学校编码：10384

学号：23120111152994

厦门大学

硕士学位论文

Android备份文件口令认证机制安全性分析及其改进

A Security Analysis on Password-Based Authentication In Android Backup Files and Its Enhancement

潘锟

指导教师：李晓潮

专业名称：集成电路

答辩日期：2014年5月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文(包括纸质版和电子版)，允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于:

(　　)1.经厦门大学保密委员会审查核定的保密学位论文，于　年　月　日解密，解密后适用上述授权。

(　　)2.不保密，适用上述授权。

(请在以上相应括号内打“✓”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。)

声明人(签名):

年　　月　　日

摘　要

在现代密码学中，无条件安全性和计算安全性是证明密码机制的两种方式。其中计算安全主要通过可证明安全理论和穷举搜索实验进行证明，在实际应用大部分采用计算安全进行分析密码机制的安全性。口令认证机制是文件存储及传输过程安全性的主要保障，在认证过程中需要利用密钥导出算法将用户口令转化为均匀分布的密钥。密钥导出算法的随机性决定了口令认证机制整体的安全性。本文采用计算安全模型，以Android 备份文件为实例，分析PBKDF2作为密钥导出算法的安全性。并针对其密钥输出结构进行改进，提出了一种基于反馈模式的密钥导出算法XKDF并给出其计算安全性证明。主要工作成果如下:

(1)在计算安全模型下，可证明安全指标表明其安全性取决于敌手的计算能力和用户口令空间大小。本文通过在GPU上兑现Android备份文件口令认证机制，并分析其密钥导出算法的不可区分优势上界，在敌手计算能力确定的情况下，测试用户口令空间大小对Android备份文件安全性的影响。

(2)提出了一种基于反馈模式的密钥导出算法XKDF，在计算安全模型下，结合随机预言机模型，利用Game-Playing技术对算法结构安全性进行论证。该算法和PBKDF2相比，其不可区分优势减小了h-1倍（h为底层块密钥的数量），增强了结构的关联性。并应用于Android备份文件中，在敌手计算能力和恢复时间相同的情况下，口令空间的查询次数减少h-1倍。

关键词：口令认证机制；密钥导出算法；计算安全

Abstract

The security of cryptographic scheme can be evaluated under two models: unconditional security and computational security. The most practical security is computational, which can be analyzed by provable security theory and exhaustive search experiment. Password-based Message Authentication CodePBMACis a mechanism that guarantee the security offile transmission and storage. Key derivation function (KDF) provides uniform distribution key in PBMAC which generated from user's password, and its randomness determines the overall security. In this thesis, we take Android mobile phone backup file as an example to elaborate the security of PBKDF2,We propose a feedback mode KDF denoted XKDF based on the output structure of PBKDF2 and present its computational security. The main achievements are as follow:

1The provable metrics comes to imply that both the space of user's password and adversary's computing powerresult in the security of KDF.We implement the Key derivation function PBKDF2 of Android backup file under the latest GPU-accelerated key recovery attack capability and analyze the impact on the security of Android under different user's password space.

2We propose a new algorithm named XKDF based on feedback mode that is proved computationally secure by using random oracle model with Game-Playing technique. Compared with PBKDF2, the adversary's advantage gained h-1(denoted block number) times , which enhanced the relation of the structure. We implement the algorithm in Android backup files, and the query to password space has reduced h-1 time under the same attack ability and recovery time.

Keywords: Password-based Message Authentication CodeKey Derivation FunctionComputational Security

参考资料

[1]Gartner June report[EB/OL].[2013-6]. http://www.gartner.com/newsroom/id/2525515

[2]Scarfone K, Souppaya M, Sexton M. Guide to storage encryption technologies for end user devices[J]. NIST Special Publication, 2007, 800: 111.

[3]Katz J, Lindell Y, 任伟. 现代密码学: 原理与协议[M]. 国防工业出版社, 2011.

[4]Spafford E H, Weeber S A. User authentication and related topics: An annotated bibliography[J]. 1991.

[5]张明杰、罗毅、牛汉春.基于SIM卡动态口令的互联网身份认证体系与应用[J].电信科学,2007,Vol.12:18-22.

[6]张立民、李章林、薛三龙等.实用型指纹识别系统的研究[J].南开大学报,2007,Vol.40,No.1;76-80.

[7]胡国安,艾明晶,骆志用.基于SOPC的指纹识别系统的设计与实现[J].计算机工程与应用,2006,Vol.42 No.8:96-99,166.

[8]R.M.Bolle,J.H.Connell,S.Pankanti,N.K.Ratha,and A.W.Senior. Guide to Biometrics Selection and System Design[M].New York:Springer-Verlag,2003.

[9]Uludag, U., S. Pankanti, S. Prabhakar and A. Jain, 2004. Biometric Cryptosystems: Issues and Challenges[J]. Proceedings of the IEEE, 2004, Vol. 92(6):948-960.

[10]Marianna B. Magno. Survey of User Authentication Mechanisms [D]. Monterey:Naval Postgraduate School, 1996.

[11]O'Gorman, L. Comparing Passwords tokens and Biometrics for User authentication [J]. Proceedings of the IEEE, 2003, vol 91(12):2019 – 2020.

[12]Kwon T, Moon H. Knowledge-based user authentication associated with biometrics[M]//Universal Acess in Human Computer Interaction. Coping with Diversity. Springer Berlin Heidelberg, 2007: 414-419.

[13]Goldwasser S, Bellare M. Lecture notes on cryptography[J]. Summer course “ Cryptography and computer security ” at MIT, 1996, 1999: 1999.

[14]Biham E, Shamir A. Differential cryptanalysis of the data encryption standard[M]. New York: Springer-Verlag, 1993.

[15]Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication[C] Advances in Cryptology—CRYPTO ’96. Springer Berlin Heidelberg, 1996: 1-15.

[16]Shriwas M S, Gupta N, Sinhal A. Efficient Method for Backup and Restore Data in Android[C] Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013: 693-697.

[17] 7-zip[EB/OL].http://www.7-zip.org

[18] PDF[EB/OL].http://www.adobe.com/products/acrobat/iso-pdf-x-32000-standards.html.

[19] OpenOffice[EB/OL].http://www.openoffice.org/.

[20] Truecrypt[EB/OL].http://www.truecrypt.org.

[21] McAfee[EB/OL].http://en.wikipedia.org/wiki/McAfee

[22] PGP.PGPWDE[EB/OL].http://www.pgpi.org/products/pgpwde.

[23] PGP.PGPSDA[EB/OL].http://www.pgpi.org/products/pgpsda/.

[24] WinRAR[EB/OL].http://www.winrar.com.cn/index.html.

[25]AES[EB/OL]/http://en/Wikipedia.org/wiki/Advanced_Encryption_Standard.

[26] Wirlpool[EB/OL].http://www.wikipedia.org/wiki/Whirlpool.

[27] CAST5[EB/OL].http://en.wikipedia.org/wiki/CAST-128.

[28]Cuda C.Programming guide[J].NVIDIA Corporation,July.2012.

[29]Brook++[EB/OL].http://en.wikipedia.org/wiki/BrookGPU

[30]OpenCL[EB/OL] https://www.khronos.org/opencl/.

[31]RSA Laboratories. PKCS 35 v2.1： Password-Based Cryptography Standard[EB/OL]. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2_1.pdf.

[32]Menezes A. Another look at provable security[M]Advances in Cryptology – EUROCRYPT 2012. Springer Berlin Heidelberg, 2012: 8-8.
[33]Menezes A J, Van Oorschot P C, Vanstone S A. Handbook of applied cryptography[M]. CRC press, 1996
[34]IETF [EB/OL].http://www.ietf.org/.
[35]Filiol E, Fizaine J. Openoffice v3. x security design weaknesses[J]. Black Hat Europe. 2009,5(8):3-14.
[36]Random Oracle Model[EB/OL].http://en.wikipedia.org/wiki/Random_oracle.
[37] M.Bellare,P.Rogaway. The Game-Playing Technique[R].Cryptology ePrint Archive,Report 2004/331,2004,http://eprint.iacr.org/
[38]冯国登.可证明安全性理论与方法研究[J].软件学报.2005(10).
[39]Frances F.Yao,Yiqun Lisa Yin.Design and analysis of password-based key derivation function[C].Topics in Cryptology-CT-RSA 2005,2005,San Francisco,CA,USA,Lecture Notes in Computer Science,Vol.3376:245-261.
[40]邹梅,吴鸿伟,周君等.Office认证机制中密钥导出函数安全性分析[J].Computer Engineering.2012,38（8）.
[41]Paoli J, Valet-Harper I, Farquhar A, et al. ECMA-376 office open XML file formats[J]. URL http://www. ecmainternational. org/publications/standards/Ecma-376. htm, 2006.
[42]周君.基于口令的密钥导出算法安全性分析[D].厦门：厦门大学,2013.
[43]Hugo Krawczyk. Cryptographic Extraction and Key Derivation: The HKDF Scheme[C]. CRYPTO 2010, LNCS 6223, 2010: 631 – 648.
[44]Wen C C, Dawson E, Nieto J M G, et al. A framework for security analysis of key derivation functions[M]//Information Security Practice and Experience. Springer Berlin Heidelberg, 2012: 199-216.
[45]吴鸿伟. 电子取证关键技术研究及在云计算平台上的应用[J]. 2014.
[46]杨胜斌. 基于 GPU 集群实现 MD5 的快速破解[J].电脑与信息技术 2013(02).
[47]黄锦增.基于GPU的常见散列算法并行实现及优化[D].华南理工大学硕士论文.2011.
[48]Negligible function[EB/OL]. http://en.wikipedia.org/wiki/Negligible_function.
[49]刘阳,基于一次性口令的身份认证系统的设计与实现[D].山东大学硕士论文.2008.
[50]M Bellare ,R Canetti,H Krawczyk. Keying hash functions for message authentication [C]. Advances in Cryptology—CRYPTO ’96, 1996,Vol. 1109:1-15.
[51]HMAC[EB/OL]. http://www.ietf.org/rfc/rfc2104.txt.
[52]John Black and Phillip Rogaway.A Block-Cipher Mode of Operation for Parallelizable Message Authentication[C]. ADVANCES IN CRYPTOLOGY — EUROCRYPT 2002,2002, Vol.2332:384-397.
[53]王大印,林东岱,吴文玲等. XOR-MAC消息认证码的安全性新证明[J]. 中国科学院研究生院学报 ,2006,No.2, Vol.23:257-262.
[54]Sobolewski J S. Cyclic redundancy check[J]. 2003.
[55]Chen L.Recommendation for key derivation using pseudorandom functions[J].NIST Special Publication.2008,800:108.
[56]Kaliski B. PKCS# 5: Password-based cryptography specification version 2.0[J]. 2000.
[57]Turan M S, Barker E, Burr W, et al. Recommendation for password-based key derivation[J]. NIST special publication, 2010, 800: 132.
[58]Merkle – Damgård[EB/OL] http://en.wikipedia.org/wiki/Merkle – Damgård_construction.
[59]National Institute of Standards and Technology (NIST), ” FIPS PUB 180-2 ” : SECURE HASH STANDARD(SHS) ”, 2002
[60]National Institute of Standards and Technology (NIST), “ FIPS 197: Advanced Encryption Standard (AES) ”, 2001
[61] FIPS 198-1,The Keyed-Hash Message Authentication Code(HMAC),July 2008.
[62]卡茨,林德尔.现代密码学-原理与协议[M].国防工业出版社,2011.
[63]吴文玲,冯登国,张文涛.分组密码的设计与分析[M].清华大学出版社,2009.
[64]EllaRE M, KIlIan J E, Rogaway P I I. The Security of the Cipher Block Chaining Message Authentication Code[J]. 2001.

[65]王鹏.一个关于MAC伪随机性与不可伪造性的注记[J].中国科学院研究生院学报,2010
[66]Bellare M． Kilian J． Rogaway P． The security of the cipher block chaining message authentication code[J]． Journal of Computer and System Sciences,2000,61：262-399.
[67] M.Bellare and P.Rogaway.Random oracles are practical-a paradigm for designing efficient protocols.In Processings of the First ACM Comference on Computer and Communications Security,pages 62-73,1993.
[68]Goldwasser S,Micali S,Rivest R． A digital signature scheme secure against adaptive chosen—message attacks[J]． SIAM Journal of Computing,l988,No.l7,Vol.2：28l-308.
[69]龚征.随机预言机模型下可证明安全性关键问题研究[D].上海交通大学博士论文.2008
[70]National Institute of Standards and Technology(NIST), ”FIPS 197:Advanced Encryption Standard(AES)”,2001.
[71]Bellare M. New proofs for NMAC and HMAC: Security without collision-resistance[M]//Advances in Cryptology-CRYPTO 2006. Springer Berlin Heidelberg, 2006: 602-619.
[72]Hellman M E. A cryptanalytic time-memory trade-off[J]. Information Theory, IEEE Transactions on, 1980, 26(4): 401-406
[73] DeskTop-gpus[EB/OL] http://www.geforce.cn/hardware/desktop-gpus.
[74] Tzeng S, Wei L Y. Parallel white noise generation on a GPU via cryptographic hash[C] Proceedings of the 2008 symposium on Interactive 3D graphics and games. ACM, 2008: 79-87.
[75]Boeing A. Survey and Future Trends of Efficient Cryptographic Function Implementations on GPGPUs[C]//Proc. of the 6th Australian Digital Forensics Conference. Perth, Australia: [s.n.], 2008.
[76]周洁. 基于GPU的WPA_WPA2_PSK高速破译方法研究[D]. 西安：西安电子科技大学,2010.
[77]乐德广,常晋义,刘祥南等。基于GPU的MD5高速解密算法的实现[J].计算机工程。2010,36（11）：154-155.
[78]Birthday attack[EB/OL].http://en.wikipedia.org/wiki/Birthday_attack
[79]Taylor series[EB/OL].http://en.wikipedia.org/wiki/Taylor_series