数字版权管理安全性评测模型研究

李润峰 马兆丰 杨义先 钮心忻
(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)
(北京邮电大学网络与信息攻防技术教育部重点实验室 北京 100876)

摘 要 根据多种现有的数字版权管理系统的设计和实现方案,提出了构成数字版权管理(Digital Rights Management,DRM)系统的最小子集和典型的系统构成。针对常见的攻击举例,设计了DRM系统安全性评价指标,指标中包含了攻击后防御强度。提出了使用层次分析法来评价DRM系统的安全性模型。在评价安全性时,依据算法、商业秘密、软件防破解能力等安全性基础进行评价。最后,使用提出的指标对现有的两种数字版权管理系统进行了评价,给出了评价的数量指标,并进行了对比评价分析,分析结果验证了评价模型的合理性。

关键词 数字版权管理,攻击后防御强度,安全性评测,层次分析法
中图法分类号 TP309 **文献标识码** A

Research on Security Evaluation Model of DRM System

LI Run-feng MA Zhao-feng YANG Yi-xian NIU Xin-xin
(Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)
(Key Laboratory of Network and Information Attack & Defense Technology of MOE, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract According to the design patterns and implementations of many existing digital rights management systems, a minimal set of DRM system and a typical DRM system were designed. Against to the usual attack, some evaluation indices were proposed in this article. One of the indices is defense intensity after attack. AHP is used in the evaluation model of the security of DRM system. To evaluate the security, encrypt algorithm, commercial secret and the ability of anti-crack were proposed as foundation of security. In the last part, two existing DRM systems were evaluated using the indices and the quantitative indicators which were given. The result of contrastive experiment indicates that the security evaluation model of DRM system is rational.

Keywords Digital rights management, Defense intensity after attack, Security evaluation, AHP

1 引言

包含音乐、视频、游戏、软件、电子书在内的数字产品越来越流行,这种流行使得数字产品被滥用,严重侵犯了数字内容提供商、数字内容分发商、运营商等市场角色的合法权益。随着这些市场角色对数字产品的版权保护意识的提高,各种商业的和非商业的数字版权系统应运而生。主要包含两种:一种是版权归属检测类技术,通过数字水印、数字指纹技术来实现;一种是注重对内容的使用控制类的版权保护技术,通过基于内容的加密等方式实现,例如方正的Apabi电子书、微软的WMRM等。

后者的显著特点是,数字内容本身与使用权限独立。数字内容持有者只有在拥有权限对象时,才能正常使用数字内容。该技术引起了研究者的广泛关注,国内学者在部分论文中对该技术进行了系统介绍[9],相当一部分学者设计了自己的DRM系统[7,8,11,12]。

多数DRM系统设计者都称自己设计的系统安全性很高,但即使已经商用的DRM系统依然存在各种各样的问题。对于使用控制类数字版权保护系统的安全性没有一个较为通用的评价标准,鉴于此,本文讨论使用控制类数字版权管理系统的安全性评价问题,并给出一个DRM系统的安全评价标准方案,以供DRM系统的设计者在设计阶段充分考虑系统的安全性问题。

2 使用控制类DRM系统通用模型

2.1 通用模型

在图1中,DRM的服务器端在内容发放之前,将内容打包加密,并把打包后的内容通过网络下载等方式发放给消费

到稿日期:2010-04-30 返修日期:2010-08-04 本文受国家973项目(2007CB311203),国家自然科学基金(60803157,90812001),国家242项目(2009A105),国家标准制定计划(20080200-T-339),国家质检公益性科研专项(10-126)资助。

李润峰(1985-),男,硕士生,主要研究方向为数字版权管理等,E-mail:runfenglee@gmail.com;马兆丰(1974-),男,博士,讲师,主要研究方向为数字版权管理、数字内容安全、计算机网络安全;杨义先(1961-),男,博士,教授,主要研究方向为密码学、计算机网络与信息安全;钮心忻(1963-),女,博士,教授,主要研究方向为数字水印、信息隐藏、隐写分析。

者。消费者在使用受版权保护的数字内容时，不能直接使用，除需要获得受保护的数字内容本身之外，还需要获取使用权限。

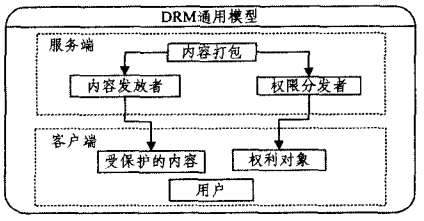

图 1　DRM 通用模型

使用控制类 DRM 系统，所包含的角色的最小子集为：

{内容打包者，权限发放者，用户}

所涉及的实体对象的最小子集为：

{原始数字内容，受保护的数字内容，权限对象}

在部分系统中权限对象又称“许可证”(license)或者许可。

2.2　关键数据

首先，在所有的使用控制类 DRM 系统中，至少包含了模型所包含的几个实体。在将媒体文件加密的过程中，涉及到两个关键数据：KeyID，Encrypt Key。它们分别表示密钥标识和加密密钥，前者用于在获取权限对象时从服务器端获取对应的解密密钥，后者用于加密内容文件，以及在消费者申请权限对象时发送给客户端，用作解密密钥。

受保护的内容文件需要在头部中包含的信息：

KeyID，URL

权限对象中至少包含以下数据：

KeyID，Encrypt Key，Rights Info

至此，以上所描述的使用控制类 DRM 通用模型是完成 DRM 保护功能的一个最小子集。

2.3　典型的 DRM 系统

实际应用的 DRM 系统一般还包括 PKI(公钥基础设施，包含 CA 系统、客户端和服务器的私钥、证书等)。

在完成权限对象的发放时需要验证客户端的身份，为了保证权限对象不被篡改，服务器端需要对权限对象进行签名。为了保障解密密钥的安全性，解密密钥需要通过某种方式加密。

一个典型的 DRM 系统呈现出来的形式也比较多样化，例如实现内容打包、权限对象发放等功能的服务器可以各自独立出现。

2.4　DRM 系统的安全性缺陷分析

即使 DRM 系统的服务端足够安全，加解密方法足够安全，数据在传输过程中足够安全，仍然不能保障 DRM 系统的安全。

权限对象中包含了解密使用的密钥，或者生成解密密钥的足够信息。当用户获得一个低权限的权限对象之后，权限对象中包含了解密的足够信息。如何防御恶意攻击者对权限对象的分析和非法解密，是一件困难的事情。中科院信息安全国家重点实验室郑晓林等[11]提出 PKIDRM 方案，采用智能卡或 USB-Key 来保护权限对象安全，但此方案要求用户购买智能卡，实现成本较高，很难实现商用化。

若设计者声称该密钥以密文形式存在，那么加密该密钥的密钥如何告知客户端。加密密钥的保护和原来密钥的保护是一个等价的问题。如果保护密钥的密钥(KEK)不是来自服务器，那么这个密钥只能由客户端通过某种方式来生成，这样便大大缩小了密钥空间。

因此，对于权限对象中加密密钥(CEK)的保护是 DRM 系统的一个安全性缺陷。

2.5　DRM 系统攻击分析举例

攻击一　在客户端没有获取权利对象的情形下还原明文，其难度相当于惟密文攻击。其难度之大，使得鲜有攻击者使用这种方法。

攻击二　利用已获取的权限对象获得加密密钥，权限对象通常以密文形式存放于本地，而加密权限的密钥必然也由本地获得，通常这个密钥会与本地信息(包括各种硬件标识、用户注册信息、用户私钥等内容)相关。这种攻击方式需要反编译客户端软件，并且获取加密密钥的密钥来源方式。FairUse4WM，freeme 等[1]软件就是通过这种方式来破解 WMRM 的。破解的前提是已经获取一个可用的许可。

攻击三：本地重放攻击。对于大多数数字版权系统而言，许可证以文件形式存放在本地。用户若获取一份若干权限的许可，在使用之前，先把这个许可备份，在使用一次之后，用备份的许可证替换掉原始的许可证。这个方法的前提是许可证以文件形式保存在本地，攻击者只需要知道存放位置即可实现，甚至不需要了解计算机知识。例如对于 Windows Media Rights Management(WMRM)系统的攻击，可以通过备份、替换一个具有隐藏只读属性的系统文件——drmstore. hds，来达到越权使用的目的。为讨论方便，本文中称这种方法为“本地重放攻击”。

3　DRM 系统安全性评价指标

3.1　抗攻击能力

3.1.1　加密打包机制与解密方式

数字内容的加密打包方式决定了它如何被解密使用，因此加密与解密放在一起来叙述。

数字版权管理的目标在于使用控制，打包加密和解密分别在服务端和客户端完成。用户使用时解密内容文件，如果通过某种方式能够获得整体的解密后的内容文件，则意味着用户可以毫无限制地使用内容文件，与 DRM 的初衷完全相悖。因此，在解密时本地是否存在整体的明文文件以及明文文件被复原的难度，是衡量 DRM 系统安全性的重要标准。

3.1.2　数据传输安全

在 DRM 系统中，客户端和服务端通常位于不同的机器或者终端上，所以包括权限对象等关键数据的传输安全也应作为 DRM 系统安全性评价指标之一。

在传输过程中，通常会使用安全套接层(Safe Socket Layer)技术来保障传输数据的安全性。传输安全的目的是保证消费者的权益，使得消费者在完成交费之后能正常获取到权限对象，这一点不同于本地安全。

3.1.3　权限对象的保护

权限对象在数字内容的使用过程中至关重要，它记录用户对数字内容使用的累计次数、使用时间等权限信息，以及正常使用数字内容所需的解密密钥。

权限对象的存储保护主要包含以下两个方面：

(1)对使用权限的完整性保护：保护使用权限不被恶意篡

改，其通常做法是由服务端使用自己的私钥对权限对象本身进行签名，而由客户端在使用之前使用服务器的公钥进行签名验证，如果发现验证不成功，则拒绝用户使用。

(2)对解密密钥的保护：在加密方法和解密方法已知的前提下，如果解密密钥在客户端以明文形式存在，则恶意攻击者可以利用密钥将数字内容复原，并不受权限信息的限制而使用内容文件。通常的保护方法是选取用户本地的硬件标识、用户注册信息、用户私钥等内容经过变换得到。

3.2 攻击后防御强度

大部分设计者虽然都声称自己的系统足够安全，但事实是，即使已被广泛应用的成熟的商用 DRM 系统，都经常被攻破。所以 DRM 系统的设计者不能假设 DRM 系统不可攻破，必须考虑被攻击后版权的受保护程度。攻击后版权可控性是 DRM 系统安全与否的一个重要评价标准。

3.2.1 版权可控性

对于不同的攻击，DRM 系统被破坏的程度可能不同，根据对版权的可控性好坏，分为以下 3 种情况：

(1)整个系统被攻破，攻击使得所有内容文件都不再受保护，可以随意分发和使用；

(2)系统部分被攻破，所有内容文件都可以在权限允许之外使用，但内容文件本身仍无法直接使用；

(3)仅针对某个客户端的单个或多个文件，文件只能在该客户端上越权使用。

3.2.2 系统可恢复性

系统设计者还应考虑到系统的可扩展性。当系统被攻破之后，通过升级系统、变换加密算法、修改加密密钥选取方式等减小系统被破解对版权所有者所造成的影响。

微软的 Windows Media Rights Management 系统对于攻击后的重要防御措施之一就是更新用户终端的个性化黑盒(individualized blackbox component，IBX)组件。

4 安全性基础

4.1 算法

对于数字版权管理系统设计方案的某个环节，它的安全性由算法保障。除非所使用的加密算法被破解，否则这个环节不可能被攻击者攻破。

这是设计方案时应该追求的一种安全性基础，如果某个方案在各个环节的安全性都依赖于算法，那么该方案就是一个安全性极高的方案。

4.2 商业机密

这种安全性依赖可称作技术壁垒，指的是设计者不公开关键环节的方案，使得攻击者根据已知信息破解的难度增加。这种方式没有被很多理论工作者提出来，但是在实际应用过程中却很常见，比如微软通过签署保密协议来保护其操作系统核心代码等。

使用的加密算法可以算作商业秘密，但不公开所使用的加密算法，通常攻击者可以根据加密方式来判断所使用的加密算法。最常见的形式是，对内容所使用的基于结构的加密方式，对保护加密密钥的密钥(Rights Encryption Key)选取方式保密。

4.3 软件防破解相关

这种安全性基础是指 DRM 系统设计者和软件开发者利用对原始代码、可执行程序等内容进行加工处理，防止攻击者通过逆向分析等方法绕过安全性保障措施来达到破解的目的。

对于攻击者而言，通过逆向工程的方法对 DRM 系统(一般是客户端)进行攻击，是代价最低的方法，因而 DRM 系统设计者应尽量避免使用这种方法来保障系统安全性。

5 DRM 系统安全性评价模型

5.1 安全性评价模型

对 DRM 系统的安全性评价采用层次分析法(Analytic Hierarchy Process，简记 AHP)来完成。根据前面的叙述，图 2 给出基本的评价模型。

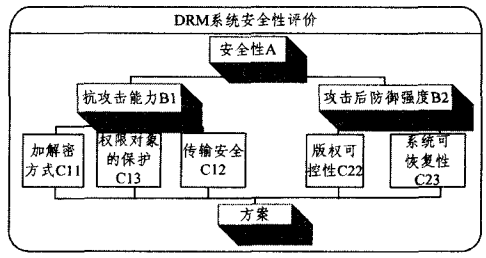

图 2 DRM 系统安全性评价模型

在评价系统安全性时，往往需要给出数值化的结果，在这里给出一个参照准则表(见表 1)。

表 1 安全参照准则表

安全性层次模型		评价准则
抗攻击能力	加解密方式	能否抵抗惟密文攻击 已知内容密钥，还原明文的难度
	权限对象的保护	能否防止篡改 能否抵御本地重放攻击
	传输安全	数据传输是否安全
攻击后防御强度	版权可控性	某个权限对象被解析，版权被破坏的程度
	系统可恢复性	系统被攻击，恢复系统功能的难易程度

在层次分析法中，确定分层模型和正互反矩阵最为关键，决定了整个模型的合理与否，而接下来的步骤则比较固定。

作为模型应用示例，根据层次分析法[2]的固有步骤，来完成一个安全性评价的参考标准：

步骤 1 使用 1－9 尺度来衡量各个因素对上层目标层的影响的大小，构造正互反矩阵。

正互反矩阵构造如下：

$$A=\begin{pmatrix}1 & 2\\ \frac{1}{2} & 1\end{pmatrix},B_1=\begin{pmatrix}1 & \frac{1}{2} & 7\\ 2 & 1 & 9\\ \frac{1}{7} & \frac{1}{9} & 1\end{pmatrix},B_2=\begin{pmatrix}1 & 2\\ \frac{1}{2} & 1\end{pmatrix}$$

矩阵 A 中，$a_{21}=\frac{1}{2}$ 表示攻击后防御强度和抗攻击能力对安全性的影响基本相同，稍弱；矩阵 B_1 中，$b_{23}^{(1)}=9$ 表示“权限对象的保护”对系统抗攻击能力的影响绝对大于“数据传输安全”。

步骤 2 根据正互反矩阵，计算权向量并作一致性检验。

由表 2 可以看出，正互反矩阵的构造通过了一致性检验。因此层次 C 的 5 个因素对于 DRM 系统的安全性的影响的大小可以使用如下权向量表示：

$W=(0.2306,0.3980,0.0382,0.2222,0.1111)$

表 2　权向量及一致性因子

矩阵	权向量	CI
A	(0.6667,0.3333)	0
B_1	(0.3458,0.5969,0.0572)	0.0109
B_2	(0.6667,0.3333)	0

对于安全性的评价，首先对方案的安全性依赖给出评价指标，在上面提到的 3 个安全性依赖中，安全性依次递减，表 3 给出了安全性的一个参考性评价指标。

表 3　防御性安全评价指标

算法	商业秘密	软件防破解能力
10	7	3

版权可控性和系统可恢复性也分为 3 个级别，见表 4。

表 4　攻击后安全性评价指标

强	中	弱
10	6	3

较强可使用 9,8 来表示，较弱可使用 4,5 来表示。

5.2　安全性评价举例

5.2.1　Windows Media Rights Management

加解密方式：使用 7 字节的 CEK 对内容进行基于结构的加密，采用微软自身设计的加密算法。安全性依赖于算法，得分：10。

权限对象的本地保护：微软宣称使用了一个全局的预设的 160 位的 ECC 密钥来保护权限对象中的 CEK。但在客户端要完成解密，客户端也必然存在或易于产生这个密钥，这个密钥的产生方式是，根据客户端的信息由服务器端生成 Indiv01.key，并传递给客户端。所以对于权限对象的本地保护还是依赖于商业秘密，得分：7。

传输安全：WMRM 作为一种方案提供给第三方，由第三方决定是否使用 https 来传递许可证，但许可证的获取一般是实时的，即：在使用数字内容时获取许可证。因此可认为其安全性等级为中，得分：6。

版权可控性：Freeme，FairUse4WM，DRMDBG 等软件都曾成功破解 WMRM 系统，但 WMRM 本身的保护机制并未被彻底破坏，破解的前提是获得一个合法的许可，然后许可对应的文件才能在本地机器上不受控制，版权在一定范围内仍可控。因此 WMRM 的版权可控性较强，得分：8。

系统可恢复性：WMRM 的各个版本均被破解过，但 WMRM 初始的设计构架能够通过更新 DRM 安全组件[10]来恢复系统。因此 WMRM 的系统可恢复性很强，得分：10。

根据上述的各项得分，WMRM 的安全性评价指标见表 5。

表 5　WMRM 安全性评价指标

加解密方式	权限对象保护	传输安全	版权可控性	系统可恢复性
0.2306	0.3980,	0.0382	0.2222,	0.1111
10	6	7	8	10

在表 5 中，第二行表示各个因素所占的权值，第三行表示 WMRM 系统各个因素的得分，容易得出 WMRM 的安全性综合评价得分：7.8500。

5.2.2　OMA DRM 2.0

加解密方式：使用 7 字节的 CEK 对内容进行基于结构的加密，采用 RC4 算法，安全性依赖于算法，得分：10。

权限对象的本地保护：OMADRM2.0 要求 CEK 使用“客户端公钥”来加密，然后使用服务器端的私钥签名，保护权限对象的完整性。在具体的实现过程中，权限对象保护依赖于“客户端公钥”。客户端私钥如何保护，私钥在客户端的存储和保护属于 DRM 实现者的商业秘密，因此得分：7。

传输安全：OMADRM2.0 中包含了在传输权限对象过程中对设备信息的验证，因此可以有效地保障数据在传输过程中的安全，得分：10。

版权可控性：由于 OMADRM2.0 在加密 CEK 时使用了客户端公钥，客户端的私钥的保存和硬件信息相关，因此 OMADRM2.0 在被破解的前提下，数字内容的版权仍在一定范围内可控，得分：6。

系统可恢复性：OMADRM2.0 针对的是手机等移动设备，系统很难通过更新来恢复，得分：6。

根据上述的各项得分，OMADRM2.0 的安全性评价指标见表 6。

表 6　OMADRM2.0 安全性评价指标

加解密方式	权限对象保护	传输安全	版权可控性	系统可恢复性
0.2306	0.3980	0.0382	0.2222	0.1111
10	6	10	6	6

在表 1 中，第二行表示各个因素所占的权值，第三行表示 OMADRM2.0 系统各个因素的得分，容易得出 OMADRM 2.0的安全性综合评价得分：7.0758。

由于 OMADRM2.0 是一个标准，基于该标准的方案有多种，因而这里选取它来进行安全评价具有很强的代表性。WMRM 系统由微软推出，并且已广泛应用，它也有很强的代表性。在比较过程中发现，商用的 DRM 系统和较成熟的 DRM 标准在权限的完整性保护方面都做得比较好。比较表 3 和表 4，WMRM 在攻击后的防御方面做得比较出色，因而得分偏高，而 OMADRM2.0 标准是由 OMA 组织制定的，它主要针对可信的移动终端，移动终端由于本身的开放性不及其它终端，在对权限对象的保护方面有先天的优势。因此，OMA 在攻击后的防御方面不必做更多的工作。

结束语　本文旨在为 DRM 系统的设计者提供安全方面的建议，比如说系统设计需要考虑到系统在受到攻击后版权的可控性和系统的可恢复性，并给出了评价模型。但对于各项指标的打分机制略显简陋。比如 OMADRM2.0 更侧重移动可信终端，而 WMRM 的应用在 PC 终端上更为广泛，软件破解的难度会因系统的开放程度而不同，在文中为简单起见做了相同处理。因此文中给出的安全性评价得分也仅供参考。

参 考 文 献

[1] wikipedia ——Windows Media DRM[OL]. http://en.wikipedia.org/wiki/Windows_Media_DRM

[2] 姜启源，谢金星，叶俊. 数学模型(第三版)[M]. 北京：清华大学出版社，2003：224-243

[3] DRM Architecture Specification, Open Mobile Alliance, OMA-Download_DRMARCH_v1_0[S]. http://www.openmobilealliance.org/

[4] OMArlin[EB/OL]. http://www.marlin-community.com

[5] Microsoft Media Rights Server. Microsoft Corp [S]. http://www.microsoft.com/windows/windowsmedia/drm/default.aspx

(下转第 56 页)

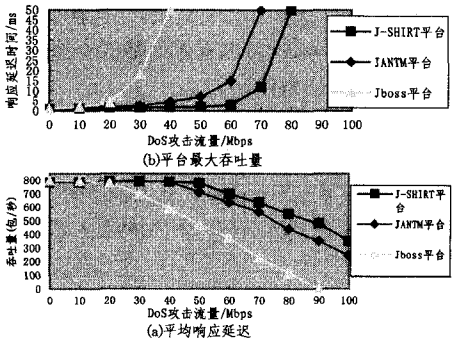

图 4 DoS 攻击下三种应用服务器平台的响应延迟时间和吞吐量的结果对比图

另外，从上述两图中可以看出，在未发生 DoS 攻击或者 DoS 攻击较弱时，本文所设计的 J-SHIRT 平台和 JANTM 平台，比起商用的 Jboss 应用服务器平台来说，其最大吞吐量较低，平均相应时间较慢。这是因为 J-SHIRT 平台和 JANTM 平台中的表决算法和容侵自治愈本身具有一定的通信复杂度，减缓了平台的响应速度。但是从上图中也可以看出，它们的通信复杂度对平台整体性能的影响不大。

以上测试实验结果说明，本文设计的 J-SHIRT 平台会增加大约 2ms 的延迟时间，并且在一个适度的网络负载下不会发生最大吞吐量下降的情况。同时也可以看出，当 DoS 攻击流量大于 60Mbps 之后，本文设计的平台最大吞吐量和平均响应延迟时间也会大幅增加。但是，总体来看，相对于其他两个测试平台，本文设计的原型平台具有更高的可靠性和生存性。

3.3 软件老化测试

本测试实验将对 J-SHIRT 平台和 JANTM 平台进行对比测试，以验证本文设计的平台是否具有预防软件老化现象发生的能力，同时也可以证明所设计的平台具有更高的可靠性和生存性。

软件老化测试实验所需的测试时间较长，通过调查研究，本次测试实验将软件老化测试时间定为 48 小时。在这 48 小时之内，客户端将向实验平台源源不断地发送数据包，平均每秒 800 个包，每个数据包大小为 2048bytes，即为平台的最高合法流量。

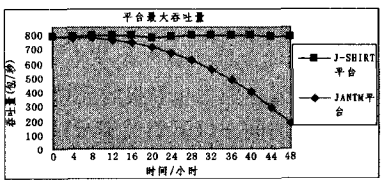

图 5 不同应用服务器平台的软件老化测试结果对比图

下面将对 J-SHIRT 平台和 JANTM 平台分别进行吞吐量对比测试。由于软件老化测试实验周期较长，以下测试实验结果只是通过 5 次反复实验测试所得，图 5 分别显示了 J-SHIRT 原型平台和 JANTM 原型平台的吞吐量的测试结果。

从图 5 中可以看出，JANTM 平台由于经过长时间不间断的运行，各应用服务器系统的资源不断消耗，资源碎片大量增加，数据污染以及数值累积错误也同时出现。最终，随着时间的推移，整个应用服务器平台不断老化，导致性能衰退，安全性降低，平台吞吐量由最初的 785 包/秒下降到 48 小时后的 180 包/秒，如果继续运行，原型平台甚至有可能面临崩溃。而本文所设计的平台针对软件老化现象有着良好的抗衰特性，在 48 小时的实验测试时间内，虽然面对高负载流量，但是依然能够保持较高且稳定的吞吐量，能够从容地面对用户的业务请求和经常发生的网络入侵，体现了本文设计的平台的高可靠性和生存性特征。

结束语 随着 J2EE 应用服务器的广泛应用，企业也对 J2EE 应用服务器系统服务的可生存性和可靠性要求越来越高，单纯地使用一种安全技术很难防范所有的攻击，本文提出一种基于 J2EE 应用服务器的容侵自治愈方法，它有效地针对容忍入侵状态中的未知状态，进行周期性恢复，使每个应用服务器防止了隐性入侵的发生，也避免了软件老化现象的出现；同时又针对具有一定连续性和成功性的入侵，引入了反应式恢复，以确保应用服务器集群能满足容忍入侵表决机制的前提条件。该设计和实现方法满足了用户对应用服务器的高可靠性和高生存性的要求。今后的工作包括：针对不同入侵和故障设计具体的自治愈算法；研究自治愈管理器中的周期性恢复时间；构建一个可信的自治愈管理器。

参 考 文 献

[1] 郭渊博，王亚弟，袁顺，等. 基于 J2EE 中间件规范的容忍入侵应用服务器及容忍入侵方法[P]. 国家技术发明专利，申请号 200710019118.9. 2007.11.20

[2] 郭渊博，马建峰. 容忍入侵的国内外研究现状及所存在的问题分析[J]. 信息安全与通信保密，2005(7)：337-341

[3] Huang Y，Kintala C，Koletis N，et al. Software Rejuvenation：Analysis，Module and Applications[C]// Proc. 25th IEEE on Fault Tolerant Computing. CA：Los Alamitos，1995：381-390

[4] Scott S. JBoss Administration and Development(Third Edition)[M]. JBoss Group，LLC，2003

[5] 袁顺，刘伟，彭亮. 容忍入侵的 J2EE 应用服务器设计与实现[J]. 计算机工程，2008，34(19)：137-140

[6] 李庆华，张胤，赵蜂. 一种基于 CORBA 分布式对象的容侵恢复策略[J]. 计算机工程，2006，32(20)：138-140

[7] 周华，孟相如，张立，等. 分布式入侵容忍系统的主动恢复算法研究[J]. 西安电子科技大学学报：自然科学版，2009，36(2)：378-384

[8] Sousa P，Bessani A N，Dantas W S，et al. Intrusion-Tolerant Self-Healing Devices for Critical Infrastructure Protection[C]// Proceedings of the 39th IEEE International. 2009：374-380

(上接第 27 页)

[6] RealNetworks，Inc.：RealSystem Media Commerce Suite Technical White Paper[S]. http://www.realnetworks.com

[7] 庄超. 一种新型的 Internet 内容版权保护的计算机制[J]. 计算机学报，2000，23(10)：1088-1091

[8] 马兆丰，冯博琴. 基于动态许可证的信任版权安全认证协议[J]. 软件学报，2004，15(1)：131-140

[9] 俞银燕，汤帜. 数字版权保护技术研究综述计[J]. 计算机学报，2005，28(12)：1957-968

[10] Microsoft Media Rights Server. Microsoft Corp [S]. http://drmlicense.one.microsoft.com/indivsite/en/indivit.asp

[11] 郑晓琳，荆继武. 一种基于 PKI 的 DRM 系统[J]. 计算机工程与应用，2006，4：128-131

[12] 李平，卢正鼎，等. 一个面向家庭网络的数字版权管理系统[J]. 计算机科学，2009，36(11)：116-119