安全+
SECURITY
2011/07 总第013
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

## 电子文档综合安全管理体系研究

## 虚拟化安全研究

## 美国政府信息安全建设综述

## 钓鱼攻击的一些研究和对策

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

2011/07 总第 013

安全+ SECURITY+

# 目录 CONTENTS

# 电子文档综合安全管理体系研究

安全研究院　李鸿培

**摘要：**本文在研究敏感信息安全管理与防泄密技术的基础上，提出了一个针对电子文档的综合安全管理系统体系架构，该系统架构将通过融合电子文档的安全存储、安全使用、安全分发与传输，以及相关网络系统环境防泄密控制等安全机制，来满足敏感信息在文档生命周期内各阶段的防泄密需求。希望该项研究能够对大家关于电子文档的防泄密管理工作有所帮助。

**关键词：**电子文档安全管理系统　电子文档管理　文档安全管理　防泄密　安全管理

## 1. 引言

随着整个社会信息化的发展，企业或政府为了提高信息处理的速度和效率，越来越多的把纸质文档转化为电子文档的形式进行存储。用于存储的信息系统与网络上，大量的关系到企业生存甚至是涉及国家机密的数据信息交互往来，诸如机密文件、商业机密信息、设计图纸、技术报告、源代码、财务数据等。这些重要信息一旦泄露或被窃取，必然会危及到国家或企业的安危，或者对企业造成巨大的经济损失。

### 1.1. 存在的问题

由于国内知识产权保护还不完善，在很多企事业单位对电子文档缺乏基本的安全管理与防护，员工可以随意上传下载和发放网络中的文件，或者通过电子邮件和移动硬盘，很轻松地把企业的许多重要信息传递到网络外部。虽然，作为公司的管理者或相关应用部门都希望公司相关的敏感信息资料（比如：财务数据、技术文档等）不能轻易地离开公司的网络环境，甚至不能在公司网络内部随意地传递与交流。但是，管理者往往面临诸多不利于数据防泄密的情况，诸如:

1) 数据分散存储

用户可能会因各种原因把数据分散存储在不同的系统中。而这种分散存储，因缺乏统一的数据管控措施，非常容易导致敏感数据的丢失或泄密。

2) 终端管理不善

不安全的终端系统是造成敏感数据信息泄露的关键点，因终端系统管理不善可能造成信息泄密的可能性主要体现在:

• 因人员频繁流动、访问权限及安全策略不能及时更新, 造成单位敏感数据的流失

• 人员出差、加班需利用便携式终端带走大量的敏感数据，但无法提供有效的监控;

• 内部人员通过终端有意或无意所导致;

• 终端遭受病毒和黑客的入侵或文件破坏;

• 对移动存储介质（移动硬盘、U 盘等）缺少有效的安全管控，导致在使用中带来安全隐患，如丢失、中毒或违规使用 U 盘拷贝信息等。

3) 文档安全管控不足

敏感文档安全管控不够，缺乏细粒度的分级管理以及有效的认证授权与访问控制措施，在存储时采用明文保存，都可能导致敏感信息的泄露。

4) 敏感信息的传输安全性问题

在数据传输过程中缺乏有效的加密措施，信息内容可能会被非法用户截获。

5) 缺乏有效的文档安全管理制度

文档管理部门缺乏有效的人员保密意识、文档安全管理制度以及相应的文档授权访问管理流程，也是造成敏感信息泄露的一个主要原因。

### 1.2. 市场需求及政策驱动

无论从国家安全的角度还是从增强企事业单位自身竞争力的角度，基于电子文档的敏感信息保护技术及系统产品的开发与研究都将具有重大的意义，并且具有极大的市场潜力。

1) 信息安全等级保护的要求

针对国家敏感信息保护的需求，国家相关主管部门制订了我国的信息安全等级保护制度，主要包括公安部牵头的“信息安全等级保护管理办法”等相关标准，以及国家保密局牵头的“涉及国家秘密信息的信息系统分级保护办法”及其相关技术标准。用于指导重要部门信息网络的安全体系建设，实现基于安全域的数据安全管理与控制，保证数据信息的安全保密性。国家主管部门不仅为国内政府机关、企事业单位提出了信息保密的具体要求，而且也提供了相关的具体技术实施标准。

2) 中国版萨班斯法案的要求

2008 年 6 月 28 日，国家财政部、证监会、审计署、银监会、保监会联合发布了《企业内部控制基本规范》，该法案被专家称为中国版‘萨班斯法案”。基于该法案的要求，中国将近 2000 家上市公司将加强对信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制。据估计，该项法案将会使中国上市公司的采购单上的数额增添 30 亿。显然，这些上市企业对于涉及其商业机密的关键数据及文档的风险管理与控制必将对电子文档的安全管理市场有极大的推动。

3) 企业保持市场竞争力的需求

面对日趋激烈的市场竞争与经济间谍案件（例如 ,2009 年的力拓商业间谍案等）的日益增多及其破坏的严重性，也迫使企业为了自身的生存或竞争力的保持，不得不重视涉及企业商业秘密数据的核心技术文档、设计图纸、程序源代码、配方、商务信息、市场竞争力分析报告以及公司财务、人事等各

种重要数据文档的使用管理；并提供完善的防泄密措施，来保护企业自身的商业权益。因此企业级客户对企业机密数据风险管理的全面解决方案的需求也是非常的明确和迫切的。

综上所述，基于企业敏感信息电子文档的归档管理与防泄密需求的市场驱动以及国内相关法规、标准的合规性要求，政府、军队、机要部门以及大型企业对电子文档综合安全管理与应用将会有更为迫切的需求，并有很好的市场前景。

## 2. 国内研究现状

目前国内在电子文档安全管理或文件安全存储领域做的比较好的企业与产品主要有：北京亿赛通 CDG 文档安全管理系统、北京博睿勤文档安全管理系统、深圳市大成天下铁卷电子文档安全系统、中科网航睿锁电子文档安全管理系统以及福建伊时代信息科技股份有限公司的网剑文件保险柜等。但目前来说，这些企业的产品多基于透明加解密与文件管理技术实现的文档的归档管理或加密存储，虽然各产品都具有自己独特的技术特色，但仍缺乏一个纵贯文档整个生命周期的数据防泄密综合管理体系。

关于数据泄密的保护不仅要保护信息系统抵御来自外部的攻击，更关键的是要加强信息系统内部用户的安全管理和安全制度的建设。这是因为：根据美国《今日》杂志的数据表明，因公司员工造成的信息失窃高达 55%，内部违规操作或越权使用已是造成企业敏感信息泄密的主要原因；而在中国，由于知识产权保护的不完善，企业面临的内部信息安全问题将更为严峻。因此，必须对这些重要数据及电子文档提供全面的、体系化的保护措施。通过对电子文档全生命周期（生成、储存、使用、外发、销毁等）的安全管理、控制、防泄密以及电子文档操作行为的监控、审计等多种安全机制的有效集成，来尽可能系统地消减因重要数据（文档）的外泄、非授权使用、被窃取以及损坏所造成的威胁。也就是说，要从电子文档入手，通过融合各种数据安全技术和管理手段，加强对电子文档生命周期各个阶段中所存在的安全风险进行管理与控制，以确保网络中重要数据的完整性、机密性、可用性；降低或消除用户敏感信息数据被有意或无意泄露的风险。

本文将紧密结合政府和企事业单位对电子文档安全保护的需求，通过融合“电子文档管理”与“电子文档安全”的各项关键技术：电子文档的加解密、安全存储与灾备、客户端的防泄密、电子文档的标识分类、用户身份认证管理与授权机制、电子文档的外发管理与控制以及电子文档的使用保护和操作审计等，试图为用户提供一个针对电子文档安全的综合管理系统体系架构，来指导用户对其电子文档进行全生命周期（创建、存储、编辑 < 增、删、查、改 >、分发、归档、销毁等）的综合管理与安全控制。

## 3. 电子文档综合安全管理系统架构

电子文档综合管理系统架构（如图 1 所示）将为用户敏感信息文档提供基于整个文档生命周期的全方面的安全防护，提供文档的安全存储、安全传输、安全使用、安全销毁，保证对文档的操作完全在可控范围内完成，从而防止敏感信息的泄露。电子文档综合安全管理系统主要包括以下几个子系统：

1) 文档加密存储子系统

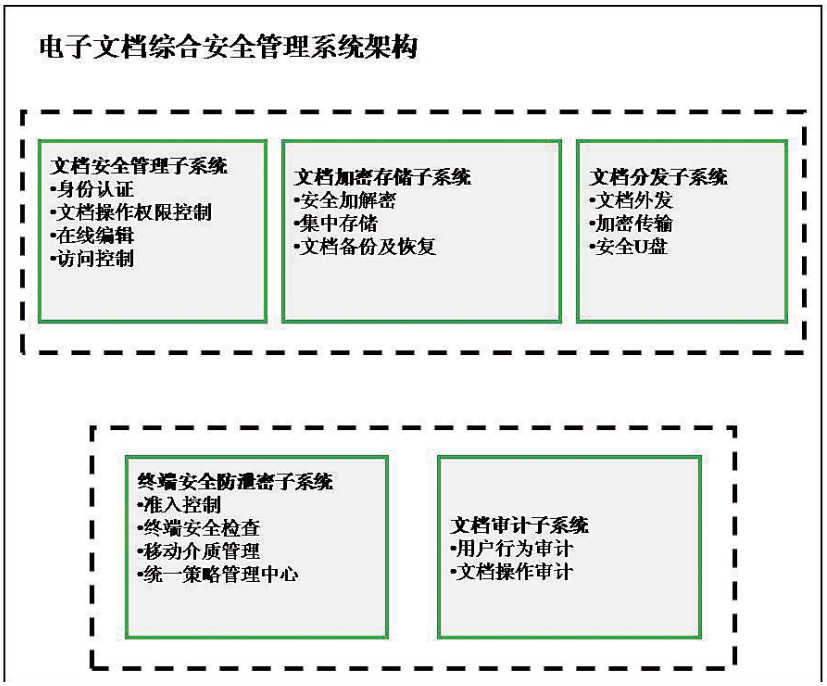



图 1 电子文档综合安全管理系统体系架构示意图

通过文件服务器实现电子文档的集中加密存储，并支持灾难备份与系统恢复能力；保证数据的集中安全存储。

2) 文档安全管理子系统

为用户提供接入电子文档综合安全管理系统的接口，具备 web 浏览器、专用客户端多种应用接口。提供细粒度的文档分级控制以及身份认证及授权访问控制能力，防止文档的非授权访问。提供文档在客户端的在线编辑功能，禁止文档在客户端本地存储，防止文档通过文档访问客户端进行泄密。

3) 终端安全防泄密子系统

提供安全技术及控制手段，保证客户端所在终端系统环境的安全性，并通过系统准入控制机制，保证访问终端系统符合文档访问的安全策略要求；防止不安全的终端系统对客户端的攻击或破坏。

4) 文档分发子系统

主要实现电子文档的分发管理与控制外发文档的受限使用。

5) 文档审计子系统

为文档加密存储子系统、文档安全管理子系统、终端安全防泄密子系统以及文档分发子系统的操作行为提供相应的安全审计功能。

### 3.1. 关键技术

由图 1 中的电子文档综合安全管理系统体系架构可知，要解决文档生命周期内各个阶段的防泄密需求，将必然会涉及到各自系统相关的多种核心安全技术的融合才能够实现，需要解决的关键技术主要有:

1) 用户身份管理与认证授权技术

需要提供多种认证技术支持，包括密码认证、USBkey 认证、生物特征认证等多重认证方式，以支持用户访问不同密级文档的认证强度，并据此进行相应的访问授权。

2) 电子文档的透明加密存储

3) 数据灾备与恢复技术

4) 电子文档的分级标识技术

5) 客户端防泄密技术

a) 系统环境的安全防护

包括系统补丁管理、安全脆弱性检查及加固、终端系统的外设管控（比如 USB 口、蓝牙、红外等）、安全的移动介质管理以及上网控制；防止人为通过电子邮件、移动硬盘、U 盘、软盘等途径盗取重要数据文档。

b) 文档的在线编辑

对于重要的已经提交到文件服务器的电子文档，只允许在授权的情况下通过电子文档的访问客户端进行在线编辑；可依据文档的重要程度、使用者的权限对在线文档进行禁止另存、拷屏、复制粘贴等操作，禁止将内存中正常显示的文档内容泄露。

6) 电子文档的外发管理技术

文档在授权外发时需要对电子文档进行使用控制的处理，比如限制外发文档的复制、打印次数，指定电子文档的自毁条件等等。

用于域间交换的电子文档的使用权限、次数、环境的限制机制以及自毁机制。

使用安全 U 盘，作为文档分发子系统的主要工具之一，进行身份认证、加密存储、解密阅读、使用范围限制、PC 绑定、强审计以及数据自毁等。

7) 电子文档的使用行为审计机制

对电子文档的创建、使用、编辑、流转提供监督和审计。实现对企业文档全生命周期各个环节的可查、可溯、可审。

8) 电子文档的安全销毁机制

通过这些技术来实现电子文档综合安全管理系统各子系统的核心功能，提供对电子文档的安全存储、安全分发、使用以及销毁等相关阶段的信息防泄密保护能力，尽可能消减有关敏感信息泄露的风险。

## 4. 总结

本文主要讨论了基于电子文档的敏感信息防泄密问题，并提出了一个基于电子文档的综合安全管理系统体系架构。

该架构主要是整合了电子文档的安全存储、安全分发与传输、安全使用及销毁各阶段的防泄密措施。依据该电子文档的综合安全管理系统体系架构的构想，可以文档集中存储的文件服务器为中心结合文档访问客户端环境（终端系统）的准入控制机制构建基于电子文档的安全域，为日后进一步实现敏感信息文档的“域内管理，域间交换”的管理控制思想奠定基础。同时，由于对文档数据进行了集中存储和严格的终端防泄密管控措施（准入控制、在线编辑、外设管控以及移动介质管理等），对敏感信息文档访问时，访问终端上将不会存储任何敏感信息；即使在敏感信息编辑的过程中，文档也只能保存到文件服务器中，尽可能地杜绝了敏感信息通过终端泄密的可能性。

由于基于电子文档的敏感信息防泄密管理是涉及到国家安全或企业生存的关键问题，因此，希望本文的研讨能够对大家关于电子文档的防泄密管理工作有所帮助。

# 企业内部异常行为建模初探

安全研究院　王卫东

**摘要：**本文从异常行为的定义入手，提出异常行为建模的方法。根据该方法，给出了基于特征和基于账户基调的两种异常行为检测规则模板，并通过实例对两种检测规则模板的使用给出了详细的解释。这些模板实际上就是异常行为检测规则的编写思路。按照这种模式，用户可以结合自己的业务特点，自定义满足定制需求的检测规则。另外，蜜网概念与异常行为检测规则的映射关系是一个有趣的发现，从而在纯理论的角度给出了蜜网概念的合理性。

**关键词：**行为建模　检测规则　行为审计　行为异常

## 1. 引言

在信息技术成熟度较高的企业中，普遍存在 IT 系统的运维或研发人员利用工作之便进行营私舞弊活动。例如，银行 IT 系统的维护人员，窃取客户银行卡账号信息并复制磁条卡窃取客户的资金。再例如，网络游戏企业的数据库维护人员，直接修改网游账号的装备类型和数量，然后再出售这些装备，从而将虚拟资产变现。还有的情况是网管维护人员的终端主机被植入木马，黑客以这个维护终端为跳板，可以远程进行恶意操作。因此对内部网络的访问行为进行监控，可以及时发现内部的恶意操作。要区分正常和恶意的网络行为，首先需要对异常行为进行建模，然后根据异常行为模型，制定检测规则。由于有些厂商将异常行为检测称为行为审计，因此检测规则也经常称为审计规则。

本文希望从异常行为定义出发，找到描述 IT 操作行为的模型，进而给出编写异常行为检测规则一般模式。按照这种模式，用户可以结合自己的业务特点，自定义满足定制需求的检测规则。

## 2. 异常行为建模

### 2.1 异常行为定义

由于不同的人对异常的理解不同，因此异常行为很难有标准的定义。但是我们可以

根据异常行为的常见特征，总结归纳出异常行为的定义。例如以非管理员 ID 直接对数据进行修改操作。再例如非营业时间业务客户端对业务系统的访问行为。还有不通过维护终端软件直接登录到服务器上进行维护操作。

异常行为定义：以不正确的身份，在不正确的时间，在不正确的位置，以不正确的方式（或通过不正确的渠道）对非授权的资源进行不正确的操作。

### 2.2 异常行为建模

从异常行为的定义可以看出，一个 IT 操作行为的属性包括: 行为人身份( Identity)、发生时间（Time)、发生位置 (Location)、行为方式 (Means)、行为的类型( 操作 ,Action)、行为对象（资源 ,Resource)。这些属性就构成了一个完整的 IT 操作行为抽象模型（简称 ITLMAR 模型 )。下面分别对每个属性作进一步的解释:

1）行为人身份：在 IT 系统中，表述身份的就是系统账号。

2）发生时间: 时间属性中包含两层概念，一个是行为发生的时刻，另一个是行为发生的频率。但频率是一个间接属性，无法从单个行为日志中直接提取。

3）发生位置：IT 操作行为发生位置信息包括: IP 地址、ATM 终端号、POS 终端号、业务终端编号等。

4）行为方式: 即以什么渠道完成的操作。例如在 IT 系统中，常见的访问方式有：专用客户端软件、中间件（对数据库访问通常采用中间件)、命令行（CLI)、远程桌面等。

5）行为对象：即各种 IT 资源，如文件、数据库表、服务器主机、数据项等。

6）行为操作：操作行为大体可以分为交易操作（转账、取现、存款、支付)、数据库操作（数据库)、文件操作三大类。

## 3. 异常行为检测规则

对异常行为的检测有两种方式，一种是基于行为的特征的检测，不针对特定的账号或账号群组。还有一种是面向特定用户的，即基于用户基本行为模式的检测。后面将给出基于前述行为模型的这两种方式的检测规则模板。

### 3.1 基于特征的检测规则的模板及实例

从前面的论述中，我们看到行为模型由 6 个元素构成。检测规则可以单独针对其中的某一个或某几个，这样通过组合计算，可以罗列出全部可能的规则模板，共 63 种（如表 3-1 所示)。其中√符号表示该模板检测所对应的元素。∀ 符号表示任意，即该规则不检测所对应的元素。

为了更好的说明检测规则模板的含义，这里用几个检测规则实例加以说明。

- 规则模板 1 实例：除中间件和 admin 账户外，其它任何身份的对数据库的访问都是违规的;

在很多 IT 系统中，只允许两个账号对数据库的访问，即中间件的账号和维护用账号 admin。因此其它账号访问数据库，一律看作违规行为。这条检测规则只关注身份和资源两个因素。

- 规则模板 3 实例：admin 账户只能在系统维护时间段从 IP 地址是 111.111.111.111 的维护终端访问数据库，其他行为都是违规的;

时间也是检测规则必须考虑的因素，有些操作一般只发生在特定时间段内，并且只

能从某个特定的维护终端主机上进行操作。

• 规则 7 实例：除了通过堡垒主机以远程桌面方式进行的更新操作，其它都是违规的。

在某些 IT 系统的维护规定中，要求维护终端先登录到堡垒主机上，再用远程桌面的方式进行维护操作。

| 规则模板 | 身份 | 时间 | 地点 | 方式 | 操作 | 资源 |
|---|---|---|---|---|---|---|
| 规则模板 1 | √ | ∀ | ∀ | ∀ | ∀ | √ |
| 规则模板 2 | √ | √ | ∀ | ∀ | ∀ | ∀ |
| 规则模板 3 | √ | √ | √ | ∀ | ∀ | ∀ |
| 规则模板 4 | √ | √ | √ | √ | ∀ | ∀ |
| 规则模板 5 | √ | √ | √ | √ | √ | ∀ |
| 规则模板 6 | ∀ | √ | √ | √ | √ | ∀ |
| 规则模板 7 | ∀ | ∀ | √ | √ | √ | ∀ |
| 规则模板 8 | ∀ | ∀ | ∀ | √ | √ | ∀ |
| ..... | | | | | | |
| 规则模板 63 | ∀ | ∀ | ∀ | ∀ | ∀ | √ |

表 3-1 63 种规则模板

但是上述 63 种规则模板是数学组合的结果，并非都可以给出实例，原因是可能存在重复包含或无现实意义的情况。例如所有元素都检测这样的检测规则现实中就很少见。

另外，规则模板 63 只检测资源这个元素，貌似也很难给出实例。因为该类规则的含义是：任何人在任何时间以任何方式对某个资源的任何操作都是异常行为，这样的规则看上去没什么意义。按一般的理解，既然所有的访问都是非法的，这个资源也就没实际意义。在现实中的确存在这样一种资源，通常称为蜜罐。这个令人惊喜的发现让我们找到了蜜罐与 ITLMAR 模型的相互印证关系。即如果认为蜜罐的存在是有意义的，则行为模型给出了这方面的定义，其对应的行为规则在某种程度上印证了 ITLMAR 模型的完备性。而如果认为 ITLMAR 模型是完备的，则在理论上推测出现实中应该有蜜罐这类设备。

### 3.2 基于账户基调的检测规则及实例

基于账户基调（profile）的检查规则是

面向特定账户（群组）的，因此检测规则只包含除身份以外的另外 5 个元素（见表 3-2）。每个账户历史上的行为记录可以构造成一个行为基调。一旦某个行为特征远远偏离这个基调，则判断为异常。同前面一样，时间元素的取值有两种可能，一个是时段（用区间符号 [] 表示），一个是频率。位置、方式、操作三个元素分别都可以有多个非数字取值，因此是个元素的集合。资源的取值可能是数值的，也可能非数值。这种检测规则通常用于检测外部用户的异常交易行为，因此这里用一个交易行为基调作为实例说明（账号 A 基调实例）。但是这个检测思想也可以应用于内部用户的访问行为监控（账号 B 基调实例）。

- 账号 A 基调实例：[12:00,13:00],[17:30,20:00]; { 超市 A，支付宝，超市 B}; {POS, onlinebank}; { 支付 , 转账 }; [0,500];

在这个实例中，账户 1 银行卡交易行为基调是：通常在中午休息或晚上下班以后购物，购物方式基本是在超市 A（工作单位附近）和超市 B（住家附近）POS 机刷卡，或是通过支付宝网络购物，还有在网上支付一些账单，通常单次交易金额一般都不超过 500 元。

- 账号 B 基调实例：[9:00,17:00]; {IP:222.222.222.222}; {CLI，远程桌面 }; { 下载，上传，打开创建 }; { 文件，数据库表 }, [0,50M] [0,0.5M]。

| 基调 | 时间 | 位置 | 方式 | 操作 | 资源 |
|---|---|---|---|---|---|
| 账户 A | [ ], 频率 | {a,b,c} | {A,C} | {xx,xx} | {} 或 [ ] |
| 账户 B | [ ], 频率 | {a,b,c} | {A,C} | {xx,xx} | {} 或 [ ] |
| 账户 C | [ ], 频率 | {a,b,c} | {A,C} | {} | {} 或 [ ] |
| ..... | | | | | |

表 3-2 基于账户基调的检测规则模板

套用交易行为基调的方法进行内部行为检测时，有时需要对某些操作赋予两个资源取值，例如下载操作，不仅要检测下载对象，还要包括下载数量。在这个实例中，下载量是 50MB，上传量是 0.5MB。

## 4. 结束语

异常行为检测规则，有白名单和黑名单两种类型。基于特征的审计规则，不针对特定的用户 ID，用否定语态表示的规则可以看作白名单（例如“除了……”），如果不用否定语态来表述，则为黑名单类型。而基于用户基调（User Profile）的规则，则肯定属于白名单类型，虽然主要用于外部用户的交易监控，但也可以用于内部用户行为的监控。

在现实的环境中，一个完整的行为可能由多个分段的活动组成，因此首先需要关联分析，将多个活动组合成一个完整的行为以后再应用上述模型进行检测。为此，不同的设备生成的日志格式和内容都有所不同，需要将这些日志做归一化处理。ITLMAR 模型不仅为制定检测规则提供了思路和方法，还为数据归一化提供了方向。

# 浅谈Botnet和蜜网

系统架构部　陈景妹

**摘要：**本文主要介绍了僵尸网络的概念、分类、检测与防范的方法，并且结合蜜网系统特点，讲述蜜网在僵尸网络检测与追踪中所起的作用以及研发方向。

**关键字：**僵尸网络（Botnet）　C&C（Command and Control ）　蜜网（Honeynet）　蜜罐（Honeypot）

## 一、什么是 Botnet?

僵尸网络（Botnet）和木马一直是安全界的热点话题。那么，什么是僵尸网络呢？僵尸网络的最简单形式是一群感染了病毒的计算机执行“傀儡牧人”的命令。“傀儡牧人”就是利用僵尸网络谋取利益或攻击其他计算机的黑客。

如何区别僵尸与其他黑客入侵？首先，僵尸网络中的客户端必须能够在客户端上采取行动而不需要黑客登录该客户端的操作系统；其次，很多僵尸客户端必须能够在黑客很少或不插手的情况下协同合作，共同完成一个任务。如果这群计算机满足以上条件，就组成了一个计算机僵尸网络。

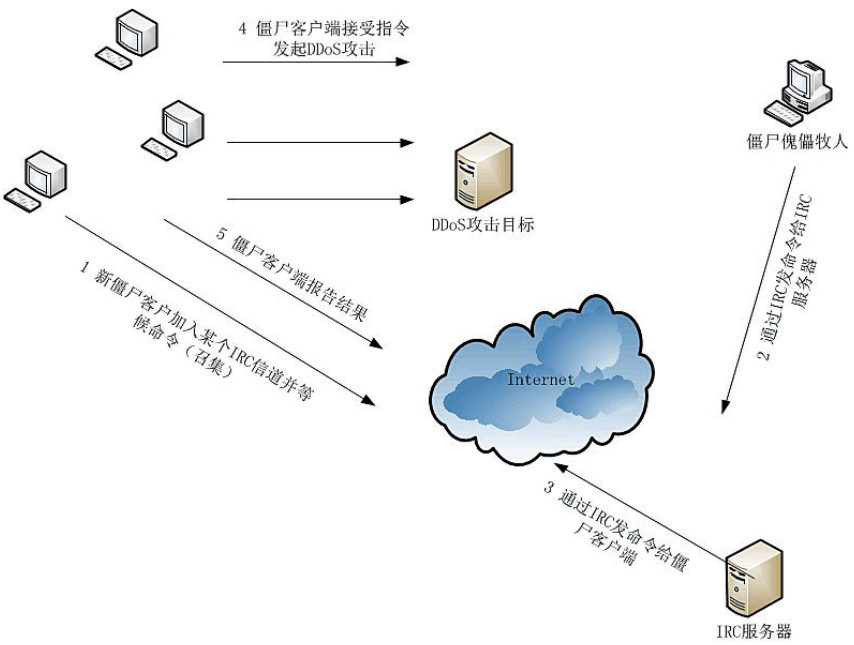



图 1.1 典型僵尸网络

图 1.2 为一个普通的僵尸网络客户端的生命周期。

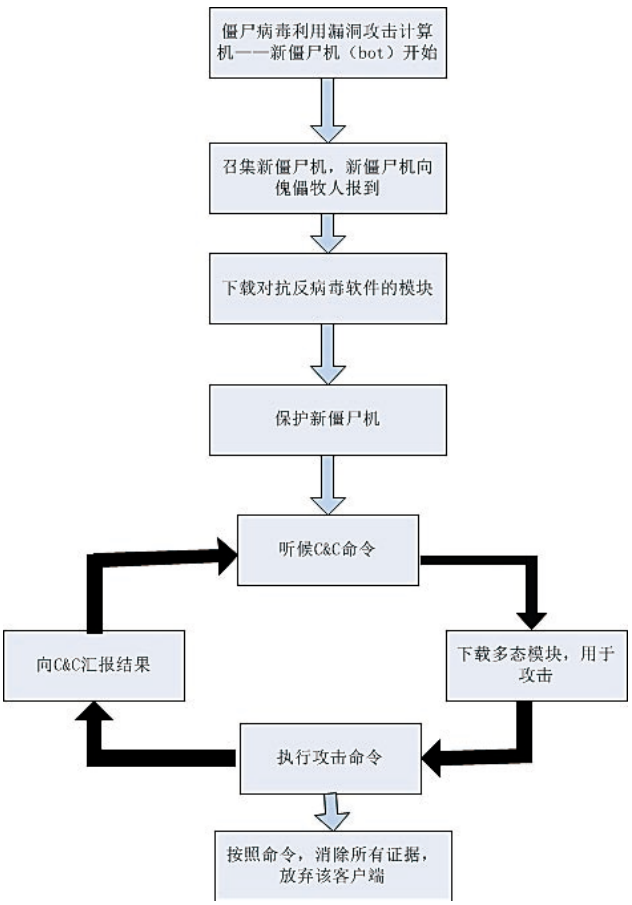



图 1.2 僵尸网络的生命周期

僵尸网络将许多病毒危害融合到一起。典型的僵尸网络由僵尸服务器（如一个 IRC 服务器）和一个或更多的僵尸客户端组成，如图 1.1 所示。在这种典型的僵尸网络中，傀儡牧人通过 IRC 信道在远程命令与控制（Command and Control，C&C）服务器上与僵尸客户端进行通讯。具体步骤可以参考图中所示。

## 二、僵尸网络的发展及分类

### 2.1. 僵尸网络 C&C 拓扑进化

Botnet 最早起源于 IRC 网络，开始作为有用的工具而没有其他恶意，它可以加入 IRC 信道，在主人忙于其他事务时为其服务，对于其它 IRC 用户来说他们只是用户，帮助用户享用并管理自己的 IRC 连接，不同于今天的僵尸网络客户端。

攻击与监测防范技术总是会起到互相促进的作用，僵尸网络控制者不断发明新技术维护僵尸网络操作，而僵尸猎人寻找并干扰僵尸网络操作，研究对抗新技术手段。

随着技术的发展，Botnet 在网络拓扑上的变化主要体现在 CC 控制信道从中心往分散方向发展，由一个 C&C 服务器向多个 C&C 进化，更进一步的向 P2P 进化，形式也多种多样，引入了基于 DNS 记录技术，基于 Web 的 C&C 等等，如图 1.3 所示。

目前僵尸网络主要可分为 IRC Botnet，HTTP Botnet 和 P2P Botnet 三种。

### 2.2.IRC Botnet

IRC Botnet 是最初的，也是目前最庞大的 Botnet 网络群。它的主要特征是利用 IRC 协议构造命令与控制信道，交互性好，容易创建，

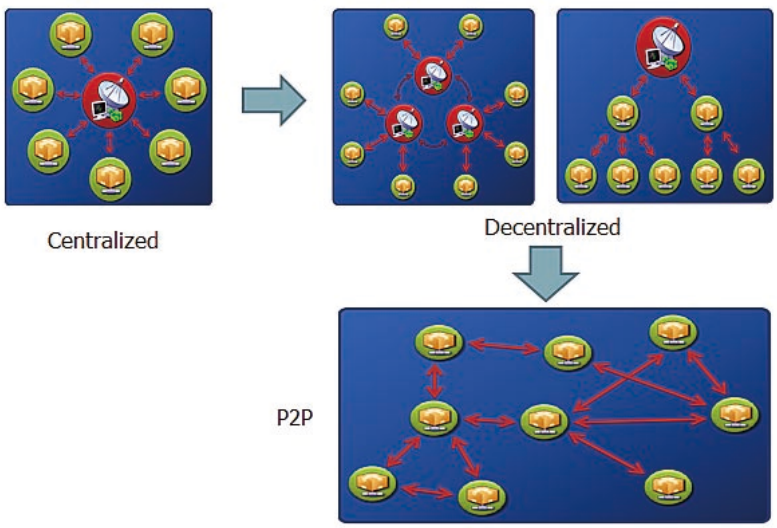



图 1.3 C&C 的拓扑结构进化

采用一个服务器能轻易创建和控制多个僵尸网络，可以方便加入冗余信息。

### 2.3.HTTP Botnet

HTTP Botnet 即基于 Web 的僵尸网络，它的特点是 C&C 服务器是 Web Server。它与 IRC Botnet 最大的不同在于控制信道，在这里使用完全不同的协议。

HTTP Botnet 有两种类型：基于回声的和基于命令的。

基于回声的 Botnet 僵尸机针对 CC 机只是声明自己存在，控制者主动连接僵尸机。在这种情况下，控制者连接每个僵尸机，通常通过特洛伊木马打开后门端口进行收集。有些情况下僵尸机会发送一个完整的 URL 给 Web Server，这个 URL 本身包括一些对控制者而言很重要的信息，例如后门端口，访问僵尸机的密码。

基于命令的僵尸网络属于基于网页的僵尸网络，是对其他类型僵尸网络的一种补充，有助于控制者管理“僵尸部队”。控制者可以通过图形用户界面的网络接口发布命令，很像使用 IRC 协议，唯一区别在于，是僵尸控制者“推”信息而不是僵尸机“拉信息”——即 C&C 主动连接所有的僵尸机发出命令，而不是僵尸机与它连接然后等待命令。

### 2.4.P2P Botnet

P2P Botnet 即利用 P2P 协议进行通信的僵尸网络。它具有僵尸机 / 控制机分散，不依赖于某一节点的特点。在此框架中，将僵尸节点分为两类，拥有静态 IP 地址并从因特网可以访问的僵尸程序称为 servent bots，这类僵尸节点承担客户端和服务器的双重角色；其他由于 IP 地址动态分配、私有 IP 或防火墙过滤等原因无法从因特网访问的僵尸节点称为 client bots，每个节点的邻居节点列表中只包含 servent bots. 僵尸网络控制者通过认证机制后，可从网络中任一节点注入其控制命令，当一个节点获取新的控制命令后，通过向其邻居节点转发，从而快速传递到每个 servent bot,client bot 则从其邻居节点列表中的 servent bots 获取控

制命令。

对于僵尸猎人来说，通过一个节点也可以发现此类 Botnet 的许多僵尸机，却很难发现全貌。

### 2.5. 其它类型 Botnet

其它类型的 Botnet，如基于 IM 传播蠕虫病毒并作为回声控制信道；利用 FTP 作为控制信道；甚至如目前微博、开心网之类的，也成为 Botnet 传播的一个很有利的场所。

### 2.6.DNS 记录技术的应用

僵尸网络中对 C&C 主机的连接通常使用域名，而不是直接连到 IP。引入域名并采用多宿技术有利于恶意者创建更多有活力的 C&C，一旦一个服务器无法使用，可以比较方便的转移指向该地址的 DNS 记录。提高了控制信道的冗余与鲁棒性。

僵尸网络控制者为了提高稳定性会玩更先进的“花招”，如使用动态 DNS 或 Fastflux DNS 技术。

动态 DNS（DynDNS）是指动态 DNS 服务的提供商，这些供应商基本上做的就是允许任何人注册一个账号，然后获得免费的 DNS 主机服务。可以自己设定域名或使用他们提供的三级域名，然后指向如自己的主页 IP 地址。这些服务对僵尸网络的控制者来说简直就是完美的，他们可以设定任意数量的可用主机，然后频繁的改变它们指向的 IP 地址。为此，自然要设定一个很低的 TTL。

Fast-flux 的目的是为一个合法域名（比如 www.example. com）分配多个（几百个甚至几千个）IP 地址，这些 IP 地址以非常快的频率更换，通过一个轮转的 IP 地址资源库及对特定的 DNS 域名资源设置具有短生命周期的解析映射进行实现。由于安全性和可用性的考虑经常会增加了第二层：匿名代理重定向。重定向机制可以干扰摧毁和反制 Fast-flux 服务网络节点的企图。事实上 IP 地址轮转池里的大量 IP 地址并不是内容请求（或者其他网络服务）的最终目的地址，受控的前端系统仅仅被部署成为重定向器，转发与真正提供内容服务的其他后台服务器之间的服务请求和返回数据。Fast-flux 的“motherships”是 Fast-flux 服务网络后面的控制要素，类似于传统僵尸网络中的命令控制 (C&C) 系统。然而与典型的 IRC 僵尸网络服务器相比，Fast-flux 的“motherships”有更多的特征。隐藏在前端代理网络节点后面的上游 fast-flux mothership 节点，实际上才是真正将内容分发到请求服务受控客户端的恶意源。据观测，Flux-herder mothership 节点机制有效地延长了在实际环境中成功运转的周期。这些节点常常提供 DNS 和 HTTP 服务，其 web 服务经常被配置成可以在单个主机上同时提供数千个虚拟网站内容。

## 三、Botnet 的危害

Botnet 是一些联网的计算机的集合，控制者利用它可以做任何想做的事情。如下是它的一些典型的应用和危害:

- 吸收新成员：每个僵尸客户端最基本的任务是吸收新成员。它通常通过扫描方式选择目标系统，利用漏洞或密码嗅探、密码猜想的方式登录攻击;
- 控制发起 DDoS 攻击：僵尸网络最早的恶意攻击就是发动 DDoS 攻击竞争者、对手或干扰傀儡牧人的人;
- 收集身份信息和金融信任;

- 发动垃圾邮件战役;
- 发动钓鱼攻击;
- 赚取点击率，欺骗广告软件公司;
- 未经用户许可，安装广告软件获取利益;
- 劫持计算机进行勒索;
- 存储并分发偷窃的或者非法（侵犯）的知识产权的信息资料;
- 用作政治目的。

## 四、Botnet 的检测与防范

僵尸网络已经成为目前因特网最为严重的安全威胁之一，同时，由于僵尸网络本身具有的特性，也使其成为了黑客们用于 DDoS 攻击、发送垃圾邮件、窃取敏感信息等各种攻击行为的高效平台。为了应对僵尸网络安全威胁，研究者已经在僵尸网络跟踪、检测与防御等多方面开展深入的研究工作。

僵尸网络的检测防范包括僵尸病毒的检测防御和僵尸节点（CC 主机和 bot 主机乃至源控制者）的检测。业务网络的僵尸病毒的检测防御，在主机端可以通过杀毒软件、HIPS 等进行查杀；网络端可以通过 NIDS、异常流量检测设备、防毒墙等网络安全设备进行。而对僵尸节点的检测，却是运营商及许多其他机构关注的重点所在，由于各种先进躲避技术的应用，且 CC 主机和 bot 主机可以方便的进行转换，给僵尸节点的检测带来更大的难度。

充分了解僵尸网络的内部工作机理，是防御者应对僵尸网络安全威胁的前提条件，僵尸网络跟踪 (Botnet Tracking) 为防御者提供了一套可行的方法，其基本思想是，首先通过各种途径获取因特网上实际存在的僵尸网络命令与控制信道的相关信息，然后模拟成受控的僵尸主机加入僵尸网络中，从而对僵尸网络的内部活动进行观察和跟踪。后文所介绍的蜜网无疑是获取实际存在的僵尸网络命令与控制信道以及僵尸病毒的天然有利途径。

僵尸病毒的检测分析包括基于二进制特征码检测和行为分析两种。基于二进制特征码检测主要针对已知僵尸病毒进行，取决于病毒库或规则库特征，而对未知的僵尸病毒则无法进行检测。行为分析则主要在虚拟、模仿或真实的环境中运行僵尸病毒，观察系统所产生的各种变化及捕获数据包进行协议分析。

在《Botnets-The Killer Web App》一书中提及了利用 ourmon 在业务网络中发现僵尸网络的方法，主要包括 TCP 异常检测和 UDP 异常检测。在异常检测一方面针对 IRC 缺省端口 6667 及 139、445 等重点端口进行检测，另一方面利用僵尸主机总要进行网络扫描以增加新成员的特性，引入了扫描权重检测方法。

TCP 扫描权重计算公式如下:

TCP work weight = (SS + FS + RR ) / TP

其中各个变量的意义如下:

SS 是采样期间计算机发送的 SYNS 总数。

FS 是采样期间计算机发送的 FINS 的总数。

RR 是采样期间返回到计算机的 TCP RESET 的总数。

TP 是采样期间计算机收发信息包（包括控制包和数据包）的总数。

公式的含义是，比较所发送的控制包和发送的所有信息包的数

量。如果值是 100%，表示或者是客户端 / 服务器的 TCP 协议损坏，或者是某人正进行某种扫描。

扫描权重检测法主要针对扫描权重超出阈值的 IP 地址及 IRC 信道结合标志位、端口特征、IP 目的地址数量和 TCP 目的端口数量等对僵尸网络进行检测。

僵尸网络的防御手段，包括遵循基本的安全策略以及使用防火墙、DNS 阻断、补丁管理等技术手段。另一种防御方法针对僵尸网络具有命令与控制信道这一基本特性，通过摧毁或无效化僵尸网络命令与控制机制，使其无法对因特网造成危害，即所谓的“斩首”行为。由于命令与控制信道是僵尸网络得以生存和发挥攻击能力的基础，因此，第二种防御方法较第一种更加有效。

## 五、蜜网的作用

蜜网技术是一种通过部署作为诱饵的主机（称为“蜜罐”），对攻击者进行欺骗，以捕获恶意软件、进行攻击方法和攻击行为研究的技术。蜜罐是一个相对“干净”、可控的主机环境，包括基于服务模仿的“低交互蜜罐”和基于真实操作系统及服务的“高交互蜜罐”，其最原始的用途是用于捕获恶意样本文件，在许多防毒厂商、安全机构中都有使用。

一般来说，蜜网系统具有三大核心需求：数据捕获、数据控制和数据分析。数据捕获包括网络和主机层面的数据捕获，是蜜网系统的基础；数据控制是蜜网系统的安全保障，避免对业务网络造成影响；数据分析针对蜜网所捕获的数据进行分析，是蜜网系统的价值所在。

“僵尸网络分析”是绿盟科技基于蜜网系统一个重要研究方向。未来的相关研究预计有两个层面，一是基于蜜网捕获数据的深入发掘及分析，通过主机样本文件的捕获和扫描识别出僵尸病毒，在蜜网网关对数据包做进一步的分析获取控制信道信息及用户名密码、命令等，并且初步得到一些僵尸 IP 及域名，通过主机行为变化监视及关联分析技术把僵尸网络涉及到的多种恶意软件及行为进行关联，以做全面的分析；另一层面，开发僵尸网络追踪系统，模拟成受控的僵尸主机加入僵尸网络中，从而对僵尸网络的内部活动进行观察和跟踪，以获取更进一步的数据。

入侵者或僵尸网络所利用的工具，并不一定就是打上了“病毒”或“木马”标签的软件，有时连常见的安全软件也会为它所用。我们曾经在现网运行的蜜罐中发现攻击者入侵后，安装了某知名主机防御系统对系统是否存在监控组件进行检查并干掉相关连接。蜜罐相对“干净”的诱捕环境，为僵尸网络不同模块或组件的关联分析提供了便利。

僵尸网络的检测是一项系统工程，未来可能涉及到多产品信息交换及联动，以及与其它机构进行信息交换，才能有效的对僵尸网络进行检测与防御。

## 六、后记

本文写作前，得知著名的僵尸网络软件 zeus 源代码泄露。好的方面，自然可以给安全工作者对僵尸网络的研究提供方便，但同时又可能出现很多修改和改进的版本，用来制作特洛伊木马，给网民带来极大的安全隐患。攻击与防范的斗争，依然持续。

# 安全基线动态调整的方法研究

行业营销中心　田民

**摘要：**本文以基线的生命周期为基础，详细探讨安全基线变更的方法论、调整安全基线的工作流程以及动态变化的安全基线对自动化检查工具的要求。

**关键词：**SCAP　安全基线　基线生命周期　基线动态变更　自动化安全基线检查工具

## 一、前言

笔者在绿盟科技去年第四期《技术内刊》中，以《业务系统安全基线的研究和应用》为题，从技术的角度上，以 SCAP 体系下安全基线的概念为引入，比较详细地阐述了电信运营商业务系统可以落实到自动化合规检查的安全基线之概念、框架、内容以及和具体业务系统相结合的应用场景。

在谈到基线变更这一问题时，在《业务系统安全基线的研究和应用》一文中概括性地阐述了安全基线需要依据业务系统的变化而进行相应的动态变化。本文将着重从安全基线自身的角度，以基线的生命周期为基础，详细探讨处理安全基线动态变化的方法、工作流程以及对自动化安全基线工具的要求。

## 二、基线的概述

### 2.1. 基线的概念

基线是一个开放的概念。从一个方面讲，不同的行业，不同的系统有着不同的基线; 从另一个方面来说，基线又具有其共性的特点。从应用的角度讲，基线具有如下三个特点:

（1）基线由基准点组成，而基准点标识了最根本的需求或要求的底线;

（2）基线在应用中主要体现为与基准点比较。更直接地说，在基线的应用过程中，最根本的行为就是比较;

（3）基线的最终目标是通过与基准的比较，明确差距，为决策提供量化的数据支持。

因此，基线是一个需求或要求的底线，在实际应用中体现为一种比较的行为，其目的是为决策提供支持。

### 2.2. 基线的生命周期

基线也是具有生命周期的。基线的生命周期如图 1.1 所示:

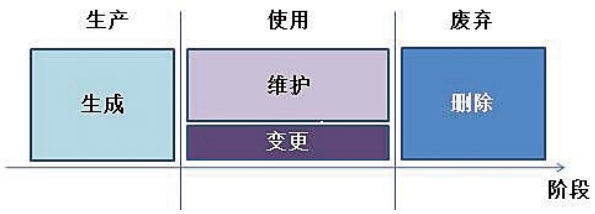



图 1.1 基线的生命周期

基线的生命周期包括三个阶段：基线的生产阶段、基线的使用阶段和基线的废弃阶段。其中，基线生产阶段的主要工作是生成基线。在使用阶段，包括基线的维护和变更两方面工作。一般来说，基线的维护占据了使用阶段绝大部分的工作。在某些情况下，基线需要进行变更，涉及到基准点的增删改等必要的更新工作。

废弃是基线生命周期最后的阶段。对于明确没有使用价值的基线，可以删除，一来简化和降低使用阶段的维护工作量，二来避免已经明确为废弃的基线因操作不慎被错误地启用。

### 2.3. 基线的变更

基线需要维持相对稳定的状态，原因在于需求的底线一旦明确，是不需要频繁变化的。越重要的基线越需要保持相对稳定的状态。然而，当组成基线的基准点由于外界的因素发生变化时，基线就需要进行相应的变化。

因此，基线不是一成不变的，也有“Cradle-to-Grave”的过程。我们知道，基线的变更涉及到对系统最根本的要求的底线进行调整，其对系统的影响是重大的，必须做到有序进行。那么，如何调整基线，进一步说，如何做到对基线变更的有效控制，对于合理使用基线，适应系统的变化，具有非常重要的意义。

## 三、安全基线动态变更的方法

安全基线，作为基线的一个组成部分，随着安全需求等因素的变化，在必要的情况下，需要进行相应的调整。

### 3.1. 影响安全基线变更的因素

在讨论安全基线变更的方法和流程之前，需要明确影响安全基线变更的因素。可能影响到安全基线调整的因素包括:

1) 安全需求;

2) 业务需求;

3) 其他因素。

首先，安全需求是安全基线最根本的影响和决定因素。安全需求直接影响到安全基线的制定和变更。以运营商的某业务系统为例，当对该系统进行重大升级改造时，如果新增设备和原有设备类型存在较大差异，特别是出现系统厂商替换的情况（如数据库从 A 厂商变更为 B 厂商），改造后系统的安全需求必然发生较大变化，必须进行安全基线的调整。该增加的增加，该修改的修改，该删除的删除。再举一个例子，对管理员登录进行严格控制是 Windows 系统的重要安全需求，从规范的角度上讲，对管理员登录口令的长度进行要求（如管理员登录口令不能短于 6 位）就是 Windows 安全基线重要的组成部分。然而，对于特定的业务关键业务主机来说，由于管理上的需要，要求管理员的口令是不能少于 8 位。这个时候就需要调整主机的安全基线，将口令长度为 6 的要求更加严格地提高为 8 位。因此，安全需求决定了业务系统安全基线的制定和调整。

其次，业务需求也是影响安全基线进行调整的重要因素。在某业务系统中，为了保证所有 Solaris 主机的安全，制定了必须关闭 FTP 端口的要求。也就是说，在这个业务系统中，Solaris 主机不能开放 FTP 端口就成为基本的安全基线。但是，对于某安装了 Solaris 操作系统的接口服务器来说，从其业务通信的角度考虑，必须要和其他服务器通过 FTP 定期传送数据。这样一来，就需要调整这个主机的基准点，放宽对端口的控制要求——允许开放 FTP 端口。因此，从满足业务运行的目的出发，可能在某些特定条件下，需要对安全基线进行适当调整。

最后，除了安全需求和业务需求之外，还有很多因素可能影响到安全基线的调整。例如上级监管部门的要求，将直接影响并导致安全基线进行调整。

### 3.2. 风险及其控制

在木桶理论中，木桶最终可以盛放多少水不是最长而是由最短的木板决定的。依据这个形象的例子，可以展开进一步的联想：如果需要调整那块最短的木板或者说调整若干块木板，是可能影响到木桶中容纳的水量的。这里做一个假设，在调整若干块木板的时候，我们加长了最短的那块木板，但是同时又将另外一块木板截短了，这块被截短的木板最后的长度甚至比之前最短的那块木板还要短，那么其结果——毫无疑问——木桶里盛放的水反而更少了。这个例子的结论是，调整木桶的木板是存在风险的，错误的调整非但不会增加、反而会减少水桶的有效容积。

对安全基线的调整亦然，同样具有风险。错误的设置可能增加了系统的风险，而不是降低了。因此，在调整安全基线之前必须要对基线进行全面的评估，明确基线调整后可能带来的影响。

当然，即便在调整之前详细评估了进行基线调整的种种后果和风险，也不能完全保证调整基线的工作就一定是安全的。因此，制定一个恢复或回滚机制来规避因错误操作带来的风险，就显得十分有必要了。

### 3.3. 安全基线变更的工作流程

从上文中可以得出以下两个结论：

1) 安全基线在其生命周期的使用阶段可能随着内外部因素的变化而调整；

2) 安全基线的调整存在风险。风险的规避需要先行规划，同时需要做好恢复 / 回滚的方案。

在图 3.1 中，以流程图的方式展现了安全基线变更调整的工作流程：

具体来说，安全基线的变更包括如下流程：

（1）选择并使用（Use）安全基线；

（2）监控（Monitor）安全基线的使用情况；

（3）系统的内 / 外部因素发生变更，对当前的安全基线设置进行审计（Audit），确认是否因系统的变更调整安全基线的设置；

（4）如果确认安全基线因系统的变化需要调整，则根据实际情况进行基线的变更（Adjust）；如果确认不需要进行基线的调整，则维持（Maintain）当前基线；

（5）当完成基线变更后，存储当前基线到基线数据库中；

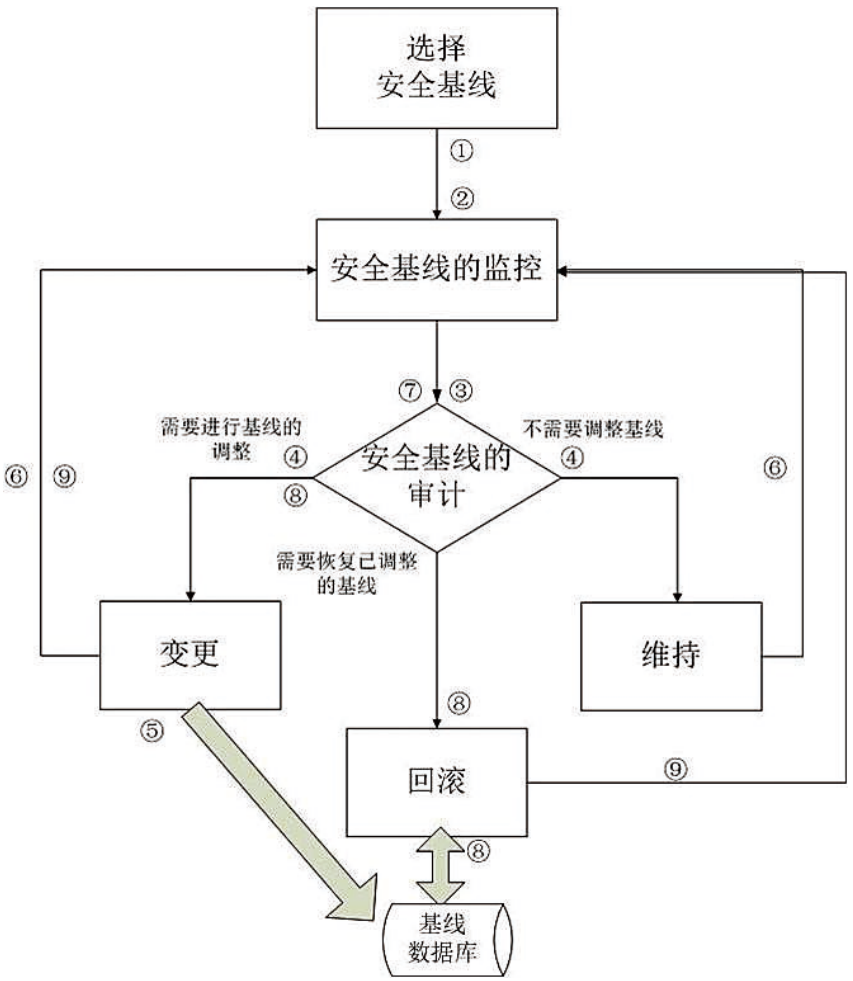



图 3.1 安全基线变更的流程

（6）继续对基线的使用情况进行监控（Monitor）；

（7）如果发现变更后的基线存在不合理或错误的情况，则进行基线的审计（Audit），确认是否存在问题；

（8）如果确认安全基线的变更的确存在问题，需要再次变更，则根据问题的原因进行基线的再次变更（Re-Adjust），并完成存储；如果确认安全基线的变更的确存在问题，需要恢复之前的基线设置，则从基线数据库中调用原有基线的设置，恢复（Retrieve）到之前的状态；

（9）完成再次变更或恢复后，对基线的使用情况进行监控。

由此可见，安全基线的变更流程是一个闭环操作的过程。基线在使用过程中，需要随时对基线的使用情况进行监控。一旦发现基线不符合系统的要求（多发生于系统变更时），就需要对基线进行调整。当发现调整后的基线设置仍存在问题时，则需要再次进行审计和调整，或采取回滚的操作，恢复到之前的某个基线设置状态。

这里需要补充一句，在图 3.1 所示的流

程中，没有体现安全基线调整之前的评估环节。但是，评估基线变化可能带来后果的工作是非常有必要的，在很多情况下可以避免调整基线带来的风险发生。当然，正像 3.2 节中阐述的那样，即便进行了基线调整的风险评估，也需要建立恢复 / 回滚机制。这在 3.2 一节中已经有所阐述，这里不再赘述。

## 四、动态变化的安全基线对自动化检查工具的要求

当前，市面上有一些基于 SCAP 理念开发的自动化安全基线检查工具。一般来说，这些自动化安全基线检查工具所检查的内容涵盖了安全配置、安全漏洞和系统状态等项目。自动化安全基线检查工具极大地方便了操作人员对系统进行基线检查的工作，提高了工作效率，降低了工作难度，得以在政府、运营商、金融、能源等诸多行业获得广泛应用。

考虑到安全基线在实际使用中可能需要随着系统的变化进行调整，对于自动化检查工具来说，需要提供相应的功能保证操作者可以随时对安全基线进行调整，并在必要的情况下进行恢复或回滚。

从实现角度上讲，自动化安全基线检查工具需要具备如下功能，来满足上述需求:

（1）支持基线模板的用户自定义设置;

（2）支持基线的恢复 / 回滚功能。

具体来说，基线模板的自定义包括对基线要求的增删改。这里我们引入一个场景。某系统中某台采用 Solaris 操作系统的关键业务处理机，出于安全的需要，要求增加一条安全配置基线要求，对管理员日志读写权限进行限制，只允许管理员可以进行读写操作。同时，由于业务的需要，系统将要扩容。在整改前，系统中使用的是思科的交换机，整改后引入了华为交换机。

不难看出，对于上面的两个情况，从配置基线的角度来说，需要依据安全需求以及系统的扩容变化相应地调整配置的基线。这样一来，对于一个自动化安全基线检查工具来说，需要能够做到: 首先，系统维护人员可以在原有的 Solaris 基线模板上设置对 sulog 的权限限制（如 600); 其次，系统维护人员可以新增华为交换机的配置模板。只有实现对基线模板方便而快捷的用户自定义操作，才可以满足基线动态变化的需求。

至于如何实现基线的恢复 / 回滚，方法有很多。可以建立一个基线数据库，存储系统在各个阶段使用过的基线模板。一旦操作者发现当前基线存在问题，可以随时回滚到之前的某个基线设置状态。至于是前一个基线，还是某一个曾经使用的基线，用户可以通过手工的方式进行选择。

## 参考资料

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

[2]. Baseline (Configuration management), Wikipedia.org. http://en.wikipedia.org/wiki/Baseline_(configuration_management)

[3]. 中国移动 SOLARIS 设备安全配置规范，中国移动通信有限公司网络部

[4]. 中国移动 Windows 操作系统安全配置规范，中国移动通信有限公司网络部

[5]. 绿盟安全配置核查系统 (BVS) 产品白皮书，绿盟科技

# 虚拟化安全研究

安全研究院　王卫东

**摘要：**本文从虚拟化定义入手，重点讨论了虚拟化环境下的安全威胁和脆弱性，给出了虚拟化环境下的安全对策。最后简要介绍了虚拟化安全产品的实现机制和功能需求。

**关键字：**虚拟化安全　虚拟化技术　虚拟化产品　虚拟化应用

## 一、虚拟化概述

### 1.1. 虚拟化定义和种类

虚拟化是软硬件的仿真，以供其它软件运行其上。这种仿真的环境称为虚拟机。根据基本的计算架构层的不同，有很多不同形式的虚拟化。由于云计算技术的普及，全虚拟化技术被广泛采用。本文讨论的范围只局限于全虚拟化的相关安全问题。

| 虚拟化类型 | 应用样式名 |
|---|---|
| 应用虚拟化 | 应用虚拟化提供了 API 的一个虚拟实现，JVM 就是一个例子。它作为 JAVA 应用程序与操作系统之间的中介。 |
| 操作系统虚拟化 | 操作系统虚拟化提供了操作系统接口的一个虚拟实现。 |
| 全虚拟化 | 一个或多个操作系统及其包含的应用程序运行在虚拟硬件之上。每个操作系统实例及其应用程序运行在一个单独的虚拟机（称为 Guest 操作系统 ,guest OS）上。 |
| 泛虚拟化 | 全虚拟化的一个变体，Guest OS 可以使用“泛虚拟化”接口，对网络和存储资源的访问速度明显加快。 |
| 网络虚拟化 | 虚拟化系统上所提供的网络功能。如相同物理主机上 VM 之间的网络通信、VLAN、NAT 等功能。 |
| 存储虚拟化 | 对现有的存储方式（NAS、SAN、磁盘镜像、GuestOS 直接访问磁盘）的虚拟化。 |

### 1.2. 全虚拟化的利弊

#### 1.2.1. 全虚拟化的好处

- 提高硬件资源的利用率；

例如，不考虑负载能力的情况下，在一个物理主机上可以同时测试某个软件在多个操作系统上运行的情况。用虚拟机可以仿真很多硬件，以测试软件的物理兼容性。

- 强化可管理性；

虚拟化允许单一的 PC 上运行多个 OS 实例，并且可以快速回复对 OS 的变更，从而强化了可管理性。

- 提高兼容性；

虚拟化允许在一个新版本的 OS 上运行一个老版本的 OS，以便在其中运行原来的应用软件。例如，某些旧有信息系统需要旧版本 Web 浏览器作为客户端才可以访问。

- 安全性的提高。

利用快速加载 OS 映像，可快速完成灾

难恢复。在某种程度上，虚拟机也将应用软件崩溃所造成的安全风险隔离开来。

1.2.2. 全虚拟化的弊端

- 被攻击的机会增加;

虚拟化在技术上增加了一个层次，同时也引入了新的被攻击机会。

- 稳定性风险增加;

虚拟化在技术上新引入的层次也增加了安全维护的风险，例如动态迁移造成的稳定性问题。

- 安全维护管理的负担增加。

在某些情况下，虚拟化增加了安全边界，并且使维持必要安全边界变得更复杂。安全策略在某些情况下无法及时执行。例如某些变更操作需要在虚拟机映像激活状态下才能完成。存储资源共享可能造成数据泄露。虚拟机之间的通信是新的管理盲点。

## 1.3. 全虚拟化的架构和类型

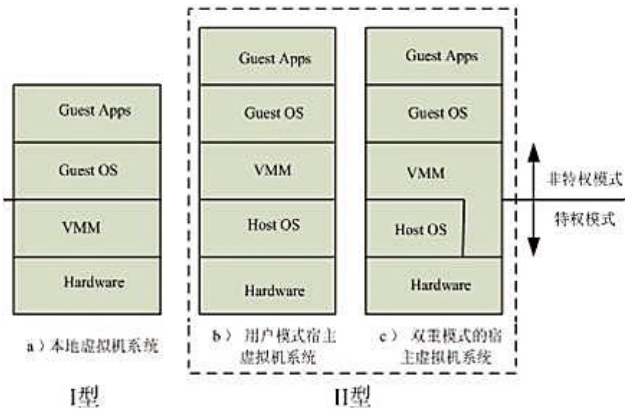



图 1.1 虚拟化架构图

如图 1.1，虚拟机主要包括 I 型（Bare-Metal，即裸机型）和 II 型（Hosted，即宿主型）两大类。I 型虚拟机主要应用于服务器虚拟化，II 型虚拟机主要应用于桌面虚拟化。

服务器虚拟化环境中，VMM( 也称 Hypervisor) 是核心。Hypervisor 不仅作为虚拟层直接安装在硬件上，实现对硬件资源的抽象，它还是一个管理控制程序，负责对硬件资源的调度、所有 VM 的管理并响应 VM 请求。

## 1.4. 虚拟化的典型拓扑与运行管理

如图 1.2，一个典型的虚拟化系统主要由存储虚拟化、网络虚拟化、服务器虚拟化、虚拟化设施管理（VIM，Virtual Infrastructure Management）等几部分组成。

虚拟化的运行管理主要依靠 VMM 和 VIM 完成。VMM 运行在各个物理服务器上，主要功能包括：对物理资源的虚拟化、VM 的启动停止以及非中断迁移、VM 间的访问控制等。VIM 是对虚拟架构进行集中管理的控制台。它的主要功能包括:

- 高可用管理：在 HA 集群中自动启动物理服务器以接管故障服务器上的应用;
- VM 动态迁移：保持应用不中断，动态地将一台虚拟机从一台物理服务器迁移到另外一台物理服务器上;
- 分布资源调度：动态监控整个虚拟环境的 CPU 和内存资源的使用情况，并根据制定的策略在物理服务器间调整所负载的虚机，实现整体资源的负载平衡;
- 虚拟镜像和快照的备份;

• 模式和格式的转换：将物理机转换为虚拟机，将其他格式的虚拟机转换为指定的虚拟机，以及将磁盘映象文件转换为虚拟机。

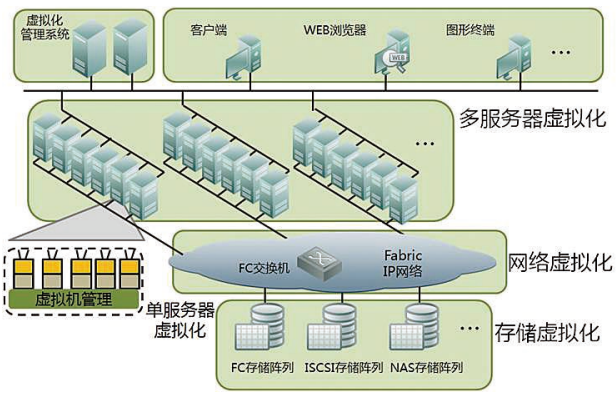



图 1.2 虚拟化拓扑结构图

## 二、虚拟化环境下的安全威胁和脆弱性

非虚拟化环境下的威胁与脆弱性，在虚拟化环境下几乎还都会存在。例如 DDoS 攻击，针对 Web 应用的攻击，数据泄露、暴力破解等等。这里只讨论由于虚拟化的原因，引入的新的或以新的形式体现的脆弱性和威胁。

### 2.1. 系统漏洞与配置错误

如同传统的 IT 系统一样，虚拟化系统中也存在大量漏洞，一部分漏洞是存在于 VM 上，另一部分则属于 Hypervisor。类似地，虚拟化系统中也同样会有配置错误的情况。VM 上可能的配置错误同非虚拟环境一样。Hypervisor 上常见的配置错误包括:

• 对于 VM 之间通讯的配置存在错误;

• 对 Hypervisor 管理接口的访问限制的配置不够严格;

• 对 VM 可访问物理接口（磁盘驱动器和网络适配器等）的配置错误。

当 VM 上存在漏洞，使得攻击者完全控制一个 VM 后，通过利用各种 Hypervisor 安全漏洞，可以进一步渗透到 Hypervisor 甚至其它 VM 中。这就是所谓的逃逸威胁。同时还可能导致数据泄露以及针对其它 VM 的拒绝服务攻击。

### 2.2. 身份认证的脆弱性

对虚拟化管理系统的主机的访问控制多数使用用户名和口令进行本地认证，这种认证方式非常容易被暴力破解。

### 2.3. 新增的监管障碍

• 流量监控的盲点;

传统网络环境中，基于区域（Zone）划分保护的硬件防火墙，以及基于行为特征分析的 IDS/IPS 对整个网络防护（从外到内、从内到外、从内到内等通信）起关键作用。但在虚拟化环境中，同一物理机上各 VM 之间通信流量根本不经过这些网络安全设备，这显然是网络安全防护中的盲点。

• 安全边界模糊化。

传统的安全域有明确的物理边界，而在虚拟化环境下，这种安全边界变得模糊起来，同一物理主机上有多个属于不同安全域的节点。

### 2.4. 隐蔽信道

隐蔽信道（Covert Channel）是指允许进程以危害系统安全策

略的方式传输信息的通信信道，是导致信息泄露的重要威胁。如图 2.1 中描述，即使在强制访问控制策略（根据 BLP 模型 [16]）下，攻击者仍然可以构建隐蔽信道实现从高安全级主体向低安全级别主体的信息传输。

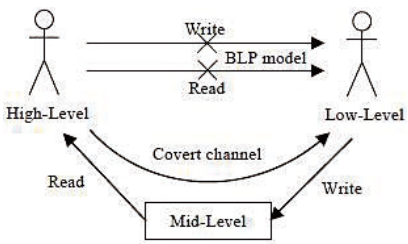



图 2.1 隐蔽通道示意图

虚拟化环境下，针对虚拟化服务器的网络攻击源头主要有三种可能:

一、是来自虚拟化环境以外;

二、是来自虚拟化系统中其它物理主机上的 VM;

三、是来自相同物理机上的其它 VM。

针对第一、二种情况引起的隐蔽信道，传统的安全防护技术就可能够应付，存在的仅仅是检测率和误报等细节问题。针对第三种情况引起的隐蔽信道，则是虚拟化引入的新威胁，需要在防护技术上作变革。

事实上，虚拟化环境下缺乏对 VM 间通信流量的可见性本身是一大安全问题（后文阐述），同一硬件上 VM 之间的通信流量根本不经安全网关、硬件防火墙等安全设备。无论是 VM 之间的攻击数据，还是攻击之后传输数据的隐蔽信道，传统的基于网络的检测技术都将完全失效，如图 2.2 所示:

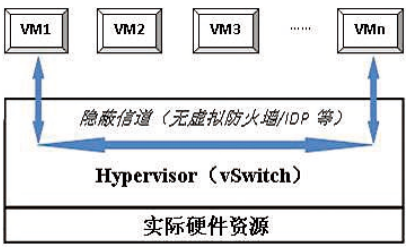



图 2.2 虚拟化环境下的隐蔽通道

### 2.5. 旁路攻击（side-channel attacks）

旁路攻击是一种新型密码分析方法，其利用硬件的物理属性（如功耗、电磁辐射、声音、红外热影像等）来发现 CPU 利用率、内存访问模式等信息，进而达到获取加密密钥，破解密码系统的目的。这类攻击实施起来相当困难，需要对主机进行直接的物理访问。例如通过监控数据进出运行着加密算法的硬件系统上的 CPU 和内存所花费的时间，来分析密钥的长度。再例如，可以对 CPU 或加密芯片的功耗进行观察分析。芯片上的功耗可以产生热量，冷却效应可以将热量移走。芯片上温度的变化引起机械伸缩，这些伸缩可以产生音量很低的噪声。

在虚拟化环境下，通过查看计算机的内存缓存，攻击者可以获得一些关于什么时候用户在同一台设备上利用键盘访问启用 SSH 终端的计算机等基本信息。通过测量键盘敲击时间间隔，他们最终可以使用和 Berkeley 一样的技术来计算出通过计算机输入了什么。还能估算出当计算机执行例如加载特定网页等这样简单任务时候的缓存活动。这种方法可以被用于查看有多少因特网用户正在访问一台服务器，甚至正在查看哪一个网页。为了让简单的攻击行为奏效，攻击者不仅能计算出哪一个服务器正在运行他们希望攻击的程序，还能找到一个在这台服务器上找到特定程序的方法。这并不容易做到，因为从定义上来看，云计算会让这种信息对用户是不可见的。

### 2.6. 数据残留

数据残留是数据在被以某种形式擦除后所残留的物理表现，存储介质被擦除后可能留有一些物理特性使数据能够被重新恢复。在虚拟化环境中，因为存储资源和计算资源的共享，数据残留有可能会无意泄露敏感信息。

## 三、虚拟化环境的安全对策

### 3.1. 变更管理

及时安装系统的各种更新。

很多产品都提供 Guest OS 离线补丁的功能，即在非启动的状态下，直接修改镜像文件中的二进制文件然后再保存。

正确配置 Hypervisor 和 VM

- 配置虚拟化设施与可信任的授权时钟服务器同步;
- 对于 VM 之间通讯以及 VM 对物理接口访问的配置存在错误;
- 对 VM 可访问物理接口的配置错误;
- Hypervisor 的隐形化处理。

### 3.2. 异常监控与攻击防护

由于 VM 的很多网络通讯无法像传统网络中那样通过监听或嗅探获得，因此必须找到一种监控 VM 网络流量的手段，并对这些流量进行分析，及时发现异常。在现实虚拟化环境中，已经出现某个 VM 对其它 VM 的攻击案例。目前这方面的解决方案和产品还基本上是空白。

对虚拟环境的攻击防护分为两方面，一方面防止从外部对整个虚拟化系统进行 DDoS 攻击防护。这与传统 IT 系统的防护完全一样，也就是在虚拟化环境的外部部署攻击防护设备。另一方面是虚拟环境内部不同安全域之间的安全防护和隔离技术。目前这种安全防护产品有的是第三方产品，有的是虚拟化产品内在的安全机制。

### 3.3. 访问控制与身份认证

通过防火墙等访问控制机制，限制远程对 Hypervisor 的管理访问。为防止对 VM 和 Hypervisor 的访问认证被暴力破解，建议使用双因子的单独的认证系统。

### 3.4. 通讯加密

在虚拟化环境中，也要对某种重要的通讯进行保护，如对 Hypervisor 的管理通讯、用户自服务的通讯等必须进行加密。

### 3.5. 灾难恢复

对虚拟化环境应制定应急预案，以确保在灾难发生时，能迅速应对。应急措施可参照 NIST SP 800-61 Revision 1, Computer Security Incident Handling Guide。

保存一份好的 Guest OS 镜像备份，可以在 VM 被攻陷或镜像文件损坏后，使用备份的镜像文件快速恢复。

### 3.6. 追踪取证

一旦确定 VM 被攻陷，应对被攻陷的 guest OS 进行研究，查找恶意软件。被攻陷的 VM 很容易封装映像文件并留下快照，形成司法证据。

### 3.7. 数据管理

虚拟化环境下的数据管理包括:

- Guest OS 镜像文件与快照(Snapshot)的统一管理;

对镜像文件和快照的访问要进行严格控制，防止非授权访问。

镜像文件要定期进行更新操作。

更新后的镜像文件要重新截取快照

- 残余数据管理。

租用设备到期归还之前或向远程办公职员提供租借来的设备之前，需要确保敏感数据被彻底删除。服务供应商应保证系统内的

文件、目录和数据记录等资源所在存储空间被释放或重新分配给其它用户前得到完全清除。可参照 NIST SP 800-88, Guidelines for Media Sanitization 中的相关要求。

镜像防篡改

检查加密校验和来判断镜像是否被篡改。

### 3.8. 定期风险评估

对虚拟化环境的安全管理，还应包括定期的风险评估工作。主要的评估项目包括：日志审计、漏洞扫描、渗透测试、配置核查、镜像文件一致性核查等内容。这些评估项目在传统 IT 环境中已经存在，所不同的是需要针对虚拟化环境的特殊性进行相应的调整。例如，日志审计规则应符合虚拟化环境中的访问授权要求。再例如，漏洞扫描和配置核查应支持对 Hypervisor 等虚拟化组件的检查。对虚拟化环境的风险评估，可参考 NIST SP 800-115, Technical Guide to Information Security Testing and Assessment。

## 四、虚拟化安全产品

为了适应虚拟化环境的要求，在虚拟环境下监控型和探测型的硬件安全产品往往以

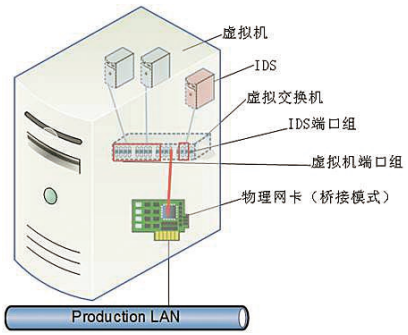



图 3.1 虚拟化环境安全产品的实现

虚拟机的形态出现的。图 3.1 以虚拟化 IDS 为例，描述了这类虚拟化产品的形态和部署方式。其它如防火墙、IPS 和漏洞扫描器等产品，形态和部署也都类似。监控类产品通常以超级虚拟机（比一般应用系统 VM 的访问权限高）的形式存在，对发生在本物理节点上的各种流量进行监控。这些流量包括：

- 进出物理节点的流量；
- 进出各 VM 的流量；
- 各 VM 之间的流量。

对于安全管理和安全审计类的产品，可以依然保持原有的产品形态，不进行虚拟化的转换。但是在功能和性能上需要做出相应的改进。例如：

- 支持同时对大批量虚拟安全设备的管理；
- 支持用户自服务；
- 支持远程加载卸载虚拟安全设备；
- 虚拟安全设备的状态监控。

## 五、结束语

随着越来越多的数据中心采用虚拟化技术，虚拟化安全问题也日益突出。本文在简述虚拟化环境中新安全威胁的基础上，梳理了虚拟化环境中的安全对策。

从传统的 IT 架构向虚拟化环境转换，要从规划和部署阶段就开始考虑安全问题。从架构的设计到虚拟化软件的选择，从加密和认证的实现方式到兼容性的测试，要有全面的考虑。在虚拟化实现阶段，要考虑安全控制措施如何实现。如监控盲点如何进行监控、访问授权的变更、性能监控等。

随着虚拟化技术的广泛应用，虚拟化环境中的安全需求会逐渐变得清晰。虚拟化安全的问题还需要不断继续跟踪研究，根据实际的业务应用，不断提出新的安全需求，逐步建立起比较完善的虚拟化安全需求的参考模型。

# 美国政府信息安全建设综述

行业营销中心　李文法　孙铁

**摘要：**本文对美国政府信息安全建设机构进行分类，给出了美国政府信息安全建设组织结构图，分析了美国相关机构制定的信息安全方针、政策、法律和法规，介绍了美国国土安全部、国家标准与技术研究院、政府审计办公室和信息基础设施保护学会等重点机构，总结了围绕国家信息安全建设战略开展的一些信息安全建设重点活动。

**关键词：**信息安全　组织结构　方针政策　重点活动

## 一、引言

随着信息技术的发展和计算机网络在世界范围内的广泛应用，网络已经成为继领土、领海、领空之后的“第四空间”，是一个国家和民族发展赖以生存的空间。国家政治、经济、文化、军事等受网络的影响日益增强，给国家安全带来了新的威胁，网络安全受到高度重视。美国是世界上最早建立和使用计算机网络的国家，他们凭借信息高速公路开始进入网络经济时代，其国家信息高速公路、全球信息基础设施相继建成，引领美国经济持续快速增长，同时在世界网络运用方面独领风骚。美国是因特网的发源地，也是当今科技发展最先进的国家，其信息化建设和信息安全发展水平一直领先于其他国家，对其信息安全建设情况进行研究，借鉴和学习其先进的理论和技术，可以使我国信息安全建设紧跟世界最新的技术和发展水平，并少走一些弯路。本文对美国政府信息安全建设组织结构、方针政策法律法规、重点机构和重点活动等进行研究。

## 二、美国政府信息安全建设组织结构

### 2.1. 美国政府信息安全机构建设概述

维护国家信息网络安全是美国政府的一项重要职责。通过强化政府的安全职能，加强网络监控力度，改组信息管理机构，设立层层主管机构，美国逐步形成一整套信息安全防范体系。为了统一领导并便于协调，美国很早就成立了由主要内阁成员参加的“关键基础设施保护委员会”。该委员会定期举行会议并提交报告，为总统了解信息网络安全状况和制定政策提供建议，并协调各项保护信息系统

计划的实施。在信息安全的组织和执行机制上，美国总统通过国家安全委员会、关键基础设施保护委员会处理和协调有关信息网络安全事务。关于信息网络安全的具体工作，分别由美国商务部下属的国家标准与技术局和国防部下属的国家安全局等分工负责。

“9 • 11”事件后，美国政府强烈认识到紧急事件发生后的应急管理中，各部门之间的安全情报等信息的流动性及共享性问题的重要性。2002 年 11 月 25 日，布什签署《2002 年国土安全法》，在原有的 23 个联邦政府部门的基础上，整合成立国土安全部。国土安全部合并了由关键基础设施保护委员会演变而来的关键基础设施保护办公室和联邦调查局的国家基础设施保护中心，是美国联邦政府确保网络安全的核心部门，负责全美联邦政府的信息网络安全问题，支持联邦政府各部门、各机构对网络攻击做出响应，对网络攻击提供实时报警、综合分析、执法调查和应急响应活动，在保障信息安全时是公共部门、私营部门和研究机构之间的指挥中枢。为更好地发挥信息网络的作用，布什还首次设立“总统网络安全顾问”一职。

面对越来越严峻的安全形势，奥巴马就职不久就要求对美国的网络安全状况进行为期 60 天的全面评估。随后，不断完善美国信息网络安全组织机构。2009 年 5 月，奥巴马发表声明，决定将成立白宫网络安全办公室，其办公室主任将担任白宫网络安全协调官。2009 年 6 月，国防部长盖茨根据奥巴马决定，发布备忘录，宣布正式成立由国防部国家安全局局长领导的美国网络司令部，统一领导军事网络空间战活动。2009 年 12 月，美国总统奥巴马正式任命白宫网络安全顾问霍华德 - 施密特为“网络沙皇”，担任白宫网络安全办公室主任一职。2010 年 5 月 23 日，美国国防部宣布，美国网络司令部正式启动，由国家安全局长基思•亚历山大任司令，将与国土安全部、国家安全局等部门密切合作，打击敌对国家和黑客的网络攻击，协调网络安全以及指挥网络战，以便有效维护美国信息网络安全。

### 2.2. 美国政府信息安全建设机构分类


图 1 美国政府信息安全机构分类

在深入分析国内外相关研究的基础上，系统总结，结合我们自己的研究成果，根据其主要职能和隶属关系，对美国信息安全机构进行分类。美国信息安全建设机构主要分为四类，依次为总统办事机构、行政执行部门、国会相关机构以及公私合作机构。如图1所示。

总统办事机构。通过对总统进行建议，制定信息安全相关的方针、政策和国家战略，并组织和协调相关信息安全机构。主要有国家安全委员会的网络安全相关子委员会、管理和预算办公室的信息政策办的信息安全相关职能单位、科学和技术政策办公室负责信息安全的研究与发展部门。

行政执行部门。是信息安全相关职能的主要执行单位。主要有国土安全部的网络安全和通信局的国家网络安全处，国防部的国家安全局、国防信息系统局和国防高级研究计划局，商务部的国家标准技术研究所及国家电信和信息署。

国会相关机构。负责制定信息安全相关法律和立法，审计和监督政府信息安全相关法律和政策的执行。主要有国土安全委员会的网络安全、基础设施保护和安全技术小组委员会（众议院），商业、科学和运输委员会的通信、技术和互联网小组委员会（参议院），国土安全和政府事务委员会的联邦财政管理、政府信息、联邦服务和国际安全小组委员会（参议院），政府审计总署。

公私合作机构。负责信息安全的相关研究和保障。主要有网络安全全国联盟、跨部门网络安全工作组、信息基础设施保护学会、信息共享和分析中心。

各类信息安全机构在白宫网络安全协调官的领导、组织和协调下，各司其职，相互协作，分别负责相关的网络安全工作，共同完成美国信息安全建设任务。

### 2.3. 美国政府信息安全建设组织结构

参考美国政府机构手册、国外关键信息基础设施美国部分和美国政府机构网站资料，在图1所示的美国政府信息安全机构分类的基础上，利用发散思维和层次化分析的思想，给出如图2所示的美国政府信息安全建设组织结构。

美国政府信息安全建设组织结构，以白宫网络安全协调官为中心，按照总统办事机构、行政执行部门、国会相关机构和公私合

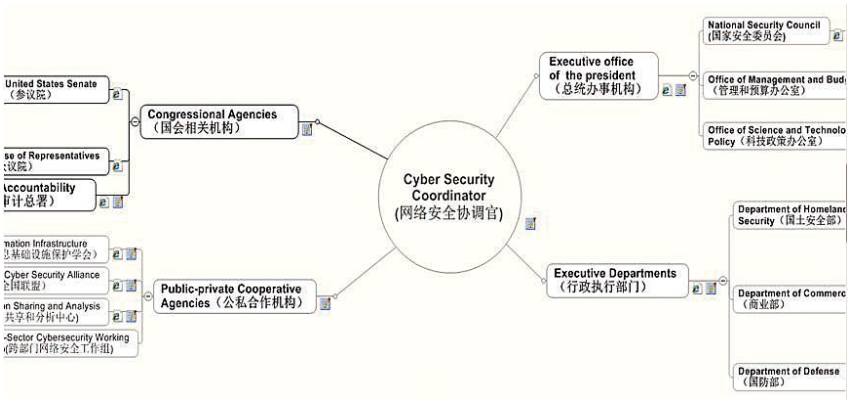



图2 美国政府信息安全组织结构

作机构分类，并以此为基础，进行细分下去，直到相关的具体信息安全机构。针对每一个机构和具体的分支机构，搭建相应的结构关系，给出相应的网络站点链接和重点标注，说明相关机构的主要职责，发布的方针、政策、法律、法规，领导或协调开展的重点活动，并进行简单总结和分析。

## 三、美国政府信息安全建设方针政策法律法规

服务于美国信息安全建设国家战略，美国政府信息安全建设的方针、政策、法律和法规根据需要，或由总统办事机构，或由行政执行部门，或由国会两院进行制定，下面从白宫和总统办事机构发布、美国行政执行部门发布、美国国会相关机构发布三个方面对信息安全方针政策法律法规进行介绍。

### 3.1. 白宫和总统办事机构发布的

2000 年 1 月，美国总统克林顿发布《信息系统保护国家计划》，该计划可以看作是美国 21 世纪信息安全的总体战略和指南，涉及到脆弱性评估、信息共享、事件响应、人才培养、隐私保护和法律改革等，侧重于保护关键基础设施网络成分而非物理成分。

2002 年 12 月，美国总统签署命令，发布《电子政务法》，该法对联邦政府信息技术管理和规划的每一个方面，从危机管理到电子档案及查询索引都做了规定。该法还第一次拨专款 3.45 亿美元支持《电子政务计划》。在具体内容中特别强调了电子政务中的信息安全问题，重新授权政府信息安全改革法，为保护政府计算机网络安全提供管理框架。

2003 年 2 月，白宫发布《保护网络空间安全国家战略》（NSSC）。NSSC 勾勒了组织打击由恐怖分子、罪犯或敌对国家发起的网络攻击的工作并确定其重点的初步框架，其战略目标是：（1）预防国家关键基础设施遭受网络攻击；（2）减少国家面对网络攻击的脆弱性；（3）将网络攻击造成的损害以及恢复时间降至最低程度。

2006 年 4 月，国家科学和技术委员会发布《联邦网络安全及信息保障研究与发展计划 (CSIA)》，确定了 14 个技术优先研究领域，13 个重要投入领域。为改变无穷无尽打补丁的封堵防御策略，从体系整体上解决问题，提出了十个优先研究项目，包括：认证、协议、安全软件、整体系统、监控检测、恢复、网络执法、模型和测试、评价标准、非技术原因。

2008 年 1 月，美国总统签署国家安全第 54 号总统令，国土安全第 23 号总统令，提出《国家网络安全综合计划》（CNCI）。这是一项多年计划，将由多个部门参加并分步骤实施，其最终目的是保护美国的网络安全，防止美国遭受敌对电子攻击，并能对敌方展开在线攻击。CNCI 包括了许多互助性的提议，其主要目标是：（1）建立一个防御线以抵御当前面临的威胁；（2）实现应对全方位威胁的防御能力；（3）巩固未来的网络空间环境安全。

2009 年 5 月，奥巴马发表信息安全评估报告《确保我们国家的网络基础设施安全》，指出来自网络空间的威胁已成为美国面临的最严重的经济和军事威胁之一，将成立白宫网络安全办公室，其负责人将协调相关国家机构制定出美国的网络安全政策，并向国家安全委员会和国家经济委员会汇报工作。报告还建议任命网络安全官员，

负责协调美国的网络安全政策和行动；对民众开展网络安全教育；制定网络安全事件应急计划等。

### 3.2. 美国行政执行部门发布的

2003 年 4 月，国土安全部（DHS）发布执行国会的《国土安全法案》的法规《关键基础设施受保护信息方案》，该法规就接收、照管和保存关键基础设施信息，保持安全性和保密性，以及处理专有或企业敏感信息的方法做出了规定。

2006 年 6 月，国土安全部（DHS）发布《国家基础设施保护计划》（NIPP）。该计划为现行和未来的保护关键基础设施和重要资源方案及活动提供了一个总体框架。NIPP 特别考虑了关键基础设施保护中网络方面的问题。

### 3.3. 美国国会相关机构发布的

2002 年 2 月，美国众议院通过了《网络安全研究与发展法》（CSRDA），该法在国家信息网络安全领域的机构建设、研究计划管理、资金投入与管理、专门人才培养等方面都规定了有效的措施。2002 年 10 月，美国国会通过《联邦信息安全管理法案》（FISMA），该法案定义了一个广泛的框架来保护政府信息、操作和财产来免于自然以及人为的威胁，保护信息和信息系统以避免未授权的访问、使用、泄露、破坏、修改或者销毁，以确保信息的完整性、保密性和可用性。FISMA 把责任分配到各种各样的机构上来确保联邦政府的数据安全，并在 2002 年成为《电子政务法》的一部分。作为补充和更新，美国政府发布了一系列 SP800，最新的发布是 2011 年 2 月发布的 SP800 ı 147。

2005 年 4 月，美国众议院国土安全委员会的经济安全、基础设施保护和网络安全小组委员会通过了《2005 网络安全增强法》，该法规定负责网络安全的国土安全部副部长为国家网络安全分部的主要行政首长，该分部负责识别、减少网络安全脆弱性和威胁，提供网络攻击告警。

2009 年 4 月，美国众议院参议员提出《2009 网络空间安全法案 (773 号 ) 》，该法案拟给予总统和国土安全部等相关部门广泛权力，包括审查认证网络安全工作人员、必要时关闭网络等，但该法案也因为给予总统过大权力而受到争议。

2010 年 3 月，美国参议院商务、科学和运输委员会通过了《网络安全法案》，该法案旨在加强美国网络安全、帮助美国政府机构和企业更好的应对网络威胁。法案要求政府机构和私营部门在网络安全领域加强信息共享，在应对“网络安全紧急情况”时加强合作。该法案还要求通过市场手段，鼓励培养网络安全人才，开发网络安全产品和服务。

## 四、美国政府信息安全建设重点机构

美国政府信息安全建设相关机构主要包括总统办事机构的信息安全相关机构、行政执行部门的信息安全相关机构、国会相关机构的信息安全相关机构和公私合作机构的信息安全相关机构，对于其中比较重要的一些，下面进行介绍:

- 国土安全部（DHS）

2003 年 3 月，美国 23 个联邦署、局、处合并成国土安全部（DHS）。DHS 协调多个联邦、州和地方政府机构，其中涵盖了负责与国土安全相关的各种任务的各种机构。与网络安全相关的是网络安全和通信局（CS&C），其下属单位有：国家通信系统处（NCS），任务是确保联邦政府的国家安全和应急通信在任何情况下都畅通无阻；国家网络安全处（NCSD），与私营、公共部门以及国际上的合作伙伴就信息基础设施保护工作开展合作，它通过建立和保持响应系统（如US—CERT），以及与安全合作伙伴共同制定和落实关键基础设施反网络风险管理计划来做到这一点；应急通信处（OEC），开发、执行和协调各级政府用于应急响应的可互用和可运行通信。

• 国家标准与技术研究院 (NIST);

美国国家标准与技术研究院直属美国商务部，其所属的信息技术分部，从事信息技术方面的基础和应用研究，以及测量技术、测试方法和信息安全方面的研究，提供标准、标准参考数据及有关服务，发布了一系列信息技术方面的标准，特别是 SP—800 系列，是信息安全方面的主要技术标准。

在信息安全领域，他们协助美国政府和产业界进行安全规划、风险管理、应急计划、加密、人员身份认证及智能卡应用等安全技术的开发、推广应用、计算机病毒检测与防治、安全教育培训等方面的工作，同时还负责制定安全技术和安全产品的国家及国际标准。

• 政府审计办公室（GAO);

政府审计办公室是国会的调查机构。国会经常委托 GAO 研究联邦政府的计划和开支。GAO 曾就关键基础设施保护和信息安全发表过多篇报告和证词。（1）2005 年 5 月，GAO 发表《关键基础设施保护：国土安全部面对负网络安全全责的挑战》，提高有关网络安全角色和能力的认识是 DHS 面对的巨大挑战之一；（2）2006 年 9 月，GAO 发表《协调联邦网络安全的研究和发展》，联邦网络安全的研究和发展应当统一协调；（3）2007 年 3 月，GAO 发表《需要不断取得进步以加强对数据安全和交换的控制》；（4）2008 年 9 月，GAO 发表《关键基础设施保护：国土安全部需要更好地履行它的网络安全责任》;（5）2010 年 3 月，GAO 发表《网络安全：在明确和协调国家综合计划方面，尽管取得了进步，但依然面临巨大挑战》。

• 信息基础设施保护学会（I3P）。

由 Dartmouth 学院负责管理的信息基础设施保护学会是一个领导着全国网络安全研究机构（其中包括大学研究中心、政府实验室和非营利研究机构）的团体。学会建立于 2001 年 9 月，主要任务是协调全国性网络安全研发计划，并在学术界、工业界和政府之间帮助架设起沟通的桥梁。I3P 识别并解决关键信息基础设施工作中的关键研究问题，同时在研究者、政策制定者和基础设施经营者之间开通交流信息的渠道。

## 五、美国政府信息安全建设重点活动

以美国信息安全建设国家战略为主线，对美国信息安全建设的主要活动进行关注，可以了解美国信息安全建设的最新情况和动态，学习和借鉴，并用于我国的信息安全建设。主要的信息安全活动有：联邦桌面核心配置（FDCC）计划、“爱因斯坦”计划、“网

络风暴”演习、“国家网络靶场”等项目。

• 联邦桌面核心配置计划（FDCC）;

2007 年，美国联邦预算管理办公室、国家标准技术研究院、国防部、国土安全部和微软开始合作开发联邦桌面核心配置（FDCC）。美国联邦政府强制规定所有使用 Windows 的计算机必须符合 FDCC 的配置计划要求。FDCC 计划的核心是制定美国联邦政府 Windows 桌面计算机的安全配置标准，又称为 FDCC 安全基线。目前美国标准技术研究院已发布基于 Windows XP 和 Vista 操作系统的 FDCC 安全基线。同时为支持 FDCC 的规划、测试和部署，微软推出了多个配套实施工具。FDCC 作为联邦政府所有桌面计算机的安全配置标准，已经成为美国国家网络安全综合计划（CNCI）的重要组成部分。

• “爱因斯坦”计划;

2007 年，美国发起“爱因斯坦”计划项目，“爱因斯坦 2”是美国联邦政府一项网络安全自动监测项目的代号，来源于《国家网络安全综合计划》，其主要功能包括实时监测各成员机构网关的流量状况、蠕虫检测、配置管理和趋势分析等。国土安全部下属的美国计算机应急响应小组的安全专家可以通过“爱因斯坦”实时纵览跨机构的安全事件，各成员组织也可以到一个安全的门户网站查看自己的网关数据。“爱因斯坦”项目是非强制性的，其成员包括国土安全部、交通部、国务院、财政部、司法部、教育部、联邦贸易委员会、美国证券交易委员会和美国国际发展署等大部分政府机构。

• “网络风暴”演习;

2006 年，美国国土安全部主持进行了有十多个州政府机构、40 多家私营公司和多个美国联盟国家参加的第一次“网络风暴”演习。以后每两年举行一次，到 2010 年，已经举行了三次。“网络风暴”演习旨在改善网络事件响应共同体的能力，促进在关键基础设施行业中公共 - 私营伙伴关系的发展，并且加强联邦政府和其在州、地区及国际层面政府伙伴之间的关系。演习的目标为：检查参与组织准备、保护和响应网络攻击相关的能力；依照国家级政策和程序，演习事件响应的高级领导决策和机构间协调；为网络事件态势感知、响应和恢复信息的收集和分发，验证信息共享关系和通信通道；检查以安全可靠而不危害产权和国家安全利益的方式跨标准边界共享敏感和保密信息的手段及过程。

• “国家网络靶场”项目。

“国家网络靶场”项目是美国为巩固国家信息安全，实现打赢网络战争的战略目标的一项重大举措，来源于《国家网络安全综合计划》，是美国《国家网络安全综合计划》中一个重要的里程碑。靶场的建设目标是，为模拟真实的网络攻防作战提供虚拟环境，针对敌对电子攻击和网络攻击等电子作战手段进行试验，以实现网络作战能力的重大变革，打赢网络战争。“国家网络靶场”将成为一种测试涉密与非涉密网络项目的国家资源。获得授权进行网络试验的政府及政府资助的测试组织可与“国家网络靶场”执行机构协调，安排靶场时间与资源。国防高级研究计划局是协调所有相关事件、时间与资源冲突的最高权威机构。“国家网络靶场”将为特定试验分配资源，建立试验平台。“国家网络靶场”将支持多任务测试、同步测试、单元等测试及测试平台。

## 六、总结

本文在深入研究美国政府信息安全建设情况的基础上，将美国政府信息安全建设机构分为总统办事机构、行政执行部门、国会相关机构和公私合作机构四类，给出了美国政府信息安全建设组织结构图；与信息安全建设机构相对应，分析了美国相关机构制定的信息安全方针、政策、法律和法规；针对需要重点关注的机构，介绍了美国国土安全部、国家标准与技术研究院、政府审计办公室和信息基础设施保护学会；最后，以美国信息安全战略，特别是《国家网络安全综合计划》为主线，总结了围绕国家战略开展的一些信息安全建设活动。

随着信息技术的不断发展和网络环境的变化，美国政府信息安全建设还有许多问题有待研究。下一步，我们将对美国政府信息安全建设情况继续研究，充分借鉴国外的先进经验，为制定符合中国国情的信息安全战略、方针和政策，提高我国信息安全的保障能力和防护水平，建立适应社会主义市场经济发展的信息安全模式而贡献我们的力量。

## 参考文献：

1、http://www.usa.gov/Agencies/Federal/Executive/Homeland_Security.shtm

2、The White House. the National Strategy to Secure Cyberspace 2003. February 2003

3、The White House. Federal Plan for Cyber Security and Information Assurance Research and Development. April, 2006

4、Steven Robinson. U.S. Information Security Law, Part Four. http://www.symantec.com/connect/articles/us-information-security-law-part-four

5、Peter H. Chen. The Strategic Evaluation of the National Strategy to Secure Cyberspace. http://www.peter-chen.com/docs/I-WPaper.pdf

6、The White House. Cyberspace Policy Review(Assuring a Trusted and Resilient Information and Communications Infrastructure). http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

7、http://csrc.nist.gov/publications/PubsSPs.html

8、Thomas J. Smedinghoff. The State of Information Security Law. http://www.cert.org/archive/pdf/state_infosec_law0801.pdf

9、张谊军，林永文，梅宏宾等，美国政府机构手册，军事谊文出版社，2000

10、郑晓林，高能，荆继武，美国信息安全发展策略导向评述，计算机应用研究 2006(09)

11、沈逸，开放、控制与合作：美国国家信息安全政策分析，复旦大学，2005

12、陈晓桦，左晓栋，美“国家网络安全综合计划”揭开神秘面纱，信息安全与通信保密，2010（4）

# 中国团购网站安全分析报告

行业营销中心　刘京威

**摘要：**据统计，团购网站自短短一年多以前在中国首次出现后，目前已发展到 3000 多家。作为互联网行业中的一个新的垂直类型，团购行业的辉煌背后，有多少网站安全漏洞会对其运营造成威胁，会成为其风光背后的隐忧，本报告将一一揭开。

**关键词：**团购网站　网站安全检测　安全分析

## 一、背景介绍

### 1.1. 行业背景

在刚刚过去的 3.15 消费者权益日中，团购安全问题被再次提出并引起热议。由于 2010 年团购网站井喷式的兴起，相关的行业规范和监管机制难以跟上，使得团购行业存在种种法律法规漏洞，这必然导致目前这种大规模的消费者投诉的态势。

许多团购企业都希望做大做强，但日益复杂的互联网安全问题，却让这些企业在团购的某些环节中，受到不法分子的利用，成为侵害消费者权益的相关人，进而蒙受巨大的商誉损失，以及直接或间接经济损失。此外，互联网安全威胁还可能导致各种各样对于团购站长和企业非常棘手的麻烦和损失，例如网站无法访问或内容显示异常，用户和企业敏感数据丢失，等等，都会进一步导致更加严重的后果。

因而，团购企业在关注对消费者的团购信誉的同时，也应该从另一个角度关注自身网站的安全，保护好自己不受侵犯，才能真正做到保护好消费者的利益。

需要特别说明的是，团购网站作为互联网行业中的一个类别，格外容易受到安全威胁。为什么这么说呢? 这跟团购网站在中国发展的历史和背景有关。

在中国互联网发展历程中，2010 年可以称之为“团购年”。在这一年中，团购网站从兴起，到短短数月间发展为“千团大战”的规模。究其原因，简单的说可以归结为其清晰且可复制的商业模式，以及较低的技术门槛，加之国内这样一个非常适合团购产业发展的环境等等。很多小型企业和有创业愿望的个人很快意识到了自己也有能力加入团购事业的大军，这就使得中国团购行业中，个人和微型企业占据很大比重。

基于以上背景，目前的大多数团购网站，注意力大多还停留在基本的如何运作、推广和盈利上，殊不知在看不见的未知领域里，存在着可以轻而易举破坏其业务的隐患，摧毁力不仅会导致直接的经济损失，还会严重影响品牌形象和企业商誉，使团购企业主和从业人员的诸多努力和积累付之东流。

### 1.2. 调查对象和目的

本报告通过对 2011 年 2-3 月期间的近

1500 个团购网站的多种安全相关指标的检测和研究，分析、展现团购企业的安全现状和存在的安全威胁及隐患。目的是使得团购站长和管理人员对于其团购网站的安全现状有所认识，并引起其对网站安全的重视，同时传达一些基本的安全知识，帮助和引导团购站长和管理人员尽快树立安全意识，使其在网站安全领域尽可能做到防患于未然。

### 1.3. 调查方法

绿盟科技通过其强大的安全检测能力，对调查对象安全相关的多种指标进行检测，再结合其安全领域多年积累的经验和知识，对检测数据进行分析及总结，得出团购网站安全现状，并分析和列举导致的原因和可能的解决办法。

### 1.4. 调查结果概览

根据检测结果，团购行业安全现状与调查前的预想基本相符，绿盟科技调查后的整体印象总结如下:

- 团购网站负责人普遍缺乏安全意识，提高团购的安全性首先需要提高团购网站负责人的安全意识;
- 大多数团购网站存在安全隐患，许多同时存在多种安全隐患，非常容易损害用户利益;
- 整个团购行业的网站安全系数偏低，有较大提升空间。

下面首先来看一个真实的安全事件。

## 二、某团购网站安全事件

### 2.1. 事件危害

流量损失：50000 IP/ 日

直接经济损失：约 10 万元

间接经济损失：因为连续两日网站无法访问，除了直接的流量和销售损失外，还会使浏览者对该团购站的品牌形象和商誉产生负面的联想，一方面导致新老客户的流失；另一方面，此消彼长，使得竞争对手获益。其造成的间接损失难以估算。

### 2.2. 事件经过

2010 年 12 月 20-21 日，运营地点在杭州的某团购网站，因先后遭受 500 万流量的 DDoS 攻击和木马攻击，导致 48 小时网站无法访问。因为服务器是托管的，没有保留场景文件，下面是访问截图:

| 时间 | 拦截内容 |
| --- | --- |
| 12:52:15 | 已拦截 IE浏览器 访问 http:// [redacted] ndex/mm.js [恶意网址] |
| 12:52:05 | 已拦截 IE浏览器 访问 http:// [redacted] index/mm.js [恶意网址] |
| 12:51:58 | 已拦截 IE浏览器 访问 http:// [redacted] index/mm.js [恶意网址] |
| 12:51:46 | 已拦截 IE浏览器 访问 http:// [redacted] index/mm.js [恶意网址] |

图表 1 访问截图

该网站服务器托管在厦门，每年费用是 2.5 万元，网站每日独立访问 IP 为 9 万左右，每日收入 2 万元左右。除了被攻击的两天没有流量外，恢复后的几天内，流量大幅削减，掉到了 4 万 IP/ 日，流量减少了一多半。事后，厦门托管机房的人解释是因为机房有服务器被感染木马导致的，同时要求站长加一台服务器，再购买一个防火墙。由于 12 月正是团购高峰期，为了避免更大损失，站长花 3 万元加了一台服务器并购买防火墙。

由上可知，此次安全事件给这个团购网站带来的直接经济损失约为 10 万元。

在这个团购网站安全事件中，暴露了 DDoS 攻击和挂马这两种网站安全问题。在后面的内容中将对 DDoS 攻击和挂马进行详细解释。

## 三、购网站可能存在的安全威胁

团购网站的安全问题可能导致许多不良后果，轻则使得网站无法访问，造成短期的流量损失，影响收益；重则会使消费者遭受重大损失，从而使企业商誉受到重创，长期影响品牌形象和收益。根据绿盟科技在安全领域的多年经验，一般来说，企业网站因安全问题而导致的严重后果主要有三类: 网站打不开，用户被仿冒网站欺骗，以及用户和企业双方的信息和数据丢失。

绿盟科技经过对现存的近 1500 个大大小小的团购网站的调查和检测，发现团购行业的安全现状存在诸多问题，随时可能遇到上述三种麻烦。下面首先列出一些较为重要的检测结果和数据:

- 至少有 58% 的团购网站的可正常访问的比例低于 80%;
- 仅开放 80 端口的网站只有 44 个，其中大部分都是大型团购网站或背靠大型互联网公司的团购网站;
- 高达 80% 的团购网站没有使用任何加密措施;
- 91% 的网站存在引用其他网站内容（即第三方内容）的情况。

由以上数据，绿盟科技认为很多团购网站运维和安全水平都比较低。一方面由于网站经常出现不可访问的情况，会直接影响形象和收入，另一方面由于缺乏必要的安全意识导致网站和团购网站用户很容易遭受损失。

后续将对这些内容进行详细说明。

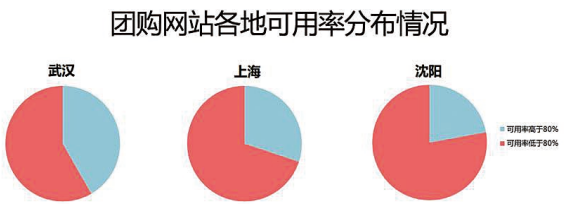
### 3.1. 网站打不开

网站能打开是用户浏览网站的基本前提。对于靠网站支撑业务的互联网行业来讲，如果网站都无法打开，一切努力、目标和愿景都会变成浮云，团购网站尤其如此。报告开头的事例，就是一个典型的因网站不可用导致损失的事例。对于站长来说，保证网站的可用性是第一步。

绿盟科技为了调查团购网站在可用性方面的现状，用了一周的时间，对大大小小将近 1500 个团购网站的可用率，分别从上海、武汉、沈阳三地共进行了近 700 次检测。检测结果令人担忧:

| | 武汉 | 上海 | 沈阳 |
|---|---|---|---|
| 可用率分布 | 站点数 ( 占总数百分比 ) | | |
| 70%-80% | 863 (58%) | 1035 (70%) | 1152 (78%) |
| 80%-90% | 0 | 0 | 42 (3%) |
| 90%-100% | 0 | 0 | 35 (2%) |
| 100% | 617 (42%) | 445 (30%) | 251 (17%) |

表格 1 团购网站可用率分布情况




图表 2 团购网站各地可用率分布情况

总结一下表格 1，值得注意的是，三地至少有 50% 的团购网站的 20% 用户访问网站时遇到无法打开网站的情况。换句话说，对于这 50% 以上的团购网站，经过检测，每 100 次访问中，就会有 20 几次无法正常显示页面。

团购网站的流量一般和收益成正比，这就可以很容易的计算出因为网页无法正常显示所带来的收益的损失量有多少，而这种损失本是可以避免的。

那么哪些具体的原因有可能导致网站不可用呢?

DDoS 攻击

通俗地说，DDoS 攻击就是通过大量恶意访问造成网站瘫痪，造成网站不可用。这是造成前面案例中的团购网站损失的原因之一。

DNS 解析错误

DNS 解析错误就是，当访问者正常的输入某网址时，本应该对应某一特定 IP 地址进而进入网站，但是因为某些原因，例如受到恶意的 DNS 劫持，使得这种对应关系被打破，进而服务器无法找到本应找到的网站，造成网站无法访问。关于 DNS 劫持，下文会进行专门介绍。

网站被挂马

当网站被挂马后，访问者在访问该网站的时候，所使用的浏览器、防病毒软件、防火墙等各类具有安全功能的软件都会发出提示，阻止用户访问被挂马站点，以确保用户安全。用户看到提示后，往往都不会再打开这个网站，因此间接导致网站不可访问。前面的案例中提到的被挂马，就属于这种情况。

### 3.2. 用户 / 网站敏感数据丢失

如果缺乏必要的安全意识，没有采取必要的安全防护工作，网站很可能遭受攻击者的攻击。导致的后果就是，网站用户或者网站本身的数据受到窃取，继而被利用来获得不法收入。因此团购站长应该尽量减少网站的漏洞，减少被入侵的入口和可能，让用户放心的在网站上进行消费。

端口漏洞

对于网站管理人员来说，关闭不必要的端口是最基本的安全常识。端口越多，安全漏洞越多。绿盟科技就此检验了团购网站的端口开放情况。结果发现，1096 个团购网站中，仅开放 80 端口的站点只有 44 个，占总数的 4%。也就是说，绝大多数网站在端口方面存在漏洞，给非法入侵者窃取数据留有机会。这个数据说明目前团购网站的站长对于网站安全的关注度比较低。

在这仅有的 44 个网站中，大部分为比较大型和知名的团购网站，例如专业团购网站拉手网，以及淘宝聚划算、新浪、腾讯、点评等互联网门户网站旗下的团购网站。这说明了背靠这些大型企业的团购网站有更强的网站管理和安全意识。

服务器漏洞

通常来说，服务器漏洞跟服务器的品牌和版本是一一对应的。根据网站使用的服务器及其版本，可以对应着找出存在着哪些漏洞。绿盟科技在本次普查过程中主要是通过版本检查的方式获取服务器的漏洞情况。

经过绿盟科技对这些团购网站的检测，发现这些团购网站使用的所有类型和版本的服务器中，使用最多的品牌是微软的 IIS，紧随其后的是 Apache；而使用最多的版本是微软的 IIS 6.0，其他版本使用情况分布不一。针对微软 IIS6.0 常见的漏洞如下:

- Microsoft IIS 脚本文件名错误解析漏洞;
- Microsoft IIS 重复参数请求拒绝服务漏洞（MS10-065);
- Microsoft IIS 认证令牌处理远程代码执行漏洞（MS10-040);
- Microsoft IIS 畸形文件扩展名绕过安全限制漏洞。

### 3.3. 用户被仿冒网站欺骗欺诈

如果说网站不可用带来的主要是短期流量和收益的损失，那么，用户被仿冒网站欺骗，带来的将不仅是对短期收益的负面影响，更是对长期商誉和品牌形象的巨大打击。从手段上来看，不法分子有各种各样的方法对网站用户进行诱骗，或对其信息进行窃取，例如通过 IM、社区、社交网站等途径发布钓鱼网站链接，利用银行或电子商务网站漏洞将网站用户直接引至钓鱼网站，等等，从而非法谋取利益。作为团购网站，属于电子商务网站的一种，很有可能成为不法分子用来牟利的跳板。因此，作为团购网站的站长，不得不考虑如何降低网站被利用的风险，防止自己的消费者因为对自己的信任而造成财产上的损失和情感上的伤害。下文将一一列举和分析有哪些安全隐患可能会造成用户受到欺诈的恶劣后果。

#### 引用其他来源内容

有网站维护经验的人都知道，建立网站和网页过程中，有时会直接通过链接引用其他网站的内容（包括文字、图片、Flash 、JavaScript 脚本等各类网站资源），使其显示在自己的网站上。网站访问者并不关心、也不知道这些资源来自于其他网站。这种来自于其他网站的内容被通称为 “第三方内容”。

由于第三方内容实际上获得了和原网站一样可以访问用户浏览器中显示的内容、甚至窃取用户的机密数据，从而导致网站 “被黑” 、“被挂马”、“被钓鱼” 等多种安全事件，最终导致用户被仿冒网站欺骗的问题。

绿盟科技对近 1500 个团购网站进行了调研和检测后发现，在中国的团购网站中，引用第三方内容是一种非常普遍的做法，以下是具体检测结果:

| | 网页 | 网站 |
|---|---|---|
| 检测总数 | 204344 | 1169 |
| 含第三方内容数 | 158271 | 1075 |
| 第三方内容所占比例 | 77% | 91% |

表格 2 第三方内容比例

从表格中可以清楚的看到，高达 91% 的团购网站引用了第三方内容； 77% 的团购网站页面引用了第三方内容。这意味着，大部分的团购网站的安全性并不完全可控，很容易受控于某些第三方网站。从包含第三方内容网站的数量分布来看，所检测的一千多个团购网站中，没有发现特定规律，有些网站没有或者只有一两个第三方内容，而引用最多的网站则高达两千多处，中间的分布也非常平均。1169 个团购网站如果平均来看，每个网站引用第三方内容的数量约为 281 个，也就是平均每个网站有 281 个机会通过被劫持第三方内容而被入侵，从而导致网站被黑、用户信息丢失等各种安全事件。

为了降低第三方内容带来的安全问题，最有效的方法就是尽量少直接引用第三方内容；确实需要引用时，应尽量选择新浪、百度、

腾讯等安全程度较高的网站内容进行引用。

网站未加密或加密有缺陷

安全加密通道 SSL 可以避免用户的数据在传输过程中被窃取，从而能够保障用户数据的安全性。与 SSL 相关的概念是 TSL，TSL 可以认为是 SSLv3 的升级版本，安全性最高。本次共检测 1480 个团购网站，其中存在不同程度 SSL 安全漏洞的网站占总数的 94% 之多。检测结果分为以下四类:

1）不支持数据加密，也就是不支持任何 SSL 和 TSL 协议。此类网站共检测出 1188 个，占总数 80%，是安全问题最大也是存在问题数量最多的一个;

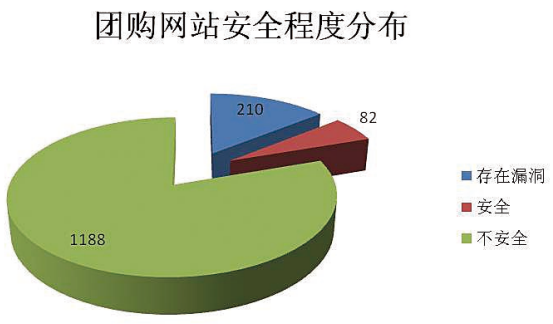
2) 版本太低。此类网站有 210 个，占 14%，它们只支持 SSLv2 协议;

3）密钥太短。有 292 个网站或多或少采用 128 位以下的算法，这是非常不安全的;

4）数据加密无漏洞。只有这类网站可以认为不存在明显的安全隐患，遗憾的是数量仅有 82 个，仅占总数的 6%。

| 类别 | 网站数量 |
|---|---|
| 安全（使用了安全加密方法） | 82 |
| 存在漏洞（使用了安全加密，但加密方法不安全） | 210 |
| 不安全（没有使用安全加密方法） | 1188 |

表格 3 团购网站加密情况检测结果




图表 3 团购网站安全程度分布情况

图表 3 中，红色部分定义为安全，指的是使用了安全加密方法的网站数量; 蓝色部分定义为存在漏洞，这部分网站使用了加密方法，但是由于版本和密钥长度原因，并不完全处于安全状态中；绿色部分定义为不安全，为完全没有使用任何加密方法的网站数量。

域名被劫持

当 DNS 劫持发生时，会使得用户流量被引导到仿冒网站，而这些仿冒网站通常又会做得和正常的网站一模一样，网站用户很难察觉。一旦用户输入了自己的支付密码就很容易导致经济损失。等用户察觉到后，通常就会把过错全部记到团购网站的头上，严重影响团购网站的信誉。

要想避免遭到 DNS 攻击，站长可以根据 DNS 相关的各项 RFC 标准，对 DNS 进行标准设置，这样就可以很大程度上减少其被攻击的风险。

绿盟科技参考 RFC 的要求为团购网站的域名服务器检查了 27 项配置，并从中选择了 3 项最为重要的标准进行了检测。以下是检测结果:

| 检查项 | 检查样本数 | 不符合 RFC 要求 | 不符合比率 |
|---|---|---|---|
| 所有域名服务器上查询到的 NS 记录都是一致的 | 1426 | 670 | 46.98% |
| 从父域 (TLD 服务器 ) 查询到的域名服务器也在授权域服务器解析到的 NS 记录中 | 1426 | 528 | 37.03% |
| TLD 返回的 DNS 记录和授权域服务器返回的 DNS 记录完全一致 | 1426 | 129 | 9.05% |

表格 4 重要度为高的 DNS 最佳实践情况

可以看到，表格中前两项的危险系数是比较大的。约 47% 的团购网站没有做到 “所有域名服务器上查询到的 NS 记录都是一致的”，37% 的团购网站没有做到 “从父域 (TLD 服务器 ) 查询到的域名服务器也在授权域服务器解析到的 NS 记录中”。

重要度为中的 DNS 最佳实践项及检测结果:

| 检查项 | 检查样本数 | 不符合 RFC 要求 | 不符合比率 |
|---|---|---|---|
| 所有授权域服务器分布在不同的 C 类地址上 | 1426 | 1228 | 86.12% |
| 有两个或以上邮件服务器 | 926 | 686 | 74.08% |
| 在授权域服务器查询您域名的 NS 记录时，同时还会返回 NS 对应的 IP 地址 | 1426 | 961 | 67.39% |
| TLD 中列出的所有域名服务器都可以为你的域名做解析 | 1426 | 670 | 46.98% |
| 所有你的 DNS 服务器允许 TCP 连接 ( 推荐能够接受 TCP 查询 ) | 1426 | 655 | 45.93% |
| TLD 返回你的 NS 记录时，同时还返回了 NS 对应的 IP 地址 | 1426 | 485 | 34.01% |
| 你的 SOA 最小 TTL 值在 3600 秒到 86400 秒之间 (1-24 小时 ) | 1293 | 256 | 19.80% |
| soa 记录的 mname( 主域名服务器 ) 在 TLD 查询到的 NS 记录中 | 1293 | 230 | 17.79% |
| 所有的 NS 记录都能够解析出正确的 IP 地址 | 1426 | 129 | 9.05% |
| MX 记录设置的邮件服务器应该是主机名而不是 IP 地址 | 926 | 44 | 4.75% |
| 所有授权域服务器 IP 都是 C 类 IP | 1426 | 18 | 1.26% |
| www 主机名解析到的 IP 地址都是共有 IP | 1426 | 2 | 0.14% |
| 所有邮件服务器设置的都是共有 IP | 926 | 1 | 0.11% |

表格 5 重要度为中的 DNS 最佳实践情况

这个表格中的项，虽然重要度略低，但由于存在危险的项目比较多且对应的危险系数比较高，也列在这里。

以上三种是使得用户被仿冒网站欺骗的原因中比较典型的，除此之外还有很多原因。因此，对于团购网站管理者来说，一方面对于已知的问题要做好具体的管理和防御工作；另一方面，如果想长久稳定的保证网站正常运营，还是应该从自身的安全知识和意识抓起，才是治本的方法。

## 四、如何回避和减少这些风险

### 4.1. 培养和提高安全意识

报告开头曾经提到，由于团购行业本身的特点以及发展的速度，中国的团购企业大多还没有意识到网站安全的重要性，缺乏相关的安全知识和安全意识。

另一方面，从以上案例和分析不难看出，网站的安全对于包含团购网站在内的所有依靠网站运营支撑业务的互联网公司来说，都是不容忽视的重要课题。

所以，现在是时候开始积累安全方面的知识，培养和提高安全意识，提高自己网站的安全系数，降低营业风险，使自己的企业得以稳步健康成长。

### 4.2. 定期为网站做安全检测，随时关注网站健康

说到网站安全，对于很多人来说是个陌生的领域，感到门槛很高。绿盟科技建议，可以从最基本的定期进行网站安全检测开始做起。目前市面上有很多免费的安全检测服务，可以选择其中比较优秀的产品或服务，定期关注自己的网站健康状态，逐步开始接触并了解这个领域。

### 4.3. 选择合适的安全产品和安全服务

如果想要最大程度上降低网站的安全风险，仅仅做定期检测是远远不够的。对于大多数团购网站来说，规模较小、技术水平和资金有限，因此，选择一个既专业、又比较低成本，且方便好用的安全产品和安全服务最为适合。

本报告下载地址：http://wsp.nsfocus.net/public_reports/tuangou2011

## 附录一：网络团购行业信用概况

### （一）行业整体信用状况

网络团购行业整体信用得分为 63.3，等级为 BBB，信用一般偏下，初步具备信用，但信用能力容易产生波动，有一定经营风险。行业内各团购网站之间以及商家之间的信用水平存在很大差异。

网络团购行业属于新兴行业，商业模式清晰，融合传统集团采购和 CPS（按销售额提成）两大模式的优点，盈利前景良好，受一部分服务类商家和年轻白领一族的欢迎，业务整体发展迅速，具备一定竞争力的第一梯队企业初步显现。

但行业整体尚处于起步和自发状态，行业内部竞争较激烈，地区发展不平衡；经营主体资质（工商营业执照和 ICP 经营许可证等）大部分不具备，经营规模普遍不大，商家议价和管理能力较弱，从业人员素质差别较大；行业自律和监管较弱，顾客满意度尚可，但公共信用记录呈负面；目前行业整体现金流良好，盈利能力一般，偿债能力一般，资产负债率一般。

### （二）行业信用状况分析

在 257 家团购网站和 5 家团购导航网站的调查样本中，团购网站得分最低的为 50.7，等级 BB-，信用不佳，信用能力较差，有较大或很大风险；信用等级 BB- 和 BB 的网站占到调查样本的 39%，表明该行业有超过 1/3 的经营主体整体信用较差，需要规范。

团购网站得分最高的为 79.3，等级 AA-，信用良好，信用能力较稳定，风险较小。信用等级 AA- 和 A 的网站占到调查样本的 7%，表明该行业有一些经营主体开始重视品牌和信誉的树立，开始重视信用的积累。

团购网站信用等级 BBB，占到 54%，说明目前有超过半数的网站信用一般，初步具备信用能力，但经营不稳定，容易产生一定波动，有一定风险。

调查发现，从 2010 年 11 月中旬开始，一小部分信用能力弱的小型团购网站在争夺

商家和顾客的激烈竞争中，举步维艰，在着手寻找投资的同时，也试探寻求与有实力团购网站的并购机会。预计到 2011 年中期，国内团购网站将开始全面洗牌。

**附录二：网站团购消费行为调查**

**（一）2010 年参加团购次数与人数比例**

在 2010 年，有超过半数人没有参加过团购，参加过 1 次和 2 次的人数比例超过 30%，超过 2 次的人数比例为 13.3%。说明团购的潜在顾客群体还很庞大，有很好的发展前景。

**（二）消费者在团购决策过程中，考虑因素排序依次为**

（1）网站品牌和诚信度

（2）价格

（3）质量

（4）网站信誉和第三方认证

（5）付费方式

（6）送货服务及售后服务

（7）订单预约速度

调查结果表明，消费者最关心的是网站品牌和诚信度，其次是价格和产品服务质量。随着团购消费者的成熟，团购低价格和高折扣已经不能作为吸引消费者的唯一法宝。

**（三）消费者团购意愿**

（1）未参加过网络团购的消费者有近半数表示愿意尝试，有超过 1/4 的人群还不知道或不了解网络团购。

（2）参加过网络团购的消费者超过 2/3 表示愿意再次团购，接近 1/2 表示愿意向朋友推荐，这些数据说明团购这种形式为大部分消费者所接受和喜爱。

**（四）网络团购的消费者了解每天团购信息的渠道**

消费者获取团购信息渠道前五位依次为搜索引擎、熟悉的团购网站、朋友推荐、导航网站和手机短信。其中搜索引擎、熟悉的团购网站、朋友推荐三者占据 67%，超过 2/3。

**（五）消费者对团购折扣的可信度**

消费者认为折扣越低，其可信度也越低，尤其是产品类团购显得更为突出。产品类团购如果是一折，则没有消费者表示相信。

- 服务类折扣低于 3 折，可信度很差；
- 产品类折扣低于 5 折，可信度也很差。

建议团购网站不要片面强调低折扣，要处理好折扣和产品服务质量的平衡关系。对于很低的折扣建议标明折扣的理由，这样有助于提高消费者的可信度。

**（六）消费者对网站钓鱼和仿冒的了解和识别情况**

钓鱼和仿冒网站现象在国内比较普遍，著名网站都曾遭遇过类似的情况，造成流量、经济或信誉损失。如中国工商银行网站 www.icbc.com.cn 被 www.1cbc.com.cn 钓鱼和仿冒，腾讯官方网站 www.tencent.com 被 www.tencnet.com 钓鱼和仿冒。

调查表明，有 83.2% 的消费者对团购钓鱼和仿冒网站不了解或不会识别，仅有 16.8% 的消费者能够识别。

目前团购网站容易被钓鱼和仿冒的原因为：

（1）网站风格、布局几乎相同；

（2）团购信息内容相似或相近；

（3）网站网址相近，不易区别，如 goutuan.net、goutuan.com、tuangou.com 和 tuangou.net 分别属于四家不同的网站；

（4）网站网址不同，但中文名称相同或相近，容易混淆，如有两家 G 团，美团和团美等。

# 钓鱼攻击的一些研究和对策

行业营销中心　陈星霖

**摘要：**近期，钓鱼攻击（Phishing Attack）频繁发生，国内多家金融机构、大型企业受到牵连。据中国反钓鱼联盟（APAC）统计，2011 年 4 月，针对支付交易类、金融证券类的钓鱼攻击，已占据所有钓鱼攻击事件的 90% 以上。如何及时、有效识别网络钓鱼相关的互联网风险，控制钓鱼攻击带来的影响，已经成为各家金融机构当前亟需解决的问题。

**关键词：**网络钓鱼　钓鱼攻击　业务风险防控　反钓鱼监控体系

## 引言

互联网技术的高速发展，电子商务平台的大规模应用和推广，黑客攻击驱动力的变化，这些都促使安全威胁也有了一些新的转变。作为一种主要基于互联网传播和实施的攻击，“钓鱼攻击”（Phishing Attack）正呈逐年上升之势，这不仅让广大用户遭受到财产和经济损失，也让金融证券机构、电子商务公司的声誉和形象受到了影响。

据中国反钓鱼网站联盟(APAC)发布的统计数据，仅 2011 年 4 月，APAC 处理的钓鱼网站达 2,635 个，其中以针对支付交易类和金融证券类的钓鱼网站居多，占比超过 90% 以上。截至 2011 年 4 月份，APAC 累计认定并处理钓鱼网站共 46,477 个。来自《2010 年中国网络购物安全报告》的分析：2010 年，包括钓鱼攻击、恶意代码在内的安全威胁，给国内网购用户带来了超过 150 亿的损失。

如何及时、准确地发现钓鱼网站，并予以有效的控制和阻断，不仅是互联网用户关注的问题，同时也是金融机构、电子商务公司亟待解决的问题。本文档将给出对抗钓鱼攻击的一些思路和建议，希望能给有意构建“反钓鱼”监控体系的机构带来一些启示。

## 一、钓鱼攻击已成为最为严重的互联网威胁之一

关于钓鱼攻击，国际反钓鱼网站工作组 APWG（Anti-Phishing Working Group）的定义如下：一种利用社会工程和技术诡计，针对客户个人身份数据和金融账号进行盗窃的犯罪机制。钓鱼攻击是一种利用社会工程技术愚弄用户的实例，凭恃现行网络安全技术的低亲和度。这类攻击最早于 1987 年问世，首度使用“网络钓鱼”这个术语则是在 1996 年，是由“Fishing”和“Phone”综合而成（最早的钓鱼攻击通过电话作案），意味着放线钓鱼以“钓”取受害人的财务数据和密码。

钓鱼攻击越来越频繁地出现在我们身边，所带来的经济损失也超过了传统恶意代码攻击，甚至已经成为经济犯罪工业化的一部分。为了避免更多的用户成为钓鱼攻击的受害者，保障他们的合法权利和财产安全，在美国和英国已经成立了专门反假冒网址等网络诈骗的组织，如 2003 年 11 月成立的 APWG（Anti-Phishing Working Group），以及 2004 年 6 月成立的 TECF(Trusted Electronic Communications Forum)。

在国内，2008 年 7 月 18 日，由银行证券机构、电子商务网站、域名注册管理机构、域名注册服务机构、专家学者组成的“中国反钓鱼网站联盟”在京正式宣布成立。联盟已初步建立了一个快速解决机制，借助停止钓鱼网站 CN 域名解析等手段，及时终止其危害。

### 1.1. 钓鱼攻击的本质分析

钓鱼攻击带来的影响不再赘述，那么钓鱼攻击是怎么发生的呢，一般会采用哪些手段，又有什么特点？知己知彼，方能有效应对、主动防范。

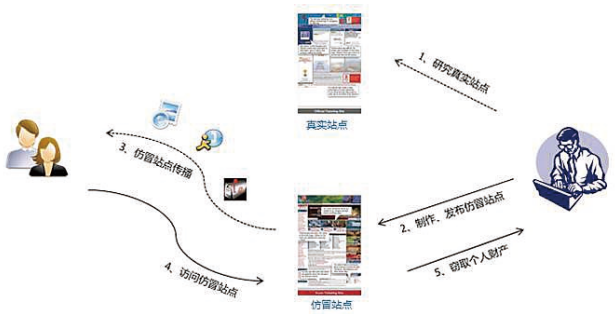



图 1 钓鱼攻击的一般过程

所谓“姜太公钓鱼，愿者上钩”，钓鱼网站一般把自己伪装成信誉卓越的机构以骗取用户的信任。通过大量散发的诱骗邮件、垃圾短信，将用户引诱到精心设计，与目标组织网站非常相似的钓鱼网站之后，攻击者再通过恶意代码窃取包括账号、密码等在内的个人敏感信息，最终得以假冒受害者，进行欺诈性金融交易。

### 1.2. 钓鱼攻击的常见手段

表 1 钓鱼攻击的常见攻击手段

| 攻击手段 | 攻击类别细分 |
|---|---|
| **由漏洞触发引起的钓鱼攻击** | 网站自身弱点 |
| | 第三方引用内容问题 |
| | 客户端弱点 |
| | 其他如弱点 |
| **非漏洞触发引起的钓鱼攻击** | 虚假诱骗 |
| | 内容仿冒 |
| | 域名仿冒 |
| | 社会工程 |
| **综合的钓鱼攻击技巧应用** | 欺骗性弹窗 |
| | 隐藏显示 |
| | 欺骗性超链接 |
| | 修改 HOSTS 文件 |
| | 恶意插件 |

钓鱼攻击常用的手段归纳起来主要分为两类，第一类主要通过漏洞触发，包括目标网站服务器漏洞（如 XSS、SQL 注入），第三方引用内容的问题（如 IFRAME 挂马），网站 IT 支撑环境相关的 DNS、HTTPS、SMTP 服务缺陷（如 DNS 劫持），以及客户端终端环境存在的隐患，攻击者利用这些漏洞结合社会工程学对受害者进行诱骗。第二类攻击手段则完全利用社会工程学的方式对受害者进行诱骗，如发送大量诱骗邮件、搜索引擎虚假信息，发布各类仿冒网站等。

### 1.3. 钓鱼攻击的特点

钓鱼攻击最大的特征即是具有极大的欺骗性。攻击者制作一个仿冒网站，类似于真实网站的克隆，再结合含有近似域名的网址来加强仿真度，进而进一步骗取用户的信任。

- 针对性、目的性很强;

通常与钓鱼攻击紧密相关的都是一些银行、商业机构的网站。网上银行、电子商务及网上购物都已经成为了与网民息息相关的服务，庞大的网络资金流动，带动了很多的新兴行业，也带来了潜在的安全隐患。

- 攻击手段综合化;

网上银行业务，及其相关的 IT 支撑系统都会存在很多安全隐患，钓鱼者会综合利用这些弱点，并结合社会工程技巧，发起攻击。如：利用 Internet Explorer 的一些漏洞去构造连接地址，或者利用漏洞去种植间谍软件或者键盘木马等等。

- 传播途径多样化;

钓鱼攻击带来的损失，一定程度上取决于钓鱼网站的传播范围。为了扩大钓鱼网站的影响，攻击者会通过搜索引擎、垃圾邮件、垃圾短信，以及虚拟社区论坛等各种渠道，发布虚假诱骗信息。

- 存活时间较短;

为了保护自己不被发现和追查，钓鱼网站一般在窃取到一定价值的信息后，会主动关停或旁靠（暂时停用钓鱼页面），小成本的钓鱼网站更是如此，很可能存活时间仅几个小时。据 APWG 统计表明，2010 年其监测到的钓鱼网站平均存活时间为 14.5 小时。

- 难以追溯和审查;

为了逃避追查，钓鱼网站往往会采用境外注册和托管方式，并经常变更托管空间，更有甚者会先入侵一台服务器，然后在服务器上面发布虚假信息。混杂着真实信息的钓鱼攻击，更难追溯和审查。

- 可识别性。

钓鱼网站并不是完全没有破绽。因为钓鱼者会尽可能少地利用资源去构造钓鱼网站，无法利用真实网站一些独有资源（如域名、USBKEY、数字验证等）。所以，通常当我们查看 HTML 源码，或者一些独有资源时，就可以较容易地识别出虚假网站。

### 1.4. 钓鱼攻击产业链分析

天下熙熙，利之所趋。钓鱼攻击带来的暴利正在催生新的地下黑色产业链，从钓鱼网站代码开发，自动化钓鱼工具生产，到钓鱼网站的销售和推广，再到用户敏感数据的收集，欺诈攻击的实施，正逐步形成一个完整的链条，并在全球范围内迅速传播。

黑色产业链下的分工和合作，使得钓鱼攻击的实现变得越来越

简单和廉价。攻击者一方面在互联网上找寻可能被渗透的主机，评估目标网站及其承载的业务流程，依赖的支撑环境所存在的弱点另一方面不遗余力地打造仿冒站点，并通过搜索引擎、垃圾邮件、垃圾短信肆意传播，去引诱尽可能多的终端用户；钓鱼者甚至开始在互联网上大肆推销钓鱼攻击外包服务，企图扩大这条黑色产业链的规模和影响。

实现一次钓鱼攻击，最简单的方式是拷贝一个 HTML 页面，上传至一个被攻陷的服务器，同时在服务器端安置可用来处理用户输入数据的脚本；也可能涉及更为复杂的网站、内容重定向，但两者的目标是一致的，构建一个假冒可信机构，并设法窃取用户的敏感信息。

使用 HTML 编辑工具能够很容易构建一个仿冒站点，攻击者还需要寻找一个托管仿冒站点的空间，这可以是一个虚拟空间，也可以是一台被攻陷的服务器。另外，一个极具诱惑力的域名对钓鱼者来说同样重要，那么申请一个有效的域名也是很有必要的一项工作。对于采用 SSL 证书的站点，钓鱼者甚至为假冒的域名注册一个有效的 SSL 证书，从而对 SSL 加密保护的口令进行记录。

钓鱼者在构建一个几乎以假乱真的仿冒站点之后，需要考虑如何将用户从一个合法的网站转移到他们所假设的仿冒站点。除非有能力改变目标站点的 DNS 解析（如 DNS 投毒），或采用其它方式进行网络流量重定向（如 pharming 攻击），钓鱼者更多依赖于某种形式上的欺骗，去引诱用户访问假冒站点。为了在尽可能短的时间内感染更多的用户，钓鱼网站主要通过垃圾邮件、垃圾短信等方式进行传播。

一次钓鱼攻击可能会依赖于多种因素，钓鱼者往往会综合考虑钓鱼网站制作、传播成本，和钓鱼攻击收益之间的平衡，采用性价比更高的方式。

## 二、关于进一步加强网上银行风险防控工作的通知

钓鱼攻击引发的安全事件，已经涉及到国内多家商业银行和农村金融机构，使得用户蒙受经济损失，也严重影响了金融机构的声誉。为了有效应对钓鱼欺诈，提高银行业金融机构网站及网上银行系统的风险防御能力，维护公众利益和银行声誉，中国银监会于 2011 年 3 月 15 日发布了《关于进一步加强网上银行风险防控工作的通知》，要求各银行业金融机构应高度重视网上银行风险管控，加强对仿冒网站等“钓鱼”欺诈事件的防范。同时，加强反“钓鱼”应急处置机制建设，有效切断“钓鱼”诈骗渠道。

- 深刻认识并重视“钓鱼”诈骗案件可能引发的各类风险，严格落实管理责任，加强主动防范、主动干预。各银行业金融机构应积极利用手工或自动化技术以及外部专业服务等多种手段、措施，加强仿冒网站的主动搜索、监测和识别；
- 强化网上银行交易环节的技术和业务防护措施，以多种方式提高网上交易的安全性；
- 加强网银可疑交易监控机制研究和系统建设；
- 做好负面舆情和客户投诉的处理工作；
- 加强“钓鱼”风险提示和公众教育。

## 三、对抗钓鱼攻击的思路和建议

钓鱼网站的频繁出现，已经影响到金融业务的拓展，损害了企业的品牌和声誉，同时还危害到社会公众利益，干扰了公众使用

电子金融产品的信心。如何及时发现钓鱼网站，有效控制钓鱼攻击带来的影响，已成为各金融机构密切关注，且急需解决的问题。

### 3.1. 传统反钓鱼解决方案的不足

为了抵御钓鱼攻击，一些企业采用了不同的防护手段。如：使用 SSL 证书加强网站合法性验证，加固 Web 服务器防止被渗透，或是购买专业安全厂商提供的金融反欺诈服务。这些防护手段在一定程度上的确能缓解钓鱼攻击带来的影响，但因为缺乏总体规划和设计，片面且单一的反钓鱼措施存在一些不足，需要加以改进。

- 解决方案的完整性不足;

传统的反钓鱼方案更多基于单一安全事件的防护需求设计，缺乏体系化的建设思路，也缺少对关键业务流程的风险分析，一些可能被钓鱼攻击利用的业务逻辑缺陷，将引入极大的风险。

在面对一些新兴的业务模式时，传统的方案显得力不从心，缺乏前瞻性的风险防范建议和扩展防护能力。如何解决 WAP 站点面临的钓鱼风险，将是下一步需要考虑的问题。

- 被动防范效果不好;

由于钓鱼攻击具有较强的欺骗性，在无法有效发现钓鱼网站的前提下，传统的反钓鱼方案多数被动呈现。主要还是依赖于客户自身的警惕性和风险意识进行防范，更多依赖最终客户的投诉和举报，来获得更多的钓鱼网站信息。

- 控制力度和范围都非常有限;

因为缺乏明确的责权定义和跨平台的合作机制，在钓鱼攻击发生之后，企业无法有效地协调相关部门进行处理。加之企业和相关部门之间存在现实的协调沟通方面的局限性，造成一起钓鱼事件发生后到最终问题的解决，常常经历较长的时间，这将极大影响用户对于企业的信任。

- 预警方式形式单一。

由于只能被动形式的接受客户的投诉与举报来获得钓鱼网站的信息，对于事件的可知、可控、可管理的三个环节，都无法得到完全保障。对于频繁发生的钓鱼攻击，企业基本没有对风险预警能力，只能在事件造成一定不良影响的形势下，通过追加公告的方式，提醒更多客户提高安全意识，避免类似的钓鱼事件发生。

### 3.2. 建立一个完善的反钓鱼监控体系

对抗钓鱼攻击的有效方法是建立一个积极、主动的“反钓鱼”监控体系，一方面依托互联网监管环境的治理，另一方面坚持贯彻“预防为主，防治结合”的方针，深入挖掘金融机构可能被钓鱼攻击利用的各种潜在威胁，主动找寻、实时监测互联网上网络钓鱼相关的安全风险，多方面积极控制钓鱼攻击可能带来的影响，为网上银行风险防控工作提供先进的技术支撑，为金融机构业务拓展提供强有力的安全保障。

总的来说，一个较为完善的反钓鱼监控体系，应该兼顾立法监管、教育和培训、举报和反馈，以及技术监控等多个层面的工作，并从预警、控制和响应三个阶段出发，提供相应的安全技术手段。

从立法监管层面谈“反钓鱼”，主要考虑如何维护一个稳定、和谐的网络社会秩序，包括互联网内容监管、域名注册监管，以及服务器运维托管监管等工作，应该尽早明确各项事务所遵循的法规、

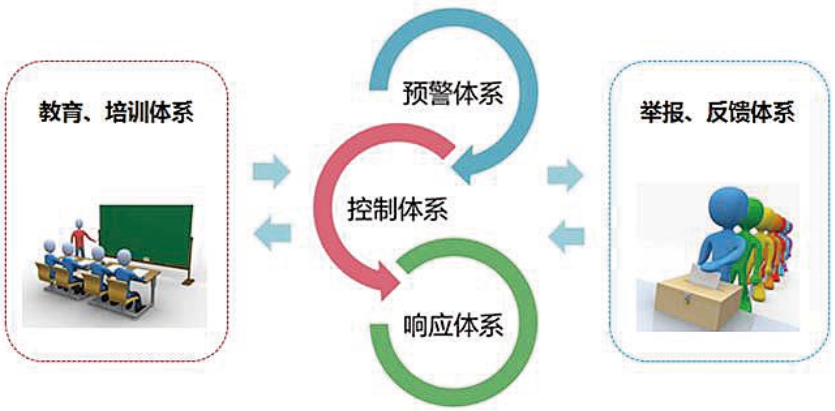



图 2 完善的反钓鱼体系架构

执行机构所肩负的责任和权力，同时协调、整合业界多种优势资源，集中投入到“反钓鱼”监控体系。

从技术监控层面对抗钓鱼攻击，应该综合考虑“预警”、“控制”和“响应”等不同阶段的防护需求和控制措施，以确保能尽早发现钓鱼网站，并通过多种技术手段予以控制。

培训和教育、举报和反馈，考虑的是如何兼顾金融机构，以及终端用户的防护需求，建立一个快捷、高效的举报平台和反馈通道，并加强终端用户的安全意识培训和教育。

用户举报和反馈一直是反钓鱼措施中最有效的部分，根据 APAC 统计数据显示，2011 年 4 月，APAC 处理的钓鱼网站总量的 90.28%，来自联盟内部成员举报。由此可见，用户反馈和举报在未来的一段时间内，仍将发挥重要作用。

金融机构可在第三方协助下，建立一个用户举报和反馈平台，主要考虑解决以下几方面的问题:

1、如何确保平台的开放性，能接受社会各界的反馈和举报;

2、如何确保流程简化，易于操作;

3、如何完成从信息收集，到数据分析，最后再到信息确认这个完整的过程;

4、如何验证用户反馈信息的可靠性。

## 四、结束语

时至今日，对抗钓鱼攻击，不再是单一用户，或某个行业单独面临的问题，而是成为了一个公众共同关注的热点。笔者在本文中介绍了钓鱼攻击常用的伎俩和特点，也谈到了对抗钓鱼攻击的一些思路。那么，金融机构应该如何建立一个完善的反钓鱼监控体系呢？我们将在下一期技术内刊中和大家继续探讨。

最终，评价反钓鱼监控体系有效性的两项关键指标是速度和效率，这使得对抗钓鱼攻击注定成为一项耗费时间的资源密集型工作。只有建立一个多方协作的合作平台，集结金融机构、域名注册和管理机构、专业安全公司、IDC，甚至互联网公司等多方优势资源，才能最大限度地发挥反钓鱼监控体系的作用。

致谢：笔者特别感谢同事刘凯提供的观点和素材，是他的分享使得作者得以顺利完成本文。

# 不同种类电子银行的安全威胁

行业技术部　徐一丁

**摘要：**电子银行业务家族日益壮大，网上银行不再是一枝独秀，最新登场的手机银行越来越普及，传统的电话银行和自助银行还将长期发挥作用。这些不同的电子银行业务形式，根据其特点，面临着不同的安全威胁。

**关键词：**电子银行　网上银行　手机银行　信息安全

## 一、电子银行的定义与分类

中国银监会发布的《电子银行业务管理办法》中对电子银行进行了定义："是指商业银行等银行业金融机构利用面向社会公众开放的通讯通道或开放型公众网络，以及银行为特定自助服务设施或客户建立的专用网络，向客户提供的银行服务。

电子银行业务包括利用计算机和互联网开展的银行业务，利用电话等声讯设备和电信网络开展的银行业务，利用移动电话和无线网络开展的银行业务，以及其他利用电子服务设备和网络，由客户通过自助服务方式完成金融交易的银行业务。"

国内电子银行概念的提出是从网上银行普及开始的，各银行普遍已经建立了电子银行的业务渠道体系。下一步，分别建立的电话银行、网上银行、自助银行等系统将整合在一起，形成完整的电子银行系统。

## 二、不同种类电子银行的安全威胁

| 电子银行类型 | 客户端典型硬件 | 典型操作系统 |
|---|---|---|
| 网上银行 | PC，笔记本 | Windows 系列 |
| 手机银行 | 手机，PDA，平板电脑 | IOS，Android，WM，Symbian |
| 电话银行 | 电视机，机顶盒 | 无 |
| 家居银行 | 电视机，机顶盒 | 机顶盒定制系统 |
| 自助银行 | ATM，存取款机，多功能媒体机 | Windows98，XP 等 |

各类电子银行的安全性，可以从客户端、传输线路和服务器端三个部分去考虑。我们在之前的技术文章中，已经讨论过网上银行的安全性问题，其中对银行服务器端的威胁与安全防护已经解释得很详细，在此就不再赘述，主要谈一谈几类电子银行客户端的安全问题。

### 1. 网上银行

网上银行用户使用 PC 或笔记本上网，利用网银的 B/S 或 C/S 客户端上网，其面临的威胁是多方面的。攻击目的一般都是获取用户的账号、口令和个人证书等信息，冒充用户身份非法转移资金。

网上银行客户端易受恶意代码、钓鱼、输入截取、证书盗取和交易篡改等攻击。恶意代码包括蠕虫、病毒、恶意脚本等，通常作为侵入客户端的第一个手段；钓鱼攻击是伪造网上银行交易系统，诱使投资者使用虚假系统登录，造成账号和口令的泄密；输入截取是获得用户的击键或鼠标点击记录，通常包括网上银行的账号与口令；证书盗取是取得用户计算机中个人证书，以冒充用户的身份；交易篡改是相对较少出现但很有威胁的一种攻击，可以将用户的网上银行操作指令内容进行非法改变，以实现其攻击目的。

网上银行客户端的安全保护需要从两个方面去考虑，一是操作系统的安全性，二是网上银行客户端本身的安全性。操作系统安全，可以从打补丁、做好安全配置、良好的上网习惯等方面着手。如果能保障操作系统的安全，可以有效防止攻击者通过控制操作系统而攻击网上银行。网上银行客户端的安全防护主要由安全控件实现，通常包括输入信息的保护、进程保护、文件保护等功能。

银行要重点加强网上银行客户端的安全性，在客户教育中强调操作系统的安全性。不过事实证明，无论银行如何加强安全教育，网上银行用户的计算机水平与安全意识还是相差很大，总是有一部分用户的水平不足，操作系统安全性很差。所以对于银行来说，技术防御手段还主要是从客户端着手，尽量多地考虑可行的安全功能，力争“在不安全的操作系统环境下，实现安全的网上银行交易”。

### 2. 手机银行

3G 和高性能智能手机的普及，使手机银行正式登场，已经向主要的业务渠道去发展。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，加上 1G 左右的 CPU 运算速度和相匹配的内存，大部分的网络应用都可以在手机上实现，例如手机上网、手机炒股、手机钱包、手机支付、移动商务、地图导航等。

将来，手机银行会与网上银行一样，成为被攻击的重点。目前手机银行的风险主要来自智能手机本身。从本质上说，手机安全和 PC 终端安全原理上一致，但手机安全也有其自身的特点，一是现有手机操作系统的安全机制可以被破解，二是手机软件市场的混乱无序。

手机操作系统在设计之初，不约而同地采取了“应用准入”的机制，即只有通过相关厂商或机构验证的软件，才可以安装在手机中。典型的当然是 Apple IOS，在 IPhone、IPAD 等设备上安装软件，必须要从 AppStore 下载。这个限制当然主要是出于商业持续赢利目的而设计，而客观上也确实能够保护那些下载者，AppStore 上出售的软件都是经过安全验证的，可以让用户免

受恶意软件的入侵。而针对性的攻击手段也已经存在，这就是越狱（Jailbreaking），它可以突破限制，让用户免费、自由地下载破解后的软件，受到“广大用户的欢迎”。但那些破解后的软件全部来自于非正规的地下开发者，其安全性完全得不到保障，很可能会有恶意代码包含在其中。

无独有偶，这方面另一个典型的例子就是 Symbian，这个手机操作系统市场曾经的老大。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。很多用户为了不受限制，同样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。

破解之后，智能手机就可以无限制地下载应用软件了，虽然这很方便，但其中的安全隐患大大提升。由于智能手机的兴起，一个规模巨大的市场被创造出来，各路开发商和团队纷纷抢占地盘，推出自己的手机应用产品，力图分得更大的一块蛋糕。这些开发团队鱼龙混杂，有非常多的非正规团队，他们编写的程序只注重功能实现，可能存在严重的安全隐患，容易被人利用。甚至地下开发者也会混迹其中，在各类手机下载网站上发布绑定了恶意软件的应用程序。

客观地讲，目前手机相关的安全事件没有传统 PC 安全事件那么多，那么严重。这是由于现阶段传统 PC 终端还是拥有最大数量的用户群，更受攻击者关注，而不是因为手机更安全。从大环境看，智能手机的综合安全能力不如传统 PC 终端。

### 3. 电话银行

电话银行出现较早，最初可以实现查询的简单功能，后来又逐步加入支付、转账等功能，而且与呼叫中心的人工服务结合起来，成为一个比较简易方便的银行业务渠道。

电话银行的安全问题比较有特点：安全隐患大而威胁小，所以总体风险不高。安全隐患大，主要由于电话传输的信号是明文，从电话机到电信运营商中间的路线如果被非法搭接，可以窃听到所有重要信息；威胁小，是因为实际情况中去非法搭接电话线路、想偷取重要信息的攻击者非常少。一方面由于攻击者有更方便攻击、更多目标的网上银行，不会去费劲冒风险在电线杆上爬上爬下做，另一方面由于电话银行的使用者并不广泛，即使监听也很可能不会得到有用的信息。

### 4. 家居银行

与电话银行类似的家居银行，是有可能受到较大威胁的。家居银行已经在某些省市出现，其业务终端是用户在家里的电视机与机顶盒，借助广电网络传输银行业务信息，进行查询、缴费等业务处理。从用户家中到广电那一端的传输是明文的，因为机顶盒通常没有加密功能。我们在对几个不同家居银行的安全测试中发现，广电网络的线路是可以进行监听的，从某户居民的有线电缆接入，可以监听到其他居民的信号。家居银行应当在机顶盒软件里加入足够强度的加密功能，防止传输的信息被非法窃听。

### 5. 自助银行

自助银行目前有 ATM（自动柜员机，取款），存取款机，多功能终端等形式，是银行在特定地点向用户提供自助服务的一种重要的

业务形式。

大部分自助银行设备被直接利用计算机技术攻击的可能性不大。自助终端设备都是银行特制的机具，虽然操作系统采用的是可能存在较多漏洞的 Windows 桌面操作系统，如 Windows 98、XP 等，但由于输入设备通常为数字和特制的键盘，无法输入计算机命令。同时终端也没有外接设备的接口，又不直接连接公共网络，因此不太可能进行攻击。这类可以存取款的设备，主要面临被偷窥用户输入的密码、通过读卡器偷取银行卡信息等威胁。

而多功能终端不同于其他自助银行设备，它可以提供通过 Internet 访问特定网站和网银的功能。其本身是一台完整的计算机，利用标准键盘输入，有鼠标，甚至可能有 USB 接口，供用户插入 U 盾。这种终端被攻击的可能性就大大增加了。攻击者可能利用 U 盘在多功能终端上植入非法程序，偷取其他用户的信息。也可能利用一些命令的操作，去打开原本不被允许访问的网站，下载木马程序。甚至直接跳出多功能终端限定的用户操作环境，进入到操作系统，这样可以进行的攻击就更多了。

## 三、全面考虑电子银行面临的威胁

以上讨论的各类电子银行，都各自面临不同的威胁，但需要注意的是这些不同类别电子银行的安全性会相互影响，如电话银行 / 呼叫中心的安全性，可能会影响到网上银行的安全性。

前不久国内银行就出现了这样一个案例：一位女士在某银行办理了信用卡，但可能个人开卡相关的信息被泄露出去，有人利用这些信息，通过电话银行激活了信用卡的网上支付功能，并且修改了短信通知的手机号码。结果她的信用卡被人在购物网站上利用网银支付功能，盗刷了 2 万余元。这是一个比较有代表性的案例，电话银行的安全漏洞影响到了网上银行的安全性，最终导致了用户资金被盗。

因此银行在考虑不同类别电子银行安全性的同时，也应注意从整体上考虑安全防范手段，如限定交易额、加强身份验证凭据、银行操作的短信通知等，都不应只考虑本类电子银行的安全威胁与保护需求，要同时考虑它们之间的相互作用和影响。

# WAF与SaaS网站监测联动

## ——一种双视图防护机制

产品管理中心　秦波

**摘要：**本文阐述了一种新的网站防护解决方案及实现原理。绿盟网站安全监测服务联动是一种有效的防护机制，它将 SaaS 扫描服务与 WAF（Web Application Firewall）联动，持续监测目标网站的脆弱性，然后由 WAF 根据其反馈结果实施防护。

**关键词：**WAF　虚拟补丁　老鹰抓小鸡　SaaS 扫描　绿盟网站安全监测服务

### 背景介绍

凭借多年安全服务经验，笔者知道想要保持网站安全的运维是不容易的。即使像微软这样的大公司，运用了 SDL 开发的产品，也仅仅是把漏洞数量下降，而难以彻底消除，更谈不上对未知漏洞的预防。据权威咨询机构 Gartner 统计，超过 80% 的网站具有严重安全漏洞，而运维管理员又难以及时修复控制。因为大部分的网站是自开发的程序，没有统一的官方补丁可用，只能依赖于开发人员紧急修复。根据 Forrester 的首席咨询师 Chenxin Wang 在 2010 年 OWASP 峰会上的演讲：修复一个在线运行的应用程序漏洞需花费 3 万美金。而来自 WhiteHat 的统计（见图 1）：修复一个应用层漏洞平均需要一百多天。由此可见应用层漏洞的修复代价是非常高昂的。

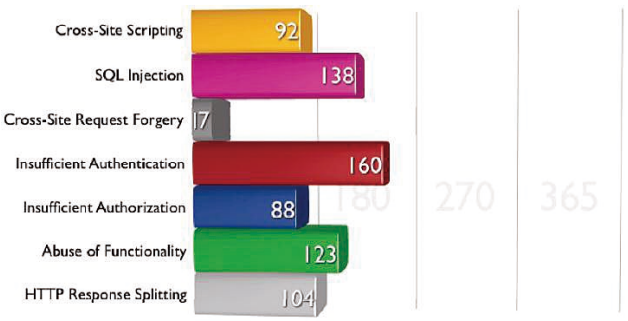



图 1 修复各种漏洞类别的平均时间

当渗透测试、开发人员或其他任何人发现了漏洞，对于网站来说解决方法可选项:

1. 软件升级、改变配置;
2. 回退到之前无漏洞的应用程序版本;
3. 升级 WAF 规则;
4. 网站紧急下线;
5. 不采取任何措施。

无论采取哪种方法都需要时间成本而且无法自动解决，即使部署了 WAF 也仍担心是否配置正确？对漏洞的利用能全部阻断吗？所以 VA 和 WAF 的联合互补是技术上天然的需要，以构成对运维阶段 Web 系统安全的安全生命周期管理。

### 老鹰抓小鸡诠释 Web 安全防护模型

在讨论如何解决 Web 系统安全问题之前，我们重温一下几个概念：威胁、资产和漏洞。简单的说，威胁是可能发生的任何潜在的

坏事，会危害到你的资产; 而漏洞是一个客观存在的弱点，是具体的，比如错误的设计、不恰当的配置或者不安全的编码。如果不了解系统的架构如何知晓对应的威胁? 又如何谈得上防护? 用老鹰抓小鸡的类比，就是母鸡必须清楚老鹰的进攻招数，同时也必须知晓小鸡们的弱点，才能更好的调整防护。

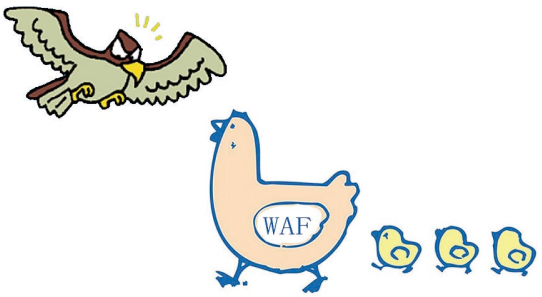



图 2 老鹰抓小鸡示意图

WAF 通常分析 Web 客户端与 Web 服务器之间的通信，用预先定义好的安全策略来阻止恶意行为。这是一种被动的、基于威胁的防护模型。而且大部分 Web 程序是自编码的，安全水平参差不齐，WAF 预置的规则主要是针对威胁层面的，而对于不同的漏洞无法用统一的安全防护覆盖。为了更好的理解这些概念，用图 3 比喻展示。

在图 3 中有三种角色：老鹰、母鸡、小鸡，母鸡代表防护设备 WAF，小鸡代表在后端的 Web Server、Application、Database，老鹰则是能发现漏洞的绿盟网站安全监测服务。母鸡能识别正常或和非正常并控制，对客户端的正常请求和攻击行为采取了相应 HTTP Response、DROP 动作。老鹰主动发现后端的小鸡脆弱性并传递

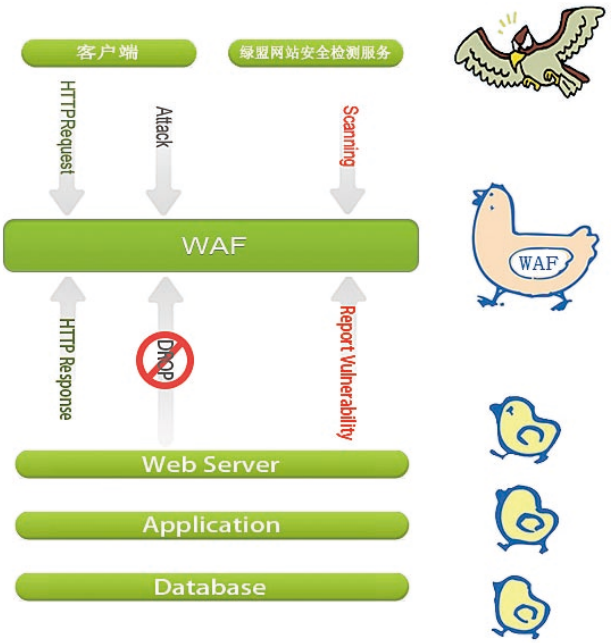



图 3 绿盟科技 WAF 的老鹰抓小鸡安全防护示意图

给母鸡，母鸡接受反馈信息后迅速调整恰当的防护配置，从而弥补了缺陷、自动有效的降低了风险。

这种“鹰眼”能力让母鸡(WAF)具有了双重防护试图: 威胁、漏洞，从被动防护到主动感知，从臃肿到精简贴合的防护策略，从手动复杂到自动简单的配置，从长时间拖延到及时处理。

WAF 的核心作用是分离 Web 传输流量里的恶意流量，内置“允许”和“不允许”的可配置安全规则。主流的 WAF 通常包括白名单和黑名单两种机制，白名单凭借自学习机制能制定“允许”，然而无

论多智能的学习也不会完美的转换成防护依据；黑名单可以拒绝包含诸如 “SELECT * FROM” 等恶意字符串，通常黑名单都是精心构建的数百条甚至更多的一个规则库，对于变化繁多层出不穷的攻击方法，这种机制是滞后而且缺乏灵活性的。目前这两种机制各有优劣，需要一起配合使用。

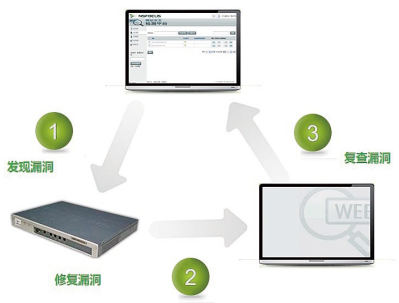



图 4 绿盟科技 WAF 虚拟补丁模块工作原理示意图

扫描器和 WAF 的结合是花费小且十分有效的漏洞解决方案，这种方式能贴合不同网站的安全状况。绿盟网站安全监测服务为 Software-as-a-Service (SaaS) 类型的扫描服务，可持续检测被保护网站的安全状况。由于 WAF 不能中断应用正常使用，所以 WAF 默认策略都是全允许，只对可疑的流量检测后才禁止，其共同点就是都关注威胁，而忽视漏洞。而老鹰抓小鸡模型弥补了这一缺陷，主动关注后端被保护服务器的漏洞，从而比攻击者占据了主动权，这是包括了威胁和模型的双视图。

国外企业对 PCI6.6 要求 Web 系统需具备漏洞扫描器和 WAF 要求，这种防护体系很好的满足了合规要求:

– Undergo application scanning and code review by an application security specialist; or,

– Install a Web application firewall in front of the Web-facing applications

## 总结

SaaS 扫描持续性评估网站漏洞，发现漏洞后把结果反馈给 WAF，并对发现的漏洞给予修复建议和可在 WAF 上的防护配置。犹如多了鹰眼的母鸡，对于后端小鸡的脆弱点了然于胸并及时调整和部署防护准备，从而更从容面对前端的攻击者，极大地加强了防护能力。核心功能总结如下:

- 提供安全扫描报告，通过对比不同周期的持续监控清楚掌握网站的运维情况;
- 虚拟补丁：网站漏洞形成针对性强的脆弱性修复配置，对攻击流量丢弃只允许正常流量通过;
- 闭环流程：从脆弱性检测到修复一体的解决方案，自动修复、节省时间和降低复杂性，降低了管理成本;
- 精准有效：对不同网站的脆弱性形成的独有的防护策略更精炼、更有效，避免臃肿的防护规则降低性能;
- 超出 PCI 合规要求：企业满足了 PCI 6.6 的两条规定。

**参考文献**:

[1]. Improving Web Application Security: Threats and Countermeasures http://www.microsoft.com/downloads/en/details.aspx?FamilyId=E9C4BFAA-AF88-4AA5-88D4-0DEA898C31B9&displaylang=en

[2]. Jeremiah Grossman: VA + WAF, yes it really works! http://jeremiahgrossman.blogspot.com/2008/03/va-waf-yes-it-really-works.html

[3]. VA+WAF: that’s hot! http://www.mikeandrews.com/2008/06/19/vawaf-thats-hot/ [4]. Vulnerability Assessment Plus Web Application Firewall (VA+WAF) http://www.whitehatsec.com/home/assets/WP_WAF061708.pdf

# USB Key安全技术漫谈

安全研究院　刘永军

**摘要：**USB Key 是一种 USB 接口的智能加密硬件存储设备，主要提供数据加 / 解密、数据完整性、数字签名、访问控制等功能。本文系统的阐述了其软硬件的构成，其相应功能的实现，以及其面临的一些安全问题。

**关键词：**USB Key 是什么　USB Key 原理　USB Key 安全

## 一、引言

USB Key 的别名很多，如“网银盾、U 盾、U 宝、支付盾……”，其实这些称呼只是不同银行和第三方支付平台对 USB Key 的不同称谓而已，万变不离其宗。但 USB Key 与 U 盘有着本质的区别，前者是用于加 / 解密、身份识别的智能存储设备，后者是普通存储设备，尽管两者外观很相似。随着互联网和电子商务的发展，USB Key 作为网络用户身份识别和数据保护的“电子钥匙”，正在被越来越多的用户所认识和使用。

USB Key 是一种智能加密存储设备，内置了单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用 USB Key 内置的公钥算法可以实现对用户身份的认证。目前 USB Key 被广泛应用于国内的网上银行、电子支付等领域，是公认的、较为安全的身份认证技术。

## 二、关于 USB Key

USB Key 是结合了现代密码学技术、智能卡技术和 USB 接口技术的新一代身份认证产品。

随着电子商务和 PKI 应用的兴起，数字证书作为确认用户身份和保护用户数据的有效手段，越来越被人们所接受，然而如何保护数字证书文件本身，又成为 PKI 体系中最薄弱的环节。数字证书（主要指包含私钥的）可以保存在各种存储介质上，如软盘、硬盘等。国内 CA 早期颁发的数字证书都是以软盘的形式发放，或者由用户从网络上下载，然后导入到系统中保存在硬盘上，其最致命的安全隐患是数字证书容易被复制、窃取。于是，专门用于存储机密信息的 USB Key，就很自然成为数字证书的最佳载体。

每一个 USB Key 都具有硬件 PIN 码保护，PIN 码和硬件构成了用户使用 USB Key 的两个必要因素。用户只有同时取得了 USB Key 和用户 PIN 码，才可以登录系统。即使用户的 PIN 码被泄露，只要用户持有的 USB Key 不被盗取，合法用户的身份就不会被仿冒；如果用户的 USB Key 遗失，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。

USB Key 具有安全数据存储空间，可以存储数字证书、私钥等机密数据，对该存

储空间的读写操作，必须通过 USB Key 内的程序实现，用户无法直接读取，其中用户私钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。

USB Key 内置 CPU，可以实现加解密和签名的各种算法，公私密钥对的产生、加解密运算在 USB Key 内进行，保证了私钥不会出现在计算机内存中，从而杜绝了用户私钥被黑客截取的可能性。

主要 USB Key 厂商有华虹、握奇、捷德等。USB Key 厂家将 USB Key 与 PKI 技术相结合，利用 USB Key 来保存数字证书和用户私钥。CSP 和 PKCS#11 是目前应用最广泛的加密设备接口标准。

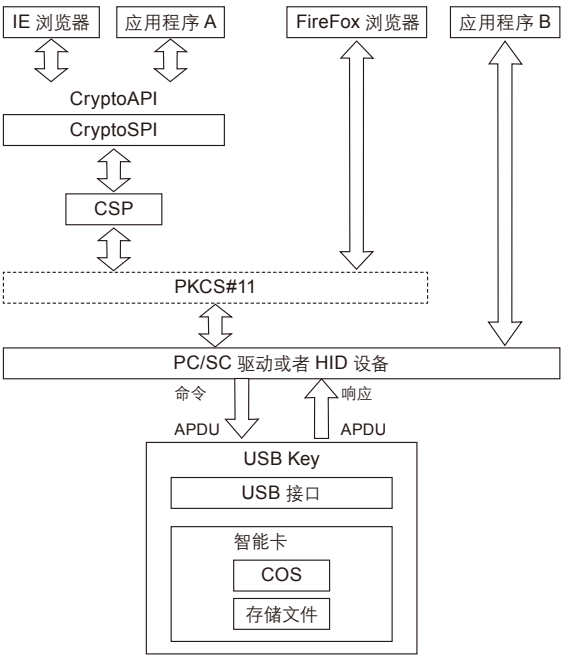
### 2.1. PKI 简介

PKI(Public Key Infrastructure，公钥基础设施 ) 被誉为现代信息社会安全的基石，也是电子商务与电子政务的关键技术。它能够为所有网络应用透明地提供加密和数字签名等密码服务所必需的密钥和证书管理功能，能够提供认证、访问控制、数据完整性、机密性和抗抵赖性等核心安全服务。通常 PKI 系统主要由认证机构、证书库、密钥备份及恢复系统、证书作废处理系统、PKI 应用接口系统等部分组成。PKI 的基础是基于非对称加密算法的。其中公钥是公开给别人的，用于数据加密、验证签名；私钥是本人私有的，要严格保密的，用于数字签名、解密数据。

机密性实现：公钥加密数据 ( 通常是对称加密密钥 )，私钥解密数据。

抗抵赖性实现：私钥签名数据，公钥验证签名。

### 2.2.USB Key 客户端系统总体实现功能图




PC/SC 接口是关于智能卡应用的国际标准，包括计算机操作系统的智能卡设备管理规范、应用接口规范等，它能实现智能卡设备的可扩展性、通用性和透明性，但它要求智能卡设备的驱动程序符合 PC/SC 的要求。

目前许多 USB Key 厂商考虑到 USB Key 设备与计算机之间的数据交换具有数据量少、传输速度要求不高的特点，因而将其配置为 HID 类设备或者通用串行总线设备，实现在 windows 环境下免安装驱动程序的特点。

智能卡的 COS 是一个小型的操作系统，固化在智能卡只读存储

器 ROM 中（防止修改等恶意攻击），控制智能卡与外界信息进行交换，管理智能卡存储器中的文件系统，并在智能卡内完成各种命令的处理。当 USB Key 接收到外部的命令数据时，COS 根据数据的情况进行相应的操作，如读写数据、进行运算等。COS 必须遵循 ISO7816—4 标准。

CSP(Cryptographic Service Providers，密码服务供应商）是加密服务供应商为了给用户提供方便，针对应用层提供的标准接口函数。用户可以直接使用微软公司的 CryptoAPI(Cryptographic Application Programming Interface，加密应用程序接口）调用 CSP 函数，来实现供应商提供的密码运算。

微软 CSP 接口为了方便上层的使用，简化了一些功能，而且由于必须经过系统层的调用，无法达到很好的扩展性。RSA 公司的 PKCS#11 标准同样定义了一套密码运算、密钥管理接口（Cryptoki），该接口与平台无关。PKCS#11 定义的接口与 CSP 相比更为灵活，而且方便开发者扩充自己的功能。考虑到灵活性、跨平台性、可扩展性等因素，许多厂商会选择在 CSP 与驱动之间实现 PKCS#11 的标准接口。如 FireFox 浏览器即使用此接口。

要开发一个 CSP，必需提供 CryptoSPI 所要求的所有函数接口（25 个），即开发一个动态库，输出 CSP 提供的所有函数。导出函数如下图:

| | | |
|---|---|---|
| CPAcquireContext | 10001650 | 1 |
| CPCreateHash | 10001740 | 2 |
| CPDecrypt | 10001730 | 3 |
| CPDeriveKey | 10001680 | 4 |
| CPDestroyHash | 10001780 | 5 |
| CPDestroyKey | 10001690 | 6 |
| CPDuplicateHash | 100017C0 | 7 |
| CPDuplicateKey | 100017D0 | 8 |
| CPEncrypt | 10001720 | 9 |
| CPExportKey | 10001700 | 10 |
| CPGenKey | 10001670 | 11 |
| CPGenRandom | 100017A0 | 12 |
| CPGetHashParam | 100016F0 | 13 |
| CPGetKeyParam | 100016B0 | 14 |
| CPGetProvParam | 100016D0 | 15 |
| CPGetUserKey | 100017B0 | 16 |
| CPHashData | 10001750 | 17 |
| CPHashSessionKey | 10001760 | 18 |
| CPImportKey | 10001710 | 19 |
| CPReleaseContext | 10001660 | 20 |
| CPSetHashParam | 100016E0 | 21 |
| CPSetKeyParam | 100016A0 | 22 |
| CPSetProvParam | 100016C0 | 23 |
| CPSignHash | 10001770 | 24 |
| CPVerifySignature | 10001790 | 25 |

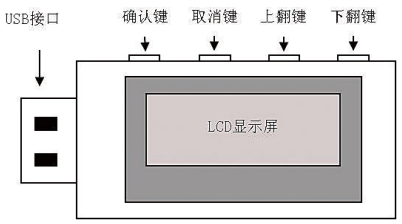
## 2.3.USB Key 分类

### 2.3.1. 一代 USB Key

一代 USB Key 指没有屏幕、语音、确认键的普通 USB Key。

### 2.3.2. 二代 USB Key

如图:




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

以貌取“物”是不可取的，有个别“滥竽充数”的“伪二代 USB Key”，徒有二代 USB Key 的外表，但其并未实现“所见即所签”，即用户所见内容并非作为签名数据，只是 USB Key 外部程序输入的显示数据，所以仍可以进行交易篡改。不过其有硬件确认键，能够防止木马偷偷进行“正常交易”，用户可参与性又强于一代 USB Key。好在

现在相关银行已经“慧眼识真”，将其清除出了二代 USB Key 的队伍。

### 2.4.USB Key 身份认证方式

#### 2.4.1 基于冲击 - 响应的认证方式

在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成随机数并通过网络传输给客户端（此为冲击）。客户端将收到的随机数和交易数据提供给 USB Key，与存储在 USB Key 中的密钥进行 MD5 运算并得到一个结果作为认证数据连同交易数据一并传给服务器（此为响应）。与此同时，服务器也使用该随机数与存储在服务器数据库中的该客户密钥和交易数据进行 MD5 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户，且能够确认数据完整性。但密钥也存在于验证服务器中，增加了安全隐患。

#### 2.4.2 基于数字证书认证方式

将转账数据和服务器回传的时间戳（防止重放攻击）的散列值用 USB Key 中的用户私钥进行数字签名，和原始数据一起发给服务器；服务器用相应用户的公钥解密签名数据获取散列值，并对原始数据使用与客户端相同算法计算散列值，两者比较，相等则能够确认客户端是一个合法用户，且能够确认数据完整性。

目前大部分银行采用了此种认证方式，但很多银行自建 CA，并未严格遵循 PKI，所以其数字证书的权威性不能够保障。

### 2.5.USB Key 数字证书及下载流程简介

现有的证书大都采用 X.509 规范，主要由以下信息组成:

版本号、证书序列号、证书签名算法、有效期、拥有者信息、颁发者信息、拥有者的公钥、CA 对以上信息的签名。

带有私钥的证书为 PKCS#12 格式，扩展名为 .pfx。不带私钥的证书格式：DER 编码二进制 X.509、Base-64 编码 X.509（扩展名为 .cer）和 PKCS#7（扩展名为 .b7b）。以 xenroll 产生证书请求和安装为例，大致过程如下:

通过 XEnroll.dll 控件的 createPKCS10 方法来生成 CSR（证书签名请求，PKCS#10 格式），其中包含由 USB Key 的 CSP 提供、在 USB Key 内部生成的公私密钥对的公钥，私钥在其生命周期中都不会离开 USB Key。

CA 会创建一个 X.509 证书，返回符合 PKCS#7 格式的证书数据。然后调用 XEnroll.dll 控件的 acceptPKCS7 方法通过 CSP 将证书保存到 USB Key 中。

## 三、Usb Key 安全问题

### 3.1. 使用注意事项

不进行交易的时候不要将 USB Key 接入电脑，只在交易时候进行接入。交易时接入 USB Key，输入 PIN 码完成交易后，立即将 USB Key 取走，防止远控木马进行伪造交易。因为如果木马事先获得了用户名、密码、PIN 码等登录信息，且用户大意没有及时将 USB Key 拔掉，此时，木马的远端控制者可以在分析清楚签名调用接口的基础上（以达到获取签名的隐蔽性），远程获得认证数据，从而进行远程交易伪造。

如果你在使用网银进行转账交易过程中电脑突然意外锁屏、黑屏、显示器断电，请立即拔掉 USB Key（推荐），当然也可以直接给主机断电（后果自负），此时很可能你的机器已经被远控木马控制，它使用障眼法迷惑你，当你还在检查电源、思考故障原因时，

木马已经在暗地里动了你的奶酪。木马若想完成上述伪造交易，还需提前获取 PIN 码。

上述伪造交易安全隐患一代 USB Key 存在，但二代 USB Key（包括伪二代）则可以防范此风险，因为其需要用户参与，按确认键才能完成交易。

通过本地程序实现交易篡改也可以绕过一代 USB Key（包括伪二代），且不需要利用黑屏等手段，更加隐蔽，这种木马可以通过二代 USB Key 或者短信交易确认进行防范。

### 3.2. 中间人钓鱼攻击

中间人钓鱼攻击并非指简单的通过钓鱼网站等手段获取用户登录密码等敏感信息，而是一个透明的中间人代理，即“中间人”需要的网银任何信息（包括签名）都由“配合”的用户正常提供，然后由其实时修改转账等机密信息完成交易。所以用户一定要能够正确识别网银网址，严防“李鬼”。

二代 USB Key 和短信交易确认也可以很好的防范这个风险。

### 3.3.ActiveX 控件及其相关 dll 漏洞

网银会提供用于签名或者密码输入保护等功能的 ActiveX 控件，但如果 ActiveX 控件或者其相关 dll 存在缓冲区溢出等安全漏洞则会“引狼入室”，为木马打开了一扇方便之门。

通过木马盗取网银的前提是要在目标机上安装木马，利用 ActiveX 控件漏洞进行网页挂马是一种常用的技术手段。

### 3.4. 下载证书的安全问题

在证书第一次下载的环节存在证书被窃取的风险，当用户输入两码下载证书时，木马可以拦截输入，获取两码，并使其通信失败，然后使用相同种类的 USB Key 下载证书，进而达到窃取证书的目的；如果用户泄露了两码信息则无需木马即可下载证书。上述为没有进行 USB Key 硬件 ID 验证的情况，即使需要硬件 ID 信息，木马也可通过相应接口获得，或者修改网银本地校验程序（如果采用本地校验）。

银行在办理网银 USB Key 时很多会替用户下载证书，这样则在很大程度上防范了用户自己下载证书的安全风险。

### 3.5.USB Key 只用于登录

有的网银只将 USB Key 用于登录身份认证阶段，这样木马伪造交易会更加简单，甚至不用获取 PIN 码；同时会增加会话劫持的风险，如果交易过程中进行数据签名则能够防范会话劫持的风险。

### 3.6. 可预知签名数据

在 USB Key 接入的情况下，如果签名数据防重放攻击的可变因素时间戳粒度不够细（如秒），则可以事先获取未来数个连续时间戳的伪造信息签名，再辅以相关信息的修改，则通过远程伪造认证、进而伪造交易的可能性还是存在的。为了获取签名的隐蔽性和效率，事先分析清楚接口调用是必须的。

此种风险可以使用更细粒度的时间戳（如毫秒）或者采用随机数进行防范。

### 参考资料

[1] 徐昊《攻击基于证书的身份认证系统》

[2] 杨瑞霞《基于 USB Key 的 CSP 实现》

[3] Richard Anderson Chris Blexrud《ASP 3 高级编程》第 25 章（证书的使用）

**绿盟科技成功承办“2011 中关村信息安全产业发展论坛”**

近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“2011 中关村信息安全产业发展论坛”在京召开。

以“RSA Conference 热点信息交流”为主题的信息安全论坛已成功举办两届，已经成为我国信息安全行业内研讨最新国际信息安全发展趋势的交流平台。本届会议依然以“RSA Conference 热点信息交流”为主题，吸引了来自安全行业、科研院所的领导专家以及行业客户等 300 多位代表参加。工信部软件服务业司司长陈伟、公安部网络安全保卫局副局长赵林、中关村管委会副主任杨建华、绿盟科技总裁沈继业出席大会并致辞，中科院教授翟起滨、绿盟科技副总裁吴云坤、首席战略官赵粮博士以及其他安全企业的代表围绕 RSA 的热点问题在会上分别做了主题演讲。并就 RSA2011 大会热点，专家和企业代表围坐一起，共同讨论未来安全发展技术趋势与产业方向。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在主题演讲中，与到场嘉宾共同分享 2011RSA 会议的感受和见闻，并阐述了国际信息安全市场的发展趋势和机遇。他指出：“在经历经济危机之后的北美市场，IT 与信息安全市场已经逐步恢复了生机，云计算、云安全依然是最大的热点，各个产业层面已经进入实际应用的阶段，而大量的传统应用，也开始向云端迁移。同时下一代防火墙技术、数据安全、合规与风险管理等等领域，也都被业内高度关注。”

在谈到绿盟科技 2011 年的参展情况时，吴云坤强调，“绿盟科技参加 2011 年 RSA 会议，在为业界带来最新的安全产品的同时，尤其重视 Web 应用安全与云安全 (Cloud Security)，在会展中展示并阐述了未来的战略架构，该架构以“硬件产品 +SaaS 模式 + 虚拟化镜像”的三种模式，将绿盟科技的 Web 安全监控、Web 应用防护、抗拒绝服务、入侵保护等多个安全模块，推向合作伙伴 ( 如可管理安全服务提供商、数据中心、云计算提供商、SaaS 提供商）与最终用户，从而使绿盟科技的产品能够更加简单地嵌入云计算环境，并与传统计算环境中的应用进行无缝结合。”

在互动交流环节，翟起滨教授和 RSA 参会企业代表围绕国际信息安全最新技术动态、热点问题、全球近期安全事件展开交流，并就国际信息安全发展趋势、国家“十二五”新形势等多方面问题进行了热烈讨论，共同勾画与展望未来信息安全发展的技术趋势和产业方向。

绿盟科技自 2008 年起开始参加 RSA 大会，是国内最早参加 RSA 的网络安全企业。如今已经有越来越多的中国信息安全企业开始进入 RSA 大会，积极关注并参与国际信息安全市场。中国信息安全行业的国际化道路已经启程。随着 2011 年初在美国硅谷及日本东京分公司的成立，绿盟科技也将会更快速地将核心技术及业务模式推向国际市场。

# NSFOCUS 2011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 ) 安全小组根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

## 1. 2011-04-18 Adobe Flash Player 对象处理远程代码执行漏洞

NSFOCUS ID: 16716

http://www.nsfocus.net/vulndb/16716

**综述：**

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 的某个对象方法在被引用时没有正确识别对象的类型，通过精心构造内存中的数据结合 Heap Spray 等技术可以利用此漏洞执行任意指令。

**危害：**

远程攻击者可以利用此漏洞，诱使受害者打开包含恶意 SWF 文件的网页或 Office 文件，从而控制受害者系统。

## 2. 2011-04-12 Microsoft IE 布局处理释放后重用远程内存破坏漏洞 (MS11-018)

NSFOCUS ID: 16689

http://www.nsfocus.net/vulndb/16689

**综述：**

Windows Internet Explorer 是微软公司推出的一款网页浏览器。

Internet Explorer 在实现上存在布局处理释放后重用远程内存破坏漏洞，导致 IE 访问未被正确初始化的内存或已删除的对象。

**危害：**

远程攻击者可以利用此漏洞，诱使受害者打开恶意的网页，从而控制受害者系统。

### 3. 2011-04-12 Microsoft Windows SMB 操作解析远程代码执行漏洞 (MS11-020)

NSFOCUS ID: 16686

http://www.nsfocus.net/vulndb/16686

**综述**:

Windows 是微软公司开发的流行操作系统。

Microsoft Windows SMB 操作解析在实现上存在远程代码执行漏洞。无需验证即可利用此漏洞。

**危害**:

远程攻击者可以利用此漏洞，发送特制的 SMB 报文到服务器，从而控制服务器系统。

### 4. 2011-04-12 Microsoft Windows SMB 客户端远程代码执行漏洞 (MS11-019)

NSFOCUS ID: 16687

http://www.nsfocus.net/vulndb/16687

**综述**:

Windows 是微软公司开发的流行操作系统。

Microsoft Windows SMB 客户端在验证特制的 SMB 响应时存在远程代码执行漏洞，无需验证即可利用此漏洞。

**危害**:

远程攻击者可以利用此漏洞，诱使受害者访问恶意服务器，从而控制受害者系统。

### 5. 2011-04-12 Microsoft Windows OpenType Font (OTF) 驱动程序栈溢出远程代码执行漏洞（MS11-032）

NSFOCUS ID: 16713

http://www.nsfocus.net/vulndb/16713

**综述**:

Microsoft Windows 是微软发布的非常流行的操作系统。

Microsoft Windows OpenType Font(OTF) 驱动程序在实现上存在栈溢出远程代码执行漏洞，成功利用此漏洞的攻击者可以在内核模式中运行任意代码。

**危害**:

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

### 6. 2011-04-21 Adobe Reader 和 Acrobat "CoolType.dll" 内存破坏远程代码执行漏洞

NSFOCUS ID: 16753

http://www.nsfocus.net/vulndb/16753

**综述**:

Adobe Reader( 也被称为 Acrobat Reader) 是美国 Adobe 公司开发的一款优秀的 PDF 文档阅读软件。

Adobe Reader 和 Acrobat 的 CoolType.dll 在实现上存在内存破坏漏洞。

**危害**:

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

### 7. 2011-04-14 Google Chrome 10.0.648.205 之前版本多个安全漏洞

NSFOCUS ID: 16719

http://www.nsfocus.net/vulndb/16719

**综述**:

Google 浏览器，又称 Google Chrome，是一个由 Google 公司开发的网页浏览器。

Google Chrome 10.0.648.205 之前版本在实现上存在多个安全漏洞。

**危害**:

远程攻击者利用此漏洞，通过诱使用户打开恶意的网页，从而控制受害者系统。

### 8. 2011-04-01 RealNetworks Helix Server "x-wap-profile" 头选项格式串处理漏洞

NSFOCUS ID: 16655

http://www.nsfocus.net/vulndb/16655

**综述**:

RealNetwork Helix Server 是一款支持多格式、跨平台的流媒体服务器软件。

Helix Server 在处理请求中的 "x-wap-profile" 头选项时存在格式串处理漏洞。

**危害**:

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，从而控制服务器系统。

### 9. 2011-04-02 IBM Tivoli Directory Server 多个安全漏洞

NSFOCUS ID: 16666

http://www.nsfocus.net/vulndb/16666

**综述**:

IBM Tivoli Directory Server 是企业身份管理软件。

IBM Tivoli Directory Server 在实现上存在多个漏洞，其中包括栈溢出和以明文形式储存用户名密码等。

**危害**:

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，从而控制服务器系统。

### 10. 2011-04-29 HP Data Protector 备份客户端服务 EXEC_INTEGUTIL 远程代码执行漏洞

NSFOCUS ID: 16791

http://www.nsfocus.net/vulndb/16791

**综述**:

HP OpenView Storage Data Protector 软件是企业环境中单个服务器自动备份和恢复的软件。

HP OpenView Storage Data 的 Backup Client Service(OmniInet.exe) 服务监听在

TCP:5555 端口上，这个服务在处理 EXEC_INTEGUTIL 消息报文时存在栈溢出漏洞。

**危害**:

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，从而控制服务器系统。

# NSFOCUS 2011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<mailto:security@nsfocus.com>> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

## 1. 2011-05-12 Adobe Flash Player 远程内存破坏漏洞

NSFOCUS ID: 16829

http://www.nsfocus.net/vulndb/16829

**综述**：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 在实现上存在远程内存破坏漏洞，恶意软件可利用此漏洞，打开 .doc 文件中嵌入的 .swf 文件或电子邮件中的 .xls 文件附件。

**危害**：

远程攻击者可以利用此漏洞，通过诱使受害者打开包含恶意 SWF 文件的网页或 Office 文件，从而控制受害者系统。

## 2. 2011-05-10 Microsoft PowerPoint 远程代码执行漏洞（MS11-036）

NSFOCUS ID: 16817

http://www.nsfocus.net/vulndb/16817

**综述**：

Microsoft PowerPoint，简称 PowerPoint，是一个由 Microsoft 公司开发的演示文稿程序。

Microsoft PowerPoint 处理特制的 PowerPoint 文件时，存在远程代码执行漏洞。

**危害**：

远程攻击者可以利用此漏洞，诱使受害者打开包含恶意内容的 Office 文件，从而控制受害者系统。

### 3. 2011-05-09 Google Chrome 未明细节远程代码执行漏洞

NSFOCUS ID: 16810

http://www.nsfocus.net/vulndb/16810

**综述**:

Google Chrome 是由 Google 公司开发的开放原码网页浏览器。

Google Chrome 在实现上存在远程代码执行漏洞，可能造成拒绝服务攻击。

**危害**:

远程攻击者可以利用此漏洞，诱使用户打开恶意的网页，从而控制受害者系统。

### 4. 2011-05-27 IBM Lotus Notes 附件处理多个缓冲区溢出漏洞

NSFOCUS ID: 16864

http://www.nsfocus.net/vulndb/16864

**综述**:

IBM Lotus Notes 软件为用户提供了单点访问功能，有助于他们创建、查询和共享知识，与团队协作，以及采取相应措施。

IBM Lotus Notes 在处理附件的实现上，存在多个缓冲区溢出漏洞。

**危害**:

远程攻击者可以利用此漏洞，诱使用户打开恶意的 Lotus 附件，从而控制受害者系统。

### 5. 2011-05-10 Microsoft WINS 服务畸形报文远程代码执行漏洞（MS11-035）

NSFOCUS ID: 16818

http://www.nsfocus.net/vulndb/16818

**综述**:

Microsoft Windows Internet Name Service (WINS) 是 Windows 网际网络名称服务。

Microsoft Windows Internet Name Service(WINS) 在实现上存在远程代码执行漏洞，如果用户在运行 WINS 服务的受影响系统上收到特制的 WINS 重复报文，可能导致远程代码执行。

**危害**:

远程攻击者可以利用此漏洞，向服务器发送特制的请求报文，从而控制服务器系统。

### 6. 2011-05-18 Cisco Unified Operations Manager 多个 SQL 注入漏洞

NSFOCUS ID: 16850

http://www.nsfocus.net/vulndb/16850

**综述**:

Cisco Unified Operations Manager (CUOM) 是 Cisco Systems 开发的语音的 NMS，可实时监控所有系统元素。

Cisco Unified Operations Manager (CUOM) 在处理某些 SQL 查询时，在实现上存在多个 SQL 注入漏洞。

**危害**：

远程攻击者可利用此漏洞控制受影响设备，访问或修改未授权的数据。

### 7. 2011-05-27 Symantec Backup Exec for Windows Server 未授权访问漏洞

NSFOCUS ID: 16891

http://www.nsfocus.net/vulndb/16891

**综述**：

Symantec Backup Exec 产品旨在满足您在业务上对于可靠数据进行备份和恢复功能。

Symantec Backup Exec for Windows Server 在实现上存在未授权访问漏洞，此问题源于缺少媒体服务器和远程代理之前的身份信息验证。

**危害**：

远程攻击者可利用此漏洞绕过身份验证，并以提升的权限执行任意 NDMP 命令。

### 8. 2011-05-25 Sybase EAServer 目录遍历漏洞

NSFOCUS ID: 16881

http://www.nsfocus.net/vulndb/16881

**综述**：

Sybase EAServer 是高性能、可伸缩、安全、开放的应用服务器，适用于适用多层架构的电子门户和互联商务解决方案。

Sybase EAServer 在实现上存在目录遍历漏洞。

**危害**：

远程攻击者可利用此漏洞，通过受影响 Web 服务器，查看任意文件。

### 9. 2011-05-06 Skype Technologies Skype for Mac 远程代码执行漏洞

NSFOCUS ID: 16813

http://www.nsfocus.net/vulndb/16813

**综述**：

Skype 是免费的全球语音沟通软件。

Skype for Mac 在实现上存在远程代码执行漏洞。

**危害**：

远程攻击者可利用此漏洞控制受影响计算机。

### 10. 2011-05-31 HP 3COM/H3C Intelligent Management Center "img.exe" 远程堆缓冲区溢出漏洞

NSFOCUS ID: 16899

http://www.nsfocus.net/vulndb/16899

**综述**：

H3C 智能管理中心（H3C Intelligent Management Center，以下简称 H3C iMC）是下一代业务智能管理平台。

HP 3COM/H3C Intelligent Management Center imcsyslogdm 组件在实现上，存在 "img.exe" 远程堆缓冲区溢出漏洞。

**危害**：

远程攻击者可以利用此漏洞，向服务器发送特制的请求报文，从而控制服务器系统。

# NSFOCUS 2011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 > 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

## 1. 2011-06-15 Adobe Flash Player 远程内存破坏漏洞

NSFOCUS ID: 17000

http://www.nsfocus.net/vulndb/17000

**综述：**

Flash Player 是一款高性能的、轻量型且极具表现力的客户端运行时播放器。

Adobe Flash Player 在实现上存在远程内存破坏漏洞，远程攻击者可利用此漏洞执行任意代码或可能造成拒绝服务。

**危害：**

远程攻击者可以利用此漏洞，诱使受害者打开包含恶意 SWF 文件的网页，从而控制受害者系统。

## 2. 2011-06-15 Microsoft IE DOM 编辑未初始化内存远程代码执行漏洞 (MS11-050)

NSFOCUS ID: 16990

http://www.nsfocus.net/vulndb/16990

**综述：**

Microsoft Internet Explorer 是微软公司推出的一款网页浏览器。

Microsoft Internet Explorer 在实现 DOM 编辑的时候访问没有正确初始化或删除的对象，存在远程代码执行漏洞。

**危害：**

远程攻击者可以利用此漏洞，诱使受害者打开恶意的网页，从而控制受害者系统。

## 3. 2011-06-14 Adobe Acrobat 和 Reader "tesselate.x3d" 远程缓冲区溢出漏洞

NSFOCUS ID: 16967

http://www.nsfocus.net/vulndb/16967

**综述：**

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

Adobe Reader 和 Acrobat 在实现上存在 "tesselate.x3d" 远程

缓冲区溢出漏洞，此漏洞源于应用程序信任了 tesselate.x3d 插件加载的特定文件中嵌入的字符串长度，应用程序将从文件中复制任意长度的字符串到静态栈缓冲区。

**危害**：

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

### 4. 2011-06-14 Microsoft Excel 内存破坏远程代码执行漏洞 (MS11-045)

NSFOCUS ID: 16976

http://www.nsfocus.net/vulndb/16976

**综述**：

Microsoft Excel 是由 Microsoft 开发的一款试算表软件。

Microsoft Excel 在处理特定的文件字段时存在内存破坏漏洞 .

**危害**：

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

### 5. 2011-06-06 Adobe Flash Player 跨站脚本执行漏洞

NSFOCUS ID: 16910

http://www.nsfocus.net/vulndb/16910

**综述**：

Flash Player 是一款高性能的、轻量型且极具表现力的客户端运行时播放器。

Adobe Flash Player 在实现上存在跨站脚本执行漏洞。

**危害**：

远程攻击者可以利用此漏洞，诱使受害者打开包含恶意 swf 文件的网页，从而在受影响站点的浏览器中执行任意代码，窃取 Cookie 身份验证凭证，发动其他攻击。

### 6. 2011-06-22 RealWin SCADA 服务器 DATAC 登录缓冲区溢出漏洞

NSFOCUS ID: 17105

http://www.nsfocus.net/vulndb/17105

**综述**：

RealWin 是运行在 Windows 平台上的数据采集与监视控制系统 (SCADA) 服务器产品。

RealWin SCADA 服务器在实现上存在 DATAC 登录缓冲区溢出漏洞，通过发送特制的包含长文件名的 On_FC_CONNECT_FCS_LOGIN 报文就能触发此漏洞。

**危害**：

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，从而控制服务器系统。

### 7. 2011-06-23 Discuz! 多个版本存储型跨站脚本漏洞

NSFOCUS ID: 17110

http://www.nsfocus.net/vulndb/17110

**综述**：

Discuz! 是一款华人地区非常流行的 Web 论坛程序。

Discuz 多个版本在实现上存在跨站脚本攻击漏洞，远程攻击者可利用这些漏洞在用户系统中执行恶意脚本代码。

**危害**：

远程攻击者可以向服务器提交恶意请求，从而向服务器注入恶意代码，在受害者的浏览器中执行任意代码，窃取 Cookie 身份验证凭证，发动其他攻击。

### 8. 2011-06-07 IBM Tivoli Endpoint 服务 POST 请求参数栈缓冲区溢出漏洞

NSFOCUS ID: 16942

http://www.nsfocus.net/vulndb/16942

**综述**：

IBM Tivoli Management Framework 可提供大量远程位置或设备的管理工具。

IBM Tivoli Management Framework 包含一个终端服务程序 (lcfd.exe)。该服务默认监听 TCP 9495 端口。在解析用户提交的 POST 请求时，进程将 POST 变量的内容直接复制到 256 字节的栈缓冲区中，这可能造成缓冲区溢出。

**危害**：

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，从而控制服务器系统。

### 9. 2011-06-10 Sybase EAServer 远程目录遍历漏洞

NSFOCUS ID: 16964

http://www.nsfocus.net/vulndb/16964

**综述**：

Sybase EAServer 是高性能、可伸缩、安全、开放的应用服务器，适用于适用多层架构的电子门户和互联商务解决方案。

Sybase EAServer 在实现上存在目录遍历漏洞，此漏洞源于 Sybase EAServer HTTPServer 限制目录遍历失败，通过指定多个目录遍历序列的文件路径，例如 "/\../\../\"，攻击者可以获取已配置的 HTTP 服务器受限目录之外的敏感文件。

**危害**：

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，读取服务器上的敏感文件，从而控制服务器系统。

### 10. 2011-06-11 Trend Micro Data Loss Prevention Virtual Appliance 5.5 目录遍历漏洞

NSFOCUS ID: 16958

http://www.nsfocus.net/vulndb/16958

**综述**：

Trend Micro Data Loss Prevention Virtual Appliance 可防止意外的和恶意的数据泄漏。

Trend Micro Data Loss Prevention Virtual Appliance 5.5 在实现上存在目录遍历漏洞，远程攻击者可利用此漏洞读取 Web 根之外的文件。

**危害**：

远程攻击者可以利用此漏洞，发送特制的请求报文到服务器，读取服务器上的敏感文件，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