Software Engineering and Applications 软件工程与应用, 2022, 11(5), 1058-1063
Published Online October 2022 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2022.115108

Hans汉斯

浅析透明加密技术在受控环境下的运用

李珊珊

中国人民解放军96843部队50分队技术室，甘肃 兰州

收稿日期：2022年8月17日；录用日期：2022年10月10日；发布日期：2022年10月19日

摘　要

在确保安全的前提下，数据加密造成信息数据在流通过程中不透明的现象是操作人员触发违规越界行为的主要动因，这种行为往往会对内网信息系统造成灾难性的后果。本文针对上述现象，提出透明加密思想，重点解决信息数据在横向沟通过程中安全性与便捷性之间的矛盾，对实现受控环境下的数据安全有重要参考意义。

关键词

数据安全，透明加密，受控环境

A Brief Analysis of Application of Transparent Encryption Technology in Classified Environment

Shanshan Li

PLA's of Technical Office of Unit 50 of 96843, Lanzhou Gansu

Received: Aug. 17th, 2022; accepted: Oct. 10th, 2022; published: Oct. 19th, 2022

Abstract

On the premise of ensuring security, the opacity of information data in the circulation process caused by data encryption is the main motivation for operators to trigger illegal cross-border behavior, which often has disastrous consequences for classified information systems. Aiming at the above phenomena, this paper puts forward the idea of transparent encryption, focusing on solving the contradiction between security and convenience of information data in the process of horizontal communication, it has an important reference significance for realizing data security in classified environments.

文章引用: 李珊珊. 浅析透明加密技术在受控环境下的运用[J]. 软件工程与应用, 2022, 11(5): 1058-1063.
DOI: 10.12677/sea.2022.115108

Keywords

Data Security, Transparent Encryption, Classified Environment

1. 引言

传统的加密手段在确保信息数据安全性的同时，也会显著降低信息数据的横向流动性，加密数据虽通过隐匿其原有的真实信息实现了保护数据的目的，但无法保证数据在存储和流通过程中处于受控状态。且在这种加密模式下，数据安全过度依赖于密码管理，用户友好性较差，密码管理不慎对数据安全造成灾难性的后果也难以避免。

透明加密技术综合运用了信息安全管理和访问控制模型两种理念，是针对操作人员违规越界行为难以杜绝、用户密码管理实现困难、数据在保密环境下流通性差等现象而设计出的一种全新概念的数据安全防护手段。

2. 当前内网受控环境下数据安全采用的主要方式

由于数据业务的高价值性，现实中存在大量通过构建内网受控环境为确保业务信息能被有效保护的现象。当前，内网受控环境既要考虑经济适应性、用户友好性、环境适应性，又要统筹好业务流动与安全防护之间的矛盾关系，大体可分为以下三种方式。

2.1. 以密码技术为核心的加密认证方式

当前，内网受控环境广泛采用基于加密手段的数据安全方法，用户从启动计算机到接触到相关数据中的每个环节均存在不同程度的密码/口令加密认证过程。这种技术适应性好、使用成本低、数据隔绝成效最为明显，只需要妥善解决好用户密码管理问题即可有效保障数据安全。

但由于实际操作过程中，口令认证环节往往不止一次，同时管理多个复杂口令的难度较大，经常出现用户忘记相关密码而导致数据无法被正常解读、用户多次输错密码造成信息系统被锁死、用户为便于使用刻意降低密码强度或者使用明文记录密码等安全问题。

单从加密认证技术来分析，数据安全还面临加密技术被反向运用(如勒索病毒恶意加密用户数据)，数据流动无法追踪(恶意用户非法存储加密数据)，加密方式被技术破解(如暴力破解、字典攻击、量子计算)等现实威胁。

2.2. 以管理手段为核心的保密工作管理

各级事业机构的保密部门可以通过强制规范密码强度、控制信息数据在保密环境下的流转范围、定期进行安全保密检查以及逐步升级信息安全防护手段等方式用以保障数据安全。

但由于信息数据具备的价值本质上会影响其产生流通属性和业务属性，若执意控制信息数据的流通，则会降低相关业务的实现价值，增加业务执行人员的不信任感和不确定性。若增强信息数据的流动效果，虽能使业务执行人员更加明确相关数据的现实意义，但会扩大涉密信息流通范围，造成数据泄露风险。

通过保密工作管理手段的方式能有效解决大多数内网保密环境下的数据安全威胁，但由于在业务办理过程中安全保密部门和业务部门的密切配合较难实现，管理投入与生产效能之间难以实现平衡。

2.3. 以访问控制技术为核心的信息加固手段

现阶段，受控环境广泛采取了基于属性的访问控制技术手段确保信息安全(以“水印系统”为典型代表)。数据文件在内网信息环境中，往往会基于用户身份、设备硬件标识、信息类型、信息状态、信息密级、修改时间等属性进行安全标识，再根据特定的访问控制策略进行信息管理。

安装此类信息加固手段后，信息系统所有指定类型的文件都是强制加密的，加密信息在内网受控环境中进行交流传输不需要操作用户进行任何特殊处理，极大地增强了加密信息的横向流动性，一旦文件离开使用环境，相关信息难以从乱码状态恢复成有效明文，从而实现保护受控信息的效果。

但由于现实业务的双向流动性，导致了基于属性的访问控制技术难以在数据双向流动的过程中同时实现机密性和完整性。采用访问控制技术进行信息加固后，仍需要配套的解码软件(如“脱水印软件”)将受控信息解码成明文，以方便完成业务流动。也就是说，以属性管理为核心的信息加固手段无法满足受控环境下的数据流动业务需求。

3. 透明加密技术能有效保证当前受控环境下的数据安全

透明加密技术是近年来发展较为迅速的一种文件加密技术，该技术不会影响使用者原有的正常操作习惯，在相应信息系统中自动加密受控数据，一旦受控数据离开内网受控环境就无法得到相应的有效解密服务，可在提升信息系统安全性的同时，达到保护文件的效果[1]。

3.1. 内网受控环境下的透明加密技术设计核心理念

数据透明思想：保持使用者原有操作习惯，将数据加密过程尽可能对用户隐藏，确保信息数据在受控的内网环境中始终保持可控状态，并且能够有效阻止信息数据被非法存储、复制、传播或者销毁。

通过建立内网信息平台与互联网预警体系的联动机制，旨在使流动到受控环境中数据完全可控，脱离内网受控环境后的相关数据被互联网预警体系定向回溯。该联动机制可自动根据相关数据的重要程度而决定存储流失数据计算机是否销毁数据、格式化硬盘或反向加密。进而减少因受控数据被违规法扩散而造成数据的泄露危害。

3.2. 内网受控环境下实现透明加密理念的关键技术

Windows 系统环境下的数据透明加密技术迄今为止主要经历了 APIHOOK 应用层透明加密技术－文件过滤驱动加密技术－内核级纵深沙盒加密技术等三次技术迭代[2]，逐步解决了容易破译、可靠性差、加解密速度慢等前期问题。但该技术不仅无法适用于国产信息平台，且难以完整构建内网受控环境下可信的数据防护体系。我们参考微软公司透明加密技术发展历程，可将国产信息平台内网受控环境透明加密关键技术整理如下。

访问控制技术：基于属性的访问控制模型(ABAC 模型)是一种使用属性作为构建基石定义并实施访问控制，为解决分布式应用可信关系提供上下文相关的细颗粒度的访问控制模型[3]。属性加密技术基于 ABAC 模型设计理念而实现，可使原始的信息数据被加密后，关于客体(即资源，如文件、数据、服务、系统设备等)的指向性特征依旧存在，主体(对客体实施访问行为的实体，如用户、计算机、网络等)对加密数据的访问会被严格明确的规范所限制，用户只能访问所属权限范围内的相关数据。

加密认证技术：包括基于密码学的安全协议、身份认证、消息确认、数字签名、密钥管理、密钥托管等技术，是保护大型网络传输信息安全的唯一实现手段，可以很小的代价，为信息系统提供一种强有

力的安全保护[4]。

零信任架构理念：信息安全管理理念下衍生出的一种以身份为中心进行访问控制模型，对访问控制进行了范式上的颠覆，引导安全体系架构从“网络中心化”走向“身份中心化”。旨在消除在信息系统和服务中实施准确访问决策时的不确定性的一系列概念、思想和组件关系(体系结构)。为了减少不确定性，“零信任”在网络认证机制中减少时间延迟的同时更加关注认证、授权、以及可信域。访问规则被限制为最小权限[5]。

边界告警技术：边界处采取技术措施或部署防护设备，如代理、网关、路由器、防火墙、加密隧道等，进行边界的监测、管理和控制，检查往来信息和协议，将恶意和非授权的通信排除在外，达到御敌于内网之外的目的。这里的边界，既指信息系统的外部边界，比如内部网络与互联网的连接处，也指信息系统的内部边界，比如不同网络域之间的连接处[6]。

3.3. 透明加密技术实现受控环境下数据安全的强大优势

一是有效解决了易用性与安全性之间的平衡悖论。当前，内网受控信息系统尽管普遍制定了十分规范的操作规程，但由于易用性过差导致操作人员对信息系统违规操作的现象仍无法避免。业务流动的双向流通性，必然带来涉密信息系统存在与外界受控环境接触的风险。透明加密有效解决了传统数据防护手段里人机交互不友好的短板，使加密认证过程不影响用户正常操作习惯，又降低了网络安防人员运维压力，显著提升了受控数据的横向流动性，可有效减低因操作人员违规操作而带来的数据泄露风险。

二是更加适应数据安全技术现实发展趋势。传统的防御理念往往告知我们，对信息系统实现物理隔离就可以确保信息安全。这种防御理念只有建立在操作人员完全可信、操作地点完全可控、相关设备完全可靠且操作人员完全严格安装操作规定进行信息处理的环境下(如机要办公)才能实现，现实中除专用系统外其他通用性强的信息系统很难达到人员、地点、设备和操作完全严格的状况。透明加密技术不仅承认网络内部和外部都存在威胁，而且还假定攻击是不可避免的(或可能已经发生)。因此，它会持限制用户只能访问完成工作所需的内容。这有效地防止了用户(包括潜在的攻击者)在网络中横向移动并访问任何不受限制的数据，更加适应数据保护的现实环境。

三是深度贯彻全周期数据防护理念。使用透明加密技术后，相关的信息数据在诞生时就被透明加密系统绑定属性值，数据明文(即原始数据)在客体(即资源，如文件、数据、服务、系统设备等)中一直保持加密状态，这种加密状态由用户认证授权设备、计算机硬件信息、软件运行状态以及网络状态等多个要素共同决定。若当前计算机满足数据被解析成明文的条件，信息数据就可以对用户显示出来。若当前计算机是互联网设备等不符合受控环境的信息设备，相关数据不会被显示或者解析出来，如果遇到需要破坏客体(即资源，如文件、数据、服务、系统设备等)进而强行搜寻或破解加密数据的情况，数据就会采取销毁、告警或破坏文件格式等相关操作。从而确保信息数据在全生命周期中的安全。

4. 一种受控环境下实现透明加密技术的解决方案

基于上述受控环境下透明加密技术的设计思想，我们脱胎于现有透明加密产品，提出一款以确保受控数据内部流通为前提的内网透明加密技术解决方案(如图 1)，旨在即确保受控数据能在内网环境下高效流通，又能低成本地有效降低受控数据不慎扩散后造成的风险隐患。

4.1. 内网受控环境透明加密技术整体设计实现方案

该方案由安装透明加密系统的涉密计算机、用户认证授权设备、涉密设备授权中心以及网络预警服务器四个部分组成。

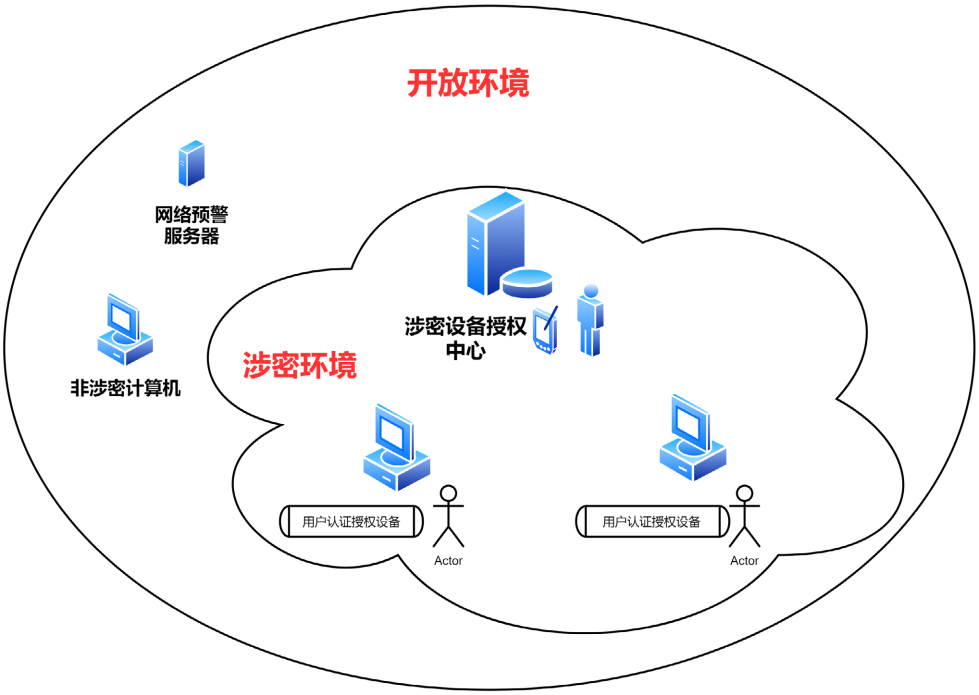

Figure 1. Solution of intranet transparent encryption technology
图 1. 内网透明加密技术解决方案

涉密计算机：用户操作的主体，安装有透明加密软件系统，可根据此计算机的所属部门、涉密等级、当前合法用户、MAC 地址以及文件来源、文件等级、网络状态等要素信息产生自动处理涉密文件的要素属性，进而在不影响用户原有操作习惯的前提下自动生成、修改、销毁、读取、隐藏、加密、解密涉密文件，以达到保护涉密文件的目的。

用户认证授权设备：一方面作为认证设备，对操作者、所连接的计算机以及该计算机所处的网络环境进行三方认证，确保当前用户有权限操作内网涉密计算机处理其用户权限内的涉密文件；一方面作为存储设备，是内网受控环境下涉密文件唯一的移动存储介质，可在允许的涉密计算机之间传播涉密文件，增强涉密文件的横向流动性。

涉密设备授权中心：存储有主体－客体之间的访问控制策略，是执行用户－涉密计算机、涉密计算机－用户认证授权设备、用户－涉密文件之间加密认证环节的重要决策方。可对涉密数据进行全生命周期的安全认证，并能降低涉密计算机加解密开销，减少加密认证环节对用户操作友好度的影响，亦可作为计算机审计系统，记录并及时阻止用户层面对涉密数据的非法操作，有效减少数据泄露的可能和安全管理人员的运维开销。

网络预警服务器：作为边界防护的补充设备，可在用户认证授权设备被互联网计算机读写时及时接收到互联网预警信息，为安全管理人员提供内网受控环境下的数据溯源依据，并激活用户认证授权设备被动防御策略(如格式化用户认证授权设备内部存储介质、反向加密非法计算机内置硬盘、上传非法计算机特征信息等)，有效辅助安全管理人员及时止损，降低涉密文件流失造成的安全危害。

该解决方案下产生的数据客体可以在涉密计算机和非涉密计算机之间流通，这种流通过程只能依赖于用户认证授权设备中的文件存储器。数据客体在非涉密环境中时刻属于受控范围，不能被用户使用脱密技术解析成明文文件，一旦检测出用户有违规操作现象，用户认证授权设备将强制执行数据防护措施(如反向加密计算机硬盘，向网络预警服务器发出告警信息，销毁涉密载体等)。

4.2. 透明加密系统中实现数据安全的技术原理

所有的信息数据均由安装有透明加密系统的涉密计算机产生，数据终端始终被用户认证授权设备认证，每项由该计算机产生的客体数据均被相应的用户认证授权设备进行非对称加密。当其他用户接触到相关客体后，若当前用户拥有涉密设备授权中心给予的用户权限，则该用户可以解析客体数据，否则客体数据不能被用户发现。存储到用户认证授权设备中的涉密文件虽然允许在非涉及计算中部分显现，但用户的违规越界行为会立即触发用户认证授权设备的防护策略(如反向加密、网络告警、设备销毁等)。由于涉密设备授权中心可以分区授权用户设备，所有用户认证授权设备的丢失不会影响整个透明加密系统的安全。

该解决方案不局限于传统 Windows 系统下基于内核级纵深沙盒加密技术[7]的透明加密技术实现，通过构建国产自主可控平台下的系统内核级沙箱加密环境，使合法操作用户始终处于重定向的安全桌面内，确保受控涉密文件在内网环境下能有效防范恶意代码或恶意人为操作对涉密文件的违规操作，进而构建出完整的信息安全管理体系，从而使实现数据安全成为可能。

4.3. 内网受控环境下透明加密技术的功能实现

用户认证授权设备具备执行数据防护措施的能力，一旦用户认证授权设备检测出用户有违规越界行为，就会立即触发安全防护策略。此时，受控环境(如互联网环境)下的网络预警服务器就会收到告警信息，对数据危害行为进行数据溯源。相关溯源日志也将通过互联网手段传送至内网安全管理人员互联网邮箱中(内网受控环境与互联网环境始终处于物理隔离状态)，指导内网安全管理运维人员更改涉密设备授权中心认证策略，使违规用户在受控环境下的相关操作也被立即受限。

该解决方案能有效防范用户层面的人为越界行为，依托自动化运维的涉密设备授权中心着重解决了因人员动态调动而导致的涉密文件难以有效重定义的管理难题，通过指定唯一移动存储介质的方式极大降低了涉密文件流传到互联网后造成的数据危害，可在完成透明加密设计理念的同时，实现数据安全。

5. 结束语

由于受控环境固有的封闭性，数据流动受限会诱发用户违规使用数据脱密手段传输涉密信息。透明加密技术充分考虑了信息数据的业务属性，在确保操作友好的前提下，有效降低了受控数据泄露的可能性，为受控环境下的数据安全提供可靠保障。

参考文献

[1] 周道明, 钱鲁锋, 王路路. 透明加密技术研究[J]. 信息网络安全, 2011(12): 54-56.

[2] 陈北陵. 透明加密技术发展[EB/OL]. https://blog.csdn.net/a15995989443/article/details/122259369, 2021-12-31.

[3] 徐云峰. 全国网络安全与执法专业丛书: 访问控制[M]. 武汉: 武汉大学出版社, 2014.

[4] 段钢. 加密与解密(第 4 版) [M]. 北京: 电子工业出版社, 2020.

[5] 王斯梁, 冯暄, 蔡友保, 等. 零信任安全模型解析及应用研究[J]. 信息安全研究, 2020, 6(11): 966-971.

[6] 朱大立. 信息安全保密常识百问[M]. 北京: 金城出版社, 2017.

[7] 许小萱. 浅析源代码防泄密中的沙盒加密技术[EB/OL]. https://blog.csdn.net/anbingsoft/article/details/110823763, 2020-12-07.