计算机应急响应服务中安全事件分类方法研究*

王常吉[1]，段海新[2]，吴建平[2]
（1. 中山大学计算机科学系，广东 广州 510275；
2. 清华大学信息网络工程研究中心，北京 100084）

摘 要：随着互联网的飞速发展，计算机安全事件的出现愈来愈频繁，愈来愈严重，计算机应急响应受到广泛关注。计算机安全事件分类方法的研究对于计算机应急响应体系的建设具有重要的意义。首先报告了计算机安全事件分类方法相关研究的现状。而后从计算机安全事件应急响应组的工作实践出发，提出计算机网络安全和计算机网络安全事件的形式化模型，并在此形式化模型的基础上，提出计算机安全事件的描述方法和分类方法。最后给出了两个具体的应用实例。

关键词：计算机安全事件；安全事件响应；分类法
中图分类号：TP393 文献标识码：A 文章编号：0529-6579（2005）S1-0115-04

1 研究背景

随着互联网的飞速发展和应用的普及，近年来计算机网络安全事件的出现越来越频繁，造成的危害也越来越严重。计算机应急响应引起了各国政府的高度重视，许多国家和地区纷纷成立了计算机安全事件响应组（Computer Security Incident Response Team，简称 CSIRT），譬如 FedCIRC，AusCERT，DFN－CERT，JPCERT/CC，APCERTF 和 EuroCERT，以及 FIRST 论坛。我国的应急响应工作起步较晚，但是发展迅速。中国教育与科研计算机网（CERNET）于 1999 年在清华大学成立了 CERNET 应急响应组（CCERT），为中国教育和科研行业的用户提供应急响应服务。国家计算机网络与信息安全管理中心于 2000 年成立了中国计算机网络应急技术处理协调中心（CNCERT/CC），负责国内各部门、行业等应急响应小组的协调工作。

网络安全是一个分布式的问题，安全事件通常涉及到多个管理域中的多个 CSIRT，而目前各 CSIRT 还是从局部的角度来处理安全事件，各 CSIRT 都有自己的事件处理系统和事件描述格式以及处理流程，对安全事件信息的处理大多是通过耗时且容易出错的手工方式进行。CSIRT 对计算机安全事件的响应能力不足的一个重要原因在于各 CSIRT 之间缺乏交流合作，而各 CSIRT 之间进行交流合作的前提条件是存在统一的安全事件分类标准。

分类学的创始人 Carolus Linnaeus 曾经说过“分类是科学研究的基础”。计算机网络安全事件分类方法的研究是应急响应相关研究的基础。通过对计算机网络安全事件的科学分类，可以提高 CSIRT 对计算机网络安全事件的响应能力和预防能力，促进 CSIRT 的交流协作，对于事件报告、事件响应、事件存储、事件分析、事件统计等具有重要的意义。

Amoroso[1] 提出理想的计算机网络安全事件分类方法所产生的分类应具备如下特征：

1）互斥性：各个类别之间必须没有重合部分，一个计算机网络安全事件只能归属于其中一个类别；

2）完备性：所有类别的叠加必须要能够涵盖所有可能性，任意一起计算机网络安全事件都能归类到一个类别中；

3）明确性：一起计算机网络安全事件属于哪个类别，应该是明确的，无歧义的；

4）可重复性：对一起计算机网络安全事件多次分类的结果应是一样的；

5）可接受性：分类方法必须容易理解、容易操作，能够被普遍接受；

6）有用性：分类法对于 CSIRT 的实际工作有作用。

计算机网络安全事件的最简单分类方法，就是枚举出单独的、已定义的计算机网络安全事件相关

* 收稿日期：2005－01－24
基金项目：国家自然科学基金资助项目（60203004）；中山大学青年教师科研启动基金资助项目（2004－35000－1131034）
作者简介：王常吉（1972 年生），男，副教授；E-mail：isswchj@zsu.edu.cn

的术语。D. Icove[2] 枚举了 24 个术语，Cohen[3] 则枚举了 96 个术语。之后，Cohen 从信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）出发，将计算机网络安全事件划分为毁坏（Corruption）、泄漏（Leakage）、拒绝（Denial）三大类。Schultz[4] 指出，依据 CIA 来界定计算机网络安全事件是不够的，某些计算机网络安全事件，譬如扫描、抵赖、盗用通信资源、欺诈、传播色情内容、滥发垃圾邮件等并不属于 CIA 的范畴。

Stalling[5] 依据攻击的行为，将计算机网络安全事件分成阻断（Interruption）、拦截（Interception）、篡改（Modification）、伪造（Fabrication）四大类。显然，Stalling 分类方法只考虑了信息流在传输过程中的威胁，没有考虑对网络和计算机系统的攻击。

Neumann 和 Parker[6] 根据经验数据，将计算机网络安全事件划分为八大类，即外部信息窃取（External Information Theft）、资源的外部滥用（External Abuse of Resource）、伪装（Masquerading）、恶意程序（Pest Programs）、绕过认证或授权（Bypassing Authentication or Authority）、经由不作为的滥用（Abuse Through Inaction）、授权滥用（Authority Abuse）、间接滥用（Indirect Abuse）。Neumann 和 Parker 分类方法最大的缺点是不直观，在实际中很难操作，难以被广泛接受。

Howard[7] 根据 CERT/CC 收集的计算机网络安全事件报告（1989－1995），将计算机网络安全事件归类为虚警、未授权的访问、未授权的使用三大类。正如作者所言，这种分类方法并不严格，其中未授权的使用是未授权的访问的一个子集，并且这种分类方法在实际中也很难操作。

Howard 和 Longstaff[8] 提出将一起计算机网络安全事件看作是由一次或多次攻击组成，每次攻击又是由一个或多个事件（Event）组成。可以由攻击者（Attacker）、攻击工具（Tool）、漏洞（Vulnerability）、攻击行为（Action）、攻击目标（Target）、未授权结果（Unauthorized Result）、攻击目标（Objective）七个要素来完整地描述一起计算机网络安全事件。Howard 和 Longstaff 分类方法具有很多优点，但对于 CSIRT 的实际工作来说，范围有点太宽，不易操作，并且对于大多数的计算机网络安全事件来说，“攻击者”、“攻击工具”和“攻击目标”等信息通常并不明确，受害者是难以获取到的，因此很难有效地指导受害者对攻击的处理。

综上所述，尽管国际上许多组织已经开展了计算机网络安全事件分类的相关研究，从简单的术语罗列和解释，发展到根据不同侧重点进行分类研究，继而发展到全面考察攻击的整个过程，以及从攻击行为表现特征的抽象分类。但由于计算机网络安全事件的复杂性，到目前为止，仍然没有一种科学的、得到业界广泛认同的计算机网络安全事件的分类。

2 计算机网络安全事件的形式化模型

计算机网络是自治的计算机系统互连而成的集合[8]。将网络以及网络交互过程中一切具体和抽象的对象（如用户、文件、进程、主机、路由器、TCP 连接等）均称为实体，则从计算机网络安全的角度来看，计算机网络所涉及的实体可以分为主体（Subject）和客体（Object）。网络中主动的实体，比如用户、发起访问的计算机或进程等称为主体（S），主体具有身份标识、地理位置、角色等安全属性，主体可以处于匿名的（anonymous）或者已认证的（authenticated）两种安全状态。网络中被动的实体，比如文件、数据等资源称为客体（O），客体具有身份标识、敏感级别等安全属性，客体可以处于完整性和可用性两种安全状态。主体对客体的使用方式称为访问（Access），比如读、写、修改、删除、执行等。访问的安全属性包括完整性和保密性，完整性是指客体的信息流在访问过程中不会被篡改、破坏、插入、延迟、乱序和丢失的特性，保密性是指客体的信息流在访问过程中不会泄漏给未授权的实体，或供其使用的特性。主体对客体的一个访问实例称为一次操作（Action），可以使用主体、时间（T）、访问方式、客体来描述。

网络安全政策（P）是指保证记算机网络的安全运行和网络中信息的安全所制定的规则，包括状态谓词（PS）和状态转移或访问规则（PA）。PS 是规定实体安全状态的一组谓词，包括 Anonymous/Authenticated（S），Integrity（O），Availability（O），Confidentiality（A），Integrity（A）。PA 规定哪些操作是合法的，哪些操作是禁止的，PA 可以表示为 $S\times A\times T\times O \rightarrow \{permit, deny\}$。

我们称一个计算机网络是安全的，当且仅当网络中所有的实体的状态和所有的访问都符合安全政策的规定。一起计算机网络安全事件包含一次或多次的攻击，这些攻击产生了一定的影响（Impact）或后果。一次攻击是指不符合计算机网络安全政策的一次或多次操作，如果攻击结果成功，将可能使实体的安全状态发生改变。图 1 描绘了本文提出的计算机网络安全的模型，图 2 描述了我们提出的计算机网络安全事件模型。本文可以用攻击主体（Subject）、攻击操作（Action）、攻击客体

(Object)、事件结果（Result)、事件影响（Impact）来描述计算机网络安全事件，其中攻击操作、攻击对象都可能有多个。

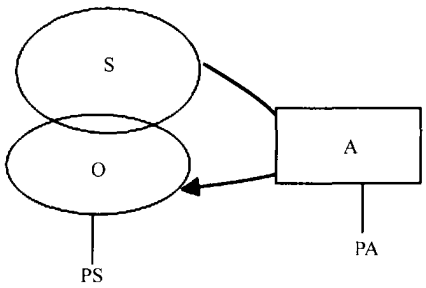

图 1　计算机网络安全模型

Fig 1　Computer network security model

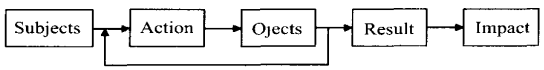

图 2　计算机安全事件模型

Fig 2　Computer security incident model

3　计算机网络安全事件的分类

基于上节所提出的计算机网络安全事件模型，我们提出依据计算机网络安全事件的五个组成要素对计算机网络安全事件进行分类，对于每个组成要素，还可以根据需要进一步细分。

3.1　基于攻击主体的分类

攻击主体是指发起攻击的实体，例如未经认证的用户（即黑客、外部用户)、认证的用户（内部用户)、病毒、蠕虫，未知的其他来源。我们还可以根据攻击主体的属性，如攻击者的国家或地区、地理位置、网络运行商、攻击者的行业（企业、教育、研究、政府、军事等）等进行详细的分类。

3.2　基于攻击客体的分类

攻击客体是指被攻击的实体，例如互联网、自治域、局域网、计算机系统、数据、服务、进程、帐号、硬件等。由于一起计算机网络安全事件可能涉及多个攻击客体，例如 Slammer 蠕虫事件是针对 SQL Server 数据库的攻击，同时也造成了 Internet 的瘫痪。因此，在实际的计算机网络安全事件分类中，可以用（直接的攻击客体，间接的攻击客体）来描述攻击客体。比如，Slammer 蠕虫事件的攻击客体是（应用，互联网)。

3.3　基于攻击操作的分类

攻击操作是指攻击主体为实现攻击的结果所采取的措施。根据攻击操作，可以将计算机网络安全事件归类为：

未授权的读：在安全政策允许之外的读操作。该操作破坏客体的保密性；

未授权的拷贝：在安全政策允许之外的拷贝操作。该操作破坏客体的机密性；

未授权的修改：在安全政策允许之外的修改操作。该操作破坏客体的完整性。

未授权的删除：在安全政策允许之外的删除操作，该操作破坏客体的可用性。

偷窃：占有目标，并在目标原存放位置不保留备份。该操作破坏客体的机密性、可用性和完整性；

窃听：读取某一通信链路或某一计算机上的输入或输出信息。该操作破坏客体的保密性。

洪泛攻击：用超出客体负载能力的方式连续访问被攻击对象。该操作破坏客体的可用性。

扫描：用以发现某范围内具有某一特征的攻击目标；

探测：用以确定特定攻击目标的某些特征；

哄骗：在网络通信中，装扮成别的实体。

利用漏洞的入侵：利用网络或系统中的漏洞，绕过系统的认证和授权，以执行安全政策所不允许的操作。

社会工程：用非技术手段获取被攻击对象的信息，例如通过收集垃圾信息、通过诱骗的手段获取口令等。

其他：以上没有包括的攻击方法。由于计算机网络安全技术和攻击技术的发展，不断地有新的攻击方法的出现，需要为此提供扩展空间。

3.4　基于事件结果的分类

根据计算机网络安全事件可能造成的结果，可以将计算机网络安全事件分成以下几类：

攻击失败：没有成功的计算机网络安全事件；

信息泄露：信息的内容被泄露给未授权访问该信息的实体；

信息破坏：未授权地改动计算机或网络中的信息；

拒绝服务：有意地使计算机或网络资源降级或阻塞；

资源盗用：未授权地使用计算机或网络资源；

授权改变：未授权地增加计算机或网络上的访问域，或者提升用户权限。

3.5　基于影响的分类

用计算机网络安全事件造成的客观影响比用攻击者的主观目的来分类更容易操作，因为在通常情况下我们没有办法得知攻击者的意图，比如黑客篡改一个公司的主页，我们很难知道他究竟是竞争对手所为，还是简单的恶作剧。

我们很难精确地计算出计算机网络安全事件所造成的影响。根据实际经验，我们按计算机网络安全事件所造成影响的性质，将计算机网络安全事件分类为政治上、经济上、时间上和声誉上共 4 类影响。对于每一类影响，可以根据影响的程度进行描述，例如无、轻、中、重、严重影响。对于经济上的影响也可以用数值来描述影响的程度。

4 应用举例

本文所提出的计算机网络安全事件的分类方法可以用于 CSIRT 归类、描述、统计以及分析计算机网络安全事件。基于 CCERT 的实际经验，以下统计信息具有重要的实用价值：

计算机网络安全事件的总数增长趋势，每周统计一次；计算机网络安全事件来源的分布，按照国家/地区的统计；每种病毒/蠕虫的变化和增长趋势和比例；攻击方式的增长趋势和比例；攻击客体的比例和增长趋势；计算机网络安全事件结果的比例和增长趋势；计算机网络安全事件影响的统计分析。

下面我们应用安全事件的分类方法来描述两个典型的网络安全事件。

4.1 Slammer 蠕虫事件

2003 年 1 月 25 日爆发的 Slammer 蠕虫事件可以用下面的方式进行分类和描述：

S=＜恶意代码＞；A=＜Exploit（SQL），Flood（UDP 1434）＞；T=＜2003 年 1 月 25 日＞；O=＜应用（SQL Server），互联网络＞；R=＜DoS，Internet＞；I=＜经济，严重＞

这样，我们就可以用文字对该事件进行简单的描述：2003 年 1 月 25 日，一种蠕虫利用 SQL Server 的漏洞感染 SQL Server，同时，该蠕虫产生的 UDP/1434 端口的流量严重影响了互联网络，导致 Internet 的拒绝服务，造成了严重的经济损失。

4.2 篡改主页

假设一名黑客在某时刻利用 IIS WebDav 的漏洞侵入了某大学的主页服务器，并篡改了主页，对该学校的声誉造成了不好的影响，同时，重新安装系统花费 2000 元人民币。于是，我们可以用下述分类方法描述该事件：

S=＜Hacker＞；A=＜Exploit（IIS WebDav），Modify＞；O=＜Web Server，Homepage＞；R=＜Corruption of Information＞；I=＜（声誉，严重），（经济，2000RMB）＞。

参考文献：

[1] AMOROSO E G. Fundamentals of Computer Security Technology [M]. Upper Saddle River: Prentice-Hall PUR, 1994.

[2] ICOVE D, SEGER K, VONSTORCH W. Computer Crime: A Crimefighter's Handbook [M]. Sebastopol: O'Reilly & Associates, Inc., 1995.

[3] COHEN F B. Information System Attacks: A Preliminary Classification Scheme [M]. Computers and Security, 1997, 16 (1): 29－46.

[4] SCHULTZ E E, SHUMWAY R. Incident Response [M]. Sams Publisher, 2003.

[5] STALLING W, Network and Internetwork Security Principles and Practice [M]. Englewood Cliffs: Prentice Hall, 1995.

[6] NEUMANN P, PARKER D. A Summary of Computer Misuse Techniques. Proceedings of the 12th National Computer Security Conference, 1989.

[7] HOWARD J D. An Analysis Of Security Incidents On The Internet. PhD. Dissertation [EB/OL] http://www.cert.org/research/JHThesis/Start.html.

[8] HOWARD J D, LONGSTAFF T A. A Common Language for Computer Security Incidents [EB/OL]. http://www.cert.org/research/taxonomy-988667.pdf.

[9] ANDREW S T. Computer Networks [M]. 3rd Ed. NY: Prentice-Hall Inc, 1996.

Research on Security Incident Taxonomy in Computer Incident Response Service

WANG Chang-ji[1], *DUAN Hai-xin*[2], *WU Jian-ping*[2]

(1. Computer Science Department, Sun Yat-Sen University, Guangzhou 510275, China;
2. Network Research Center, Tsinghua University, Beijing 100084, China)

Abstract: Security incidents are becoming more common and more serious with the flying development of Internet. There is an increasing need for taxonomy of incident to facilitate for incident reporting, incident handling, incident statistic, incident analysis and collaboration among Computer Security Incident Response Teams (CSIRT). The previous researches on the taxonomy of computer security incident are summarized firstly, the description method and taxonomy of security incident are then presented based on the formal model of network security and security incident. And two examples using the proposed taxonomy of security incident are given in the end.

Key words: computer security incident; computer security incident response; taxonomy