· 发展趋势 / 热点技术 · 文章编号：1000—3428(2002)10—0003—04 文献标识码：A 中图分类号：TP393.08

计算机漏洞分类研究

单国栋，戴英侠，王 航
(中国科技大学研究生院信息安全国家重点实验室，北京 100039)

摘 要：漏洞的发现、利用和防御是网络攻防的焦点。通过对计算机漏洞的分类研究，有助于增强人们对漏洞本质的理解以及针对性地消除漏洞，特别是对发现未知漏洞具有积极作用。该文首先介绍计算机漏洞研究的现状，然后分析漏洞的概念、研究方法及分类模型，最后讨论漏洞研究存在的问题和发展趋势。

关键词：计算机漏洞；分类模型；弱点；逻辑错误

Study on Computer Vulnerability Taxonomy

SHAN Guodong, DAI Yingxia, WANG Hang
(State key Lab of Information Security, Graduate School of USTC, Beijing 100039)

【Abstract】 Network attack and defense are focused on how to discover, exploit and prevent computer vulnerabilities. The taxonomy of computer vulnerabilities can result in an increased understanding of the nature of software vulnerabilities, which contributes to eliminating them respectively and is of great benefit to finding unknown vulnerabilities. In this thesis, the history and status quo of vulnerability studies are first reviewed. After that, the paper presents the concept, research method and taxonomy model of vulnerability. Finally, it discusses the problems and future trend in the studies of computer vulnerabilities.

【Key words】 Computer vulnerability; Taxonomy model; Weakness; Logic error

1 研究现状

20世纪70年代中期，美国启动的PA (Protection Analysis Project) 和RISOS(Research in Secured Operating Systems)计划被公认为是计算机安全研究工作的起点。1980年，美国密执安大学的B.Hebbard小组使用“渗透分析”(Penetration Analysis)方法成功地发现了系统程序中的部分漏洞。1990年，美国伊利诺斯大学的Marick发表了关于软件漏洞的调查报告，对软件漏洞的形成特点做了统计分析。1993年，美国海军研究实验室的Landwher等人收集了不同操作系统的安全缺陷，按照漏洞的来源、形成时间和分布位置建立了3种分类模型。普渡大学COAST实验室的Aslam和Krsul在前人成果的基础上，提出了更为完整的漏洞分类模型，并建立了专用漏洞数据库。MITRE公司从事的"公共漏洞列表"(Common Vulnerability Enumeration,CVE)工作，为每个漏洞建立了统一标识，方便了漏洞研究的信息共享及数据交换。

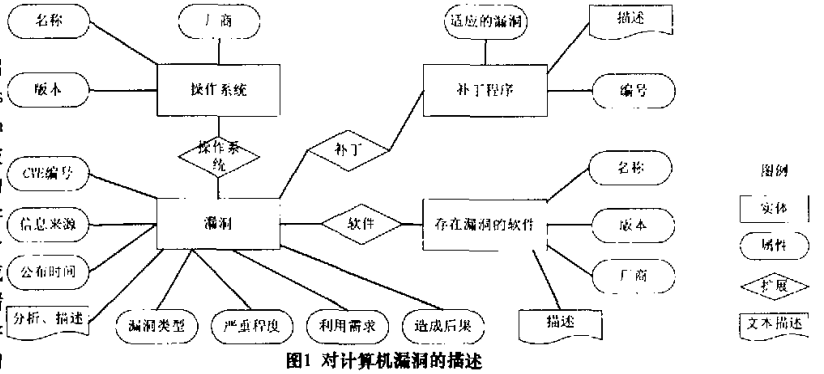


图1 对计算机漏洞的描述

2 概念描述

Denning在《Cryptograph and Data Security》一文中从访问控制的角度给出了漏洞的定义。他认为，系统中主体对对象的访问是通过访问控制矩阵实现的，这个访问控制矩阵就是安全策略的具体实现，当操作系统的操作和安全策略之间相冲突时，就产生了安全漏洞。

Bishop和Baily在<< A Critical Analysis of Vulnerability Taxonomies>>中认为，计算机系统是由若干描述实体配置的当前状态所组成的，这些状态可分为授权状态、非授权状态以及易受攻击状态、不易受攻击状态。容易受攻击的状态是指通过授权的状态转变从非授权状态可以到达的授权状态。受损状态是指已完成这种转变的状态，攻击是非受损状态到受损状态的状态转变过程。漏洞就是指区别于所有非受损状态的容易受攻击的状态特征。

漏洞具有以下特点：(1)编程过程中出现逻辑错误是很普遍的现象，这些错误绝大多数都是由于疏忽造成的。(2)数据处理(例如对变量赋值)比数值计算更容易出现逻辑错误，过小和过大的程序模块都比中等程序模块更容易出现错误。(3)漏洞和具体的系统环境密切相关。在不同种类的软、硬件设备中，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。(4)漏洞问题与时间紧密相关。随着时间的推移，旧的漏洞会不断得到修补或纠正，

基金项目：国家重点基础研究发展规划项目,项目编号:G1999035801;国家自然科学基金，项目编号：90104030

作者简介：单国栋(1970～)，男，硕士生，主要研究方向为网络入侵检测技术、安全操作系统；戴英侠，教授；王 航，硕士生

收稿日期：2001-11-18

新的漏洞会不断出现，因而漏洞问题会长期存在。

漏洞的上述特点决定了漏洞完整描述的独特性。在对漏洞进行研究时，除了需要掌握漏洞本身的特征属性，还要了解与漏洞密切相关的其它对象的特点。漏洞的基本属性有：漏洞类型、造成的后果、严重程度、利用需求、环境特征等。与漏洞相关的对象包括：存在漏洞的软(硬)件、操作系统、相应的补丁程序和修补漏洞的方法等。图1是一个典型的漏洞库所包含的漏洞信息。

3 底层分析

由于对程序内部操作的不了解，或者是没有足够的重视，程序员总是假定他们的程序会在任何环境中正常地运行。当程序员的假设得不到满足，程序内部的相互作用和安全策略产生冲突时，便形成了安全漏洞。因此，研究漏洞的形成机制需要深入分析程序内部的相互作用和安全策略的关系。图2是漏洞分析的基本模型。

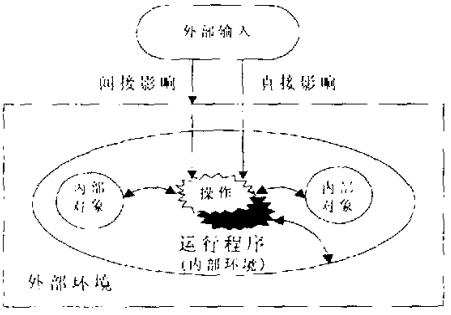
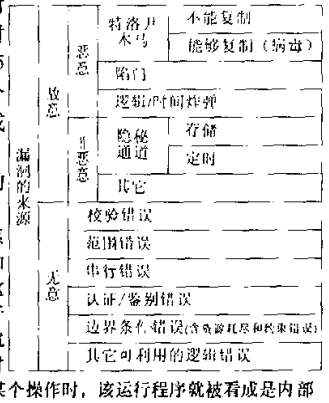


图2 程序内部的相互作用

在这个分析模型中，我们将软件的运行抽象成程序的内部对象、运行环境和外部输入之间的相互作用。它包括环境、受影响的对象、对象所受的影响、影响对象的方式以及外部输入5个部分。通过分析每个作用是否和安全策略(或程序员的假设)相违背，就可以找到产生漏洞的深层原因。



(1)环境 我们认为“系统”是由“应用程序”和“运行环境”组成的，这样，所有的被认为不属于运行程序的代码和部件就属于环境。环境是相对的，当针对运行程序中的某个操作时，该运行程序就被看成是内部环境，其它程序则认为是外部环境。内部对象以及外部输入之间的相互作用使环境具有动态特征和共享特性，这使程序的安全策略实行起来更加困难并容易发生错误。从安全策略的角度出发，执行每个操作时都需要考虑以下环境实体：环境名称、程序运行的目录、创建的临时项目、内存空间、输入的数据、存储的文件、对象属性、对象性质、网络标志等。

(2)对象 程序代码和数据空间中的任何一个元素都被认为是一个内部对象。对于一个特定的操作而言，这些对象又构成了内部环境，每个对象就是一个环境实体。这些内部对象有：命令提示、用户文件、系统相关文件、公共文件、系统目录、系统分区、堆中的数据和可执行代码、栈中的数据和可执行代码、栈中的返回地址、系统程序、用户程序、系统信息、系统函数或服务程序库、网络联接、用户名、域名、CPU时间、电子邮件、网络端口、网络数据包、内部系统名称、系统设备、地址映射等。

(3)对象所受的影响 程序内部的相互作用导致内部对象的改变，变化包括：完全取代、可写、可读、可追加、被创建、被显示、所有权被改变、权限被改变、可预测、能够动态加载和连接、被耗尽、被毁坏、被导出、被锁、被调试、被关闭、被终止等。

(4)影响对象的方式 包括：连接或绑定连接、向堆栈缓冲区拷贝数据、配置错误、使用特殊字符、修改环境变量、修改编码、改变对象名字、继承不必需的特权、提供不适当的权限、系统调用泄露敏感信息、访问相关路径、不能正确完成保护机制、使用代理绕过保护机制、使用死循环消耗资源、临界选择错误等。

(5)外部输入 用户通过外部输入直接或间接地影响程序的内部操作，控制程序的运行步骤，从而完成需要的程序功能。一般的输入类型有：环境变量、命令行选项、网络数据、临时文件、配置文件、数据文件、系统用户信息、系统调用的参数、库调用的参数、可移动介质等。

4 分类模型

漏洞研究的抽象层次不同，会对同一个漏洞作出不同的分类。例如我们最常见的“缓冲区溢出”漏洞，从最低层次上来说可能是访问校验错误；从高一些的层次看，是一个同步错误或条件校验错误；从更高的层次看，这则是一个逻辑错误。至今为止还没有一个比较完美的漏洞分类方案，包括权威的漏洞信息发布网站www.Securityfocus.com上的分类也不能让人满意。

1993年，美国海军研究实验室的Landwher等人收集了不同操作系统的安全漏洞，并按照漏洞的来源、形成时间和漏洞代码的分布位置进行了分类。尽管这些分类还不够准确，概念上存在交叉和模糊现象，但这种分类方法第一次引入了时间和空间的概念，有助于系统设计人员对安全漏洞的理解，有助于建立更加安全的软件系统。图3是Landwher的3种分类模型。

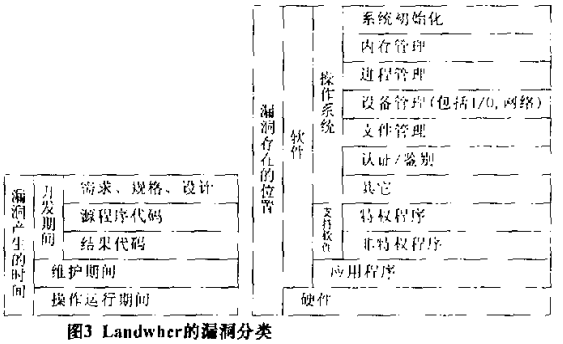


图3 Landwher的漏洞分类

普渡大学COAST实验室的Aslam从漏洞的形成原因角度对Unix操作系统的漏洞进行了深入研究，并建立了较为详细的分类模型。后来，该实验室的Krsul对此分类做了进一步的修改完善。美国南科罗拉多州大学的Knight在前人成果的基础上，增加考虑了社会和人的因素对于计算机安全的影响，使计算机漏洞的研究更加科学、全面。

图4是目前较为广泛接受的漏洞分类模型。计算机系统的漏洞被划分成两个方面的因素和4个基本类别。从漏洞的利用时效上讲，社会工程和逻辑错误形成的漏洞可以很快地产生作用，而管理策略失误和系统弱点的影响要过一段时间才能显现出来；从漏洞的利用需求来看，利用计算机本身的

漏洞比利用社会工程和策略失误的漏洞需要更多的专业技术知识。

	计算机的作用	人的作用
即时	逻辑错误	社会工程影响
一段时间	系统弱点	管理策略失误

图4 计算机漏洞的基本类型

计算机因素的漏洞分类如图5所示。

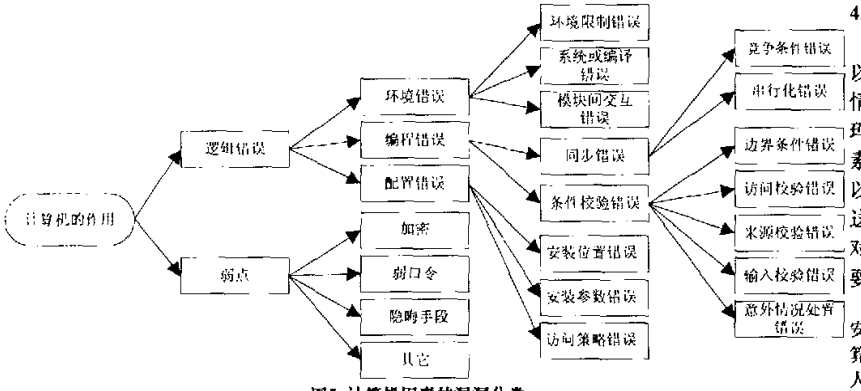


图5 计算机因素的漏洞分类

4.1 逻辑错误

逻辑错误对计算机系统的安全有直接的影响，通常是软件程序或硬件设计上的"Bug"，也是漏洞研究的主要内容。这种类型的漏洞大多是由低质量的程序代码等技术原因造成的，一般可分为环境错误、配置错误和编程错误。

(1)环境错误

环境错误是由于没有能够正确处理程序运行时环境限制造成的错误。这类错误依赖于操作环境，典型的环境错误漏洞包括：

· 操作环境的限制导致的错误；
· 由于操作系统或编译器缺陷形成的错误；
· 独立正确运行的程序模块之间发生相互作用时产生的错误；
· 异常处理时产生的意外结果。

(2)编程错误

编程错误一般是在软件开发时，由于程序设计错误、错误的需求或逻辑错误而形成的缺陷。包括：

1)同步错误，即由于指令或数据的操作顺序发生变化而产生的错误，它又可以分为两个操作之间的竞争条件错误和不正确的串行操作而引起的串行化错误。

2)条件校验错误，计算机的每个操作步骤都会受到具体条件的限制，只有满足一定的条件，系统操作才会顺序地正常进行。当条件丢失、条件表达错误时，就形成了条件校验错误。程序中的条件校验应该包括以下内容：

· 约束检查：在执行某个操作之前，系统必须保证该操作能够分配到必需的资源。例如输入/输出操作，系统必须保证用户/程序不读写其地址边界之外的文件。

· 访问权限检查：系统必须保证用户/程序能够访问到其权限范围之内的对象，这种检查机制依赖于系统的访问控制机制。

· 有效输入检查：对运行程序的任何直接输入都必须进行有效性检查。检查的内容包括：字段值相关性、语法、参数的类型和数量、输入字段、外部输入的字段或参数等。

· 主体来源检查：主体指用户、程序、主机或共享的数据对象。系统必须验证主体来源，防止自身受到攻击。

· 异常检查：系统必须能够处理由于功能模块、设备故障导致的意外情况。

(3)配置错误

从广义上讲，系统配置可以看作软件资源和硬件资源的组合。这样，计算机系统提供的应用程序和各个服务程序就是配置的一个部分。配置错误可以分为：

· 程序安装在不合适的位置；
· 程序安装时参数设置错误；
· 程序在安装时的访问权限错误。

4.2 系统弱点

系统弱点指的是系统难以克服的错误或缺陷。许多情况下，没有人能够发现或理解这种隐含的不安全因素，弱点往往要等很长时间以后才能明显体现出来。从这个角度讲，系统安全是相对的。计算机系统的弱点主要体现在以下几个方面：

· 通过隐晦手段获得的相对安全。通常情况下，我们会对计算机系统安全措施进行保密，但人们通过研究，最后总能明白它是如何工作的。所以这种隐晦的安全机制并不能从根本上保证系统的安全。

· 加密信息已经被公认为是加强计算机安全的最好方法，但加密技术本身也存在许多的缺陷，如密码的捷径、计算机的速度、缺乏足够的随机密钥等。这些缺陷会使加密的效果并不是绝对安全的。如果忽视其弱点的话，可能造成的后果将会是灾难性的。

· 口令安全是计算机安全中最关键的问题，每种形式的安全最终都趋向于依靠某种形式的口令。实际上，大量存在的弱口令和静态口令非常容易被破解。

· 人们研究发现，老化的软、硬件会影响安全问题，这是任何一个单元部件都存在的固有缺陷。

4.3 社会工程

即通过"非技术手段"对目标计算机系统进行攻击的一种方法。它可能是单位内部人员的蓄意破坏，骗取进入计算机系统的途径，或者从废弃物中寻找有用的信息等。在许多情况下，通过社会工程直接获取信息可能会更容易些，有时候社会工程可能是获取网络信息的唯一方法。社会工程方面的漏洞包括偷盗、内部间谍、信息猎取、犯罪破坏等(见图6)。

人的作用	社会工程	偷窃
		破坏
		内部间谍
		信息猎取
		其它
	管理策略失误	物理安全策略
		人员安全策略
		数据安全策略
		其它

图6 人员因素的漏洞

4.4 管理策略失误

即计算机系统的日常管理和应急措施方面的不足，例如不充分的软件备份、没有灭火器等保护设备。管理策略失误并不一定会导致入侵事件，但是，许多"天灾人祸"如天气灾害、电子毁坏、硬件故障等可能会触发这类漏洞的发生。这些容易失误的策略一般可分为：物理安全策略、数据安全

策略、人员安全策略等(见图6)。

5 讨论

目前的漏洞分类研究工作还存在以下问题：(1)分类标准和研究层次缺乏统一规范，漏洞分类存在一定程度的概念模糊和交叉重叠现象；(2)可以公开得到的漏洞信息大多数都是关于漏洞的功能性描述，如果将所有的漏洞都按分类要求进行描述，需要非常大的工作量。(3)漏洞分类和未知漏洞之间的关系还不清楚，也就是说，可以找出某类漏洞的共同特征，但还不能确定具有这些特征就一定会产生漏洞。

未来的漏洞研究工作将着重于以下目标：(1)对系统危害程度的评估。通过对受危害的系统漏洞信息的比较研究，能够得出可以量化的衡量标准。(2)建立漏洞预测模型，推测可能出现的未知漏洞。(3)在分析已知的漏洞特征的基础上，改进软件设计模型，避免在以后的软件中再出现已知的漏洞类型。

参考文献

1 Denning D E.Cryptography and Data Security.Addison-Wesley Publishing Company,1983

2 Marick B.A Survey of Software Fault Surveys.University of Illinois at Urbana-Champaign,1990

3 Bishop M,Bailey D A Critical Analysis of Vulnerability Taxonomies Department of Computer Science at the University of California at Davis,1996

4 Aslam T,Krsul I.Use of a Taxonomy of Security Faults Eugene Spafford.In Proceedings of the 19th National Information Systems Security Conference,1996

5 Krsul I.Software Vulnerability Analysis.Department of Computer Sciences, Purdue University, 1998

6 Knight E Computer Vulnerabilities http://www.securityparadigm.com/, 2000

☆☆

(上接第2页)

作的形式化描述也是百家争鸣，这样容易造成误解和歧义，也妨碍了OLAP技术的进一步发展和应用。以后对于OLAP基础理论的研究还将继续，直到被广泛认可的概念模型出现，而提高OLAP产品的性能也将成为OLAP技术研究的要点。总之，为推进OLAP技术的发展，应关注并投入较大精力于它的核心技术数据立方体领域，深入研究以下内容：

(1)研究能够被普遍接受的数据立方体概念模型，设计和实现更为灵活适用的多维数据查询语言；

(2)研究有效的数据立方体操作代数，支持统一的数据立方体操作定义及查询的优化处理；

(3)研究数据立方体操作和其他挖掘算法的集成技术，支持大规模数据的多级分析综合和联合挖掘；

(4)拓展数据立方体操作符，研究提升OLAP工具自动化性能的方法和算法，使冗余、错误倾向较多的多维数据人工分析过程更加自动化；

(5)有效处理数据立方体中的层次问题，采用合适的聚集策略提高聚集效率(如用当前技术处理全聚集、拓展选择部分数据进行聚集、考虑所应用的聚集函数类型减缓局部汇总压力等)。

参考文献

1 Marc G A Foundation for Multi-dimensional Databases.In Proc.of VLDB,1997:106-115

2 Agrawal R, Gupta A, Sarawagi S.Modeling Multi-dimensional Databases IBM Research Report,IBM Almaden Research Center,1995-09

3 Li C,Wang X S.A Data Model for Supporting On-line Analytical processing In Proceedings Conference on Information and Knowledege Management,1996:8188

4 Gyssens M,Lakshmanan L V S,Subramanian I N.Tables as a Paradigm for Querying and Restructuring.ACMPODS,1996:93-103

5 裴 健,唐世渭,杨冬青等.联机分析处理数据立方体代数.软件学报,1999,10(6):561-569

6 李建中,高 宏.一种数据仓库的多维数据模型.软件学报,2000,11(7) 908-917

7 Gray J,Chaudhuri S,bosworth A,et al.Data Cube: a Relational Aggregation Operator Generalizing Group-by,Cross-by,Cross-tab and Sub-totals.Data Mining and Knowledge Discovery,1997,1 (1):29-53

8 Anindya D,Helen T.The Cube Data Model:A Conceptual Model and Algebra for On-line Analytical Processing in Data Warehouses. Decision Support Systems,1999,27:289-301

9 Agrawal R.On the Computation of Multidimensional Aggregates.In Proc of VLDB,1996:506-521

10 Harinarayanan. Implementing Data Cubes Efficiently . SIGMOD Record,1996,25(2):205-227

11 Dar S.Answering SQL Query Using Views.In Proc of VLDB,1996. 318-329

12 Gupta A.Aggregate Query Processing in Data Warehouse Environments.In Proc.of VLDB,1995:358-369

13 Mumick I S.Maintenance of Data Cubes and Summary Tables in a Warehouse.In Proc.of SIGMOD,1997:100-111

14 Quass D,Widom J On-line Warehouse View Maintenance for Batch Updates.In Proc of SIGMOD,1997:393-404

15 Gupta H.Selection of Views to Materialize in a Data Warehouse In Proc.of ICDT,1997:98-112

16 Gupta H.Index Selection for OLAP.In Proc of ICDE,1997:208-219

17 Rafanelli M.STORM:A Statistical Objects Representation Model.In Proc.of SSDBM,1990:14-29

18 Pedersen T B.Extending Practical Pre-aggregation in On-line Analytical Processing In Proc.of VLDB,1999: 663-674

19 Jagadish H V.What Can Hierarchy Do for Data Warehouse?In Proc of VLDB,1999:530-541

20 Cognos Software Corporation.Power play 5.http /www.Cognos .com / powercubes.Index.html,1997

21 Jan J,Fu Y.Discovery of Multilevel Association Rules from Large Databases.In Proc of VLDB,1995:420-431

22 Sarawagi S.Explaining Difference in Multidimensional Aggregates In Proc.of VLDB,1999:42-53

23 迟忠先,王红新,于凤友. 数据仓库中聚集管理与导航策略.小型微型计算机系统,录用

24 Frkd&ic Gingras,Laks V S.Lakshmanan.nD-SQL:AMulti-dimensional Language for Interoperability and OLAP In Proc. of the 24th VLDB, 1998:134-145

25 Liang W,Wang H,Orlowska M E.Range Queries in Dynamic OLAP Data Cubes.Data & Knowledge Engineering,2000 (34) 21-38

26 Lehner W.Modeling Large Scale OLAP Scenarios.In Proc.of the International Conference on Extending Database Techology,1998

27 Baralis E,Paraboschi S.Materialized View Selection in Multidimensional Database. In Proc.of VLDB,1997:156-165

28 Cabibbo L,Torlone R.Querying Multidimensional Databases In Proc. of the 6th DBPL Workshop,1997:253-269

29 Li Jianzhong , Srivastava J D R. Aggregation Algorithms for Very Large Compressed Data Warehouses.In Proc.of VLDB,1999.651-662

30 Shukla A,Prasad M,Jeffrey D,et al.Materialized View Selection for Multidimensional Datasets.In Proc.of VLDB,1998:488-499

31 Kim D W,Lee Eun Jung.An Efficient Processing of Range-MIN/MAX Queries over Data Cube.Information Sciences,1998,112:223

32 Ho C T,Agrawal R.Range Qqueries in OLAP Data Cubes In Proc.of ACM SIGMOD International Conference on Management of Data, 1997:73-88

33 Pourabbas E,Rafanelli M.Hierarchies and Relative Operators in the OLAP Environment. SIGMOD Record, 2000 29(1):32-37