doi :10.3969/j.issn.1671-1122.2023.10.005

基于细粒度访问控制的勒索软件防御系统设计

朱怡昕[1,2]，苗张旺[3]，甘静鸿[4,5]，马存庆[1]

（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100085；2. 中国科学院大学网络空间安全学院，北京 100049；3. 国家信息中心，北京 100045；4. 中国人民公安大学信息网络安全学院，北京 100038；5. 漳州市公安局台商投资区分局网安大队，漳州 363000）

摘　要：勒索软件是网络犯罪的主要形式之一，危害着公共社会的安全。当前的防御方案主要通过访问控制，存在授权粒度太粗、权限管理不灵活和无法正确处理异常等缺陷。为了防御勒索软件、保护主机文件资源的安全，文章提出一个基于细粒度访问控制的勒索软件防御方案，该方案包括 3 个主要功能，首先对文件系统的细粒度动态的访问控制；然后通过上下文的程序意图进行分析；最后对异常进行分级确认。文章实现了方案原型，分析结果表明，该方案可以有效拦截勒索软件的文件行为，并且能够减小勒索软件带来的损失。

关键词：勒索软件防御；访问控制；上下文分析；分级确认；细粒度

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2023）10-0031-08

中文引用格式：朱怡昕，苗张旺，甘静鸿，等 . 基于细粒度访问控制的勒索软件防御系统设计 [J]. 信息网络安全，2023，23（10）：31–38.

英文引用格式：ZHU Yixin, MIAO Zhangwang, GAN Jinghong, et al. Design of Ransomware Defense System Based on Fine-Grained Access Control Scheme[J]. Netinfo Security, 2023, 23(10): 31–38.

Design of Ransomware Defense System Based on Fine-Grained Access Control Scheme

ZHU Yixin[1,2], MIAO Zhangwang[3], GAN Jinghong[4,5], MA Cunqing[1]

(1. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*; 2. *School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049, *China*; 3. *National Information Center*, *Beijing* 100045, *China*; 4. *School of Information and Network Security*, *People's Public Security University of China*, *Beijing* 100038, *China*; 5. *Network Security Brigade of Taiwan Security Investment Zone Branch of Zhangzhou Public Security Bureau*, *Zhangzhou* 363000, *China*)

Abstract: Ransomware has become one of the most dominant forms of cybercrime, endangering the security of public society. The goal of this paper is to defend against ransomware to protect the security of host file resources, but current defense schemes using access control schemes still have defects such as too coarse authorization granularity,

收稿日期：2023-06-26

基金项目：国家重点研发计划 [E250351112]

作者简介：朱怡昕（1997—），女，四川，硕士研究生，主要研究方向为网络信息安全；苗张旺（1991—），男，河北，助理研究员，博士，主要研究方向为网络空间安全与人工智能；甘静鸿（1995—），女，福建，硕士研究生，主要研究方向为警务大数据分析技术；马存庆（1984—），男，青海，高级工程师，博士，主要研究方向为密码工程与应用、信息保护技术。

通信作者：朱怡昕 903480254@qq.com

inflexible permission management, and inability to properly handle exceptions. In this paper, a ransomware defense scheme based on fine-grained access control, which includes three main functions, firstly, fine-grained dynamic access control to the file system was proposed. Secondly program intent analysis by context. Finally hierarchical confirmation of exceptions. This paper implements a prototype of the scheme, which can effectively intercept the file behavior of ransomware after analysis and reduce the damage caused by ransomware.

Key words: ransomware defense; access control; contextual analysis; hierarchical confirmation; fine-grained

0 引言

勒索软件是一种恶意代码，它通过加密用户文件来向用户索要高额赎金。近年来，随着加密货币的兴起使得支付手段变得更隐秘，促进了勒索软件的进一步发展。因此，勒索软件已经成为网络犯罪中主要的形式之一。勒索软件对主机文件资源造成了较大威胁，而勒索即服务的存在使得发起勒索攻击变得更容易[1]。

对大多企业而言，勒索软件的攻击已经成为重大威胁[2]。勒索软件报告[3]显示，大多企业在防御勒索软件方面不够重视，使得职工没有足够的防御意识，远程办公的工作者和设备易受到勒索软件攻击，勒索软件会通过攻击远程主机和设备，窃取企业的重要文件资源，导致企业遭受巨大损失。

为了防御勒索软件的攻击并保护主机上的文件资源，目前开放操作系统使用的方法是通过面向账户或单个应用程序的访问控制[4]来实现。但是，该方案存在不足，如访问控制粒度过粗、授权方案不灵活以及没有考虑用户处理异常的能力。为了解决上述问题，本文提出一个基于细粒度访问控制的勒索软件防御方案。该方案对当前的访问控制方案的3个主要功能进行了改进：1）对文件系统进行细粒度访问控制；2）对白名单应用程序进行行为监控，检测其是否存在异常行为；3）对异常情况进行分级，并提供云端监管协助用户处理异常。

1 相关工作

目前对勒索软件的研究主要分为分析型和对抗型[5]两类。分析型研究侧重于勒索软件的内部结构和行为，勒索软件与主机操作系统的交互方式等。这种研究可以进一步分为静态分析和动态分析[6]。勒索软件的对抗型研究被划分为预防、检测和早期防御3类。

1.1 勒索软件分析

勒索软件的生命周期从恶意代码传播开始，一直到受害者收到赎金通知[7]。生命周期如图1所示，可描述为以下6个环节：1）利用代码下载、邮件附件或驱动下载来帮助恶意软件进入受害者的设备；2）恶意程序在主机中植入并收集记录主机的信息；3）勒索软件联系其C&C（Command and Control）服务器获取加密密钥[8]；4）勒索软件开始搜索具有特定扩展名的用户相关文件，如pdf、docx、xlsx、pptx和jpg等；5）将目标文件移动并进行加密；6）向受害者发送包含赎金要求的声明。

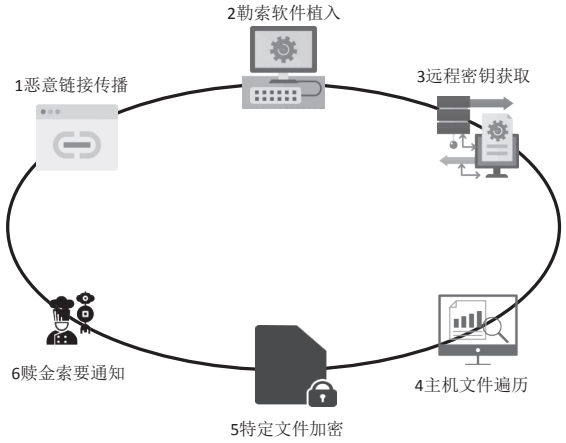

图 1 勒索软件生命周期

针对勒索软件的分析可划分为基于静态特征的分析和基于行为的分析两类。静态分析是在不运行其代码的情况下从源代码和二进制字符串中提取结构特征[9,10]的分析方法。静态分析是安全且高效的方法，但无法应对被混淆的勒索软件。动态分析是在程序执

行期间对其进行行为分析。MCINTOSH[11]等人将勒索软件的行为进行分析发现勒索软件在对文件的操作上存在频繁访问文件夹、大量创建读写等操作，即修改尽可能多类型的文件，使得良性应用程序行为变化。

1.2 勒索软件对抗

勒索软件对抗研究分为预防、检测和早期防御3类。勒索软件的预防是通过预防文件资源等被损坏来保护潜在受害者免受勒索攻击，例如，通过限制和监控对加密工具的访问等方式降低被勒索软件感染的风险，但已存在自带加密工具的勒索软件[12]。PRAKASH[13]等人建议停用负责创建卷影副本的VSSVC.exe服务，使得用户更多地参与管理阴影副本，容易出现人为错误。

勒索软件的检测分为基于误用的检测和基于异常的检测[1]两种。基于误用的检测是基于勒索软件的静态特征和行为特征，例如，“CryptoDrop”[14]利用目标文件的静态特征来识别这些文件因勒索攻击而发生的变化，但基于误用的检测无法检测未知攻击。基于异常的检测通过对正常事件进行建模以检测未知攻击，但存在较高的假阳性[15]。

勒索软件的早期防御是在勒索软件加密文件或造成重大损害之前拦截勒索软件的攻击行为，目的是保护主机的文件资源不被损害。其中操作系统使用访问控制机制来限制应用程序对主机文件资源的使用，从而对勒索软件的攻击进行防御。

1.3 访问控制

访问控制是一种安全机制，用于授权、拒绝用户或系统实体访问资源数据。访问控制是计算机安全的基础，它通过限制用户在系统中的行为和权限来保护数据和系统资源的安全。

在工业应用中，为了保护用户隐私和数据安全，许多开源系统采用基于用户的访问控制（User-Based Access Control，UBAC）或基于角色的访问控制（Role-Based Access Control，RBAC）的安全模式。这些安全模式是假设主要威胁来自其他用户或恶意攻击者，因此通过该访问控制方案可以实现对勒索软件的早期防御。然而，随着计算机、智能手机和平板电脑的普及以及大数据时代的发展，当用户在设备上运行勒索软件时，勒索软件可以获取用户的权限和对用户资源的操作权限，在单用户环境中造成主要的网络安全威胁。因此，基于用户或角色的访问控制方案目前已无法有效应对勒索软件的攻击。

Android和iOS等移动操作系统使用基于应用程序的访问控制方案。一般情况下，当应用程序第一次请求访问某文件资源时，系统将提示用户确认授权。但应用程序的请求信息可能会误导用户，使得授权的应用程序操作行为是违背用户本意的。基于应用程序的访问控制方案虽然在一定程度上改善了系统的安全性，但该方案同样存在访问控制粒度太大、授权不灵活以及异常处理不恰当等问题。

2 方案分析

本章针对勒索软件早期防御中的访问控制方案进行分析，总结现有方案存在的缺陷。

2.1 方案介绍与分析

勒索软件通过多态和混淆等技术逃避常见的安全软件签名匹配检测[5]。基于机器学习的动态检测具有高检测率、低假阳性的优势，但它更关注检测勒索软件而不是保护目标文件。基于机器学习的检测方法在单独使用时频繁报错，但在辅助其他安全防御措施时（如利用收集到的上下文数据），可以达到不错的防御效果[16]。此外，与用户相关的一些因素也导致勒索软件反复出现，例如，用户不能始终监控后台的文件系统活动[11,14]，用户意识不到勒索软件的攻击已发生，或发现问题时损失已无法挽回[17]。

计算机和移动设备的普及使得用户能在自己的设备上单独访问许多资源。虽然Android和iOS等移动操作系统试图通过为每个应用程序引入基于权限的访问控制来改善勒索软件防御现状，但Windows等桌面操作系统往往采用基于角色的访问控制，而应用程序之

间并没有隔离[18]。开放式架构的设计加上应用程序权限管理的缺乏，导致在桌面和服务器平台上勒索软件攻击数量的激增[19]。由于开放操作系统缺乏合适的访问控制机制来应对勒索软件的攻击，只能使用针对一般恶意软件的方式来防御勒索软件[4]，因此，当下的问题是如何设计一个访问控制实现对用户资源文件的管理。

2.2 问题总结

基于访问控制的勒索软件防御方案的缺陷有授权粒度太粗、权限管理不灵活和异常处理不恰当。

2.2.1 授权粒度

访问控制系统应反映用户的意图，以预防勒索软件的入侵[13]。但访问控制的授权粒度太粗，容易造成用户做出违背意愿的授权，即权限请求发起后，程序获取同类所有访问目标的所有权限，或程序无访问同类所有目标的任何权限。例如，正常使用主机时，用户需要用photoshop.exe对图片p1.jpg进行修改，此时如果是首次访问该图片，那么操作系统会发起应用程序的操作权限请求，用户一旦授权，photoshop.exe对所有图片资源就有了所有操作权限，包括删除、移动等，而用户的本意是利用photoshop.exe对图片p1.jpg进行修改。如果获得用户授权的应用程序是恶意程序，就可以利用这样的授权方案进行违背用户意图的操作，甚至发起勒索软件攻击。

2.2.2 权限管理

访问控制系统对权限管理不灵活，主要体现在对程序意图不评估，导致不能及时发现程序的异常行为。如果授权应用程序具有某文件资源的权限，就默认应用程序对已授权资源的所有操作都是良性的，因此勒索软件通过篡改良性应用程序，可以在后台对文件系统发起攻击。例如，photoshop.exe获取了对所有图片资源的权限，但由于用户点击了某恶意链接，使得恶意代码在后台将photoshop.exe修改为一个本质是恶意程序的“良性程序”。这样的“良性程序”可以利用没有被操作系统收回的权限进行勒索攻击，而访问控制系统会对该“良性程序”的异常行为视而不见，既不反馈给用户，也不加以制止，直至勒索行为发生，造成重大损失。

2.2.3 异常处理

目前的防御方案让用户处理所有的异常，却忽略了用户的防御水平是参差不齐的。用户由于不能一直监控程序的后台操作，因此对异常行为可能无法理解，甚至直接忽略，导致无法及时拦截勒索软件的攻击行为，损失加重。例如，只会使用图表编辑的文员在办公，潜伏在主机上的勒索软件向用户要求对某敏感文件资源的权限。该用户由于对勒索行为不够了解，随意点击了同意，允许了勒索软件对敏感文件资源的写入、删除等操作。此时尽管防御系统发起异常警告，但用户误以为是普通的程序运行，允许了勒索软件继续操作，软件加密文件资源的同时，还会通过企业的内网感染其他设备，最终给企业造成重大损失。

3 方案设计

为了解决当前勒索软件防御方案存在的问题，更好地保护主机的文件资源，本文设计了基于细粒度访问控制的勒索软件防御方案。如图2所示，该防御方案包含权限管理模块、程序意图分析模块和异常处理模块，对前文总结的3个问题做出了改进。

本方案的主要工作流程如图3所示，首先监控程序的所有行为，并通过白名单细粒度地管理程序的行为；然后对异常的文件行为和程序意图发起警告；最后系统对异常进行分级处理，以保证文件资源的合法使用，防御勒索攻击。下面将详细介绍每个模块的功能，并介绍使用的技术路线与实现手段，分析其可行性。

3.1 权限管理模块

权限管理模块使用细粒度的访问控制对文件资源的使用进行管理，以尽早拦截异常的应用程序文件行为。该模块通过拦截应用程序对资源任何未授权的访问，以保证文件资源的合法使用，同时通过细粒度的设置白名单的方式实现对文件资源的细粒度管理。

与现有防御方案不同的是：1）本文所提方案中的

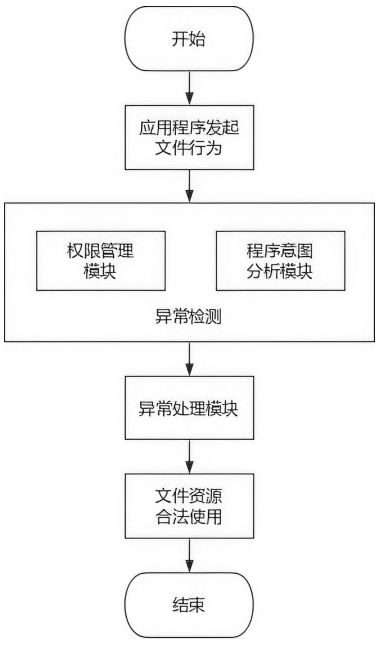

图 2 方案设计

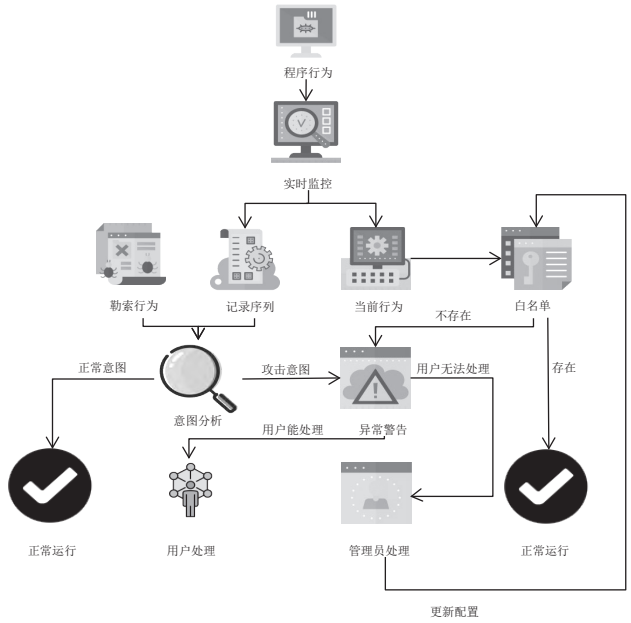

图 3 防御系统的工作流程

细粒度指的是当前应用程序对当前某一对象的某一操作，避免了用户做出违背自身意愿的授权；2）本文所提方案的访问控制是在应用程序完成授权操作后立即收回权限；3）本文所提方案设置细粒度的白名单，白名单中记录的是良性应用程序的可访问的资源和允许的操作。

如图 4 所示，当应用程序 test1 发起对 protec1.txt 文件的删除操作的权限请求，与白名单比对失败后向用户发起授权请求，若授权失败就阻止该程序的操作。

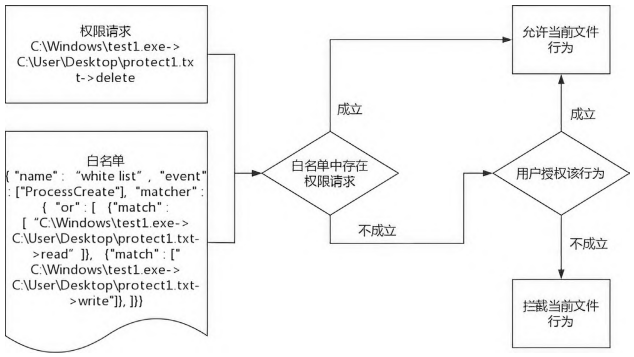

图 4 权限管理模块案例

权限管理模块需要实现的主要功能是文件行为的监控和连接。该模块通过开发内核驱动程序监控输入输出请求包（I/O Request Package，IRP），实现对终端所有进程的监控和拦截，即实现对文件行为的监控和过滤。白名单使用的是 json 格式的规则文件，能够实现文件操作与白名单的快速比对。

3.2 程序意图分析模块

白名单的设置可以缓解频繁的授权请求，但也带来了新的安全隐患。白名单中的程序拥有敏感文件的操作权限，如果该程序被篡改为勒索软件，那么系统将无法识别正在发生的可疑行为。因此需要对应用程序的意图进行分析，以尽早拦截异常的文件操作，防御勒索软件攻击。程序的行为能够反映它的意图，因此程序意图分析模块使用应用程序的行为序列来分析程序意图。与现有勒索软件的异常检测不同的是：1）该模块针对每个程序的行为序列进行分析，而不是对主机所有程序的行为进行建模；2）该模块预先在沙箱中收集程序的正常行为序列，作为标准行为序列；3）行为匹配使用相似度，时间空间开销更小。

如图 5 所示，程序意图分析模块利用当前应用程序的行为序列与标准行为、勒索行为分别进行匹配，将得到的相似度进行比较，得出程序意图是否异常的结果。

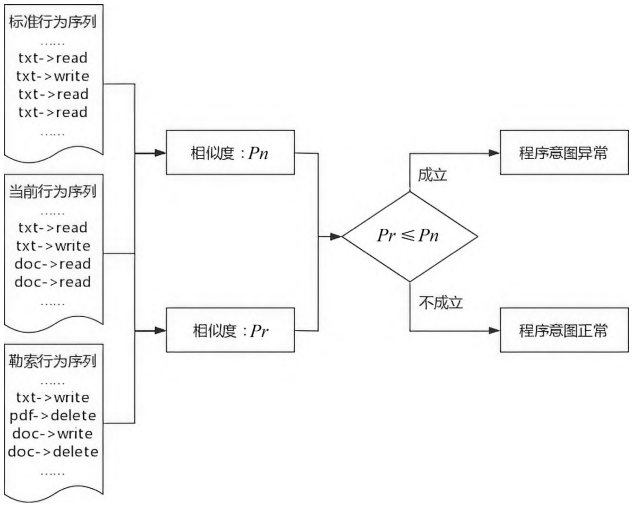

图 5 程序意图分析模块案例分析

程序意图分析模块利用Windows sandbox对应用程序的行为进行收集，可以记录程序执行期间对文件系统的操作，记录的格式为文件类型-操作类型。同时，该模块采用行为匹配的方式来计算相似度，通过上下文分析应用程序的意图及时发现异常程序，防止勒索行为的发生，保护文件资源的安全。

3.3 异常处理模块

异常的处理结果也会影响系统的总体防御效果。异常处理模块考虑用户无法处理异常的情况，将服务器端作为远程管理员为用户提供技术支持。该模块将异常进行分级，让用户处理力所能及的异常，让管理员处理更复杂的异常，实现对异常的正确及时处理。与现有的异常处理方案不同的是：1）将异常分级处理，而不是由用户处理所有异常；2）服务器具有云端监管功能，对用户主机提供技术资源支持，配置主机白名单。

如图6所示，该模块记录用户的身份标识，判定用户是否能处理当前异常。对于无法处理的异常上报给服务器，服务器根据异常的处理结果对主机的白名单等进行管理更新。

异常处理模块中需要实现安全信道和异常分级。安全信道需要保证用户与远程管理员之间传输消息的不可抵赖性、机密性和完整性。因此该模块采用AES加密消息，RSA加密对称密钥和签名的方式，并通过

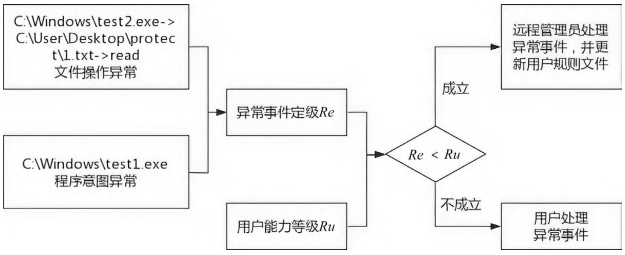

图 6 异常处理模块案例分析

TCP连接的方式保证通信安全。该模块首先对用户的处理能力和异常的复杂度进行定级；然后将当前异常事件的等级与用户的能力进行匹配，判断用户是否能够处理；其次系统将用户无法处理的异常信息上报服务器，避免用户做出错误的决定，造成风险；最后根据异常处理结果对主机规则文件更新，使规则文件更适配用户使用主机，降低异常警告的频率。

4 实验与结果

本文所提系统由权限管理模块、程序意图分析模块和异常处理模块3个功能模块实现，并构建了一个用于测试系统可用性的威胁模型。

4.1 实验环境

本文所提方案原型是基于内核驱动开发，运行环境为Windows10，Intel Core i7-6700 CPU，8 GB RAM。在测试环境中，存放的文件主要包含文档文件与图片文件两类。其中，文档文件包含docx、pptx和pdf等类型，图片文件包含png和jpg等类型。在实验环境下，选择文档处理程序WPS.exe和图片处理程序XiuXiu.exe作为良性程序样本，构建威胁模型作为勒索软件进行攻击。

4.2 威胁模型

鉴于勒索软件的文件操作特性，本文设计具有遍历功能与加密功能的威胁模型。由于本文所提系统的设计基础是应用程序的文件行为，因此在威胁模型的构建中不考虑注册表行为、网络传输行为等异常行为，本文实验中将该威胁模型命名为ransom.exe。该威胁模型采用的攻击方式为：在后台遍历当前文件下的所有文件，并将文件改为随机的字符，造成文件乱码，使得文件信息无法被正常查看。

4.3 实验结果

原型在客户端实现了实时监控、白名单功能，可以捕获执行文件操作的程序、资源路径和操作类型。对于异常的文件行为可以在捕获后立刻拦截。

在客户端发生异常时，通过弹窗警告，用户可以云端联系向远端管理员获取帮助。云端管理员与客户端通过安全信道进行信息传输，云端管理员将处理结果返回给客户端后立刻执行，并记录日志。

4.4 运行展示

方案原型部署在用户端和服务器端，实现了基于细粒度访问控制的勒索软件防御系统的功能。本节展示了方案原型的前端界面。如图7所示，用户可以查看原型运行中拦截记录的详细信息，包括时间、进程名称和操作目标等。

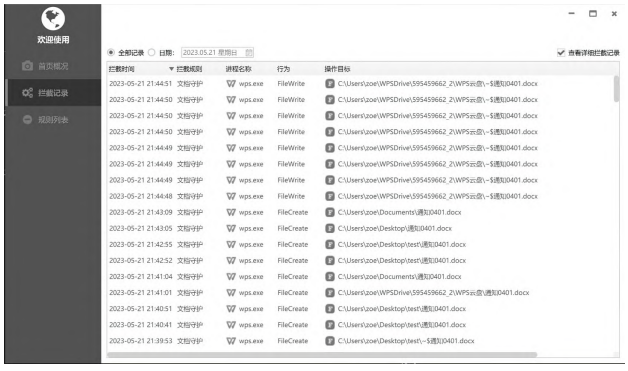

图 7 用户端界面

当异常的文件行为发起时，系统将会进行异常警告，阻止当前的异常操作。如图8所示，当记事本对没有权限的txt1.txt进行强制操作时，系统将发起警告。

图 8 异常文件行为的警告界面

服务器端管理员的使用界面如图9所示。管理员既可以为用户配置规则文件，也可以对用户能力和用户白名单等数据进行管理。

图 9 服务器端界面

5 结束语

本文针对现有勒索软件防御方案进行分析，发现了3个缺陷。通过对缺陷分析，提出了基于细粒度的访问控制的解决方案。该方案通过对文件细粒度管理、程序意图分析与检测以及云端监管来协助用户处理异常的方式，保护文件资源的合法使用，实现对勒索软件攻击行为的防御。本文实现了方案原型，经过测试与分析，该方案能够抵御勒索软件的攻击，保护主机的文件资源，当异常发生时，系统可以快速有效地处理防御勒索软件对主机的攻击。

参考文献：

[1] MELAND P H, BAYOUMY Y F F, SINDRE G. The Ransomware-as-a-Service Economy within Thedarknet[J]. Computers & Security, 2020, 92: 101762-101780.

[2] GUO Chun, CHEN Changqing, SHEN Guowei, et al. A Ransomware Classification Method Based on Visualization[J]. Netifo Security, 2020, 20(4): 31-39.
郭春，陈长青，申国伟，等 . 一种基于可视化的勒索软件分类方法 [J]. 信息网络安全，2020，20（4）：31-39.

[3] FORTINET. The 2021 Ransomware Survey Report[R]. Sunnyvale: Fortinet，1290667-0-0-EN，2021.

[4] MCINTOSH T, KAYES A S M, CHEN Y P P, et al. Dynamic User-Centric Access Control for Detection of Ransomware Attacks[J]. Computers & Security, 2021, 111: 102461-102476.

[5] AL-RIMY B A S, MAAROF M A, SHAID S Z M. Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions[J]. Computers & Security, 2018, 74: 144-166.

[6] DARGAHI T, DEHGHANTANHA A, BAHRAMI P N, et al. A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features[J]. Journal of Computer Virology and Hacking Techniques, 2019, 15(4): 277-305.

[7] LEONG R, BEEK C, COCHIN C, et al. Understanding Ransomware and Strategies to Defeat it[J]. White Paper (McAfee Labs), 2016, 16: 1-16.

[8] ZIMBA A. Malware-Free Intrusion: A Novel Approach to Ransomware

Infection Vectors[J]. International Journal of Computer Science and Information Security, 2017, 15(2): 317−325.
[9] ZHANG Pengtao, TAN Ying. Hybrid Concentration based Feature Extraction Approach for Malware Detection[C]//IEEE. 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE). New York: IEEE, 2015: 140−145.
[10] WANG Ping, WANG Y S. Malware Behavioural Detection and Vaccine Development by Using a Support Vector Model Classifier[J]. Journal of Computer and System Sciences, 2015, 81(6): 1012−1026.
[11] MCINTOSH T R, JANG−JACCARD J, WATTERS P A. Large Scale Behavioral Analysis of Ransomware Attacks[C]//Springer. 25th International Conference, ICONIP 2018. Berlin: Springer, 2018: 217−229.
[12] ANDRONIO N, ZANERO S, MAGGI F. Heldroid: Dissecting and Detecting Mobile Ransomware[C]//Springer. International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer, 2015: 382−404.
[13] PRAKASH K P, NAFIS T, BISWAS S S. Preventive Measures and Incident Response for Locky Ransomware[J]. International Journal of Advanced Research in Computer Science, 2017, 8(5): 392−395.
[14] SCAIFE N, CARTER H, TRAYNOR P, et al. Cryptolock (and Drop It): Stopping Ransomware Attacks on User Data[C]//IEEE. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). New York: IEEE, 2016: 303−312.
[15] KAUR R, SINGH M. A Survey on Zero−Day Polymorphic Worm Detection Techniques[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1520−1549.
[16] UGARTE−PEDRERO X, GRAZIANO M, BALZAROTTI D. A Close Look at a Daily Dataset of Malware Samples[J]. ACM Transactions on Privacy and Security (TOPS), 2019, 22(1): 1−30.
[17] KHARRAZ A, KIRDA E. Redemption: Real−Time Protection Against Ransomware at End−Hosts[C]//Springer. International Symposium on Research in Attacks, Intrusions, and Defenses. Berlin: Springer, 2017: 98−119.
[18] SERVOS D, OSBORN S L. Current Research and Open Problems in Attribute−Based Access Control[J]. ACM Computing Surveys (CSUR), 2017, 49(4): 1−45.
[19] CONTI M, GANGWAL A, RUJ S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective[J]. Computers & Security, 2018, 79: 162−189.

电子科技大学计算机（网安）学院算法与逻辑团队在 Information and Computation 上发表研究成果

近日，电子科技大学计算机科学与工程学院（网络空间安全学院）算法与逻辑团队2021级博士生彭俊强以第一作者身份在CCF理论计算机科学领域A类期刊Information and Computation（I&C）上发表题为“Further Improvements for SAT in Terms of Formula Length”的论文。论文第二作者和通讯作者为肖鸣宇教授。

该论文研究了著名的布尔可满足性问题（SAT问题）的算法与计算复杂性，得到该问题精确求解中，以问题输入CNF公式的总长度L为度量的当前最佳运行时间上界，改进了十余年前CHEN和LIU于2009年给出的结果。

SAT问题是第一个被证明的NP完全问题，在计算复杂性理论里扮演着重要角色，也在人工智能、运筹学和电子设计工程等众多领域中有着重要且基础的应用。该经典问题的运行时间上界在过去几十年里一直被深入研究。本论文作者通过设计新的分支算法，并运用测量治之（Measure–and–Conquer）的分析技术深入分析，最终取得了这项突破。

彭俊强同学为电子科技大学计算机（网安）学院2021级直博研究生，他从本科阶段开始进入算法与逻辑团队学习，在肖鸣宇教授的指导下从事SAT及其相关问题的研究工作。在博士学习的前两年已经发表两篇CCF A类和一篇CCF B类论文。

算法与逻辑团队由欧洲科学院院士、新西兰院士Bakh Khoussainov教授和肖鸣宇教授共同组建，周毅副教授、郝东副教授和许超助理教授、日籍Toru Takisaka副研究员等多位老师参与。该团队致力于基础理论研究，以探索算法难题和解决重要的科学问题为宗旨，激发和培养学生及青年老师对算法和基础理论的兴趣，为算法及相关研究方向感兴趣的师生提供一个交流平台。算法与逻辑团队目前重点关注的研究方向包括：算法设计与分析（包括近似算法、参数算法、精确算法、在线算法等）、逻辑、图论与图算法、组合优化、算法工程、机制设计与算法博弈论、形式化方法与认证等。

算法与逻辑团队以科研育人为首要任务，培养出了众多优秀的学生。近两年本科生第一作者在WWW、IJCAI、SODA、COCOON、Discrete Mathematics等CCF A类会议和重要刊物上发表5篇论文。除论文外，算法与逻辑团队学生还在多项科技竞赛中斩获重要奖项，仅2023年上半年就获得2023年华为软件精英挑战赛全球总决赛冠军，2023年全国大学生数学竞赛（非数学类）全国第一名，IEEE极限编程竞赛世界第四名（第五次进入世界前十名）等。（来源：电子科技大学，https://news.uestc.edu.cn/?n=UestcNews.Front.DocumentV2.ArticlePage&Id=90399）