传播体系；信誉本身不应脱离特定场景存在；并通过基于向量矩阵的计算模型进行信任关系评估。

2.1 信誉体系

为帮助描述信誉体系，首先需要定义特定场景中，需要参与威胁评估的评价目标及其行为。

评价目标：$T=\{t_1,t_2,\cdots t_N\}$,

评价目标向量：$\forall v\in V, v=(t_i,t_j)$，其中 $t_i,t_j\in T$. (1)

评价目标 t_i 是信誉评价的目标。同时其作为信息载体，将为后续分析提供历史上的行为以及对未来行为的预期。评价目标向量 v_i 是两个评价目标之间的单向联系，用于定义从 t_j 对 t_i 的评估，因此在大多数情况下 $(t_i,t_j)\neq(t_j,t_i)$。

场景：$\forall s\in S, s(v)\in\{exist,nonexist\}, v\in V.$ (2)

场景 s 是针对特定应用场景上下文，用于威胁分析的一组相互有关系的评价目标向量集。场景是根据真实行为涉及的评价目标训练并动态构建的，但并不包含动作自身。

行为预期：$\forall v\in V, E(v,\alpha)\in\{did,will,never\}$，其中 α 是发生在任意评价目标向量上的某种行为。 (3)

E(v,α) 是发生在任意评价目标向量 v 上，对某种特定类型行为 α 的历史情况与未来预期。随着 α 不同，评价目标向量上可以有多个不同类型的行为历史和预期。

信 誉：$R(s,v)\in\{trustworthy,unknown,untrustworthy\}$，其中 $s(v)=exist, v=(t\_i,t), v\in V$ 且 $t\_(i),t\in T$. (4)

信誉 R(s,v) 表示在特定场景 s 中，评价目标 t_i 的信誉，评价的来源是该场景中评价

目标向量 v 里与之直接相关的 t。信誉是根据历史行为和信任累计来获得的，被用于评估特定行为的信任评级，同时也被当前信任关系和结果所影响。

行为权重: W(s,α)=[0,N]. (5)

行为权重 W(s,α) 表示在场景 s 中，行为 α 的价值或影响力。这种权重是针对行为自身，而与评价目标无关。

信任 θ(s,v,α)∈{trust,untrust}. (6)

信任 θ(s,v,α) 表示在场景 s 中，针对评价目标向量 v 中的评价目标，特定行为的信任策略。

2.2 分析方法

在基于信誉对威胁进行分析时，一个基本原则是通过引入基于历史行为记录的信誉，将单次事件变为重复博弈，并结合行为预期评估信任策略，反过来形成正反馈并影响信誉。

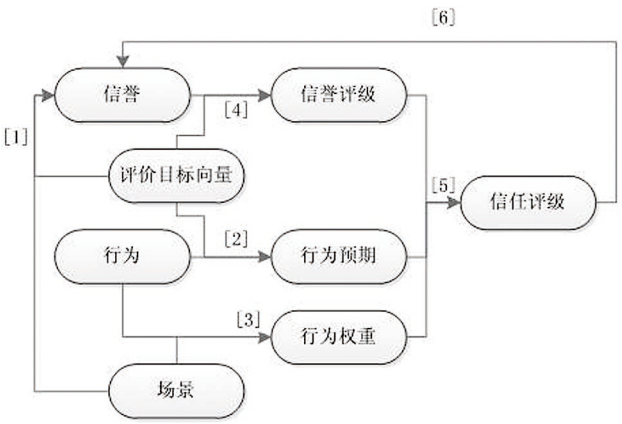


图 3 基于信誉的威胁分析模型

在进行威胁分析时会分为三个阶段：数据准备、数据分析和威胁评估。

数据准备阶段会根据事件的影响范围和类型，定义一组评价目标向量，描述事件中哪个评价目标对哪个评价目标产生了影响；以及与之相关场景所涉及到的一组待评估行为，作为实际威胁分析目标；并根据场景获取对应的一组针对特定评价目标向量的信誉信息 [1]，引入历史维度降低噪音影响。

数据分析阶段，首先会根据历史情况给出某个特定行为，在某个评价目标向量上的行为预期 [2]，这个评估本身是无选择倾向性的，只是简单描述一个对未来的预期；其次评估此行为在场景中的行为权重 [3]，不同场景中行为权重是可进行动态训练的；最后根据评价目标向量给出相应的信誉评级 [4]，其间接包含了场景的影响。

威胁评估阶段，则是对行为预期结合行为权重，在特定信誉评级下的综合评定，根据预设计算模型获得针对场景下安全威胁的信任评级 [5]；最终反馈到评价目标向量在此场景下的信誉 [6]。

在这样一个威胁分析方法中，定义信誉和信任的关键因素，将包含评价目标向量、行为历史与预期、特定场景中行为权重以及历史信誉等多个不同纬度。其中行为预期和信誉评级本身隐含时间维度，评价目标向量和特定场景中行为权重则可动态训练。这一方面避免纯静态模型适用面较窄的问题，另一方面可以通过时间维度对最终评估结果的正向奖励，让长期参与者受益，鼓励建立并维护信誉。

此外，这个分析方法并不是直接针对事件自身，而是通过将事件切分为一组评价目标向量进行分析。这一方面可以细化事件在特

定场景中，其不同行为的影响权重；另一方面也很容易扩展到对多个相关事件的关联分析，天生具有多级信任传递的能力。

2.3 计算模型

基于上述的模型定义和分析方法，可以建立基于信誉的威胁评估计算模型如下:

$$\theta(s,v,a)=F(R(s,v),E(v,a),W(s,a)). \quad (7)$$

其中，R、E、W 分别对应上面的信誉、行为预期和行为权重，θ 是 R、E、W 的复合函数，最终可通过 θ 与预设的评价矩阵进行形式逻辑推演，获得定义信任评级的真值表，以及信誉反馈信息。

三、场景

3.1 动态行为分析

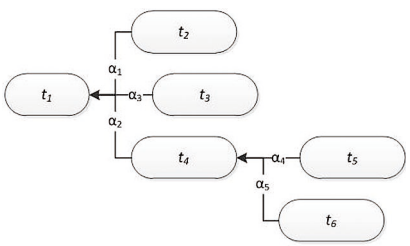


图 4 威胁分析示例

以动态页面行为分析的场景为例，在对页面 t_1 进行威胁分析时，我们可以把评价目标定为页面加载时会被动态自动加载的脚本 (Script) 或帧 (Frame)。

这样我们定义获取到一组评价目标向量，如 $v_1=(t_1,t_2)$ 表示页面 t_2 对 t_1 的影响。而根据页面动态行为的不同，我们可以抽取一组评价目标向量上的行为；α_1 表示表示页面 t_2 对 t_1 的动作，例如动态加载脚本并执行。

根据行为历史发现页面 t_2 的动态加载页面行为经常发生，因此给出的行为预期是会发生 (will)；而动态加载脚本在动态页面评估场景中，权重较高为 0.8，毕竟大部分恶意代码执行都依赖于脚本执行。虽然如此，对动态加载页面这个场景，我们可以通过信誉信息了解到，页面 t_2 所在站点页面对页面 t_1 所在站点来说信誉良好 (trustworthy)。因此虽然此行为本身很敏感 (行为权重较高)，但对于此次评估来说，最终信任评级会获得信任 (trust)。

而对于一个被恶意代码感染的页面，如页面 t_3 被插入到页面 t_1 中，因为行为历史中从来没有发生过，页面 t_3 所在站点对页面 t_1 所在站点的动态加载脚本行为，所以行为预期会是从未发生 (never) 且信誉评级为未知 (unknown)，进而对此次评估来说，最终信任评级会获得不信任 (untrust)。进而会影响到此站点对页面 t_1 所在站点甚至所有站点的信誉。

反过来对一个已知信誉良好站点，即使行为预期是从未发生 (never)，因为其信誉良好 (trustworthy)，仍会获得信任 (trust) 的最终信任评级。这可以很大程度上降低对此类站点敏感行为的误判。

四、总结与展望

本文针对互联网领域的新兴安全威胁的特点，结合重复博弈降低信息不对称性的思想，提出一种基于信誉的威胁分析方法。该方法通过引入多评价维度、多行为场景和多参与者，将单次的事件变为重复博弈，鼓励参与者建立并维护信誉，最终减少在威胁分析中的误判和漏判。

此外，在信誉系统及其应用方面的进一步研究，也是笔者持续关注的领域，下一步的研究方向包括:

- **信誉传播性分析**

与传统的静态预建模威胁分析方法不同，基于信誉的分析方法天生是动态且可训练的。其隐含以信誉为主线，在不同评价目标的广度，和时间维度的深度上，通过主动信任评级和被动信誉反馈的传播性。因此如何通过强化不同维度传播性，以整体模型稳定性来弱化单点噪音，是需要我们仔细考虑的问题。

- **威胁影响面评估**

从信誉的传播性换个方向考虑，则可通过逆向追溯，以特定的行为模式识别，来评估特定威胁或同类威胁的影响面。这种评估方法可用于发现未知威胁，并根据统计进行早期预警。而通过引入信誉这一参考评价因素，可以大大降低计算量和误报率。

- **信誉系统自身安全性**

而对于信誉系统自身的安全性，考虑到可影响点只涉及真实的行为历史，进行欺骗的时间成本会比较高。但在定义场景和评价矩阵时，仍需对恶意干扰噪音的识别和弱化进行研究。

参考文献

[1]CNNIC. 中国互联网络发展状况统计报告 [R], 2010. CNNIC. Statistical Survey Report on Internet Development in China, 2010.

[2]Williamson O E. Markets, Hierarchies: Analysis and Antitrust Implications [M]. New York: Free Press, 1975.

[3]Williamson O E. The Economic Institutions of Capitalism [M]. New York: Free Press, 1985.

[4]Nash J. Non-Cooperative Games [C]. The Annals of Mathematics 54(2):286-295, 1951.

[5]Glicksberg I L. A further generalization of the Kakutani fixed point theorem, with application to Nash equilibrium points [C]. Proceedings of the American Mathematical Society, 3(1):170–174, 1952.

[6]Resnick P, Kuwabara K, Zeckhauser R, Friedman E. Reputation Systems [D]. Communications of the ACM, 43(12), pp. 45-48, 2000.

[7]Aberer K. P-Grid. A self-organizing access structure for P2P information systems [D]. Proceedings of the Ninth International Conference on Cooperative Information Systems, Trento, Italian, 2001.

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

[9]Abdul-Rahman A, Hailes S. Supporting Trust in Virtual Communities [D]. Proceedings of the 33rd Hawaii International Conference on System Sciences, Maui, Hawaii, 2000.

[10]Mui L, Mohtashemi M, Halberstadt A. A Computational Model of Trust and Reputation [D]. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Maui, Hawaii, 2002.

安全度量知多少

产品管理中心　王卫东

摘要：本文从安全度量所要解决的问题为切入点，详细解释安全度量定义、目的以及客户价值。并从安全度量的对象、导向、一般过程。指标体系的模型、实施步骤等方面，阐述了安全度量的方法论。最后指出了实施安全度量项目必将面临的一些挑战。

关键词：安全度量　测度　ROI(Return On Investment)

一、前言

随着信息技术的广泛应用，国家和社会对信息化的依赖度越来越大，信息安全已成为国家安全的重要组成部分。然而由于不断增长的复杂性和不安全部件及网络间的互连，信息系统越来越容易受到伤害，即使已经有相当多的安全防护手段被广泛应用，其产生的安全效果和效率往往也不为人所知。因而如何度量信息系统的安全保障水平，也就受到了越来越多的关注。信息安全度量作为一个研究领域就提供这样的功能。它主要是解答以下几个方面的问题:

- IT 系统是否足够安全了?
- IT 系统现在是否比以前更安全了?
- 跟同行相比，我们的 IT 安全做的如何?
- IT 安全投资是否适度和均衡?
- IT 系统的安全是否合规?
- IT 安全的工作的有效性如何?
- IT 安全的工作效率是怎样的?

二、信息安全度量的定义和特性

2.1 度量、测量与测度

在不太严格的表述中，度量与测量有时互换使用。但实际上这个两个词是有明确区别的。测量是一次性的，通常是为了检测一个单一的事件，而在某一时点采集数据。测量可以用来提供某一时点的绩效快照。度量是基于一段时间周期的测量，用于支持更细致的分析并检验趋势和变化模式。

测度就是测量指标，根据其含义的复杂程度，分为基本测度和衍生测度（复合测度）。

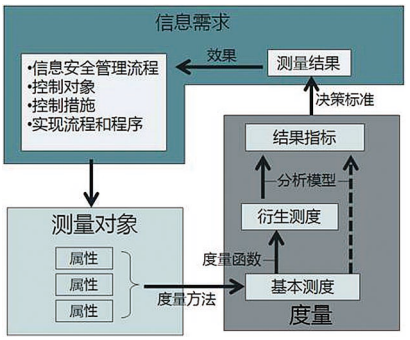


图 2-1 信息安全度量模型

基本测度用来度量安全对象的某个基本属性。衍生测度是由若干个基本测度根据一定度量函数（即计算方法）计算得来。而结论性指标则是按照一定的分析模型，由衍生测度计算出来。

测度的有四种标准的刻度：名目分类、排序、间隔、比率。其中基本测度主要使用

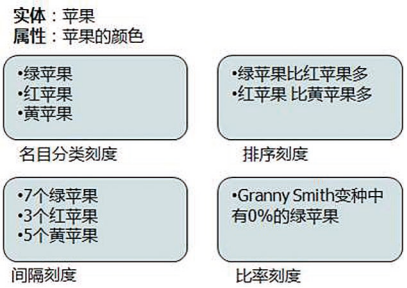


图 2-2 测度的刻度

后两种刻度，而衍生测度通常使用前两种刻度。基本测度往往是安全控制措施的覆盖率、实现率等。

2.2 信息安全度量的定义和特性

根据 NIST SP 80-55 中的对安全度量的定义，“度量是一种工具，它通过采集、分析、报告与绩效相关的数据，用来推进决策并改善绩效和问责。”

- **目标导向**：信息安全度量是基于信息安全的绩效目标为目的。也就是从度量指标的选择到度量步骤的实施，都要围绕着安全绩效目标来进行。

指标量化：信息安全度量方法是通过量化安全控制的实现、效果和效率，来监控信息安全目标和目的实现的程度。

- **连续跟踪**：信息安全度量必须产出可量化的信息以用于通过比较或代入计算公式的方式来分析并参照相同的参考点跟踪变化。通过比较连续的度量结果可以发现信息安全的改善与不足。也就是测度应该是可重复的，也是切合实际的，在实际上可以被用来诊断或改进的基础。

- **明确指向**：测度测量一个流程的特定部分或一个特定的安全控制措施。

- **可被测量**：测度应该是一个可以实践被测量的指标。

- **目标可达**：定义每个基本测度，都应该给出该测度的理想目标值。而这个目标值应该是可以实现的。

- **时间无关**：不受时间的限制，测度数据可以被足够频繁的采集。

安全度量的内容至少应该包括以下几个主要方面的信息：系统的脆弱性、外部环境的威胁、安全控制措施的效率 / 效能、系统合规状况、安全的投入产出比（ROI）。

三、安全度量的目的与客户价值

3.1 度量目的

信息安全度量的目的分为三个层次，最高层是战略目的。度量结果将影响整个公司

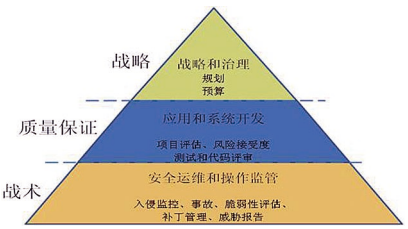


图 3-1 不同层次的信息安全度量的目的

的战略和治理，具体体现在工作规划和财务预算两个方面。中间的层次是质量保证目的。主要是针对应用和系统开发、系统建设等方面的工作，具体包括项目评估、系统测试、代码评审、过程监理方面的内容等。对底层是战术层面目的，包括安全运维和操作监管等方面的要求，如入侵监控、事故响应、脆弱性评估、访问控制、安全相关的人员管理等多种安全监控措施和安全管理要求。

3.2 信息安全度量的具体需求

- **了解当前的水平和状态**

信息安全度量首先要反映组织当前的信息安全工作的状态，为日后的监控和改进建立一个基准。

- **识别风险**

识别资产中存在脆弱性和威胁，脆弱性被利用的可能性有多大，以及威胁的烈度有

多强。一旦攻击成功或是脆弱性被利用，可能产生的影响是什么。从而最终确定哪些资产需要保护，以及它们的价值。

• **识别差距**

通过评估安全控制措施的有效性及其差距，可以了解安全控制措施的工作有多好，差距是什么？与差距相关的风险是什么？这里的差距包括两个方面，一是安全控制措施与现实的业务环境需求的差距，另一层含义是组织当前的安全水平与业界标杆的差距。

• **推进正确的活动**

确定差距造成的风险后，就可以识别出需要修补的薄弱措施以及工作的优先级，进而基于资产的风险水平做出资源的部署。

• **辅助决策**

安全度量的结果信息应能对企业整体的规划，尤其是信息安全方面的规划提供决策的依据。

• **呈现绩效和问责**

通过将企业的业务流程划分成各个岗位职责，识别每个岗位职责的风险控制点，并对每个控制点进行度量，得到每个岗位的信息安全绩效。进而根据绩效进行问责。

通过对安全控制措施的 ROI 分析，可以了解信息安全工作整体的绩效水平。

四、安全度量的方法论

4.1 安全度量的对象

广义上来说，安全度量的对象包含两方面内容：安全控制措施和安全控制目标（资产）。对应安全控制目标的度量，主要度量资产的风险状态。这部分工作有相当部分属于风险评估的范畴。因此一般所说的安全度量，更多的是强调对安全控制措施的度量。但是如果将人员也看作资产的一部分，人员安全也是安全度量的一个重要内容。

4.2 测度的类型（度量的导向）

所谓测度的类型（或度量的导向），也就是从哪些角度进行度量。对于这个问题，大体上有两种表述的方式，其本质是一样的，只是在分类范围和强调的侧重有所不同而已。对测度分类的不同理解，将影响到对测度指标体系的建立。

4.2.1 实施测度、效能/效率测度、影响测度。

• **实施测度**

实施测度用于呈现信息安全项目实施、特定的安全控制措施和相关的策略及流程的进度。例如“信息系统中具有被批准的信息系统安全规划的所占百分比”和“信息系统中具有作为配置要求的口令策略所占百分比”。

实施测度还可以在系统层次上进行检验。例如，“在一个系统中，具有标准配置的服务器所占比例”。 实施测度所要求的数据很容易从安全评估报告、季度和年度的 FISMA 报告、行动和里程碑计划（POA&M）和其它常用的信息安全项目活动的记录和跟踪方式。

开始的时候，实施测度的值可能小于 100%，但是随着安全项目及其相关的策略和流程的成熟，它应该达到并保持在 100%。 此时，组织应该将度量的重点放在效能 / 效率及影响测度上。随着组织的信息安全项目的参与以及绩效数据变得更加可用，度量将集中在项目的效能和效率以及安全控制措施实施的结果。一旦信息安全被整合到组织的流程中，这个流程是可重复的，度量数据采集变成全自动的，信息安全相关活动和事件对任务或业务影响可以用度量数据的分析和关联来确定。

• **效能 / 效率测度**

效能 / 效率测度是用来监控项目层次上的流程和系统层次上的安全控制措施，看其是否被正确实施、是否按预期操作和是否满足期望的输出。这些测度将注意力集中在评估的证据和结果上，而且也要求多个数据点来定量表示信息安全控制措施的实现，以及对组织信息安全态势上的结果效应。例如“企业操作系统漏洞中已经安装了补丁或已经用其它方式降低风险的所占比例”，它度量的是 NIST SP 800-53A 中漏洞修补控制措施的实现（SI-2），因为度量呈现是漏洞风险是否被降低的结果。同时，这个结果还显示了安全告警和公告控制措施（SI-5）的有效性，因为任何小于目标值的度量结果，都说明缺乏接收告警并成功的利用它们降低漏洞风险的能力。

效能 / 效率测度表达了安全控制措施实现结果的两个方面：结果自身的稳健性，称为效能。 以及结果的时间性，称为效率。再例如 “由访问控制的不妥配置引发的信息安全事件所占” 依赖于下列控制措施的实现和效能相关的信息: 事件监控(IR-5)、审计监控、分析和报告(AU-6)和配置变更监控(CM-4)。此外，“系统组件定期接收维护的所占比例”依赖于下列安全控制措施的效率：定期的维护（MA-2）和支持周期（SA-3）。

效能 / 效率测度为决策者提供以前策略和采购决定结果的关键信息。还能提供对改善信息安全项目绩效的深刻见解。效能 / 效率测度可以进一步用于连续监控工作的数据源，因为它们有助于确定控制措施的效能。效能 / 效率测度的结果，可以用于确定是否选择的控制措施在功能上是恰当的，并有助于促进排出正确活动优先次序。效能 / 效率测度也许要求将信息安全项目活动的数据与从自动监控和评估工具中获得的数据融合在一起。这种融合的方式可以直接与安全控制措施实现关联在一起。

• **影响测度**

影响测度是用于清晰的表达信息安全措施对组织任务的影响。这些测度天生就是组织专有的，因为每个组织有独立的任务。根据组织的任务，影响测度可以用来量化:

√信息安全项目或通过处理信息安全事件引出的成本而导致的成本节省

√通过信息安全项目赢得 / 保持公众信任的程度

√其它任务相关的信息安全影响

这些测度组合了安全控制措施实现结果的信息和各种资源信息。它们可以提供信息安全对组织价值最直接的观察，并且这些观察是管理层想要获得的。例如，“部门的信息系统预算专门用于信息安全的所占比例”依赖于下列 NIST SP800-53A 中的安全控制措施的实现、效能以及产出：资源的分配（SA-2）和采购(SA-4)。另一个更一般化的，与预算相关的影响测度是“信息安全投资报告的数量”，这个测度不是检验安全控制措施的影响，而是评价信息安全投资组合与预算流程之间的关系。影响测度要求以一种可以直接关联信息安全活动和事件的方式，在组织范围内的追踪各种信息源。

4.2.2 适应力、合规、ROI 测度

第二种分类方法体现了一种新的安全管理理念。这种理念认为，安全不是没有漏洞，而是如何很好的管理漏洞并挫败利用漏洞的企图；安全也不是没有攻击，而且在攻击来临的时候，如何让业务继续可用。安全也不

是没有中断，而且在中断发生后如何能迅速恢复。因此安全度量的侧重不是安全控制措施，而是系统的整体恢复能力或称适应力。在这个分类方法中，将影响测度分成了两个部分，一个是合规方面的影响，另一个是财务方面的影响。

适应力就是 IT 基础设施（包括物理的、人员的、IT 和安全控制措施）所具有的一种能力。该能力可以在保持基本服务并保护关键资产的同时，先发制人地击退攻击，并可以最小化崩溃和被攻陷的范围。适应力从物理安全、人员安全、IT 安全以及运营安全四个工程域来体现。

- **物理安全**：聚焦在物理实体（设施、资产、人）的防护。
- **人员安全**：各种不间断的措施，用来减少内部人员或已知的外部人员（如合作伙伴）对组织的逻辑和物理资产进行偶然和故意的修改、毁坏、侵吞、滥用、错误配置、非授权分发和不可用性。
- **IT 安全**：共同作用于 IT 设施使其达到并维持机密性、完整性、可用性、可靠性、可追溯性和真实性的内在技术特性和功能。
- **运营安全**：标准化的运营安全流程定义了用户、系统系统资源之间交互的本质和频率，目的是：（1）到达和维持一个已知的安全系统状态。（2）阻止偶然的或故意的对系统资源的偷窃、改变、滥用、毁坏、发布等行为。

合规是对各种法规的遵从。狭义上的合规是指对通用的或行业特定的法规的遵从。广义的合规还包括对企业自身的规范或政府的行政命令的遵从。狭义的合规包括对四个方面要求的遵从：财务金融、医疗保健、个人隐私、国家安全。

ROI 主要是度量组织在信息安全方面的投入是否足够，资源投入在 IT 安全的各个方面（如软件、硬件、服务、培训等）是否均衡，在各方面的投入是否取得了相应的成效。

4.3 安全度量的流程

对应安全度量的流程，不同的文献和标准中，表述不尽相同，但步骤大体上是相似的。Debra S. Herrmann 认为，安全度量的流程如图 4-1 所示：

图 4-1 Debra S. Herrmann 的安全度量流程

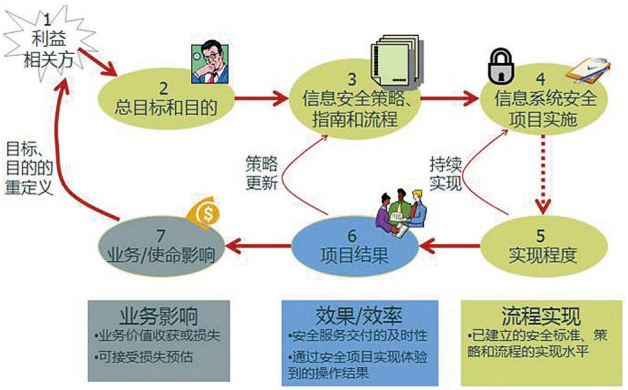


图 4-2A 信息安全度量开发流程

NIST SP800-55 Rev1 中，将安全度量的过程分为两个流程：信息安全度量开发流程（如图 4-2A 所示）和信息安全度量实施流程（如

图 4-2B 所示)。

图 4-2B 信息安全度量实施流程

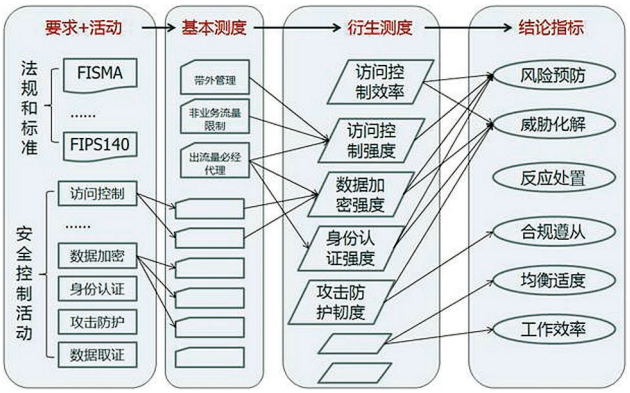


图 4-3 安全度量测度模型

ISO 27004 中，将安全度量分为四个步骤：(1）开发测度；(2）执行度量项目；(3）分析并报告结果；(4）对度量项目自身的评估与改进信息安全度量开发流程。

无论怎样表述安全度量的步骤，有两个最关键的步骤是相同的，一个是度量指标的建立，另一个是度量数据的采集。

4.4 安全度量指标体系模型

经过多年的信息安全度量实践，不同的组织和学者提出了很多测度指标体系模型，大体上可以分为三类，一类是民间的非盈利研究机构提出的模型，一类是基于能力成熟度模型（CMM）的模型，最后一类是一些被广泛应用的标准规范。无论哪种体系模型，基本测度、衍生测度、结论指标的层次关系都是一样的。图 4-3 只是给了一个测度模型范例，测度具体的名称和定义可以根据实际度量项目自行定义。例如结论指标可以采用平衡记分卡的模型。

4.4.1 CIS 的共识测度定义

共识测度定义是 CIS 发布的一个文档，它为 6 个重要的业务功能给出了 20 个测度定义，其它的业务功能的测度正在定义中，有待补充。这些尚未给出测度的业务功能包括: 数据 / 信息、反病毒控制、认证和授权、数据和网络安全、软件开发生命周期、补救努力、第三方风险管理 、附加的财务及影响度量、认证和授权。

4.4.2CISWG 的 ISPE 测度

CISWG（Corporate Information Security Work Group ）2005 年 1 月发布了一份关于信息安全最佳实践和度量的报告，将信息安全活动分为治理、管理和技术三个层次的 30 个信息安全项目单元(ISPE, Information Security Program Element)。标有 (B) 的单元，表示该单元是安全基线单元，该报告的附录 B 帮助组织选取初始的最小基线测度集合。基线测度与 13 项最小的基本信息安全实践相关联，

业务功能	管理视角	定义的测度
事件管理	对安全事故的检测、精确识别、处理和恢复做得如何?	• 事故发现平均时间 • 事故的数量 • 被内部控制措施检测到的事故比例 • 安全事故发生的平均间隔时间 • 从发现到控制的平均时间 • 恢复的平均时间
漏洞管理	在漏洞管理方面做得如何?	• 脆弱性扫描的覆盖率 • 无已知严重脆弱性的系统所占百分比 • 已知脆弱性的数量
补丁管理	维护系统补丁的能力如何?	• 补丁策略的合规 • 补丁管理的覆盖率 • 补丁安装的平均时间 • 部署重要补丁的平均时间
应用安全	是否可以依赖业务应用的安全模型来进行有计划的操作?	• 应用的数量 • 关键应用所占的比例 • 风险评估的覆盖率 • 安全测试的覆盖率
配置管理	系统配置的变化是如何影响组织的安全的?	• 完成变更的平均时间 • 具备安全评审的变更的比例 • 具有安全例外的变更比例
财务	信息安全支出的水平和用途是什么?	• IT 安全支出占 IT 预算比例 • IT 安全预算的分布

表 4-1 CIS 共识测度

被用来作为一个起点。该报告的附录 C 中提出的 5 项基本实践和标有 (SME) 的单元是为中小企业（雇员少于 500 的企业）提供的。

• **治理**

(1) 审查监督风险管理及与信息安全相关（如 SOX,HIPPA,GLBA,PCI-DSS）的合规工作

(2) 批准及接受概要的信息安全计划原则，并批准信息安全关键管理职责的任命

(3) 努力保护所有与信息安全相关的各方利益

(4) 评审与战略伙伴和第三方公司相关的安全策略

(5) 努力保证业务连续性

(6) 评审对内部和外部信息安全计划进行审计的规定

(7) 协同管理层确定向董事会汇报的信息安全度量内容

• **管理**

(8) 建立信息安全管理策略和控制以及监控合规

(9) 分配信息安全角色，职责，技能要求，强制推行基于角色的信息访问权限分配

(10) 评估信息风险，建立风险阈值并积极管理以缓解风险

(11) 确保实现对战略伙伴和其它第三方的信息安全要求

(12) 识别并给信息资产分类

(13) 制定并测试业务连续性规划

(14) 在采购，开发，运营和维护信息系统期间，批准信息系统的架构

(15) 保护物理环境

(16) 确保对信息安全规划的内外部审计及时跟进

(17) 协同安全人员确定向管理层汇报的信息安全度量内容

- **技术**

(18) 用户识别和认证

(19) 用户账号管理

(20) 用户权限

(21) 配置管理

(22) 事件和活动日志记录并监控

(23) 通讯，电子邮件和远程访问安全

(24) 恶意代码防护，包括病毒，蠕虫，木马 (ISPE24)

(25) 软件变更管理，包括补丁 (ISPE25)

(26) 防火墙 (ISPE26)

(27) 数据加密 (ISPE27)

(28) 备份和恢复 (ISPE28)

(29) 事故和脆弱性的检测和响应 (ISPE29)

(30) 协同管理层确定向董事会汇报的信息安全技术度量内容 (ISPE30)

每个单元对应若干个测度，对其进行度量。总共有 99 个测度。治理层面 12 个，管理层面 42 个，技术层面 45 个。其体系基本上是参照 NIST SP800-53 中的控制措施。没有考虑开发流程，也没有考虑 ROI 的问题。

4.4.3 SSE-CMM(ISO/IEC 21827)

SSE-CMM (System Security Engineering Capability Maturity Model) 的全称系统安全工程能力成熟度模型，它是国际系统安全工程协会 (简称 ISSEA，International Systems Security Engineering Association) 编制的一个规范，被国际标准化组织采纳为 ISO/IEC 21827，其中包含了 22 个过程域:

PA01 执行安全控制

PA02 评估影响

PA03 评估安全风险

PA04 评估威胁

PA05 评估漏洞

PA06 创建保障证据

PA07 协同安全

PA08 监控安全态势

PA09 提供安全输入

PA10 规范安全需求

PA11 验证和确认安全

PA12 保证质量

PA13 管理配置

PA14 管理项目风险

PA15 监控技术努力

PA16 规划技术努力

PA17 定义组织的系统工程流程

PA18 改进组织的系统工程流程

PA19 管理产品线演进

PA20 管理系统工程支持环境

PA21 提供持续的技巧和知识

PA22 与供应商协调

其中前 11 个过程域是与系统安全工程相关的，后 11 个是从 SE-CMM 引用的。

ISSEA 的度量工作组（MWG，Metrics Working Group）基于这个规范编写了 87 安全度量的测度。编写方法采用了 NIST SP800-55 中的模板，使用 ISO/IEC 21827 中的过程域（PA, Process Areas ）和最佳实践（BP, Best Practices）作为目的和目标。但是这些测度缺少清晰的分类，也没有明确的体系。

4.4.4 IA-CMM V3.1

IA-CMM 是由美国国防部下属的国家安全局 (NSA，National Security Agency) 编写的一个规范，由 9 个过程域组成:

IA-PA01: 提供培训

IA-PA02: 与客户的组织协调

IA-PA03: 指定初始的信息安全需求

IA-PA04: 评估威胁

IA-PA05: 评估脆弱性

IA-PA06: 评估影响

IA-PA07: 评估信息安全风险

IA-PA08: 提供分析和结果

IA-PA09: 管理信息安全保证流程

每个过程域中又包含若干个最佳实践，共 39 个最佳实践。这个规范的内容基本上从其它规范中引用的，也没有专门依据该模型的测度，因此这模型的参考意义比较有限，可以作为其它模型的一个补充。

4.4.5NIST SP800-53 Rev3

《联邦信息系统和组织中建议的安全控制措施》（NIST SP800-53 Rev3）将安全控制措施分为 18 个活动族，每个活动族用两个字母来命名。另外每个活动族分别属于某个通用分类：管理、运营和技术。其中前

缩写	活动族	类型
AC	访问控制 Access Control	技术
AT	意识和培训 Awareness and Training	运营
AU	审计和问责 Audit and Accountability	技术
CA	安全评估和授权 Security Assessment and Authorization	管理
CM	配置管理 Configuration Management	运营
CP	意外事故预案 Contingency Planning	运营
IA	事故和鉴定 Identification and Authentication	技术
IR	事故响应 Incident Response	运营
MA	维护 Maintenance	运营
MP	介质防护 Media Protection	运营
PE	物理和环境防护 Physical and Environmental Protection	运营
PL	规划 Planning	管理
PS	人员安全 Personnel Security	运营
RA	风险评估 Risk Assessment	管理
SA	系统和服务的采购 System and Services Acquisition	管理
SC	系统和通讯防护 System and Communications Protection	技术
SI	系统和信息整合 System and Information Integrity	运营
PM	项目管理 Program Management	管理

表 4-2 NIST SP800-53 安全控制活动族

17 个活动族与 FIPS 200 中的最小安全要求有对应关系，最后一个 PM 活动族在 FIPS 200 中没有涉及。为了识别每个安全控制措施，在活动族后面加一个数字来表示。例如 CP-9 是连续性规划（CP）族中的第九个控制措施。

每个控制措施的描述包括以下几个组件：控制描述、补充指南、控制扩展、参考依据优先级和基线分配（推荐的优先级代码用于实施安全控制措施期间的后续决策，初始分配给安全控制措施和控制扩展的低、中、高影响。）下面以 AU-5 作为范例说明。

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

针对保护的信息系统的某个特定方面，简要描述其需要的安全能力，如与安全相关的活动或需要执行的行动。控制描述特定的安全相关的活动或由组织或信息系统所执行的动作。有些控制措施允许组织给某些参数定义输入值来提供灵活性。灵活性通过使用指定 (assignment) 和可选 (selection) 操作来实现。组织可以通过灵活运用这两种操作，来支持特定的任务、业务和运营需求。例如组织可以指定当审计流程失败事件发生时信息系统的动作。指定系统中被审计的事件，执行系统备份的频率，口令使用的限制或组织策略和流程的分发列表。

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

补充指南：对控制措施相关的补充信息，属于期望实现的内容。

Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].

(2) The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [Selection: rejects; delays] network traffic above those thresholds.

References: None.

capability exists.

参考依据：法律、行政命令、指令、政策、标准、规范、指南。

Priority and Baseline Allocation:

P1	Low AU-5	Mod AU-5	High AU-5 (1)(2)

优先级和基线分配：推荐的优先级代码用于实施安全控制措施期间的后续决策，初始分配给安全控制措施和控制扩展的低、中、高影响。

4.4.6 ISO/IEC 27002

ISO 27002(2005) 将安全控制措施分为 11 个大类，共 39 个主要安全控制类别。以下是安全措施的具体分类，后面的数字是各分类中包含的主要安全控制类别，每个类别又由若干个控制措施组成。每一项控制措施有一个简要说明和具体的实施要求。

(a) 安全方针 (1)

(b) 信息安全组织 (2)

(c) 资产管理 (2)

(d) 人力资源安全 (3)

(e) 物理和环境安全 (2)

(f) 通信和操作管理 (10)

(g) 访问控制 (7)

(h) 信息系统获取、开发和维护 (6)

(i) 信息安全事件管理 (2)

(j) 业务连续性管理 (1)

(k) 符合性 (3)

ISO 27002(2009) 征求意见稿中，将安全控制措施重新梳理整合成 6 个大类:

1. 安全战略和治理

2. 信息安全管理和运营

3. 信息安全

4. 物理和环境安全

5. 人员安全

6. IT 安全

新的分类显得比以前更加合理。每个分类中的控制措施仍然由简要说明和实施要求两部分组成。除了分类做了调整，还对 2005 版的一些提法做了修改，增加了一些控制措施。

4.5 测度的编写

很多研究机构和商业公司都提出了一些安全度量的测度，但总体上还是比较零散，没有比较完整的体系。《安全和隐私度量的完全指南》一书中罗列了 900 多个基本测度。Metricscenter.net 网站上收集了一批依照不同的体系模型整理的基本测度。无论依照什么体系模型，基本测度的模板都一样的，基本上都包括表 4-3 中所列的元素。

4.6 度量数据的采集

一个成熟的项目通常使用多重的跟踪机制，来记录并量化其绩效的各个方面。可用的数据越多，度量的难度越小而数据自动采集的能力越高。数据采集自动化从数据源自动获取数据的能力与人工录入数据能力的对比。手工数据的收集包括编写问卷和对组织的职员进行访谈和调查。更有用的数据是来自半自动和自动的数据源 ---- 例如自评估工具，认证和鉴定数据库以及事件报告 / 响应数据库。

项目	描述
名称	对基本测度的命名
ID 号	唯一性编号
类型	测度类型, 类似 NIST SP 800-55 中的，实现程度、有效性、时效性、影响
目的	通过采集测度值所获得的所有功能，无论测度是被用来做内部绩效测量或者外部报告，也无论希望从测度洞察到什么，或是为了合规或法律的原因而采集测度。
描述	对量化测度的说明，测度的含义信息以及它的演化趋势；趋势的可能原因；纠正已发现缺陷的可能的解决方案；绩效目标；表示哪种趋势是对于绩效目标的正向趋向。
日期	创建和最后一次修订的日期
期望值	实现一个或多个被度量对象所期望达到的目标值
数据源	用来计算测度的数据存放地方
采集方式	问卷或访谈、自动工具、查阅文档
参考依据	法规、标准、规范、指南
公式	计算测度数值的表达式
频率	数据采集的时间周期
所属控制组	对应被度量的控制措施所属控制组
问题表述	通过问卷调查方式收集时，给出问题的表述

表 4-3 基本测度模板

成熟的数据采集是那种全自动的，所有的设计都是通过自动的数据源来收集的，没有人工参与和介入。

可以在现实中获得并用于绩效改进的测度的类型，依赖于安全控制实现的成熟度。虽然不同类型的测度可以同时使用，安全度量问题的原始焦点转移到信息安全项目实施的成熟度。随着信息安全项目目标和战略规划的文档化和实施，采集它们的输出结果的能力也会改进。

可能数据源包括:

- 系统日志
- 防火墙日志
- 求助热线日志
- 审计报告
- 用户调查
- 红蓝对抗评估
- 渗透测试、社会工程测试
- 漏洞扫描数据
- 配置核查数据
- 软件测试报告

4.7 度量数据的分析与度量结果呈现

度量数据的分析就是将数据代入到度量函数（见图 2-1）中，得到衍生测度的度量结果，再利用分析模型（见图 2-1）对衍生测度的值进行分析，得到结论性指标的结果。

度量函数实际上一种综合基本数据的计算方法，常用的方法有取极值、取平均值、取加权平均值、直接求和、间接求和（对各测度值给出评分，然后对评分求和）等。

分析模型实际上可以理解成一个评分体系，也就是对各个测度值给予一个分值，并给出计算总得分的方法。用户一般都希望用一个总的得分来表示信息安全工作的绩效和水平，尽管这样做未必合

理，但毕竟是现实的需求。给出总分的方法大致上可以分为两种，一种是得分制，通常是将满分值（100 或 10）分摊到各个测度上，该测度值满足目标值，则得分。最后的总得分反应的是信息安全工作在哪些方面做得比较好。还有一种方法是减分制，先假设信息安全工作十分完美，每检测到一个不满足目标的测度值，就减掉相应的分值。最终的得分直接反应的是信息安全工作的短板。减分值在本质上反应了信息安全度量的核心理念，即关注信息安全工作在哪些方面做得不够好，需要改进。而且减分制不用考虑总分值如何按比例分摊，直接扣减即可。调节权重参数相对容易。

结论性指标可以有多种形式，可以根据用户的习惯和偏好进行选择。例如可以用能力成熟度模型、平衡记分卡、自定义的能力指标等。例如，自定义的能力指标可以从事前、事中、事后以及效用 / 效率、影响等多个角度去考虑，因此信息安全保障能力可以定义为六个方面的能力：风险预防能力、威胁化解能力、反应处置能力、合规遵从能力、均衡适度能力、工作效率能力。

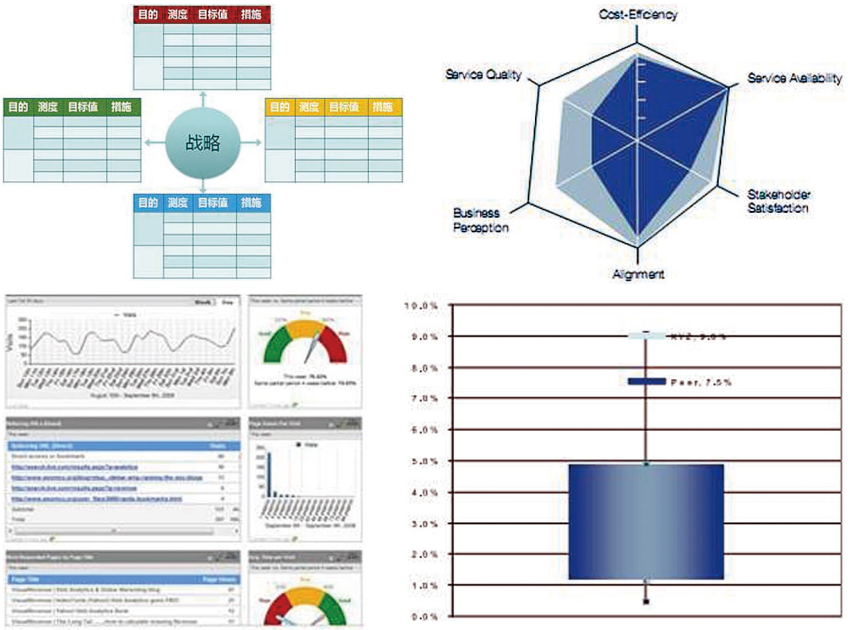


图 4-4　结论性指标的呈现方式

结论性指标的呈现也有很多方式，常见的有平衡计分卡、雷达图、蜡烛图、仪表盘（见图 4-4）等方式。

五、安全度量面临的挑战

5.1 安全度量的现状和实际操作还无法完全满足各方的期望

调查研究表明，利益相关方的期望对信息安全度量的成功有着很大的作用。这些期望基本都围绕着安全度量的可行性和度量结果的参考价值。理解并进一步满足这些期望有助于那些准备开展安全度量项目的组织获得成功。

5.2 安全度量的方法论在标准化、对领导力的依赖、数据建模等方面尚存缺陷

5.2.1 标准化的最小测度集合

采用一个最小的可裁剪的测度集是安全度量的良好起点。类似很多体育比赛中的标准化的统计，可以生成更新一层的兴趣。新

期望	挑战
信息安全度量是有限的工作将在短时间内完成。	信息安全度量只有把监控和改进信息保障状态及长期态势作为目标的时候才是有效的。
支持安全度量的数据的存在形式可以被直接用来度量。	支持安全度量的数据必须以特定的格式才能被识别、采集、存储及用于分析。 对数据采集和分析流程微小变更的预期将破坏数据对安全度量支持的质量，进而破坏用安全度量提供决策分析参考信息的可能性。
为安全度量设置不现实的目标，例如当组织还没有成熟的信息保障流程和足够的数据就将目标设定为识别产出的度量。 “要多久能看到安全度量返回的结果？”是利益相关方常问的问题。	期望与现实的差距造成了安全度量成功的不利条件。
在安全度量项目周期中过早的渴望自动度量变成自己计算。“要多久才能自动进行度量过程？”也是常见的问题。	过早的自动度量并自动计算往往产生相反的作用，除非度量已经被验证并被证明是可靠的和成功的。
度量应该有助于确定信息安全和保障的最大的 ROI，并定期的生成 ROI。高层管理者通常想利用度量来知道安全项目的 ROI。	常见的障碍是缺少对其它基本度量类型的强调和侧重。度量影响或者产出不是简单的计算，它要求一个成熟的度量项目进行之前要进行高精度的测量。

表 5-1 期望与挑战

的测度可以随着时间推移加入进来，但是核心的测度列表应保持固定以适应对技术变更的逾越。

5.2.2 数字驱动的风险度量从基础上破灭

风险是内在的关键的信息安全项目的元素。风险的复杂性决定了它很难用简单的量化模型来呈现。例如将复杂的网络流量浓缩成红绿灯将导致错误的度量。

5.2.3 持续和维护安全度量

安全度量项目的持续性与组织的领导力有很大关系。只要对项目的强有力的支持一直保持，安全度量项目就会健康的开展。不刷新基础数据的停滞的度量项目无法用于绩效优化的操作。安全度量项目的维护规划应该作为标准操作流程（SOP）或绩效管理规划的一部分。

5.2.4 定义和词汇

安全度量的方法正在趋于一致，包括一个通用的定义和词汇集合。然而要提高一致性的程度并在安全度量实践者中取得共识，还有更多的工作要做，董事会同意采用已有的标准和定义（NIST SP800-55 Rev1、ISO/IEC 27004、DHS SwA Framework）有助于保障安全度量工作的一致性。

5.2.5 已有的方法及方法论的不完善性

度量的方法及方法论已经有很多种，但是没有一个是完整的但又有很多可取之处。探索这些已有的方法与还没有被识别的附加的特性的组合将有助于推进安全度量谜题的解决，也有助于已有或正在出现的度量实现的持续改进。对通用定义达成共识以及董事会对已有的度量方法论及解决方案的认知是弥补差距的关键。

5.2.6 零散数据升华到一致的管理层测度

ISO/IEC 15939 和 ISO/IEC 27004 提供的模型具有一定借鉴作用，可以将个体的数据点升华为复合的指标，并用平实的语言来描述给各种受众。虽然通过案例研究的方式可以呈现这个升华的过程，但是个案的成功并不能证明这种过程具有普适性。

5.3 度量技术在实时性、自修复、通用性、自洽性等方面还存在缺陷

跨越技术差距对实现下一代稳定的信息安全度量非常关键。解决这些差距将有助于通过改进系统和网络的信息安全态势来完善效能 / 效率、影响性的安全度量项目。

5.3.1 实时和 / 或自修复的度量

因为实例反馈和即时诊断理念的盛行，时髦的专业人士广泛涌现。除了资金雄厚的场合，提供实时度量让信息安全行业有点捉摸不透。。“自修复”度量是一个安全度量的新术语，可以改善绩效自动化的活动。

5.3.2 改进数据格式的通用性

鼓励产业界设计和销售的商业产品使用标准格式采集和编制数据。将有益于创建和对比不同系统和组织的原始度量。

5.3.3 缺少可支撑已有结论的数据

“信息安全可以通过度量来证实”的理论的前提具备可信的用标杆数据来支撑。也就是通过对不同渠道采集的数据进行关联分析，来验证对度量标杆的假设。例如，“通过安全培训，用户可以更勤于选择更好的密码”关联来自培训统计、咨询台电话记录、密码破解工具的数据可以证实或证伪这个假设。许多类似的假设需要统计数据来呈现它们是真的正确或不正确。再例如，为什么每隔 90 天更换一次密码是最经济和最安全的，至今没有数学上的或者统计结论上的数据支撑。如果调查统计的结果，发现 90 天更换一次密码被破解的概率最小，则能可以把“90 天更换一次密码”作为安全度量的标杆使用。然而很多支撑数据涉及安全事故或当前的安全状况，需要各组织机构自愿的分享才能够得到。多数组织出于家丑不外扬的顾虑，不愿意公开与安全事故相关的情况和数据，使得建立标杆的工作相当困难。

六、结论

信息安全度量的概念从提出到具体的实践已经经历了 10 多年的时间，逐渐形成了比较成熟但不是非常严谨和完整理论体系，还需要进一步统一共识。目前更多的还是停留在方法论的层面，缺少具体实务性的操作指导。

业界在安全度量方面也开展了大量的实践。但由于理论体系的局限，安全度量的概念尚没有被用户广泛接受。安全度量项目还是以手工采集数据为主，基本上都是以咨询服务的形式开展。缺少自动化的 IT 工具，导致安全度量的可比性、权威性以及效能 / 效率都还不令人满意。

为了应对安全度量面临的挑战，需要在以下几个方面做更深入的工作：鼓励厂商、用户、权威机构、学术界等各方面的专家共

同研究制定统一的度量模型和方法论。

广泛宣讲安全度量的方法论和过程，使用户的期望更加回归理性和符和实际。

鼓励行业客户尽可能的将自身的安全措施和当前状况共享出来，以便制定出科学客观的行业标杆。

鼓励安全厂商技术创新，提高安全度量操作的自动化和可持续性。进而提高度量工作的效率。

随着信息安全的新技术、新模式的采用和推广，如云计算的普及、物联网的兴起，还需要开发新的安全度量测度来度量新的目标对象。

参考书目

1.Debra S. Herrmann, "COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS----Measuring Regulatory Compliance,Operational Resilience, and ROI" ISBN 0-8493-5402-1

2.Information Assurance Technology Analysis Center (IATAC), "Measuring Cyber Security and Information Assurance" State-of-the-Art Report (SOAR) May 8, 2009

3.Corporate Information Security Working Group, "Report of the Best Practices and Metrics Team." Revised January 10, 2005

4.The CIS Security Metrics, "Consensus Metric Definitions v1.0.0 " May 11 2009

5.ISSEA Metrics Working Group,"SSECMM-Metrics"

6.NIST SP800-55 Rev1 《信息安全绩效度量指南》

7.NIST SP800-53 Rev3《联邦信息系统和组织中建议的安全控制措施》

8.ISO 27002(2005) 《信息安全管理实用规则》

9.ISO 27004() "Information technology—Security techniques—Information security management—Measurement "

网络协议分析方法探究

开发中心　程利军

摘要：现在有很多的软件采用了自定义的协议，作为工程师，往往需要对这些协议进行识别和分析。本文介绍了一般分析未知协议的方法和步骤。

关键词：网络协议　协议分析方法　逆向分析

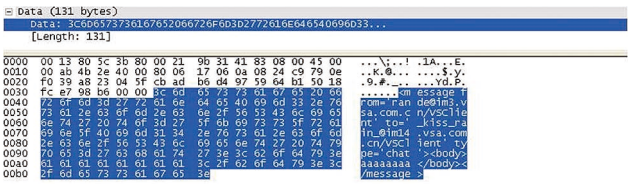
在网络传输数据流中，有着各式各样已知的、未知的协议和数据，对于已知协议的数据，我们可以参考相关协议描述文档，也可以使用一些现有的工具对其进行识别和分析，如 wireshark、Microsoft Network Monitor 3.3 等工具。

而对于未知的网络协议，这部分一般是由网络程序自己定义的一些数据结构，我们往往没有现成的文档和工具可以参考使用。（注：这里所指的未知的网络协议，一般是指应用层协议）

而我们在工作过程中，经常需要对这些使用未知协议的网络软件进行分析，通过识别其数据包进而对其进行监控、阻断等操作。

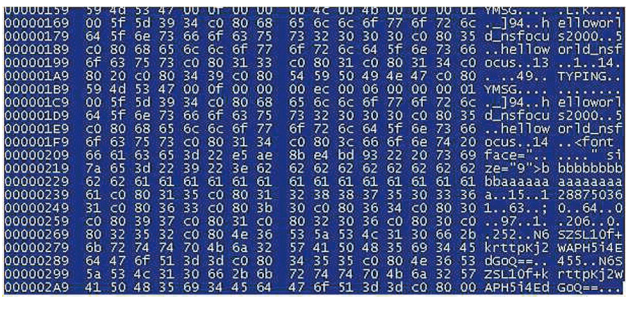
当然对于一些简单的网络协议，我们可以直接通过数据包就可以发现其中的规律，如下是游戏平台 vs client 中与好友交互聊天时的数据包，我们可以看到它的数据采用 xml 的结构，结构大体如下：

<message from=’ {sender}’ to=’ {reciver}’ type=’ chat’ ><body>{data}</body></message>



而更多的情况，我们面对的是复杂的协议，里面有各种自定义的字段的数据包，我们就需要通过逆向的手段来分析它们的意义了。

譬如雅虎通聊天时产生的数据包如下：



我们无法分辨里面字段的具体意义。

下面以雅虎通为例，通过简单的分析聊天数据包的数据结构，给大家介绍，处理未知协议时的一般方法。

准备工具:

Olldbg(OD)：用于动态调试

Wireshark：用于抓取相关数据包

IDA：用于静态分析

我们登录雅虎通，并打开 wireshark。

然后使用 od 附加到 YahooMessenger 进程上，然后在 WSARecv 函数下断点。

（注：在动态跟踪网络交互软件的时候，一般会在一些常见的处理网络数据的 API 下断点来调试。

下面列举了常见的可以从网络套接字里读取数据的 API 调用。

read/write

recv/send

recvfrom/sendto

WSARecv/WSASend

WSARecvFrom/WSASendTo

ioctl

ioctlsocket

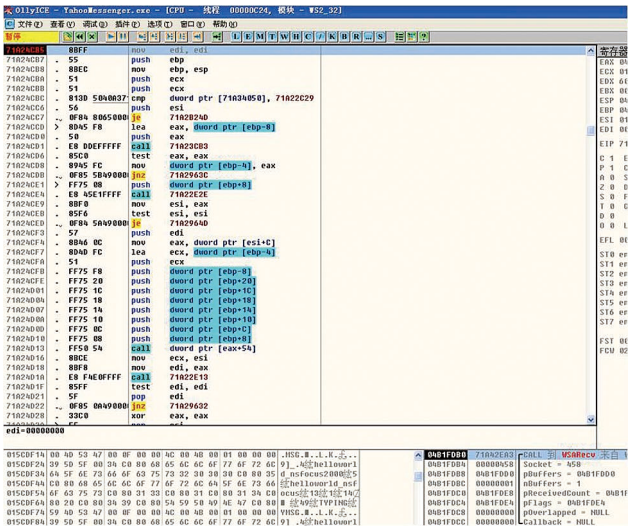
WSARecvDisconnect/WSASendDisconnect

WSARecvEx/WSASendEx

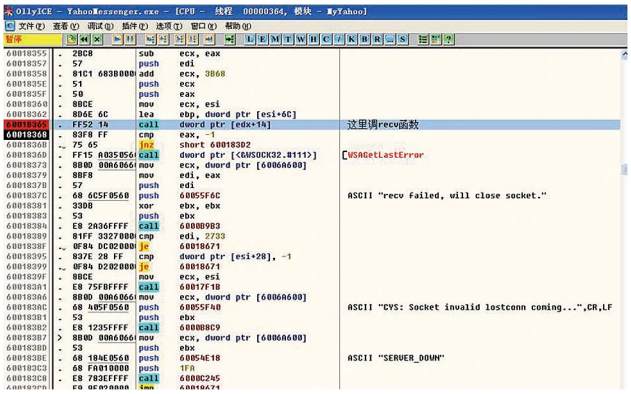
recvmsg/sendmsg

WSARecvMsg/WSASendMsg

接下来给这个已登录的雅虎通发信息，Od 成功断在了 WSARecv 函数的地方，如下图:



我们单步运行几步，走到了 myYahoo.dll 的领空。



接下来的部分便是处理该数据包的部分了。

收到的数据包如下:

0000 59 4d 53 47 00 0f 00 00 00 fa 00 06 00 00 00 01 YMSG.....

0010 00 48 7f 7c 34 c0 80 68 65 6c 6c 6f 77 6f 72 6c .H.|4..helloworl

0020 64 5f 6e 73 66 6f 63 75 73 32 30 30 30 c0 80 35 d_nsfocus2000..5

0030 c0 80 68 65 6c 6c 6f 77 6f 72 6c 64 5f 6e 73 66 ..helloworld_nsf

0040 6f 63 75 73 c0 80 31 34 c0 80 3c 66 6f 6e 74 20 ocus..14..<font

0050 66 61 63 65 3d 22 e5 ae 8b e4 bd 93 22 20 73 69 face="....." si

0060 7a 65 3d 22 39 22 3e 6c 6c 6c 6c 6c 6c 6c 6c 6c ze="9">llllllll

0070 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c llllllllllllllll

0080 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c c0 llllllllllllll.

0090 80 31 35 c0 80 31 32 38 38 37 36 33 36 32 37 c0 .15..1288763627.

00a0 80 36 33 c0 80 3b 30 c0 80 36 34 c0 80 30 c0 80 .63..;0..64..0..

00b0 39 37 c0 80 31 c0 80 32 30 36 c0 80 30 c0 80 32 97..1..206..0..2

00c0 35 32 c0 80 46 42 78 31 68 66 68 34 57 5a 63 55 52..FBx1hfh4WZcU

00d0 67 62 59 44 30 78 70 54 79 44 59 7a 4c 58 66 6b gbYD0xpTyDYzLXfk

00e0 4f 67 3d 3d c0 80 34 35 35 c0 80 46 42 78 31 68 Og==..455..FBx1h

00f0 66 68 34 57 5a 63 55 67 62 59 44 30 78 70 54 79 fh4WZcUgbYD0xpTy

0100 44 59 7a 4c 58 66 6b 4f 67 3d 3d c0 80 00 DYzLXfkOg==...

我们用 ida 加载 myyahoo.dll，然后静态分析。

由上面可知在 60018365 处调用 recv 函数，ida 直接跳转到这个地址。

发现如右上图代码:

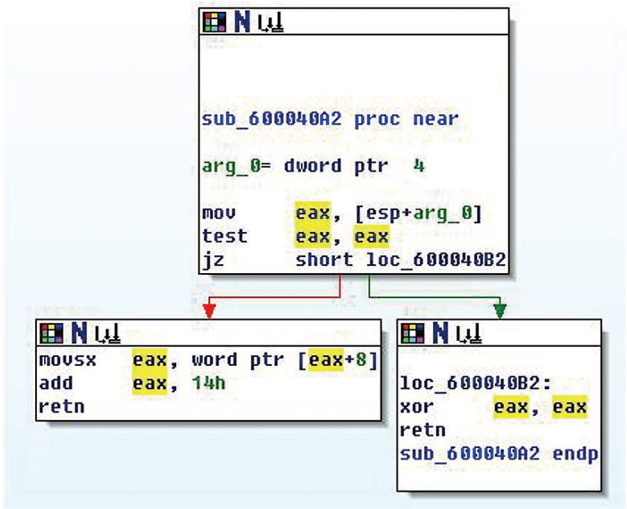
Call dword ptr[edx+14h] 处调用 recv 函数，执行成功后，返回数据包的长度。

接下来对收到的数据包进行处理（见右下图）。

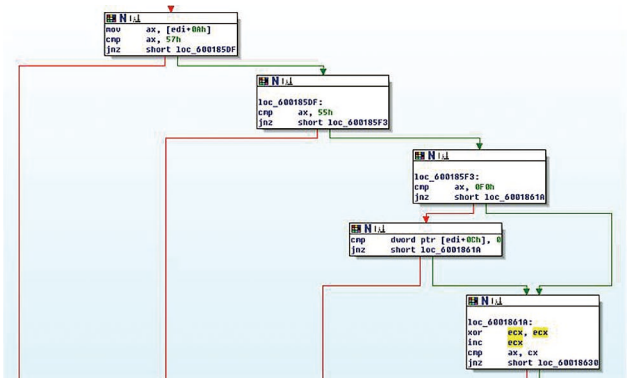
```
sub_60018348 proc near
push    ebx
push    ebp
push    esi
mov     esi, ecx
mov     eax, [esi+3B68h]
mov     edx, [esi]
sub     ecx, eax
push    edi
add     ecx, 3B68h
push    ecx
push    eax
mov     ecx, esi
lea     ebp, [esi+6Ch]
call    dword ptr [edx+14h]
cmp     eax, 0FFFFFFFFh
jnz     short loc_600183D2
```

```
mov     ebx, offset Str ; "YMSG"
push    ebx             ; Str
call    strlen
push    eax             ; Size
push    ebx             ; Buf2
push    ebp             ; Buf1
call    memcmp
add     esp, 10h
xor     ebx, ebx
test    eax, eax
jnz     loc_6001867B
```

比较前四个字节是不是 “YMSG”，可以看出，它通过这个标记来确定是否为雅虎通协议的数据包。



可以看到第 8 个字的偏移处是数据长度，而 0x14 则是数据头的大小，两者相加，为整个数据的大小。



在 0x0a 偏移处取值，与 0x57,0x55,0xF0 比较，可以确定，这个值是 type, 而聊天的这个数据包中的这个值为 0x06。

经过上面的分析

// 大小为 0x14 的数据头的大体结构如下:

Struct yahoo_header

{

DWORD flag;//always 〃YMSG〃

DWORD unknown;// 这个值是固定的，为 00 0f 00 00

WORD data_length;// 是长度

WORD type;// 类型. 有 4B,57,55,F0

DWORD unknown;//status,

DWORD sessionid;// 一个随机值，每次建立会话后固定.

}

接下来我们来找处理消息体的地方:

```
.text:0060CB33          push    ebx
.text:0060CB34          mov     ebx, ds:strstr
.text:0060CB3A          push    esi
.text:0060CB3B          push    offset aA_0     ; "纰"
.text:0060CB40          push    [ebp+SubStr]    ; Str
.text:0060CB43          call    ebx ; strstr
.text:0060CB45          test    eax, eax
.text:0060CB47          mov     esi, [ebp+arg_C]
.text:0060CB4A          pop     ecx
.text:0060CB4B          pop     ecx
.text:0060CB4C          mov     [esi], eax
.text:0060CB4E          jz      short loc_60CBA6
.text:0060CB50          push    [ebp+SubStr]    ; SubStr
.text:0060CB53          mov     byte ptr [eax], 0
.text:0060CB56          call    ds:atoi
.text:0060CB5C          mov     ecx, [ebp+arg_4]
.text:0060CB5F          mov     [ecx], eax
.text:0060CB61          mov     edi, [esi]
.text:0060CB63          add     edi, dword_869DF4
.text:0060CB69          mov     [esp+10h+var_10], offset aA_0 ; "纰"
.text:0060CB70          push    edi             ; Str
.text:0060CB71          call    ebx ; strstr
.text:0060CB73          test    eax, eax
.text:0060CB75          pop     ecx
.text:0060CB76          pop     ecx
.text:0060CB77          mov     [esi], eax
.text:0060CB79          jnz     short loc_60CB89
.text:0060CB7B          push    eax             ; Val
.text:0060CB7C          push    edi             ; Str
.text:0060CB7D          call    ds:strchr
.text:0060CB83          pop     ecx
.text:0060CB84          pop     ecx
```

根据上述代码结合数据包，我们可以知道，它的数据部分采用 id + 0xc080+value+0xc080 这样的结构组成，所以数据部分的结构如下:

```
struct small_struct
{
  char id;
  WORD flag;//always 0xc080
  char value[n];
  WORD flag2;//always 0xc080
}
  struct yahoo_data
{
  small_struct data[N];
}
```

通过上述的分析，我们简单的得到了雅虎通协议包的大体结构。

```
struct yahoo_msg_data
{
  yahoo_header header,
  yahoo_data data
}
```

文章到这里就该结束了，希望大家看后会有所收获. 。

参考文献

IDA Pro 代码破解揭秘 (第七章)

智能化测试漏洞发掘技术浅析

研究部　曲富平

摘要：本文对现有漏洞发掘技术的优缺点进行了比较，并进一步介绍了漏洞发掘技术的最新进展。

关键词：漏洞发掘　智能化

漏洞，作为挂马工具甚至信息战中重要一环，最近也受到越来越多的关注。对于普通人来说，发掘各种软、硬件的新漏洞，是一件很神秘的事情。而对于专业人员来说，发掘漏洞需要的是耐心、积累、运气和方法。

随着时间的推移，初级漏洞在流行软件里逐渐消失，因此漏洞发掘的方法也在进化。从简单的代码扫描、无格式简单二进制Fuzz，到复杂代码审计（自定义检测规则）、复杂二进制文件格式生成与Fuzz，发现的漏洞类型越来越复杂，但这并不代表使用方法的终结，好戏还在后头……

几个概念

漏洞发掘

在总结已有漏洞模式的基础上，通过人工或者自动化方法，对目标（软、硬件平台，网络应用等）进行新漏洞的发现及确认。

动态测试

通过人工或者自动化方法，通过运行软件来检验软件的动态行为和运行结果的正确性。

静态分析

无须执行被测对象，而是借助人工审查或者专用的软件测试工具，对被测对象的代码或者二进制镜像进行检测。

覆盖率

软件测试的一个度量，用以衡量运行代码占总代码的比例，覆盖率越高，测试也越充分。

漏洞发掘的常用手段

静态代码审计

在源代码可获得的前提下，通过人工审核或者自动化工具来进行代码检测。

比较有名的商业自动化工具有:

- Coverity：开发者前身来自于斯坦福大学，以研究程序Bug为主要方向，曾经找到Linux内核/MySQL/ Android等多种开源软件的许多Bug。
- Fortify：生产专门用于目标安全的静态分析工具，客户包括美国国土安全部、NASA等多家大型政府机构及商业银行。
- Klocwork：生产专门用于目标安全的静态分析工具，客户包括AMD、AOL、

Cisco、Philips、QualComm 等多家大型公司。

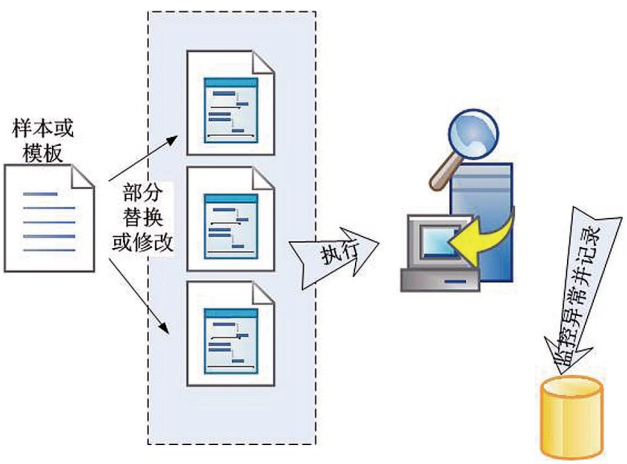
Prefast：内嵌在微软 Visual Studio 2005 之后的版本里，可以检测用户编程时遇到的不少问题 。

静态代码审计兼有静态分析和代码审计两者的特点。优点是分析面广，可在不考虑覆盖率和运行环境的情况下，能够发现很多潜在的问题；缺点也很突出，发现的问题不一定在真实环境里触发（不一定能运行到潜在的问题代码），对于没有源代码的很多商业程序也不适用。

动态 Fuzzing

采取动态测试的方式，以已有的二进制文件或者文本模板为基础，对待测目标的外部接口进行充分检测，可以用下面的图例表示：

动态 Fuzzing 的特点也很明显。优点是不需要源代码，Fuzz 出的结果如果出现异常可以立即作为分析使用，对测试目标不需要有深入了解；缺点是受测试样本 / 模板的局限很大，造成测试的覆盖率很低，对于有校验 / 压缩等情况，如果 Fuzz 较弱，可能会做很多的无用功。



新进展—智能化测试

无论是动态 Fuzz 还是静态代码检测，突出的问题就是分析过程不够智能，没有一个学习与反馈的机制，以测试图片浏览器为例：

- 静态代码检测，假如我们手头有这个浏览器的源码，并且也用静态分析工具找到了一个溢出点，这时我们仍然难以得到可以触发漏洞的样本图片。
- 动态 Fuzzing：从网上找到一些图片样本，并在样本上做少许改动进行 Fuzz，这样 Fuzz 也未必经过溢出点，而且从覆盖率来看，fuzz 后的样本和原样本也未必有太大区别。

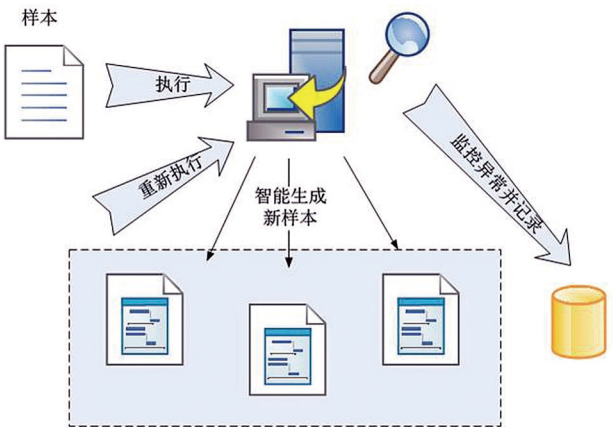
因此，我们需要更智能的方法，用更智能的测试用例来获得触发样本。

智能化测试的简单原理如下所示：

目前的尝试包括：

a)SAGE：微软的一个研究项目，基于源代码的分析工具。纯静态分析，可以利用源代码的各种有利信息（如类型信息），利用符号执行和约束求解来对潜在漏洞触发点进行搜索。目前根据微软给出的论文，其分析结果与实际结果常常有较大差异。

b)SmartFuzz/CatchConv：由 UC Berkeley 的研究人员发起，在 Linux 平台上采用基于 valgrind。纯动态分析，不依赖源代码。



相对于 zzuf 等纯二进制 Fuzz 工具来说，效率并不高，发现新的路径能力也不够强。

c)EXE/KLEE：由斯坦福的研究人员发起（该研究人员也是 Coverity 的研究者）。基于 LLVM 生成的中间代码进行分析，覆盖率高，目前只能分析小范围的目标。KLEE 最突出的特点，是能直接给出符号解（文件的内容，标准输入等）。

d)Intscope：由北大研究人员发起，为纯静态检测。基于二进制代码，检查的漏洞类型单一，只有整数溢出类型。根据论文描述，已经检测出多个开源 / 闭源软件的整数溢出漏洞。是否能直接给出符号解目前还不是很清楚。

e)BitBlaze：有 UC berkeley 的研究人员发起。基于 Qemu 的动态检测，不能产生新的路径、只能动态跟踪污点数据并给出报警，适用于监控恶意软件。

f)Funnywei 在最近几年的 Xcon 和 VARA 会议上也有一些关于动态检测的议题。

不足与展望

智能化测试虽然有很多优点，但是也有一些难以解决的问题：

- 关于测试规模与覆盖率：对于简单的测试对象（如数千行代码），智能化测试可以给出所有分支的测试样本，但是对于大规模的商业代码，每个分支都测试到需要大量的资源，由于分支数量是指数级增长，因此需要一些规则对分支进行选取，会带来一定的覆盖率损失。SmartFuzz 在测试的时候使用了 Amazon 的云计算，可见这种方法对资源的要求之大。
- 关于适用范围：目前的智能化测试最适合用来测试二进制格式的数据文件解析，尤其像 KLEE 这种工具，如果规模小，可以直接把所有的分支测试结果样本输出。但是对于文本格式的解析（如 HTML/JS）或者基于 OpCode 的虚拟机平台（如 Flash 的 DOABC Tag）并不适合，这是因为可能的分支数量实在太多（子子孙孙无穷匮也），智能化测试不可能穷举出所有可能的情况。
- 关于检测漏洞的类型：只能以常规漏洞为主，无法检测出逻辑型的漏洞，这是因为逻辑型的漏洞通常难以用规则来定义，个体差异太大。目前这种类型的漏洞还是只能通过人工的方法代码审计或者编写静态分析规则。

希望不久的将来，会出现更多更好的智能化测试工具供漏洞研究人员使用。

绿盟科技荣获 2010 年度十大金融科技杰出企业称号

11 月 26 日，绿盟科技应邀出席 2010 年度中国金融科技发展论坛，并荣获“2010 年度十大金融科技杰出企业”称号。本次论坛以“金融信息安全”为主题，吸引了来自金融管理机构、中央部委以及银行、证券、

保险等领域的信息科技工作者、IT 专家约二百余人出席此次会议。绿盟科技金融行业安全顾问徐一丁发表题为“金融基础设施安全保障”的演讲。

徐一丁在演讲中指出，随着金融业务的高度 IT 化，IT 基础设施的安全性也越来越重要。金融机构在设计 IT 基础设施的保护措施时，需要从业务需求出发去考虑。业务目标和拓展模式将直接影响 IT 系统的功能与安全目标，基于这样的安全目标去考虑相应的威胁与保护手段，才能做到有的放矢。同时，金融机构之间业务目标和自身条件差异巨大，决定了 IT 基础设施的要求也随之提高。如银行和证券公司在业务连续性方面的要求比保险公司高得多；各银行常见的保证金第三方存管业务，对大型银行和中小银

行也不同。金融机构需要充分考虑这些因素，制定出能够切实满足业务目标的 IT 基础设施保障方案。

作为长期服务于金融行业客户的网络安全企业，绿盟科技一直以来凭借扎实的技术与专业的服务能力，针对金融行业的网上银行、网上证券、网上支付及其他各类金融业务，提供自己的解决方案。在深入研究金融行业监管部门的安全合规要求基础上，探寻其安全风险及保护技术。发布的解决方案包括《网上银行 DDoS 攻击防御方案》、《网上银行安全评估及专项服务解决方案》、《网上证券防盗买盗卖安全解决方案》、《证券行业安全综合方案》等。

云安全监测保障金融网站安全—绿盟科技参加第五届中国金融 CIO 年会

日前，绿盟科技应邀参加“第五届中国金融 CIO 年会”并做主题演讲。本次年会以“云计算时代的技术应用创新之道”为主题，吸引了来自工商银行、农业银行、中国银行、建设银行、中信银行、光大银行、中国证券业协会、银河证券、中国再保险公司、中国人寿、泰康人寿等几十家单位的多位信息化资深专家及领导。

会上，绿盟科技金融行业销售总监郝东林以“金融网站的云安全监测”为主题进行了演讲。他指出，“随着金融网上交易、电子商务的快速发展，金融机构网上交易将成为主要模式。如何实现金融网站和网上交易的实时监测、实时监控、实时安全，已经成为金融机构面临的共同问题。针对金融网站和网上交易面临的现实问题，比如出现问题无

绿盟科技郝东林在做主题演讲

法实现实时通知、无法 24 小时监控、缺乏历史数据进行长期风险分析等，绿盟科技推出了基于云安全平台的绿盟科技网站安全监测服务。该服务采用透明部署模式，无需改变现有网络结构和管理体系，有效地解决了令管理者头痛的问题。”

中国银行 IT 蓝图办公室总经理王世辉做了“银行业的 IT 规划战略”的主题演讲，王总在演讲中指出，“银行业的 IT 和战略是投资回报率最高的，而交易和信息则是关键基础之一”，针对交易和信息的重要性，王总也做了深入的需求剖析。

据悉，绿盟科技的云安全监测服务自推出以来，已经在国内数家金融行业客户中得到广泛应用。作为“巨人背后的专家”，多年来，绿盟科技一直关注应用层的安全研究。目前，针对金融业的行业特点，从 IT 风险管理咨询与评估、金融行业数据中心整体安全、Web 应用安全解决方案等，绿盟科技已真正实现为客户的 IT 安全保驾护航。

绿盟科技 IPS 蝉联入侵防御硬件市场第一名

近日，国际权威咨询机构 IDC 发布了《2010 年上半年中国 IT 安全硬件市场 2010-2014 分析与预测》报告。报告显示，绿盟科技 IPS 产品以 18.4% 的市场占有率蝉联中国入侵防御硬件市场第一名。2010 年，中国 IT 安全硬件市场延续了快速增长的势头，上半年整体实现了 18.9% 的增长。其中，统一威胁管理、入侵防御和安全内容管理分别以 28.6%、28.1% 和 64.7% 的增长率成为增长最快的三类产品。

根据 IDC 报告的统计数据显示，绿盟科技网络入侵防护系统和网络入侵检测系统表现强劲，其市场总体份额超出国内外其它同类产品，继续占据国内入侵防御和检测市场的领导者地位。而就在 10 月 18 日，绿盟科技刚刚获得了 Frost&Sullivan 颁发的“2010 中国 IDS/IPS 市场占有率领导者奖项”，成为首个蝉联 BPA 最佳实践奖的中国信息安全厂商。

作为漏洞分析和攻防研究领域的领导厂商，绿盟科技时刻关注各类安全威胁变化，并持续提升产品和服务品质。经过 5 年潜心研究与发展，绿盟科技 IPS 在 2010 年 3 月顺利通过 NSS Labs 严格测试，并获得国内首个、全球第四个“Recommended”级别认证，能够为用户提供具有国际品质的高性价比入侵防护解决方案。

绿盟科技发力 DNS 防护，全面布局域名安全

10 月 26 日，绿盟科技（NSFOCUS）在北京举办了 DNS 域名安全防护产品新闻发布会。此次 DNS 域名防护专项产品的发布，标志着绿盟科技已经全面进入 DNS 域名安全领域。绿盟科技副总裁吴云坤出席此次会议，并做主题演讲。发布会吸引了众多知名 IT 媒体的参与和关注。

近年来，DNS 域名已经成为整个互联网发展的基础服务，DNS 域名安全逐渐成为网络安全的热点，对互联网的发展具有决定性影响。《中国域名服务及安全现状报告》

中的一组数据表明，截至 2010 年 8 月 10 日，监测到国内的域名服务器总量为 978,713 个，超过 4% 的递归域名服务器端口随机性较差，容易遭受 DNS 劫持攻击，远高于全球范围 0.98% 的平均水平。对国内重要信息系统所涉域名抽样统计发现，57% 的域名解析服务处于有风险的状态，其中 11.8% 的域名因配置管理不当，处于较高风险状态。潜在的 DNS 域名安全隐患以及已经发生的事件，都表现出 DNS 域名安全维护处于相对“粗放”的状态，整个 DNS 域名安全服务链条也需要进行强化。

“DNS 既是基础设施，需要保护它；也是制高点，能够利用它做安全的工作”，吴云坤副总裁表示。绿盟科技致力于 DNS 域名漏洞的研究，深刻掌握 DNS 域名安全的核心与本质，从而得以有步骤有重点地从各个方面入手，包括 DNS 域名可用性、DNS 域名解析正确性、DNS 域名合法性以及 DNS 攻击检测与防护，全面布局 DNS 域名安全产品及解决方案的发展规划，整体性覆盖 DNS 基础架构、DNS 服务及 DNS 应用层面。

2006 年，绿盟科技黑洞产品为 IDC

提供抵御 DDoS 的能力。2009 年绿盟科技投资 DNSpod，保护 DNS 域名服务商。2010 年 8 月，推出针对普通用户的 DNS 监测服务；同月推出基于网站信誉库的 DNS OpenAPI，紧密关联各类域名系统，有效检测网站挂马；同月，成为 StopBadware 的数据提供商，有效提升中国地区恶意网站数据的及时性和准确性；9 月推出针对网站用户的 DNS 域名安全监测服务；10 月携手 CNNIC，为站点进行网站结构分析、漏洞分析，帮助 Web 站点提高安全性。10 月，绿盟科技发布 DNS 域名防护专项产品。

“这个产品完全不影响用户的现有基础架构，部署简单灵活，DNS 域名安全性以及业务的可持续性，得到极大提升。您随时可以通过可视化的窗口，掌控 DNS 运行信息”，绿盟科技产品市场经理崔云鹏说到，“在未来，还可以实现检测非法网站、僵尸网络，以及实现客户端访问域名的安全性。”产品推出的背后，正是绿盟科技全面布局 DNS 域名安全防护的结果。

DNS 域名安全强化与稳固，让用户得以整体化、全方位强化 DNS 域名以及相关架构，将更多的时间和精力投入到业务本身。此次 DNS 域名安全防护产品的成功发布，标志着绿盟科技 DNS 域名安全防护架构及解决方案已经成熟。

北京市委常委、海淀区委赵凤桐书记参观调研绿盟科技

近日，北京市市委常委、海淀区委赵凤桐书记在区委常委、区委办公室刘鸿主任，海淀园管理委员会王际祥常务副主任，海淀区委办研究室党慧海副主任，海淀区紫竹院街道工作委员会田桂茹书记等领导的陪同下，来绿盟科技调研并指导工作。

绿盟科技总裁沈继业热情接待，并代表公司对赵书记一行的到来表示欢迎。随后沈总向赵书记汇报了公司发展历史与现状、规模、产品、经营等几方面情况，分析了国内

赵凤桐书记参观绿盟科技

信息安全市场情况，并重点介绍了公司国际市场开拓的情况。

听取汇报后，赵凤桐书记对绿盟科技近年来取得的成绩给予了高度评价。他指出：中国信息安全产业的发展前景很好，信息安全行业从认识到发展有个过程，目前信息安全产业迎来快速发展的时代，企业要抓住时机。同时他还建议绿盟科技作为行业技术领先企业，应该积极参与标准的制定，更好的在国际市场中发展。

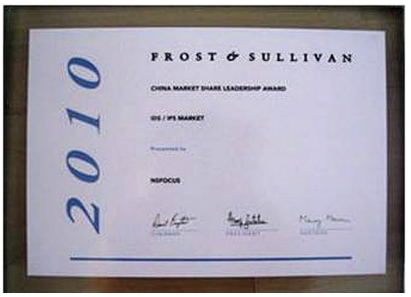
绿盟科技喜获 2010 中国 IPS/IDS 市场占有率领导者奖

在政府、国防、金融、电信等大型客户刚性需求的拉动下，中国 IDS/IPS 市场同比实现了 19.5% 的强势增长，而绿盟科技则以 28.2% 的市场份额位居第一。”

近日，绿盟科技在新加坡举行的 Frost&Sullivan 年度颁奖盛典上喜获“2010 中国 IPS/IDS 市场占有率领导者奖（2010 China Frost&Sullivan Market Share Leadership Award in the IDS/IPS Market）”，这是绿盟科技在继去年获得“2009 中国 IPS/IDS 市场增长战略领导者奖”之后，再次摘取最佳实践大奖（Best Practices Award）。

Frost&Sullivan 最佳实践奖（BPA），是对来自全球和各个地区的企业在领导力、技术创新、 客户服务和战略产品开发等各方面取得的卓越表现以及杰出成绩的认可。该奖项创立以来，先后有华为、中兴、上海贝尔等中国通信企业获得该奖项。2009 年，绿盟科技成为第一个获得该荣誉的信息安全厂商，2010 年蝉联该奖项，无疑是对绿盟科技持续创新能力和市场领导力的认可。

据来自 Frsot&Sullivan 的专家介绍，“全球经济危机的背景下，中国信息安全市场同样受到了一定影响，但随着混合威胁的增加和 IPS 产品的成熟，用户认识到 IPS 已经成为网络信息安全建设必备的安全产品。因此，在政府、国防、金融、电信等大型客户刚性需求的拉动下，中国 IDS/IPS 市场同比实现了 19.5% 的强势增长，而绿盟科技则以 28.2% 的市场份额位居第一。通过评选过程中对 IDS/IPS 市场参与者、最终用户和供应商的大量访谈，以及广泛深入的市场研究工作，我们认为绿盟科技公司能够取得这样的好成绩，主要得益于其保持技术领先的



全球性思维、产品与服务相结合的前瞻性战略以及对垂直行业的深入理解。”

绿盟科技作为国内最早从事入侵检测与攻防技术研究的信息安全厂商之一，凭借多年的积累，在 2005 年率先发布了国内第一款具有完全自主知识产权的 IPS。绿盟科技也是国内发布自主研究安全漏洞最多的安全公司，超过 40 个自主发掘漏洞被国际 CVE 组织收录；同时拥有国内第一个数目超过 15,000 条的中文漏洞信息库。

绿盟科技的专家在会上表示，“绿盟科技通过在网络安全领域 10 年的积累，通过对攻防的底层研究，漏洞库、规则库、信誉库这样一些核心资源的积累，NSFOCUS 已经牢牢树立了在亚太区安全领域的技术领先地位。今年 3 月，绿盟科技 IPS 还获得了亚太区第一个 NSS Labs 颁发的 Recommended 级别认证。除了在日本市场与美国市场之外，绿盟科技已经开始进入东南亚市场，希望能够找到更多的合作伙伴，向用户提供更加优质的产品。”

Govware2010：绿盟科技首推信息基础防护架构

近日，绿盟科技（NSFOCUS）应邀出席了由新加坡内政部举办的 GovernmentWare 2010 安全技术研讨会。在此次国家级安全会议上，绿盟科技首次推出了关键信息基础防护 (CIIP) 战略架构，获得国际安全界同行的高度评价。全球众多知名 IT 企业与国家级安全机构，均出席此次盛会。

基础设施一直是黑客长期关注的目标。包括近期的 Stuxnet 蠕虫攻击事件，就是利用多个 0day 和 SIMATIC WinCC 系统漏洞，对西门子公司的数据采集与监控系统进行攻击，从而直接破坏工业基础设施的恶意代码攻击。未来，关键信息基础设施的防护将面临更多的安全威胁与挑战。

此次 Govware 会议上，新加坡内政部及法律部高级部长 HO PENG KEE 先生指出：政府、公司和商业团体的重要信息基础设施，正日益成为网络犯罪分子和网络间谍的攻击目标，这些攻击随时都有可能发生。业界越来越关注，如何采用正确的 IT 安全战略，在目标、可用性及成本之间寻求一个合适的安全平衡性，主动减少来自网络的安全威胁。

“关键信息基础设施（CII）是指与国家安全、经济、社会以及公共健康安全相关的信息系统，这些系统与我们日常生活密切相关，比如业务监控和数据采集（SCADA）系统，时刻监测和管理着我们的电网，比如通讯网络时刻连接着我们的通信。因此，构建关键信息基础设施保护（CIIP）体系，正在成为各国政府在信息安全方面，优先考虑的事情之一”，绿盟科技首席战略官赵粮博士在会上指出。

CIIP 问题由于其涉及层面多，且与业务关系紧密，要做到行之有效，需要在业务可用性及成本之间寻求一个战略平衡点。绿盟科技作为亚太区云安全组织的倡导者，先行感知到这一问题的重要性，积极推动 CIIP 技术体系架构工作。在研究过程中，参考了国际云安全联盟提出的云安全理论，从 CII 运营与治理两个方面，整合技术与策略防护措施，为企业及组织提供大纵深、立体化的 CIIP 战略架构，并就 CIIP 实战进行了积极的探索，取得了丰硕的成果。

会上，绿盟科技受邀作为特别嘉宾，针对“保护关键信息基础设施 CIIP”的主题

绿盟科技首席战略官赵粮博士做主题演讲

阐述了绿盟科技的观点以及在中国如何保护基础设施的安全。绿盟科技首席战略官赵粮详细讲解了奥运会期间绿盟科技如何帮助运营商抵御针对网络基础设施和重要站点的海量 DDoS 的经验，同时在新兴的 HoneyNet 侦测僵尸网络攻击、DNS 域名安全保障、Web 服务防护等方面围绕 CIIP 技术体系架构详细阐述了未来 CIIP 可能遭受的安全威胁以及防护的思路。

10 年来，绿盟科技致力于网络和应用安全问题的研究。绿盟科技安全专家团队，从底层分析和掌握 Stuxnet 蠕虫、Web Malware、Botnet 等威胁的技术原理，从而针对这些互联网安全威胁，凭借扎实深厚的安全服务和安全产品，实现先行预防、实时防护和应急响应与恢复三个阶段的完整方案。此次在国家级安全会议上推出 CIIP 技术体系架构，对于国际同行共同抵御 CII 威胁，具有积极而广泛的意义。

此次会议主办方，正是看重绿盟科技在 CIIP 方面的经验，包括在奥运会期间信息基础设置防护，以及各类国家项目中网络流量清洗、DNS 域名防护方面的经验，特邀绿盟科技的专家介绍 CIIP 经验。

微软 0day 漏洞 绿盟科技 Web 应用防火墙提供零配置防护

9 月 20 日，绿盟科技（NSFOCUS）快速响应微软 0day 漏洞，绿盟科技 Web 应用防火墙可提供零配置防护。此次漏洞 Microsoft .NET Framework 设计上的缺陷，使用称为 Padding Oracle 的攻击方式，从而达到获取关键信息的目的。Microsoft .NET Framework 是微软通用的软件开发平台及工具包。由于设计的原因，使用 .NET Framework 所编译的 ASP.Net 应用中没有正确的实现加密，攻击者可以解密并查看敏感数据。此次 0day 漏洞中使用的 Padding Oracle 攻击方式，可以意译为加密预言。

在加密领域，预言（oracle）是指在提问时提供的提示系统。对于 ASP.NET 中的 padding oracle，攻击者可以通过向 Web 服务器发送密文文本，然后通过检查所返回的出错代码，判断是否正确的加密。通过反复上述操作，攻击者就可以解密剩余部分的密文文本。成功利用这个漏洞的攻击者可以查看目标服务器上加密的数据，如 View State，获得读取目标服务器上的文件，如 web.config。

这种针对 ASP.NET 0day 漏洞的攻击利用，攻击者必须发送大量请求，大量的 404 或 500 的 Http 返回码回应客户端。绿盟科技 Web 应用防火墙基于自身对 Http 协议的深度理解和控制，通过智能跟踪会话过程能主动发现异常 Http 会话，纠正 Web 服务器的出错信息脆弱处理机制，防止信息泄露，对异常态的 HTTP 响应页面进行修改过滤或者伪装，防止敏感信息泄露，让黑客无从利用实施攻击，从根源上杜绝这类漏洞。

由于微软官方还未提供相应安全补丁，因此该漏洞很可能造成严重的危害。绿盟科

技建议相关用户按照临时解决方法进行配置（请参考绿盟科技紧急通告：http://www.nsfocus.net/vulndb/15780）。对于没有部署绿盟科技相关产品的用户，请尽快咨询绿盟科技技术服务人员，以获得临时性解决方案。

受影响系统:

Microsoft .NET Framework 4.0

Microsoft .NET Framework 3.5 SP1

Microsoft .NET Framework 3.

Microsoft .NET Framework 2.0 SP2

Microsoft .NET Framework 1.0 SP3

国际云安全联盟中国区分会成立 沟通分享 共筑产业链

9 月 2 日，绿盟科技在北京隆重举办云安全联盟（CSA）高峰论坛暨中国区分会成立大会。此次大会以“沟通分享，合作共赢”为主题，本着“引进来，走出去”的精神，探讨云安全的实质内涵及发展趋势，交流国内外云计算和云安全的最新研究成果，分享云安全应用的实践经验。国际云安全联盟主席 Dave Cullinane 应邀出席峰会，并做主题演讲。

Dave Cullinane 在发言中介绍了云安全联盟所取得的成绩、云安全所处的阶段以及面临的主要问题。他说，“目前，云计算正在改变商业机构运用信息技术的方式。信息安全领导者们正在思考并实施如何在不影响业务的前提下，基于云安全实践方案，快速应用云计算”。

众所周知，云计算是互联网和大规模数据中心不断发展的产物，云计算的深入发展将给现有的信息产业结构带来颠覆性的变革。云计算在未来 10 年里，将成为影响整个 IT 行业的关键性技术，几乎所有知名 IT 提供商、互联网提供商，甚至电信运营商都在提供或准备提供云服务。云计算的蓬勃发展，对现有的信息技术体系架构带来了新的影响，而云计算广泛应用的首要问题就是安全问题。围绕云安全的话题，与会的各重量级嘉宾，包括运营商行业的专家、Frost & Sullivan 安全分析师、盛大网络首席安全官、知名安全企业的 CSO 们，分别阐述各自的观点，分享在云安全平台建设和应用方面的实践经验。

绿盟科技副总裁吴云坤表示，云安全的

问题大家已达成共识。多年来，绿盟科技始终致力于网络安全方面的研究，积累了大量的数据，我们愿意与各方面展开积极的合作，分享数据和经验。不久前，绿盟科技已经与 StopBadware 达成战略合作，与 Google 等合作伙伴一起，为其评估网络恶意软件提供数据。

在本次峰会上，中国区分会也正式成立。“CSA 中国区分会将继承 CSA 的宗旨和目

标，致力于提升中国地区的云安全实践，帮助中国地区专家和业内人士进行社区分享，增进与国际同行间的交流”，绿盟科技首席战略官、分会理事赵粮博士在会上指出，“在未来的 12 个月中，分会将进一步明确项目计划，推动项目进展，并提交项目成果。继此次峰会后，还会在上海、广州、香港等地，积极开展地区性的技术交流研讨活动，吸引更多同行的加入，扩大分会影响，使之走向成熟，并进一步获取更多的支持”。

此次高峰论坛围绕各行业在云计算、云安全等方面的热点问题，交流国内外云安全的最新技术、解决方案和研究成果，并深入探讨云计算及云安全对信息产业等社会各行业发展的影响。此次大会的成功举办，也将推动并加快中国和亚太地区在云安全方面的实践和创新。


聘书

兹聘请北京神州绿盟科技有限公司
何坤 同志为互联网网络安全应急专家
组委员，聘期两年。

绿盟科技专家入选互联网网络安全应急专家组

在最近召开的互联网网络安全应急专家组成立大会上，绿盟科技何坤成为互联网网络安全应急专家组委员，这是专家组中为数不多的企业代表之一。

专家组成员分别来自国家计算机网络应急技术处理协调中心、工信部电信研究院标准所、国家信息技术安全研究中心、中国信息安全测评中心、中国电信、中国联通、中国移动、中国互联网络信息中心的领导。新组建的专家组将承担起研究网络安全形势、分析安全事件原因、评估安全事件危害和事件定级，应急处置措施建议等工作。

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

此次绿盟科技成员成为互联网网络安全应急专家组委员，是工信部对绿盟科技技术能力的认可，也是对绿盟科技在配合国家主管部门进行安全事件预警、应急事件处置等工作的认可，绿盟科技将再接再厉，充分发挥公司在政策理解和技术方面的优势，为互联网网络安全贡献自己的力量。

绿盟科技与 StopBadware 达成战略合作 信誉服务国际共享

绿盟科技与国际网络安全权威组织 StopBadware 达成战略合作。作为数据提供方，协同 Google、AOL、PayPal、Mozilla 等机构一起，建立更为全面、及时、准确的恶意网站数据库，实现了全球互联网用户共享数据，共同维护互联网良好秩序。绿盟科技目前是中国唯一一家与 StopBadware 形成合作的安全厂商。

StopBadware 是全球最大搜索引擎 Google 的恶意网站数据的提供方，同时 Google 也向 StopBadware 开放数据。现今，搜索引擎是现今网民使用最为频繁的互联网入口之一，因此也是攻击者挂马的主要对象。为确保用户搜索信息时免受恶意网站影响，Google 从 2008 年开始在搜索结果里对恶意

网站进行明确标识，提示用户不要访问恶意网站。绿盟科技与 StopBadware 合作之前，StopBadware 除了来自于 Google 搜索引擎的数据之外，缺乏来自于中国大陆地区准确、及时的数据。因此，在一定程度上产生了错误地封杀很多中国大陆网站的现象。绿盟科技通过长期的对互联网挂马技术的研究和数据积累，对中国大陆地区的网站数据有准确的把握。此次绿盟科技与 StopBadware 的合作，增强了 StopBadware 获取中国地区恶意网站数据的及时性和准确性；降低了搜索引擎等第三方误判中国站点的可能性，同时更全面、更开放地向全世界互联网用户提供网络安全信誉服务。

互联网信誉服务是绿盟科技根据多年安全研究形成的知识积累。通过对 IP 地址、域名和 URL 等不同资源的内容和行为进行分析和记录，能够对互联网相关资源进行威胁分析和信誉评级。由于同时汇集了来自于授权客户和第三方合作伙伴的威胁反馈、自身安全产品的安全事件以及安全研究团队的风险预警，将当前的安全信息与目标站点的历史信息进行整合，从而建立了针对互联网的长期信誉追踪机制。

“基于云计算的 Web 安全服务的发布是绿盟科技长期以来对互联网安全所做努力的一个里程碑，与 StopBadware 的合作更是其中的一个关键环节。通过绿盟科技的 Web 信誉库过滤机制与 StopBadware 的反馈流程相结合，必将为我们客户带来更多价值，并推动 Web 安全服务的发展。” 绿盟科技副总裁吴云坤说。

StopBadware 执行董事 Maxim Weinstein 同时表示：“StopBadware 和绿盟科技的愿景都是旨在提高互联网的安全性，让每个互联网用户放心使用。我们期待能够学习绿盟科技在安全领域的见解，分享安全信息，了解中国及其他亚太国家 Web 安全的发展形势。”

绿盟科技获 2010 年度值得 CSO 信赖的信息安全产品奖

绿盟科技产品市场经理李晨做主题演讲

绿盟科技赢得 2010 年度值得 CSO 信赖的信息安全产品奖

8 月 19 日，由《计算机世界》主办的“2010 中国信息安全年会暨第八届中国 CSO 俱乐

部大会”在北京香格里拉饭店隆重举行。2010 年最值得 CSO 信赖的品牌、服务、方案多项大奖也在此次盛会上揭晓。绿盟科技“网站安全监测服务”云安全解决方案荣获 2010 年度值得 CSO 信赖的信息安全产品奖，这一结果充分肯定了绿盟科技在云计算及安全服务领域取得的成就。

作为信息安全产业每年举办一次的盛会，本次大会分设三大主题，分别是“云时代的信息安全”、“保护云时代的数据安全”及“保护云时代的 Web 安全”，聚集中国各行各业信息安全主管与产业界领导、专家、厂商，就云计算环境下的 Web 安全、数据安全、架构安全等话题进行深入研讨和交流。

在本次大会“保护云时代的 Web 安全论坛”上，绿盟科技产品市场经理李晨以《NSFOCUS Security As a Cloud Service》为主题发表演讲，为听众阐述了绿盟网站安全服务为用户提供的服务与价值。“网站安全监测服务”是绿盟科技“安全即服务”中的一项服务内容。通过对服务站点 7*24 小时不间断的远程透明式监测，提供安全检查、事件监测、风险分析服务，帮助网站管理人员从繁重的日常安全维护工作中解放出来。该项服务基于绿盟科技“云”平台，将安全作为一种“云”服务进行交付，并能够通过 Open API 的方式将信誉数据甚至安全检测能力与合作组织进行分享与融合。

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”到今年推出的基于“云平台”的网站安全监测服务，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。

NSFOCUS 2010年9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. 2010-09-15 Microsoft Windows Print Spooler 服务不充分用户权限限制漏洞（MS10-061）

NSFOCUS ID: 15750

http://www.nsfocus.net/vulndb/15750

综述：

Windows 是微软发布的非常流行的操作系统。

Windows 打印后台程序没有充分的限制访问该服务的用户权限。

危害：

攻击者可以利用此漏洞，提交特制的打印请求来，在 Windows 系统目录中创建文件或完全控制服务器系统。

2. 2010-09-15 Microsoft MPEG-4 编解码器媒体文件解析远程代码执行漏洞（MS10-062）

NSFOCUS ID: 15749

http://www.nsfocus.net/vulndb/15749

综述：

Windows 是微软发布的非常流行的操作系统。

Windows 媒体编解码器中所捆绑的 MPEG-4 编解码器，没有正确的处理使用 MPEG-4 音频编码的媒体文件，如果用户打开一个特制的媒体文件，或从网站或提供 Web 内容的任何应用程序接收特制的流式内容，该漏洞则可能允许远程执行代码。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意 MPEG-4 文件来，从而控制受害者系统。

3. 2010-09-09 Adobe Reader CoolType.dll 库 TTF 字体解析栈溢出漏洞

NSFOCUS ID: 15720

http://www.nsfocus.net/vulndb/15720

综述：

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

Adobe Reader 的 CoolType.dll 库在解析字体文件 SING 表格中的 uniqueName 项时存在栈溢出漏洞。

危害：

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

4. 2010-08-31 QuickTime QTPlugin.ocx 控件 _Marshaled_pUnk 参数验证漏洞

NSFOCUS ID: 15676

http://www.nsfocus.net/vulndb/15676

综述：

Apple QuickTime 是一款非常流行的多媒体播放器。

QTPlugin.OCX 控件检查对象的属性中是否存在 _Marshaled_pUnk，如果存在就通过将地址从 ASCII 表示转换为数字表示进行散列，之后将所生成的指针用作了 pStm CoGetInterfaceAndReleaseStream 以获取所列集接口的 IUnknown 指针，这样就获得了对 IStream 指针的控制。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

5. 2010-09-19 .NET Framework ASP.NET Padding Oracle 攻击信息泄露漏洞

NSFOCUS ID: 15780

http://www.nsfocus.net/vulndb/15780

综述：

Microsoft .NET Framework 是一个流行的软件开发工具包。

使用 .NET Framework 所编译的 ASP.Net 应用中没有正确地实现加密，攻击者可以解密并篡改敏感数据。

危害：

利用这个漏洞的攻击者，可以查看目标服务器上加密的数据，如 View State，获得读取目标服务器上的文件，如 web.config。

6. 2010-09-15 Samba SID 解析远程栈溢出漏洞

NSFOCUS ID: 15751

http://www.nsfocus.net/vulndb/15751

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 sid_parse() 函数及相关的 dom_sid_parse() 函数中在读取 Windows SID（Security ID）的二进制表示时没有正确地检查输入长度，存在栈溢出漏洞。

危害：

攻击者可以利用此漏洞，发送 sid 溢出 smbd 服务器中用于存储 SID 的栈变量，从而控制服务器系统。

7. 2010-09-10 Safari 5.0.2 和 4.1.2 更新修复多个安全漏洞

NSFOCUS ID: 15732

http://www.nsfocus.net/vulndb/15732

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 浏览器中存在多个漏洞，包括执行任意代码，或意外执行非指定目录中的恶意程序。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

8. 2010-09-02 Cisco WebEx ARF 文件解析堆溢出漏洞

NSFOCUS ID: 15692

http://www.nsfocus.net/vulndb/15692

综述：

WebEx 是全球最大的网络通信服务供应商，可提供电信级网络会议解决方案。

WebEx Player 在解析 ARF 文件格式中所定义的字符串时存在堆溢出漏洞。

危害：

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

9. 2010-09-01 Novell NetWare OpenSSH 实现栈溢出漏洞

NSFOCUS ID: 15688

http://www.nsfocus.net/vulndb/15688http://www.nsfocus.net/vulndb/13804

综述：

Novell Netware 是一款商业性质的网络操作系统。

NetWare 的 SSHD.NLM 模块及其 SFTP-SVR.NLM 子模块中存在栈溢出漏洞。

危害：

通过认证的攻击者可以利用此漏洞，指定超长的文件路径，从而控制服务器系统。

10. 2010-09-01 VLC 媒体播放器 smb:// URI 处理栈溢出漏洞

NSFOCUS ID: 15707

http://www.nsfocus.net/vulndb/15707

综述：

VLC Media Player 是一款免费的媒体播放器。

VLC 媒体播放器在处理 .xspf 文件中超长的 smb:// URI 时候存在栈溢出漏洞。

危害：

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

NSFOCUS 2010年10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. 2010-10-14 Microsoft IE 多个未初始化内存远程代码执行漏洞（MS10-071）

NSFOCUS ID: 15878

http://www.nsfocus.net/vulndb/15878

综述：

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

Internet Explorer 访问未正确初始化或已被删除的对象的方式中存在远程执行代码漏洞。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

2. 2010-10-14 Microsoft Windows 嵌入式 OpenType 字体引擎整数溢出漏洞（MS10-076）

NSFOCUS ID: 15882

http://www.nsfocus.net/vulndb/15882

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 的 t2embed.dll 库中在将嵌入式 OpenType 文件转换为 TrueType 格式时存在整数溢出漏洞。

危害：

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

3. 2010-10-14 Microsoft .NET Framework JIT 编译器优化远程代码执行漏洞（MS10-077）

NSFOCUS ID: 15880

http://www.nsfocus.net/vulndb/15880

综述：

Microsoft .NET Framework 是一个流行的软件开发工具包。

.NET Framework 中的 JIT 编译器在优化代码时存在漏洞，当用户访问承载了特制 XBAP 的网页时就可能触发内存破坏。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

4. 2010-10-21 Oracle 2010 年 10 月更新修复多个 Java 安全漏洞

NSFOCUS ID: 15917

http://www.nsfocus.net/vulndb/15917

综述:

Java 运行时环境(JRE)为 JAVA 应用程序提供可靠的运行环境。

Sun Java 中存在多个安全漏洞，用户受骗访问了恶意网页就会导致拒绝服务、泄露敏感信息、操控某些数据、绕过安全限制或完全入侵用户系统。

危害:

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

5. 2010-10-19 RealPlayer SP 1.1.5 和 RealPlayer Enterprise 2.1.3 更新修复多个安全漏洞

NSFOCUS ID: 15901

http://www.nsfocus.net/vulndb/15901

综述:

RealPlayer 是一款流行的多媒体播放器。

RealPlayer 中的多个组件在解析媒体文件中的各种字段时存在多个缓冲区溢出和数组索引错误。

危害:

攻击者可以利用此漏洞，诱使受害者打开恶意媒体文件，从而控制受害者系统。

6. 2010-10-18 Solaris rpc.cmsd 服务远程整数溢出漏洞

NSFOCUS ID: 15892

http://www.nsfocus.net/vulndb/15892

综述:

Solaris 是一款由 Sun 开发和维护的商业 UNIX 操作系统。

Solaris 中所运行的 rpc.cmsd 服务在处理 RPC 请求的时候存在整数溢出漏洞。

危害:

攻击者可以利用此漏洞，向该服务提交恶意 RPC 请求，从而引发拒绝服务甚至控制服务器系统。

7. 2010-10-19 IBM Informix Dynamic Server oninit.exe 服务远程栈溢出漏洞

NSFOCUS ID: 15898

http://www.nsfocus.net/vulndb/15898

综述:

IBM Informix Dynamic Server 为企业提供运行业务所需的任务关键型数据基础设施。

Informix Dynamic Server 中默认绑定在 TCP 9088 端口上的

oninit.exe 服务没有正确地过滤用户所提交请求，超长请求可能会在日志功能中触发栈溢出。

危害：

攻击者可以利用此漏洞，向该服务提交恶意请求，从而控制服务器系统。

8. 2010-10-20 Oracle Enterprise Manager Grid Control HTTP 请求远程溢出漏洞

NSFOCUS ID: 15912

http://www.nsfocus.net/vulndb/15912

综述：

Grid Control 是为整个 Oracle IT 架构提供中心化监视、管理、生命周期管理功能的系统管理软件。

Grid Control 的 EM Console 组件在处理超长的 HTTP 请求时存在缓冲区溢出。

危害：

攻击者可以利用此漏洞，向该服务提交超长的 HTTP 请求，从而控制服务器系统。

9. 2010-10-20 SAP Crystal Reports GIOP 请求解析多个堆溢出漏洞

NSFOCUS ID: 15904

http://www.nsfocus.net/vulndb/15904

综述：

SAP Crystal Reports 是功能强大的报表解决方案。

SAP Crystal Reports 中默认监听于 TCP 1024 以上端口的 CMS.exe 和 JobServer.exe 进程在解析 GIOP 请求时存在堆溢出漏洞。

危害：

攻击者可以利用此漏洞，向该服务提交恶意请求，从而控制服务器系统。

10. Novell iManager getMultiPartParameters 任意文件上传代码执行漏洞

NSFOCUS ID: 15831

http://www.nsfocus.net/vulndb/15831

综述：

Novell iManager 是一款基于 WEB 的应用程序，可以使用无线设备管理、配置 NovelleDirectory 对象。

iManager 包含的 Web 应用实现上存在漏洞，其中的 getEntry 可以被用来往磁盘上写入任 意文件。

危害：

攻击者可能利用此漏洞向服务器上传 JSP 脚本文件，从而控制服务器系统。

NSFOCUS 2010年11月之十大安全漏洞

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

1. 2010-11-04 Microsoft IE CSS 标签解析远程代码执行漏洞

NSFOCUS ID: 15972

http://www.nsfocus.net/vulndb/15972

综述：

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

Internet Explorer 在解析 HTML 时错误地分配了不充分的内存用于存储特定的 CSS 标签组合，用户受骗访问了恶意网页就会导致覆盖一个字节的虚表指针，调用内存中受控的数据。

危害：

攻击者可以利用此漏洞，诱使受害者打开恶意网页，从而控制受害者系统。

2. 2010-11-05 Adobe Reader 内存破坏代码执行漏洞

NSFOCUS ID: 15978

http://www.nsfocus.net/vulndb/15978

综述：

Adobe Reader 是非常流行的 PDF 文件阅读器。

Adobe Reader 的 EScript.api 实现上存在内存破坏漏洞，当在 PDF 文档中调用 printSeps() 时会导致堆破坏。

危害：

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

3. 2010-11-10 Microsoft Word RTF 文件解析栈溢出漏洞 (MS10-087)

NSFOCUS ID: 15990

http://www.nsfocus.net/vulndb/15990

综述：

Word 是微软 Office 套件中的文字处理工具。

在处理 RTF 文档中的特定控制字时 Word 未经执行长度检查便将其属性字符串拷贝到了栈缓冲区中，这可能触发栈溢出。

危害：

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

4. 2010-11-04 Adobe Shockwave Player Shockwave Settings 窗口释放后使用漏洞

NSFOCUS ID: 15973

http://www.nsfocus.net/vulndb/15973

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 Player 中自动安装的兼容性组件中存在释放后使用错误，其实是可能会调用已被卸载的函数库中的函数。

危害：

攻击者可以利用此漏洞诱使受害者打开恶意网页，从而控制受害者系统。

5. 2010-11-23 Microsoft Windows 任务调度服务本地权限提升漏洞

NSFOCUS ID: 16021

http://www.nsfocus.net/vulndb/16021

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

任务调度服务没能正确阻止用户通过 COM 接口修改 XML 定义文件中的某些字段，导致恶意

用户操纵一个有效的 XML 文件并绕过 CRC 校验。

危害：

攻击者可以利用此漏洞提升权限，从而对系统资源进行非授权的访问。

6. 2010-11-02 ProFTPD 多个模块目录遍历和缓冲区溢出漏洞

NSFOCUS ID: 15963

http://www.nsfocus.net/vulndb/15963

综述：

ProFTPD 是一款开放源代码 FTP 服务程序。

ProFTPD 的 src/netio.c 文件中的 pr_netio_telnet_gets() 函数在处理包含有 TelnetIAC 转义序列的用户输入时存在栈溢出。此外 mod_site_misc 模块中存在多个输入验证错误。

危害：

远程攻击者可以利用此漏洞，向 FTP 或 FTPS 服务提交恶意输入，任意写入、删除服务器文件，直至控制服务器系统。

7. 2010-11-17 HP LaserJet 打印机 PJL 接口多个目录遍历漏洞

NSFOCUS ID: 16009

http://www.nsfocus.net/vulndb/16009

综述:

HP LaserJet 是 HP 推出的激光打印机系列。

HP LaserJet 打印机的 PJL 接口存在多个目录遍历漏洞。

危害:

攻击者可以利用此漏洞，向打印机的 PJL 接口提交恶意请求，读取系统上的任意文件。

8. 2010-11-16 IBM OmniFind 多个远程安全漏洞

NSFOCUS ID: 16007

http://www.nsfocus.net/vulndb/16007

综述:

OmniFind 是一款企业搜索和文本分析平台。

OmniFind 的企业版中存在多个安全漏洞，包括权限提升、脚本注入、栈溢出、会话固定、信息泄露等多个漏洞。

危害:

攻击者可以利用这些漏洞提升权限、执行跨站脚本、跨站请求伪造、会话固定攻击，或完全入侵有漏洞的系统。

9. 2010-11-11 LANDesk 管理套件 HTML 表单请求命令注入漏洞

NSFOCUS ID: 15995

http://www.nsfocus.net/vulndb/15995

综述:

Landesk 管理套件是一款网络管理系统，可控制桌面，服务器和移动设备等。

Landesk 没有正确地验证提交特制请求的用户来源，存在命令注入漏洞。

危害:

攻击者可以利用此漏洞，向 Landesk 服务器发送恶意数据，从而控制服务器系统。

10. 2010-11-09 Novell GroupWise Internet Agent 组件 Content-Type 多个值解析栈溢出漏洞

NSFOCUS ID: 15986

http://www.nsfocus.net/vulndb/15986

综述:

Novell GroupWise 是一款跨平台协作软件。

Novell GroupWise 的 Internet Agent 组件中的 gwia.exe 模块负责解析服务器所接收到的邮件消息。在解析 Content-Type 头中由分号所分割开的实体的时候存在栈溢出漏洞。

危害:

攻击者可以利用此漏洞，向 GroupWise 服务器发送恶意邮件消息，从而控制服务器系统。

巨人背后的专家

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

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

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

NSFOCUS

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com