文章编号：1005-8451（2015）02-0013-04

信息安全漏洞分类研究

司　群
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：信息安全漏洞是造成信息安全问题的重要原因之一，是实施网络攻防的关键要素，如何及时有效发现漏洞信息，减少对社会、国家信息安全的不利影响，对安全漏洞的研究成为信息安全领域的重点，漏洞分类研究是漏洞研究的基础。本文简要介绍及总结国内外关于安全漏洞的定义和分类，并对未来的安全漏洞分类工作进行了展望。

关键词：信息安全；安全漏洞；漏洞分类
中图分类号：U29-39　　**文献标识码：**A

Classification research on information security vulnerabilities

SI Qun
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: Information security vulnerability was one of the important causes of information security problems and the key factor to implement network attack and defense. How to find vulnerabilities information and reduce the adverse impact on the society and the national information security, the research on vulnerability became the focus of information security domain, and the classification of vulnerability was the basis of vulnerability research. This paper briefly introduced and summarized the definition and classification of security vulnerabilities at home and abroad, and also prospected the future security vulnerabilities classification work.

Key words: information security; security vulnerabilities; vulnerabilities classification

随着网络信息技术在各行各业的信息系统中的普遍应用，信息系统的安全漏洞也日益暴露出来，这些安全漏洞使得信息系统面临来自网络的各种威胁，如网络攻击、黑客入侵等导致信息系统信息泄露甚至于系统瘫痪，严重危及到企业的安全。因此，研究漏洞的攻防技术，加强网络防护成为保护信息系统的关键，安全漏洞的分类研究又是研究漏洞的基础，充分掌握漏洞的含义、分类成为本文研究的重点。

1　安全漏洞定义

信息安全漏洞最早是在1982年由美国著名计算机专家D.Denning博士提出的，她是从访问控制的角度，将漏洞定义为：导致操作系统执行的操作和访问控制矩阵所定义的安全策略之间相冲突的所有因素[1]。1992年，D.Longley等人[2]从风险管理的不同角度把安全漏洞划分成3个方面描述：（1）存在于自动化系统内部控制、安全过程以及管理控制等3方面的缺陷，它可能被网络攻击者所利用，进而对关键数据进行破坏处理或者非法获得对信息的非授权访问；（2）在组织、人员、程序、物理层、硬件或软件方面存在的缺陷，它通常能够被利用而损害自动数据处理的行为或系统；（3）在网络信息系统安全中，广泛存在着其不足或缺陷。1996年，根据状态空间描述的方法，M.Bishop等人[3]为漏洞给出了其详细定义，认为“利用管理、程序或者技术上所存在的失误，攻击者得到了网络安全操作权限或未被授权的非法访问。在这些安全控制上的失误被称之为安全隐患或系统漏洞”。2006年，在《信息安全关键技术语词汇表》中，美国国家标准与技术研究所（NIST）给出的定义是：漏洞是指存在于网络信息系统、内部控制、系统安全过程或实现过程中的、可触发的或被威胁源能够攻击的系统弱点。2009年，在ISO/IEC SC27《SD6：IT安全术语词汇表》中，对信息系统漏洞的定义是：漏洞是指在某些环境中违反安全功能要求的TOE中的弱点；它是通常可以被一个或多个威胁利用的一个或一组资产的弱点；

收稿日期：2014-10-08
作者简介：司　群，工程师。

是在信息系统安全控制过程中，或者是在其环境的设计、实施中所存在的弱点、特性或缺陷。

这些关于信息安全漏洞的定义或者解释的角度虽各不相同，但是却有以下 3 个共同的特点：（1）漏洞是信息系统自身具有的弱点或者缺陷；（2）漏洞存在环境通常是特定的；（3）漏洞具有可利用性，若攻击者利用了这些漏洞将会给信息系统安全带来严重威胁和经济损失。

综合考虑中国信息安全工作实际，本文这样描述信息安全漏洞的概念：漏洞是信息技术、信息产品、信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于信息系统的各个层次和环节之中，一旦被攻击者恶意利用，就会对信息系统的安全造成损害，进而影响构建于信息系统之上正常服务的运行，危害信息系统及信息的安全属性 [4]。

2 国外研究现状

漏洞分类主要是研究者从不同角度描述漏洞，是漏洞研究的基础之一，如从漏洞的成因、漏洞被利用的技术及漏洞作用范围等进行分类研究，国外当前主流的漏洞分类主要有以下几类方法：

（1）从对操作系统研究提出的漏洞分类。如操作系统安全性分析研究 RISOS 项目将漏洞分为 7 类：不完全的参数合法性验证、不一致参数合法性验证、隐含的权限、非同步的合法性验证、不适当的身份标识 / 认证 / 授权、可违反的限制、可利用的逻辑错误。

（2）从软件错误角度的漏洞分类方法：T.Aslam 等人将漏洞分为编码错误和意外错误等。由于该分类方法存在二义性和非穷举性，I.V.Krsul 对该方法进行了扩展及修改，形成完整的分类方法，将漏洞类型分为：操作错误、编码错误、环境错误及其他错误 4 大类。

（3）多维度分类方法。如 M.Bishop 等人根据时间、漏洞成因、利用方式、漏洞利用组件数、代码缺陷和作用域 6 个维度分别进行了分类。

（4）广义漏洞分类方法。如 E.Knight 将网络漏洞分为策略疏忽、社会工程、技术缺陷和逻辑错误。

（5）抽象分类方法。如美国 MITRE 公司的通用缺陷列表（CWE，Common Weakness Emulation）提供了根据漏洞机制进行分类的方法，它将漏洞大致分为 12 大类，包括随机不充分、被索引资源的不当访问、在资源生命周期中的不当控制、相互作用错误、控制管理不充分、计算错误、不充分比较、保护机制失效、名称或引用的错误解析、异常处理失败、违反代码编写标准和消息或数据结构的不当处理等。

3 国内漏洞分类

和其他事物一样，安全漏洞具有多方面的属性，也就可以从多个维度对其进行分类，重点关注基于技术的维度。注意，下面提到的所有分类并不是在数学意义上严格的，也就是说并不保证同一抽象层次、穷举和互斥，而是极其简化的出于实用为目的分类。它可以分为 3 大类，其分别为：基于利用位置的分类、基于威胁类型的分类和基于技术类型的分类。

3.1 基于利用位置的分类

（1）本地漏洞，即需要操作系统级的有效帐号登录到本地才能利用的漏洞，主要构成为权限提升类漏洞，即把自身的执行权限从普通用户级别提升到管理员级别。

（2）远程漏洞，即无需系统级的帐号验证即可通过网络访问目标进行利用，这里强调的是系统级帐号，如果漏洞利用需要诸如 FTP 用户这样应用级的帐号要求也算是远程漏洞。例如：Microsoft Windows DCOM RPC 接口长主机名远程缓冲区溢出漏洞（MS03-026）（CVE-2003-0352）攻击者可以远程通过访问目标服务器的 RPC 服务端口无需用户验证就能利用漏洞，以系统权限执行任意指令，实现对系统的完全控制。

3.2 基于威胁类型的分类

（1）获取控制，即可以导致劫持程序执行流程，转向执行攻击者指定的任意指令或命令，控制应用系统或操作系统。威胁最大，同时影响系统的机密性、完整性，甚至在需要的时候可以影响可用性。主要来源：内存破坏类、CGI 类漏洞。

（2）获取信息，即可以导致劫持程序访问预期外的资源并泄露给攻击者，影响系统的机密性。其主要来源：输入验证类、配置错误类漏洞。

（3）拒绝服务，即可以导致目标应用或系统暂时或永远性地失去响应正常服务的能力，影响系统的可用性。主要来源：内存破坏类、意外处理错误处理类漏洞。

3.3 基于技术类型的分类

基于漏洞成因技术的分类包括：内存破坏类、逻辑错误类、输入验证类、设计错误类和配置错误类。

3.3.1 内存破坏类

此类漏洞的共同特征是由于某种形式的非预期的内存越界访问（读、写或兼而有之），可控程度较好的情况下可执行攻击者指定的任意指令，其他的大多数情况下会导致拒绝服务或信息泄露。 对内存破坏类漏洞再细分下来源，可以分出如下子类型：栈缓冲区溢出、堆缓冲区溢出、静态数据区溢出、格式串问题、越界内存访问、释放后重用和二次释放。

（1）栈缓冲区溢出，是最古老的内存破坏类型。发生在堆栈中的缓冲区溢出，由于利用起来非常稳定，大多可以导致执行任意指令，威胁很大。此类漏洞历史非常悠久， 1988 年著名的 Morris 蠕虫传播手段之一就是利用了 finger 服务的一个栈缓冲区溢出漏洞。在 2008 年之前的几乎所有影响面巨大的网络蠕虫也基本利用此类漏洞

（2）堆缓冲区溢出，即导致堆缓冲区溢出的来源与栈溢出的一致，基本都是因为一些长度检查不充分的数据操作，唯一不同的地方只是发生问题的对象不是在编译阶段就已经确定分配的栈缓冲区，而是随着程序执行动态分配的堆块。堆溢出特有的溢出样式：由于整数溢出引发 Malloc 小缓冲区从而最终导致堆溢出。

（3）静态数据区溢出，即发生在静态数据区 BSS 段中的溢出，是非常少见的溢出类型。

（4）格式串问题，即在 *printf 类调用中由于没有正确使用格式串参数，使攻击者可以控制格式串的内容操纵 *printf 调用越界访问内存。此类漏洞通过静态或动态的分析方法可以相对容易地被挖掘出来，因此目前已经很少能够在使用广泛的软件中看到了。

（5）越界内存访问，即程序盲目信任来自通信对方传递的数据，并以此作为内存访问的索引，畸形的数值导致越界的内存访问，造成内存破坏或信息泄露。

（6）释放后重用，这是目前最主流最具威胁的客户端漏洞类型，大多数被发现的利用 0day 漏洞进行的水坑攻击也几乎都是这种类型，每个月各大浏览器厂商都在修复大量的此类漏洞。技术上说，此类漏洞大多来源于对象的引用计数操作不平衡，导致对象被非预期地释放后重用，进程在后续操作那些已经被污染的对象时执行攻击者的指令。与上述几类内存破坏类漏洞的不同之处在于，此类漏洞的触发基于对象的操作异常，而非基于数据的畸形异常，一般基于协议合规性的异常检测不再能起作用，检测上构成极大的挑战。

（7）二次释放，即一般来源于代码中涉及内存使用和释放的操作逻辑，导致同一个堆缓冲区可以被反复地释放，最终导致的后果与操作系统堆管理的实现方式相关，很可能实现执行任意指令。实例： CVS 远程非法目录请求导致堆破坏漏洞（CVE-2003-0015）

3.3.2 逻辑错误类

涉及安全检查的实现逻辑上存在的问题，导致设计的安全机制被绕过。例如：Real VNC 4.1.1 验证绕过漏洞（ CVE-2006-2369 ），漏洞允许客户端指定服务端并不声明支持的验证类型，服务端的验证交互代码存在逻辑问题。

3.3.3 输入验证类

漏洞来源都是由于对来自用户输入没有做充分的检查过滤就用于后续操作，绝大部分的 CGI 漏洞属于此类。所能导致的后果，经常看到且威胁较大的有以下几类：SQL 注入、跨站脚本执行、远程或本地文件包含、命令注入和目录遍历。

（1）SQL 注入，即 Web 应用对来自用户的输入数据未做充分检查过滤，就用于构造访问后台数据库的 SQL 命令，导致执行非预期的 SQL 操作，最终导致数据泄露或数据库破坏。(2)跨站脚本执行(XSS)，即 Web 应用对来自用户的输入数据未做充分检查过滤，用于构造返回给用户浏览器的回应数据，导致在用户浏览器中执行任意脚本代码。(3) 命令注入，即涉及系统命令调用和执行的函数在接收用户的参数输入时未做检查过滤，或者攻击者可以通过编码及

其他替换手段绕过安全限制注入命令串，导致执行攻击指定的命令。（4）目录遍历，即涉及系统用于生成访问文件路径，用户输入数据时未做检查过滤，并且对最终的文件绝对路径的合法性检查存在问题，导致访问允许位置以外的文件。多见于 CGI 类应用，其他服务类型也可能存在此类漏洞。

3.3.4 设计错误类

系统设计上对安全机制的考虑不足导致在设计阶段就已经引入安全漏洞。

3.3.5 配置错误类

系统运行维护过程中默认不安全的配置状态，大多涉及访问验证的方面。（系统以不正确的设置参数进行安装；系统被安装在不正确地方或位置）

4 结束语

漏洞分类研究是一项长期并极具挑战性的课题，通过对安全漏洞的分类方法的综述研究可以看出，漏洞种类非常复杂，技术难度也相当大，所以提出一个广泛适用的漏洞分类方法是一项艰巨的任务。

参考文献：

[1]. Denning D. Cryptography and Data Security[M]. Reading, MA, USA: Addison-Wesley, 1982.

[2].Longley D, Shain M, Caell W. Information Security: Dictionary of Concepts, Standards and Terms[M]. New York, USA: MacMillan, 1992.

[3] Bishop M, Bailey D. A Critical Analysis of Vulnerability Taxonomies, Technical Report CSE-96-11[R]. Davis, USA: Department of Computer Science at the University of California at Davis, 1996.

[4] 吴世忠 . 信息安全漏洞分析回顾与展望 [J]. 清华大学学报（自然科学版），2009（S2）.

责任编辑 方 圆

（上接 P7）

关系的电子支付平台、12306 客户服务网站、客运清算系统、旅客服务系统等信息系统纳入安全方案中进行统筹考虑，并根据各系统在铁路总公司、铁路局、站段 3 级纵向系统中的安全性要求，参照本文第 3.2 节中的总体设计思路，建立图 2（见 P7）所示的铁路客票系统安全结构总图。

根据“两个中心、三重防护”的设计理念，铁路客票系统的安全管理由铁路总公司安全管理中心统一处理，身份认证及密钥由铁路总公司 PKI/CA 认证中心统一分发。

铁路客票系统在铁路总公司、铁路局和车站之间通过客票网相连，旅客服务系统在铁路局与车站间通过旅服网相连，在铁路总公司、铁路局、站边界处部署纵向区域边界安全子系统。

铁路总公司级客票核心系统、电子支付平台、12306 网站、运输清算系统之间建立横向区域边界安全防护子系统；客票网与内部服务网之间部署内网安全子系统，内部服务网与外部服务网之间部署外网安全子系统，外部服务网与银行网之间进行交叉认证，互联网边界部署外部访问控制系统，各系统内部根据不同的安全等级要求部署相应措施的安全应用环境子系统。

铁路局级客票核心系统、电话订票系统、旅客服务集成管理平台之间部署横向边界安全子系统，客票网和旅服网之间部署内部网络安全子系统，根据安全需要部署安全应用环境子系统。

车站级系统主要是各类终端设备，安全防范重点是终端接入，可以根据各类设备所属系统的安全等级，部署不同措施的安全应用环境子系统。

4 结束语

本文论述的铁路信息系统安全体系方案，是基于从上至下的一种设想，不论是对建立铁路行业信息系统的整体安全体系，还是就某一个分布式跨地区的单一信息系统安全体系的建设，都具有借鉴意义。

参考文献：

[1] 铁路信息化领导小组办公室 . 铁路信息化总体规划 [Z]. 北京：铁道部，2004，12：9-11。

[2] 沈昌祥 . 构造积极防御的安全保障框架 [J]. 网络安全技术与应用，2003（11）.

[3] 刘永华 . 网络信息安全技术 [M]. 北京：中国铁道出版社，2011，7：96-99.

责任编辑 方 圆