基于逻辑口令锁的整盘加密新方案

赵福祥[1,2] 庞辽军[2] 王育民[2]
(西安外事学院信息工程学院 西安 710077)[1] (西安电子科技大学ISN国家重点实验室 西安 710071)[2]

摘 要 随着可调加密模式的引入,整盘加密相对于文件级加密提供了更优化的抗攻击能力,既能保持加密数据的机密性,还能实现对磁盘结构元数据的隐蔽。然而,现有的磁盘加密方式在拓宽机密数据覆盖的同时也加深了对磁盘主密钥的依赖。被单个密钥所加密的数据量提高后,就引出了密钥管理的难题:怎样使密钥的获取便利与如何减小计算和存储负荷。为解决这类问题,提出一个基于逻辑口令锁的整盘加密方案,并对其进行安全性和性能分析。分析发现,该方案具有比现有磁盘加密方式更高的安全性与效率。

关键词 计算机安全,磁盘加密,可调分组密码,密钥管理
中图法分类号 TP393.08,TP309.7,TN918.4 **文献标识码** A

New Scheme of Full Disk Encryption Based on Logical Password Lock

ZHAO Fu-xiang[1,2] PANG Liao-jun[2] WANG Yu-min[2]
(School of Information Engineering, Xi'an International University, Xi'an 710077, China)[1]
(The National Key Laboratory of ISN, Xidian University, Xi'an 710071, China)[2]

Abstract Full disk encryption, which not only holds the secret of encrypted data but also conceals the meta data of disk structure, can give the more optimized defense against attack than file-system-level encryption as the tweakable enciphering mode introduced. However, the current disk encryption will raise dependence on the master key while broadening the coverage of confidential data, because the mount of data encrypted by single key will also be increased, Thus it causes the key distribution problems whether the master key can be derived conveniently and how the workload of computation and storage will be reduced. To solve this, a scheme of full disk encryption based on slide password lock was described and an analysis of environment and efficiency on the scheme was given.

Keywords Computer security, Full disk encryption, Tweakable block cipher, Key management

1 引言

在计算机安全中,磁盘加密是密码学的一项重要应用,它为存储数据提供了不可缺少的机密性。依据威胁模型(TM, threat model),整盘加密能提供比文件系统加密更为优化的安全目标。这是因为:首先,它对元数据进行加密,通过扩大加密数据覆盖,从而可取得比文件加密方法更全面的整体安全性;其次,它基于磁盘扇区加密,可实现与文件管理无关的透明加密[1]。由于整体安全防御性能的提高,使得磁盘加密能在易遭盗窃的单机系统上独立实现[2]。

整盘加密的需求促成了可调加密新模式的理论研究,提出了CMC[3],EME[4],EME*[5],XCB[6],HCTR[7],HCH[8],PEP[9],TET[10],HEH[11]等算法。其解决问题的关键就是克服水印攻击(watermarking attack),以消除加密算法中可能的结构性痕迹残留,使攻击者无法实施结构分析攻击。理论上的进展只解决了实际系统中的部分问题。一个完整的系统当然不可缺少相应密钥管理与之相协调[12],并且加密算法的机密性也主要来自密钥中信息的不确定性,因而密码系统中对密钥的防护就显得至关重要。尤其对于防御单薄的单机系统,在无法借助其它安全工具时,密钥的防护就显得更为困难。因为它不仅要提供密钥的机密性,而且要提供抵御篡改的可靠性,还要保持获取和管理的易用性以及不添加设备的经济性。上述的整盘加密算法均不能解决这些问题。

鉴于以上考虑,本文提出基于逻辑口令锁的整盘加密方案,建立了一个单机使用与可调密码模式相称的整盘加密系统。第2节讲述逻辑口令的密钥管理;第3节通过改进密钥管理提出了一个新的基于逻辑口令锁的整盘加密方案;第4节对方案的安全性、工作性能及效率进行分析;最后根据本方案的研究总结出了以软件方法增加系统灵活性,使硬件与软件相结合的结论。

2 逻辑口令锁的密钥管理

使用逻辑口令锁管理磁盘密钥,是为了和现有的计算机安全管理相衔接。借用登录计算机账户的安全信息,在系统中设置逻辑口令锁,来控制磁盘的加密主密钥的获取。作为完整的密钥管理设计,除实现这一功能外,还必须完成必要的

到稿日期:2009-11-26 返修日期:2010-02-22 本文受国家自然科学基金(No. 60803151)资助。
赵福祥 博士生,主要研究方向为网络与信息安全,E-mail:zhaofuxiang@yahoo.com.cn;**庞辽军** 博士,教授,主要研究方向为密码与信息安全;**王育民** 博士生导师,IEEE高级会员,主要研究方向为密码与信息安全。

其它管理功能，包括账户的添加与删除、密钥的丢失恢复等。

2.1 账户的添加、修改与删除

添加账户时，用户需向系统管理员注册，由系统管理员以注册用户的账户口令的参数建立映射，即属于该账户的逻辑口令锁，然后隐藏相关的安全参数。修改账户就是修改其逻辑口令锁的映射，而删除账户就是删除映射。

2.2 丢失口令的恢复

丢失口令的恢复是以建立问题与答案关联的逻辑口令锁实现的，它的操作方式与常态下主密钥种子获取方式相同，仅把问题与回答的映射替换为口令映射。恢复主密钥后再由管理员重新设置其账户口令。

2.3 逻辑口令锁的方案框架

常工作状态下，用户登录后首先需要获取磁盘主密钥，它是方案中重要的环节，因为其使用频度最高。方案框图如图1所示。左边输入是用户注册的账号 ID_A 和口令 PW_A，右边是用户登录的账户 ID_x 和口令 PW_x，TM_A 为时间序数。两对应参数比较的结果将构成一个逻辑开关函数，其返回值作为磁盘主密钥的种子 MK_{seed}，再由 MK_{seed} 生成磁盘主密钥 K_M，最后以预设加密分组模块检测 K_M。若成功，则进入磁盘加/解密状态，失败则向用户提示账户密码错误。

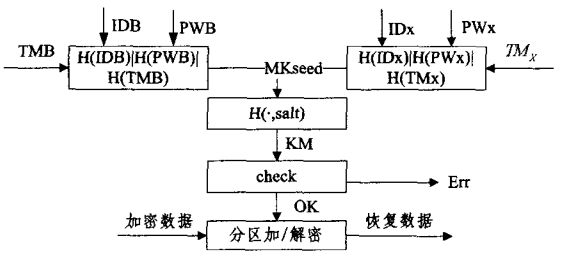

图1 基于逻辑口令锁的整盘加密方案

3 基于逻辑口令锁的整盘加密

为取得合理安全性所需满足的要求，基于逻辑口令锁的整盘加密将采用以下方法。

3.1 双层密钥获取结构

所谓双层密钥获取结构就是在多账户口令和主密钥之间建立两级获取关系的映射，前一级映射是不同账户口令信息获取后的开启逻辑锁映射，后一级映射为获取共有磁盘主密钥的映射。当账户的秘密信息正确时，则获取磁盘主密钥；当信息错误时，得到的就不再是磁盘主密钥。然后通过验证该密钥的正确性来区分它们。

让磁盘主密钥与账户的信息相分离的处理方法，将使磁盘主密钥的安全再不会受到账户信息泄露的直接影响，既容纳多个账户，也为加入与删除及密钥恢复等管理维护操作提供了基础。由于生成磁盘主密钥需要一个共享的秘密种子参数，双层密钥获取结构还为从账户信息到共享秘密种子的建立映射以及秘密参数的隐藏提供保证。

3.2 基于账户口令的逻辑口令锁

磁盘主密钥种子是由系统管理员 A 设置的一个秘密参数，是一对模素数的代数和。设 α,β 为模素数，其中 M 为模数。而主密钥种子为

$$MK_{seed}=(1-\left\lceil\frac{h(ID_x)-h(ID_A)}{M}\right\rceil)\alpha+\left[(1-\left\lceil\frac{h(PW_x)-h(PW_A)}{M}\right\rceil)\otimes(1-\left\lceil\frac{h(TM_x)-h(TM_A)}{M}\right\rceil)\right]\beta \quad (1)$$

式中，ID_A 为 A 的身份，PW_A 为对应口令，TM_A 为时间序数，ID_x 为登录者的身份，PW_x 为登录者口令，TM_A 为时间序数，$h(\cdot)$为密码哈希函数。当确定了磁盘主密钥种子 MK_{seed} 后，再以某个加盐的密码哈希函数 $h(\cdot,salt)$获取磁盘主密钥

$$K_M=h(MK_{seed},salt) \quad (2)$$

然后以此加密验证密钥的数据 D_{check}，得到相应密文 C_{check}，并在磁盘中注入 D_{check} 和 C_{check}，最后删除 K_M。当主密钥建立后，其它用户 B 可向系统管理员 A 注册账户 ID_B 和口令 PW_B，系统管理员 A 为其建立相对主密钥获取式：

$$MK_{seed}=(1-\left\lceil\frac{h(ID_x)-h(ID_B)}{M}\right\rceil)\alpha+\left[(1-\left\lceil\frac{h(PW_x)-h(PW_B)}{M}\right\rceil)\otimes(1-\left\lceil\frac{h(TM_x)-h(TM_B)}{M}\right\rceil)\right]\beta \quad (3)$$

获取密钥后通过密钥验证数据，判断其所取密钥的正确性，若正确则返回磁盘主密钥，若错误则返回账户密码错误提示。

3.3 安全参数的拆分与隐藏

可登录的计算机系统都设有账户口令等机密参数的安全防护区，只需对一对模素数做扩展性防护。由于磁盘主密钥并不保存在磁盘中，通过式(2)生成需要的这些参数，因此对其隐藏就显得格外重要。方案中包括了这些参数的拆分隐藏与反程序跟踪陷阱设置。除防止攻击者扫描窃取外，由于磁盘的磁道本身易于损坏，还需兼顾系统对它们的可靠获取。为此，方案采用了基于(t,n)门限的拆分与隐藏来实现秘密的多份额可靠备份。令存在一个消息 M，简单的秘密拆分方法是生成与原消息相同数位的随机数 $S_1\cdots S_{n-1}$。然后计算出 S_n，即存在以下关系

$$S_n=M\oplus(\bigoplus_{i=1}^{n-1}S_i) \quad (4)$$

则消息 M 就可以拆分成为 n 个分量 $S_1\cdots S_n$，通过变换式(4)，可得如下等式

$$M=(\bigoplus_{i=1}^{n}S_i) \quad (5)$$

式中每个分量都具有同等的作用，任何分量值的变化都会改变 M 的输出位。由于磁盘存储的风险，并不能保证 n 个分量中每个都被毫无差错地获取，实际要根据扇区数据损坏率 p 设计基于(t,n)门限的接入方案，所谓(t,n)门限可以通过一个$t-1$阶多项式来构造。

$$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0 \quad (6)$$

式中，$a_1\cdots a_{t-1}$为随机常量，而 a_0 用作实现(t,n)门限的秘密。通过方程(5)中不同二维平面的点采样计算，则得到一个 n 点坐标序列$(x_i,f(x_i))$。若要恢复这 $t-1$ 阶多项式的相关系数，则需代入 n 序列中任意 t 个点，任何少于 t 个点的计算都不足以恢复秘密来实现(t,n)门限的功能。通过对主密钥的拆分和隐藏，提高了主密钥的接入门限，使主密钥抗主动攻击和磁盘损坏能力都有所增强。

4 方案分析

4.1 安全性分析

本方案是一个配套的密钥管理方法，其安全性分析应该分别针对外部攻击者和内部攻击者。

定理 1 本文提出的基于逻辑口令锁的整盘加密能够有效地抗击外部攻击。

证明：所谓外部攻击者是不具有账户的攻击者，主要攻击方法是扫描磁盘从而获得磁盘主密钥，但可证明这样的攻击是不可实现的。首先，构造(t,n)门限的$t-1$阶多项式的系数$a_1\cdots a_{t-1}$为随机常数，攻击者若无法获取这组常数，则无法构造出这样的多项式，也无法恢复磁盘主密钥；其次，当攻击者已知这样的生成多项式时，设系统的初始数据占据了磁盘的n个分区，恢复磁盘主密钥需要t个数据，而这t个数据随机分布在n个分区中，则找全恢复磁盘主密钥的数据的概率为$P=1/n^t$。当n取值足够大时，P足够小。

定理 2 本文提出的基于逻辑口令锁的整盘加密能够有效地抗击内部攻击。

证明：所谓内部攻击者为有账户的攻击者，其主要攻击方法是过期口令攻击和伪造账户攻击，首先，两种攻击方法都要获取磁盘主密钥，都必使用账户口令，而前者的过期口令无法通过口令检测，因为当$TM_x\neq TM_B$时，式(3)无法取得单倍的β，而α,β为模素数，即不存在$\beta=m\alpha$，使得m为整数，因而不能取得正确的MK_{seed}；其次，对于后者可证明攻击者无法借助自己的口令生成其它账户口令，因为$h(\cdot)$为单向密码函数，求出其逆的值是困难的。当$h(PW_x)\neq h(PW_B)$时，攻击者从其口令获取其它用户的口令概率不高于猜测口令的概率。当$h(PW_x)=h(PW_B)$时，由于不同账号使得$TM_x\neq TM_B$，故攻击者并不能借此获得其它用户口令。

通过定理 1 和定理 2 的分析发现，本文方案能够抗击各种外部、内部攻击，具有合理的安全性。

4.2 工作性能分析

现有方案在获取磁盘主密钥时，或采用直接基于口令方法，或者采用加密预密钥方法。前者只能设置单一账户而不适合多账户的环境，后者需要在磁盘中隐藏密钥而增加风险性。本文针对这两种方法的不足，提出了一个更合理的安全管理方案。表 1 给出了本方案与现有方案(包括硬件方案)的工作性能对比。表中把现有方案归为硬件、直接口令和加密预密钥 3 类。从表 1 可以看出，本文方案归属软件方案，如同其它所有软件方法，也需要额外增加预引导。除此不及硬件方案外，在其余密钥的保存与管理的性能项目中，软件方案明显优于硬件方案。而软件方案中，本文方案除主密钥存储项外，其余性能基本一致。

表 1 本方案与现有方案工作性能比较

方案 / 功能	硬件	直接口令	加密预密钥	逻辑口令锁
安全结构	预置/外设备	单层结构	双层结构	双层结构
主密钥存储	加密拆分/安全器件	生成/无副本	加密拆分	生成/无副本
系统结合	独立	完全	完全	完全
用户对象	无关	单账户	多账户	多账户
磁盘启动	无引导	预引导	预引导	预引导

磁盘主密钥在硬盘上加密存储，仍会留下被扫描和跟踪的隐患，而本文方案所采用的即时生成的方法，则让攻击者无法在磁盘上寻找到主密钥的踪迹，消除了这种隐患。因此本方案的性能均是软件方案中最优的。

4.3 效率分析

从方案设置看，磁盘读取数据和写入数据的时间为运行可调密码算法必须消耗的时间，对任何整盘加密系统来说都是一致的。额外增加的开销仅是在用户注册时设置逻辑口令锁的时间消耗，这一部分工作只在用户注册时进行一次，只要设计得合理，就不会影响系统的性能。磁盘加解密时获取磁盘主密钥时间仍是决定其性能的关键因素。根据现有方案中只有一些磁盘加密和解密的技术数据，图 2 和图 3 给出了以 P4 类计算机为样机的测试数据对比，图中包含了本方案与现有类似方案 TKS1 和 TKS2 读写磁盘过程的效率，扇区长度选择从 1 千字节到 64 千字节，随分组数据量加大，未加密的数据吞吐量始终保持最高。其次是本方案的数据吞吐量，而方案 TKS1 和 TKS2 的吞吐量均低于本方案。从图中数据结果看，逻辑口令锁方案的读写磁盘性能是略优于已有方案的。

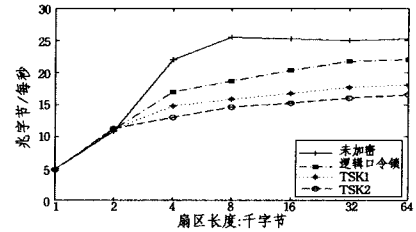

图 2 不同扇区长度时写磁盘的吞吐量

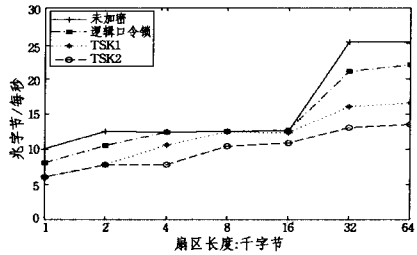

图 3 不同扇区长度时读磁盘的吞吐量

结束语 整盘加密不仅需要理论上的可调加密模式来克服水印攻击，而且需要实际应用上恰当地获取与保存密钥，来阻止密码算法抗攻击强度的降低。整盘加密是一项综合技术。我们所选取的技术方案理应强化核心加密算法的技术意图，不仅使其效能得以充分发挥，还具有独创的系统特色。随着密码芯片等硬件技术的成熟，单纯从加解密技术实现来说，虽然能取得更高速率，但软件实现方法却能更丰富与灵活地应用，正是这样的原因促使了两种方法的同步发展。

参 考 文 献

[1] Gjøsteen K, et al. Security Notions for Disk Encryption[C]// Computer Security -Proc of the 10th European Symposium on Research in Computer Security (ESORICS'05). LNCS 3679. Springer, 2005: 455-474

[2] Dowdeswell R C, et al. The Cryptographic Disk Driver[C]// Proceedings of the Annual USENIX Technical Conference. FREENIX Track, June 2003: 179-186

[3] Rogaway Halevi S. A Parallelizable Enciphering Mode [C]// Oksmoto Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems(CT-RSA 2004). LNCS 2964. Berlin: Springer-Verlag, 2004: 292-304

(下转第 109 页)

括 RSTC(Reduced Static Topology Control)问题和 RDTC(Reduced Dynamic Topology Control)问题，并且证明了 RSTC 问题和 RDTC 问题都是 NP-难的，同时非形式化地讨论了更实际的拓扑控制问题的计算复杂性；在此基础上，本文进一步讨论了关于拓扑控制协议设计的原则性问题，提出了设计能量高效的拓扑控制协议的 3 个必要性原则，即功率控制与睡眠调度相统一的原则、负载感知原则和与路由机制相结合的原则。根据这 3 个原则设计能量高效的拓扑控制协议是我们正在进行的工作。希望本文的研究成果有助于探索更好的拓扑控制协议。

参 考 文 献

[1] Poduri S, Pattem S, Krishnamachari B, et al. A unifying framework for tunable topology control in sensor networks[R]. CRES-05-004. Center for Robotics and Embedded Systems, University of Southern California, 2005: 1-15

[2] Kirousis L M, Kranakis E, Krizanc D, et al. Power consumption in packet radio networks[J]. Theoretical Computer Science, 2000, 243(1/2): 289-305

[3] Clementi A, Penna P, Silvestri R. On the power assignment problem in radio networks[J]. ACM/Kluwer Mobile Networks and Applications(MONET), 2004, 9(2): 125-140

[4] Narayanaswamy S, Kawadia V, Sreenivas R S, et al. Power control in ad-hoc networks: theory, architecture, algorithm and implementation of the COMPOW protocol[C]// Proceedings of European Wireless Conference. Florence, 2002: 156-162

[5] Kawadia V. Protocols and architecture for wireless ad hoc networks [D]. University of Illinois at Urbana-Champaign, 2004

[6] Kubisch M, Karl H, Wolisz A, et al. Distributed algorithms for transmission power control in wireless sensor networks[C]// Yanikomeroglu H, ed. Proceedings of IEEE Wireless Communications and Networking Conference(WCNC). New York: IEEE Press, 2003: 16-20

[7] Li L, Halpern J Y, Bahl P, et al. A cone-based distributed topology control algorithm for wireless multi-hop networks[J]. IEEE/ACM Transactions on Networking, 2005, 13(1): 147-159

[8] Li N, Hou J C. Topology control in heterogeneous wireless networks: problems and solutions[C]// Proceedings of the IEEE Conference on Computer Communications (INFOCOM). New York: IEEE Press, 2004: 232-243

[9] Santi P. Topology control in wireless ad hoc and sensor networks[J]. ACM Computing Surveys, 2005, 37(2): 164-194

[10] Chen B, Jamieson K, Balakrishnan H, et al. SPAN: An energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks[J]. ACM Wireless Networks, 2002, 8(5): 481-494

[11] Kumar S, Lai T H, balogh J. On k-coverage in a mostly sleeping sensor network[C]// Haas ZJ, ed. Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom). New York: ACM Press, 2004: 144-158

[12] Xing G L, Wang X R, Zhang Y F, et al. Integrated coverage and connectivity configuration for energy conservation in sensor networks[J]. ACM Transactions on Sensor Networks, 2005, 1(1): 36-72

[13] Xu Y, Heidemann J, Estrin D. Geography-informed energy conservation for ad hoc routing[C]// Rose C, ed. Proceedings of the ACM International Conference on Mobile Computing and Networking(MobiCom). New York: ACM Press, 2001: 70-84

[14] Deb B, Bhatnagar S, Nath B. A topology discovery algorithm for sensor networks with applications to network management[R]. DCS-TR-441. Department of Computer Science, Rutgers University, 2001

[15] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks[J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 660-669

[16] Xing G L, Lu C Y, Zhang Y, et al. Minimum power configuration in wireless sensor networks[C]// Kumar PR, Campbell AT, Wattenhofer R, eds. Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc). New York: ACM Press, 2005: 390-401

(上接第 97 页)

[4] EME Halevi S. Extending EME to Handle Arbitrary-Length Messages With Associated Data[C]// Canteaut A, Viswanathan K, eds. Proc of the 5th International Conference on Cryptology in India(INDOCRYPT 2004). LNCS 3348. Berlin: Springer-Verlag, 2004: 315-327

[5] McGrew D A, Fluhrer S R. The Extended Codebook (XCB) Mode of Operation[EB/OL]. http://eprint. iacr. org/, 2004/278

[6] Wang P, Feng D, Wu W. HCTR: A Viriable-Input-Length Enciphering Mode[C]// SKLOIS Conference on Information Security and Cryptology(CISC 2005). LNCS 3822. Berlin: Springer-Verlag, 2005: 175-188

[7] Chakraborty D, Sarkar P. HCH: A New Tweakable Enciphering Scheme Using the Hash- Encrypt-Hash Approach[C]// Barua R, Lange T, eds. Progress in Cryptology(INDOCRYPT). LNCS 4329. Berlin: Springer-Verlag, 2006: 287-302

[8] Chakraborty D, Sarkar P. A New Mode of Encryption Providing a Tweakable Strong Pseudo- Random Permutation[C]// Robshaw B J M, eds. Fast Software Encryption(FSE'2006). LNCS 4047. Berlin: Springer-Verlag, 2006: 293-309

[9] Halevi S. Invertible Universal Hashing and the TET Encryption Mode[C]// Menezes A, eds. Advances in Cryptology(CRYPTO 2007). LNCS 4622. Berlin: Springer-Verlag, 2007: 412-429

[10] Sarkar P. Improving upon the TET Mode of Operation[C]// Nam K H, Rhee G, eds. Information Security and Cryptology (ICISC 2007). LNCS 4817. Berlin: Springer-Verlag, 2007: 180-192

[11] Lopez M C, Chakraborty D, Henriquez R F. Efficient Implementations of Some Tweakable Enciphering Schemes in Reconfigurable Hardware[C]// Srinathan K, Rangan P C, Yung M, eds. Progress in Cryptology(INDOCRYPT 2007). LNCS 4859. Berlin: Springer-Verlag, 2007: 414-424

[12] 伏晓，等. 网络安全技术管理研究[J]. 计算机科学，2009，36(2)：15-18，54