基于多维角度的攻击分类方法*

郭 林[1,2], 严 芬[1,2,3], 黄 皓[1,2]

(1. 南京大学 软件新技术国家重点实验室, 江苏 南京 210093; 2. 南京大学 计算机科学与技术系, 江苏 南京 210093; 3. 扬州大学 信息工程学院 计算机科学与工程系, 江苏 扬州 225009)

摘 要: 提出了一种新的基于多维角度的攻击分类方法,给出分类的标准和结果。通过对诸多攻击样例的分类来验证所给的攻击分类方法,并对此攻击分类的方法作了客观的分析评价。

关键词: 安全; 攻击; 攻击分类; 分类原则; 分类标准

中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2007)04-0139-05

Method of Classifying Attacks Based on Multi-dimension

GUO Lin[1,2], YAN Fen[1,2,3], HUANG Hao[1,2]

(1. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing Jiangsu* 210093, *China;* 2. *Dept. of Computer Science & Technology, Nanjing University, Nanjing Jiangsu* 210093, *China;* 3. *Dept. of Computer Science & Engineering, Institute of Information Technology, Yangzhou University, Yangzhou Jiangsu* 225009, *China*)

Abstract: A new attack classification method was put forward and delivered the criterion and results of the classification. This method is validated by classifying many attack samples. At the same time, an objective analysis and estimate of this classification method were given.

Key words: security; attacks; attack classification; classification principle; classification criterion

0 引言

在计算机技术和网络技术发展及应用范围不断扩大的同时,对计算机和网络的攻击也日益增长。根据美国权威安全事件应急处理组织 CERT/CC 最新发布的统计报告[1], 2003 年 CERT/CC 受理的安全事件报告达到了137 529起,比 2002 年增加了 50% 以上。

对计算机系统产生的一次危害可能由一个攻击行为或一系列的攻击行为造成。攻击技术发展迅速,迫切需要对攻击行为进行深入细致的研究和分析,以便及时发现攻击行为的发生,发掘攻击行为之间内在联系,从而有效地检测和对抗攻击,减小攻击造成的危害。目前,各种不同攻击检测和防御产品大量出现。但是,由于当前研究人员对攻击理解的差异,对攻击的判定和特征提取方法的不同,给各防御系统之间的交互和协作带来了困难。研究攻击分类能有效地解决上述问题。对攻击合理分类是研究攻击的前提。它可以为攻击提供统一的描述语言,便于不同研究组织之间进行交流;使用系统的方法来认识、描述攻击有利于简化对攻击的理解,把握攻击的本质特征和基本原理,更好地检测和防御攻击。

近几年来,关于计算机和网络攻击以及漏洞分类方法的研究,为攻击分类的研究作出了不少贡献。但是,这些分类方法主要存在着以下几方面的缺点:①对网络攻击事件的分类随意性很强;②对同样的攻击事件判定结果不同;③对于网络攻击事件所造成的危害和潜在的危险缺乏统一的衡量准则。研究攻击分类的目的是为了给出一个普遍适用的认识和理解攻击的框架。本文提出了一种新的攻击分类方法。这个分类方法主要是在对目前已存在攻击的研究的基础上提出的。分类的结果也同样适用于对未出现的攻击进行分类和系统的描述。

1 相关工作

1.1 攻击分类的基本原则

20 世纪 90 年代中后期,研究人员对攻击分类的原则进行了较多的探讨[2~6]。研究者们从不同角度考虑攻击分类。文中提出攻击分类应该遵循的原则主要有以下几条:

(1) 互斥性——各类别应是互斥的,没有交叉和覆盖现象;

(2) 穷举性——全部类别包含所有类型攻击;

(3) 无二义性——各类别精确、清晰,没有不确定性;

(4) 可重复性——不同人根据同一原则重复分类的过程,得出的分类结果应该一样;

(5) 可接受性——分类符合逻辑和直觉,易于被大多数人接受;

(6) 可用性——分类对不同领域的应用具有实用价值;

(7) 适应性——可适应于多个不同应用要求;

收稿日期: 2006-02-13; 修返日期: 2006-04-14 基金项目: 国家“863”计划资助项目(2003AA142010); 江苏省高技术研究计划资助项目(BG2004030)

作者简介:郭林(1976-),男,工程师,硕士研究生,主要研究方向为网络与信息安全、恶意代码检测(glince@163.com);严芬(1978-),女,讲师,博士研究生,主要研究方向为网络与信息安全;黄皓(1957-),教授,博导,博士,主要研究方向为网络与信息安全.

(8) 原子性——每个分类无法再进一步细分。

除此之外,还有客观性、可理解性、稳定性等原则。从已有的分类实践中可以看出,一般以 Amoroso[2] 提出的六个分类原则为主要原则,即互斥性、穷举性、无二义性、可重复性、可接受性、可用性。

1.2 攻击分类的研究现状

目前已有的攻击分类[7] 主要有:

(1) 基于经验术语的攻击分类

Icove[8] 将攻击分成病毒和蠕虫、拒绝服务、特洛伊木马、隐蔽信道、搭线窃听、会话劫持、IP 欺骗等二十余类。Cohen[9] 将攻击分为特洛伊木马、伪造网络资料、冒充他人、网络探测、时间炸弹、获取工作资格等十余类。

(2) 基于单一属性的攻击分类

Landwehr 等人[10] 从漏洞的产生、引入时间、在计算机中的位置三个方面对计算机系统的安全漏洞进行分类。Bishop[11] 提出了使用六个属性分类 UNIX 漏洞,即漏洞的性质、漏洞的引入时间、利用漏洞可以得到的结果、漏洞造成的影响、利用漏洞时所需的最小组件数目、漏洞定义的来源。Neumann 和 Parker[12] 对攻击技术进行分类,分为外部滥用、硬件滥用、伪造、有害代码、绕过认证或授权、主动滥用、被动滥用、恶意滥用、间接滥用九类。Cohen[13] 对攻击后果进行分类,分成破坏、泄漏、拒绝服务三类。Russell 和 Gangemi[14] 则将其分成破坏信息的保密性、完整性、真实性、可用性四类。

(3) 基于多维属性的攻击分类

Lindqvist 等人[6] 结合攻击技术和攻击产生的后果进行分类。Howard[4] 提出基于攻击实施过程的分类,用攻击者类型、使用的工具、攻击机理、攻击的结果、攻击的目的五个阶段来描述攻击。Christy[15] 在 Howard 的基础上对一些项进行了扩充。Perry 和 Wallich[16] 基于攻击者和攻击后果进行分类。Hansman[17] 基于攻击媒介、攻击目标、利用的漏洞、攻击造成的后果进行分类。文献[18] 从攻击对平台的依赖性、攻击入口、攻击点、攻击结果、攻击的传播性五个角度分类攻击。

(4) 基于应用的分类

OASIS WAS TC 较早地对 Web 应用漏洞进行分类,并使用 XML 语言描述漏洞,提高了分类方法的互用性[19]。Alvarez 和 Petrovic[20] 基于对 Web 攻击过程生命周期的理解来分类 Web 攻击。Weaver 等人[21] 从目标发现、选择策略、触发方式等角度对计算机蠕虫进行了描述。Mirkovic 等人[22] 根据自动化程度、扫描策略、传播机制、攻击的漏洞、攻击速度的动态性、影响等属性对 DDoS 攻击进行了分类。

(5) 基于检测的攻击分类

Kumar[23] 提出了以检测为目的的攻击分类法,分类的依据是攻击在系统审计记录中表现出来的特征。文献[24] 对 Kumar 的分类方法的缺点进行研究和改进,提出了一种面向检测的网络攻击分类方法——ESTQ 方法。

正如本文前面所提到的,这些分类方法也存在着不足之处:基于经验术语的攻击分类方法利用攻击中常见的技术术语、社会术语等来对攻击分类,分类的结果逻辑性和层次结构不清晰,使用的术语内涵往往定义不清楚,不易被普遍接受;基于单一属性的分类方法仅从某个特定的角度对攻击分类,因而对攻击的描述比较片面;基于多维属性的攻击分类方法比单一属性的分类方法要好,对攻击的描述更清楚,但是,从已有的工作来看,用于描述攻击的属性仍不全面,不适合很好地理解和描述攻击。为了更好地分析攻击行为,以便及时检测到攻击的发生,发现各攻击行为之间的内在联系,本文提出一种新的基于多维角度的攻击分类方法。

2 基于多维角度的攻击分类方法的研究

2.1 分类的依据

定义 基于多维角度的分类方法主要是指同时抽取攻击的多个属性,并利用这些属性组成的序列来表示一个攻击过程,或由多个属性组成的结构来表示攻击,并对过程或结构进行分类的方法。

从多维角度描述和分类攻击的方法,可以克服单一属性描述攻击时的片面性和局限性的缺点。该方法将攻击理解为一个动态的过程,将攻击过程分解成相互关联的几个独立阶段,对攻击各阶段的属性及其相互关联关系进行描述,从而准确、全面地描述攻击全过程中的各个阶段。

首先要考虑应该基于哪些属性对攻击进行分类才能得到好的分类结果;其次要考虑如何能让分类结果刻画出攻击的过程性特点。因此,分类结果要尽量满足分类的主要原则,直观易理解,并符合人们的习惯,要能较全面地描述攻击,说明攻击过程的生命周期。多维角度攻击分类的基本思路是利用属性序列描述攻击过程,利用属性结构表示攻击。通过分析研究,提出了以下分类攻击的属性:

(1) 攻击技术方法(Method);

(2) 攻击的平台(Platform);

(3) 攻击的平台依赖性(Platform);

(4) 攻击编程经验(Experience);

(5) 攻击的来源(Source);

(6) 攻击入口(Entry);

(7) 漏洞的利用(Vulnerability);

(8) 攻击的对象(Object);

(9) 攻击的意图(Intention);

(10) 攻击的后果(Results);

(11) 攻击的破坏程度(Destructive);

(12) 攻击的防治难度(Prevention and Cure Difficulty);

(13) 攻击的传播性与繁殖能力(Spreading and Propagating Ability)。

属性(1)、(5) ~(10) 组成七元组的形式,清楚地描述出攻击过程;属性(2) ~(4) 对攻击的难度和范围作进一步描述;属性(11)、(12) 进一步说明攻击造成的后果;而属性(13) 对攻击的复杂性进行补充说明。

2.2 分类标准和分类结果

(1) 攻击技术的分类

选择攻击技术来描述攻击,可用于说明和理解入侵使用的技术方法,让系统管理员迅速采取措施以阻止进一步的攻击。分类方法,即根据此属性进行分类时,重点考虑两个方面:兼顾

一般的攻击术语或攻击种类对攻击技术的描述,从而使分类结果直观、易被接受;使分类结果具有结构性和层次性,能清晰地描述复杂的攻击技术。本文将其分为五类,即伪造信息攻击、拒绝服务攻击类、信息利用攻击类、数据驱动攻击类、信息收集攻击类。分类结果如图 1 所示。

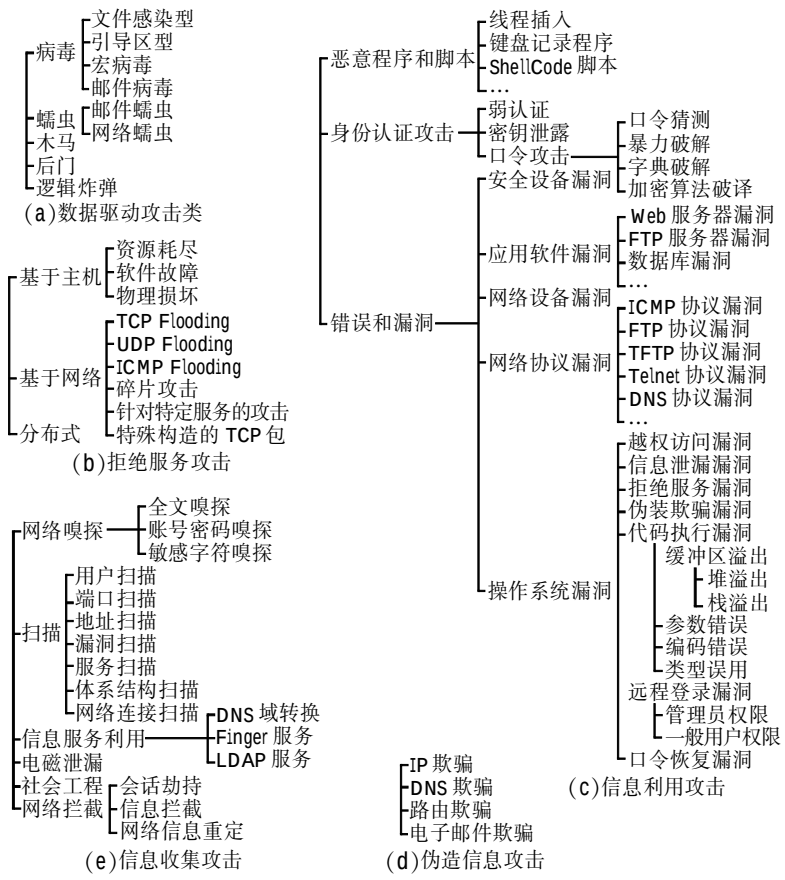

图 1　攻击分类

(2) 攻击平台的分类

攻击平台是指攻击针对哪些操作系统平台展开。通过它可以知道某种攻击将会对哪些操作系统产生威胁。分类方法是先根据不同的操作系统平台分类,同一操作系统的平台再根据不同的版本及版本号分类。本文将其分五类:①Solaris 家族和 Solaris 8、9、10 等;② UNIX 家族为 Linux 2.2、2.4 等;FreeBSD 4.8、5.1 等;③Microsoft 家族为 Windows 95、Windows 98、Windows 2000、Windows XP、Windows 2003 Server 等;④MacOS家族为 MacOS X10.1、10.2 等;⑤其他。

(3) 攻击平台依赖性的分类

平台依赖性反映出攻击对操作系统平台的依赖程度。大部分攻击都是针对特定的某种或某几种平台发起的,攻击与攻击目标所在的平台有很强的相关性。攻击平台依赖性的分类主要是确定攻击与攻击目标平台之间的对应关系。本文将其分三类:①平台依赖性强。攻击与攻击目标平台之间存在一对一的关系。②平台依赖性弱。攻击与攻击目标平台之间存在一对多的关系。其包含两种情况,即攻击对应于一类操作系统平台中的若干个不同版本,或对应于两类以上的操作系统平台。③无。攻击与任何一种攻击目标平台之间不存在相关性。

(4) 攻击编程经验的分类

从攻击需要的编程经验可以看出实施攻击的难度。大量的攻击工具软件的存在屏蔽了攻击的复杂度。利用攻击工具软件,攻击者不需要编程经验,就可以达到攻击的目的;但是当攻击者为了逃避检测或者实现特定的攻击目的时,需要修改攻击参数、代码或攻击脚本等,攻击者就要拥有一定的编程知识。本文将其分为三类:①不需要编程经验;②需要少量的编程经验;③需要丰富的编程经验。

(5) 攻击来源的分类

攻击来源分类主要是确定攻击相对于被攻击目标的位置。本文将其分为三类:①远程网络,即外部网络连接及数据访问;②本地网络,即内部网络连接,以及同一网段中不同部门间的连接;③物理主机,即攻击者直接接触或操作受害的计算机及系统。

(6) 攻击入口的分类

攻击入口简单地理解为攻击者进入到被攻击目标的通道。攻击入口的分类主要是确定系统与外界,或者是内网与外网进行信息交换的接口。本文将其分为四类:①用户接口,指在操作系统上安装的各种应用服务系统所提供的与外界进行交互的接口;②网络协议接口,指操作系统能够与外界进行网络通信所提供的接口,以及内网能够与外网通信所提供的接口;③网络管理接口,指操作系统在基本网络通信配置基础上,增加网络管理功能时,所涉及到的网络管理、配置模块与外界的接口;④设备接口,指操作系统与各外围设备之间进行通信所提供的接口,特别指外围设备驱动程序。

(7) 漏洞利用的分类

CVE 是众多权威机构和大厂商直接支持的共同规范。目前,大多数的安全产品都遵从 CVE 对漏洞的描述。属性 1 对攻击技术进行分类时,已经对直接利用错误和漏洞进行的攻击进行了描述。利用此属性分类攻击,可以从另一个方面描述攻击的漏洞利用类型。在根据漏洞分类攻击时,首先以 CVE 库中对漏洞攻击的描述为基准进行分类;若某漏洞在 CVE 库中还未出现的话,再考虑根据漏洞的来源等对其进行分类描述,即 CVE 库和漏洞。后者主要有三种来源:①设计中的漏洞,即弱的或者不正确的设计错误;②实现中的漏洞,即弱的或不正确的输入验证、弱的或不正确的访问验证、竞争条件错误、违反约束条件错误、域错误等;③配置管理中的漏洞,即配置错误、策略错误、软件安装的位置错误等。

(8) 攻击对象的分类

攻击对象是能够被攻击且能够对目标系统造成间接或直接影响的攻击点。一般情况下,目标系统是拥有硬件资源、数据并能够对外提供服务的综合体。所有的攻击都是针对系统的这些组成部分发起的。本文将其分为六类:①硬件资源,即主机、外围设备、网络设备;②网络,即本地网络、广域网、VPN;③系统,以攻击软件系统为目标,如操作系统、应用系统;④系统的成分,指系统的组成部分,如组件、构件、模块等;⑤数据,即系统数据、用户数据、应用数据;⑥服务,指系统或应用提供的服务。

(9) 攻击意图的分类

攻击者一般采用破坏、收集、占用、利用等手段来达到他们的攻击意图。攻击意图的分类主要反映攻击者对系统发起攻击后要达到的目的。本文将其分为七类:①获取信息,获取权限(提升权限)等;②修改信息,即系统及用户的相关信息被修改;③删除信息,即系统及用户的相关信息被删除;④利用服务,即利用系统功能发起渗透攻击的手段;⑤拒绝服务,即网络或系统资源被滥用,正常的操作受到影响或功能丧失;⑥增加服务,即攻击者按照攻击意图增加系统服务,如植入木马、预留

后门等; ⑦执行代码, 即攻击者可以在目标主机上执行任意代码。

(10) 攻击后果的分类

攻击后果用于根据系统的安全策略判断入侵造成后果的严重程度。攻击后果分类指根据攻击造成的结果来进行分类。本文将其分为四类: ①破坏性信息的机密性, 信息出现在不该出现的地方; ②破坏性信息的完整, 未授权地修改信息; ③破坏性信息的可用性, 计算机或网络服务不能被正常使用; ④破坏性信息的真实性, 出现虚假的信息。

(11) 攻击破坏程度的分类

攻击的破坏程度用来说明攻击后果所造成直接破坏的严重性。本文将其分为三类: ①破坏性大, 攻击的后果产生较强的破坏性, 造成系统和服务不能正常使用; ②破坏性适中, 攻击后果产生破坏性, 威胁到数据的正常使用, 但不足以威胁系统和服务的正常使用; ③破坏性小, 攻击后果产生很小的破坏性, 造成的破坏结果可以被修复。

(12) 攻击防治难度的分类

攻击的防治难度用来说明防御和抵抗攻击的复杂程度。本文将攻击的防治难度分为两类: ①困难, 攻击复杂性大, 攻击本身产生的后果严重, 或者将会在此攻击的基础上产生破坏性很大的攻击; ②容易, 攻击不复杂, 攻击没有太多的破坏力, 攻击结果不存在被进一步利用的价值。

(13) 攻击传播性与繁殖能力的分类

对于具有传播能力的攻击来说, 一类是负载传播, 如利用邮件作为传播途径的蠕虫; 另一类就是主动传播, 如利用缓冲区溢出漏洞进行传播的蠕虫, 在内存中进行自我复制, 并发起对其他系统的攻击。攻击的传播性与繁殖能力的分类主要按照攻击的传播能力和繁殖能力的强度来进行分类。本文将其分为三类: ①无传播和繁殖性, 即一对一地发起攻击, 没有任何传播和繁殖能力; ②传播和繁殖性弱, 即被动激活, 传播和繁殖需要外界帮助; ③传播和繁殖性强, 即能够主动激活, 自动进行搜索, 并进行自动繁殖和广泛传播。

3 基于多维角度的攻击分类方法的分析评价

Amoroso 攻击分类的原则是攻击分类方法应该具有的理想特性, 根据 Amoroso 攻击分类原则, 对基于多维角度的攻击分类方法进行分析和评价。

3.1 分析评价结果

(1) 满足 Amoroso 分类基本原则中的互斥性、可接受性、无二义性、可用性原则;

(2) 选择的多维属性较全面地概括了攻击在各个方面的特性;

(3) 分类结果的层次清楚、分类项目具体明确, 便于扩展和描述;

(4) 结合了基于攻击过程对攻击的描述方法, 分类结果可用来描述攻击的过程;

(5) "攻击技术"属性分类攻击时, 兼顾了传统的、易被接受的基于经验术语对攻击的分类思想, 所划分的五大类技术既符合经验术语的描述, 又有较好的逻辑结构和层次性;

(6) 分类的结果可以用来作为进一步研究攻击的基础, 并用来指导安全软件的设计。

3.2 攻击分类的实例

表 1 是对若干攻击实例按照多维角度的攻击分类方法进行分类的结果。

表 1 攻击实例分类结果

攻击实例	Code Red	wu-ftpd	梅丽莎	Land	Netspy	TCP SYN 扫描
攻击技术	网络蠕虫	栈溢出	邮件病毒	构造 TCP 包	木马后门	端口扫描
攻击来源	外部网络 内部网络	内部网络	外部网络 内部网络	内部网络	外部网络 内部网络	外部网络 内部网络
攻击入口	网络协议 接口	用户接口	用户接口	网络协议 接口	用户接口	网络协议 接口
漏洞利用	CVE-2001- 0500	CVE-1999- 0368	程序弱 验证漏洞	CVE-1999- 0016	无	协议栈 设计缺陷
攻击平台	Microsoft	UNIX	Microsoft	Windows, UNIX	Microsoft	Windows, UNIX
攻击对象	应用服务 (IIS)	数据	应用服务	路由器	服务	本地网络
攻击意图	拒绝服务 增加服务	获取系统 权限	拒绝服务 修改信息	消耗系统资源 拒绝服务	获取信息 执行代码	获取信息
攻击后果	拒绝服务	信息 机密性	拒绝服务 信息完事性	拒绝服务	信息 机密性	信息 机密性
破坏程度	大	适中	大	大	适中	适中
防治难度	困难	困难	容易	困难	困难	容易

以 Code Red 攻击为例, 说明利用本文所给属性序列描述攻击过程的方法。Code Red 攻击属于数据驱动攻击类—蠕虫子类—网络蠕虫攻击类别。攻击者来源于外部网络或者内部网络, 以网络协议接口(Web 应用提供的与用户的接口) 为攻击入口点, 使用特殊构造的输入脚本, 利用 CVE-2001-0500 漏洞(IIS Web 服务器的. ida/. idq 缓冲区溢出) , 从受感染的机器扫描同一网段内的其他机器, 并且通过 80 端口传播到其他的 Web 服务器上, 采用缓冲区溢出的方法进行攻击, 可以在 Web 服务器上留下后门, 以取得受影响 Web 服务器的超级用户的安全权限, 达到增加服务和拒绝服务的攻击意图, 造成破坏信息机密性和可用性的攻击后果。攻击的危害性较大, 当攻击者获得了系统权限后, 就可以进行更进一步的破坏操作。该种攻击具有很强的传播性与繁殖能力, 攻击的传播速度快, 难以防范。

从而可以看出, 多维角度的攻击分类方法能够清晰地分类攻击, 描述攻击各方面的属性, 分类结果可用于理解攻击。可见, 此分类方法是可行的、有效的。

4 结束语

本文基于多个属性对攻击进行分类, 提出了相应的分类标准, 给出了分类结果。本文还对分类方法进行分析和评估, 并通过列举对攻击示例的分类验证了分类方法的有效性, 达到了预期的研究目标。研究工作为进一步开展攻击技术研究, 寻找更好的攻击检测、攻击防御和响应的方法, 对安全系统、安全产品的研究和实现等工作奠定了良好的基础。

参考文献:

[1] ERT/CC statistics(CERT coordination center) [EB/OL]. http://www.cert.org/stats.

[2] AMOROSO E G. Fundamentals of computer security technology[M].

[S.l.]: Prentice Hall PTR, 1994.

[3] BISHOP M. Vulnerabilities analysis: proc. of the 2nd International Symposium on Recent Advances in Intrusion Detection[C]. [S.l.]: [s.n.], 1999.

[4] HOWAD J. An analysis of security incidents on the Internet[D]. West Lafayette: Carnegie Mellon University, 1997.

[5] KRSUL I. Computer vulnerability analysis[R]. [S.l.]: The COAST Laboratory, Department of Computer Sciences, Purdue University, 1997.

[6] LINDQVIST U, JONSSON E. How to systematically classify computer security intrusions: IEEE Symposium on Security and Privacy[C]. Oakland: [s.n], 1997: 154-163.

[7] 刘欣然. 网络攻击分类技术综述[J]. 通信学报, 2004, **25**(7): 30-36.

[8] ICOVE D, SEGER K, VONSTORCH W. Computer crime: a crime-fighter's handbook[M]. [S.l.]: O'Reilly & Associates, Inc., 1995.

[9] COHEN F. Information system attacks: a preliminary classification scheme[J]. **Computers and Security,** 1997, **16**(1): 29-46.

[10] LANDWEHR C E, BULL A R, MCDERMOTT J P, *et al*. A taxonomy of computer program security flaws[J]. **ACM Computing Surveys,** 1994, **26**(3): 211-254.

[11] BISHOP M. A taxonomy of UNIX system and network vulnerabilities [D]. [S.l.]: Department of Computer Science, University of California at Davis, 1995.

[12] NEUMANN P G, PARKER D B. A summary of computer misuse techniques: proceedings of the 12th National Computer Security Conference[C]. Baltimor: [s.n.], 1989: 396-407.

[13] COHEN F B, Protection and security on the information superhighway [M]. New York: John Wiley & Sons, 1999.

[14] RUSSELL D, GANGEMI G T. Computer security basics[R]. Sebastopol: O'Reilly & Associates, Inc., 1991.

[15] CHRISTY J. Cyber threat & legal issues: Shadowcon Conference [C]. [S.l.]: [s.n.], 1999.

[16] PERRY T, WALLICH P. Can computer crime be stopped?[J]. **IEEE Spectrum,** 1984, **21**(5): 34-35.

[17] A taxonomy of network and computer attack methodologies[EB/OL]. (2003-11-07). http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/2003/hons_0306.pdf.

[18] 张涛, 董占球. 网络攻击行为分类技术的研究[J]. 计算机应用, 2004, **24**(4): 115-118.

[19] OASIS W T C. OASIS Web application security technical committee [EB/OL]. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=was.

[20] ALVAREZ G, PETROVIC S. A taxonomy of Web attacks suitable for efficient encoding[J]. **Computers & Security,** 2003, **22**(5): 435-449.

[21] A taxonomy of computer worms[EB/OL]. http://www.cs.berkeley.edu/~nweaver/papers/taxonomy.pdf.

[22] MIRKOVIC J, MARTIN J, REIHER P. A taxonomy of DDoS attacks & DDoS defense mechanisms[R]. [S.l.]: University of California, 2002.

[23] KUMAR S. Classification and detection of computer intrusions[D]. West Lafayette: Purdue University, 1995.

[24] 王晓程, 刘恩德, 谢小权. 攻击分类研究与分布式网络入侵检测系统[J]. 计算机研究与发展, 2001, **38**(6): 727-734.

(上接第 126 页)

3.3　多参与性和多代表性

每一个有效的群签名来自 t 个本系统成员,分别来自系统中不同群组,代表本组签署文件。一旦群签名成功签署,不同群组的利益均被考虑,因而整个系统就会良性、高效地运作。当然,如果有某个文件只代表部分组的利益,那么其他组就会拒绝参与该文件的签署。

3.4　验证的匿名性和身份的可追查性

从群签名验证式可以看出,任何验证者只需利用群公钥验证群签名。他们不清楚具体是哪些人参与了签名,因而具有签名验证的匿名性;如果发生纠纷,本方案可以通过 r 个群组秘书和群管理员追查签名者,从而可知哪些成员参与了签名。

4　结束语

本文给出的 (t, n) 门限签名方案,使所有不同部门的成员能代表本部门利益,各部门一起参与生成有效的群签名。缺少任何一个或数个部门的参与均无法生成有效的群签名。这种现象在现实世界中是经常遇到的,因而本方案是很实用的。

参考文献:

[1] ESMEDT Y, FRANKEL Y. Shared generation of authenticator and signatures: Advances in Cryptology—CRYPTO'91[C]. [S.l.]: [s.n.], 1991: 457-469.

[2] HARN L. Group-oriented (t, n)-threshold digital signature scheme and digital multi-signature[J]. **IEE Proc. Computer. Digital Techniques,** 1994, **141**(5): 307-313.

[3] WANG Chingte, LIN Chunsing, CHANG Chinchen. Threshold signature schemes with traceable signers in group communications[J]. **Computer Comm.,** 1998, **21**(8): 771-776.

[4] TSENG Y M, JEN J K. Attacks on threshold signature schemes with traceable signers[J]. **Information Processing Letters,** 1999, **71**: 1-4.

[5] LI C M, HWANG T, LEE N Y. Threshold multi-signature schemes where suspected forgery implies traceability of adversarial shareholders: Advances in Cryptology—EUROCRYPT'94[C]. [S.l.]: [s.n.], 1995: 194-204.

[6] 王贵林, 卿斯汉. 几个门限群签名方案的弱点[J]. 软件学报, 2000, **11**(10): 1326-1332.

[7] 张建中, 肖国镇. 可防止欺诈的动态秘密共享方案[J]. 通信学报, 2000, **21**(5): 81-83.

[8] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. **IEEE Trans. Inform. Theory,** 1985, **31**(4): 469-472.

[9] 王晓明, 符方伟. 一种安全的群签名方案[J]. 电子与信息学报, 2003(5): 657-663.