在于服务器的主密钥 x,我们称这种保护随机数的方法为方案 III.事实上,方案 III 易遭受智能卡丢失攻击.假设攻击者$\mathcal{A}$已获得智能卡内秘密参数信息,则$\mathcal{A}$可以直接猜测合理的 (ID_i^*,PW_i^*),计算 $d_2^*=h(PW_i^*\|ID_i^*)$,并验证计算的 d_2^* 是否等于提取的 d_2:如果相等,则表明$\mathcal{A}$猜测的 (ID_i^*,PW_i^*) 是正确的.攻击过程无需侦听通信信道,针对方案 III 的离线口令猜测攻击更易实施.

Table 4 A taxonomy of improvement strategies

表 4 改进策略分类

方案	描述	可能存在的问题	典型失效协议
方案 I	*ID*,*PW* 保护随机数	内部攻击	第 4.1 节,Wu 等人[64]
方案 II	用户的生物特征保护随机数	内部攻击、隐私泄露	第 6.1 节,Odelu 等人[67]
方案 III	服务器主密钥保护随机数	无本地验证、智能卡丢失攻击	Namasudra 等人[70]
方案 IV	服务器无 *PW*,注册阶段仅发送 *ID*	无本地验证、用户不能自选口令	Wang 等人[71]、Amin 等人[72]
方案 V	不选随机数,使用 *ID* 保护 *PW*	智能卡丢失攻击、内部攻击	Amin 等人[73]
方案 VI	不选随机数,使用生物特征信息保护 *PW*	隐私泄漏、内部攻击	Farash 等人[69]
方案 VII	不选随机数,服务器公钥保护 *PW*	内部攻击	Sood 等人[55]

为防止智能卡丢失攻击和内部人员攻击,Wu 等人[74]给出另一种以服务器主密钥保护随机数的方案 III.在注册阶段,用户向服务器发送$\{ID_i,RPW_i\}$.服务器选择随机数 e_i,计算 $T_1^*=h(ID_S\|x\|e_i)\oplus RPW_i\oplus h(ID_i\|e_i),T_2^*=h(ID_i\|e_i)\oplus RPW_i$,服务器将 $\{T_1^*,T_2^*,e_i\}$ 写入智能卡并发送给用户.用户收到智能卡后计算 $T_1=T_1^*\oplus r_i,T_2=T_2^*\oplus r_i$,并用 T_1,T_2 替换 T_1^*,T_2^*.然而在 Wu 等人的[74]方案中,由于智能卡无法获知服务器主密钥 x,因此不能验证用户输入的口令是否正确.口令验证过程由服务器实现,则不能实现“口令本地自由更新”.

方案 IV 也存在两种实现方法.

- 文献[71]中,Wang 等人提出一个高效的基于动态 ID 的远程用户口令认证协议.该协议注册阶段仅将用户身份标识 ID_i 发送给服务器,由服务器选择用户口令,并将口令 PW_i 以明文发送给用户.可见,Wang 等人的协议[71]不支持用户自由选择口令,仍然存在内部攻击威胁.
- 文献[72]中,Amin 等人对方案 IV 的实现方法略有改进.用户在注册阶段发送身份标识 ID_i,服务器返回智能卡后,用户再输入选择的 PW_i.经分析,Amin 等人的方案[72]缓解了上述内部攻击,但存在两种类型的智能卡丢失攻击:一是直接利用智能卡内存储的秘密参数进行口令猜测;另一种是借助智能卡内信息和公开信道中的消息进行口令猜测.因此,方案 IV 也不可取.

与上述方案不同,文献[73]在注册阶段未选择随机数,用户计算 $HPW_i=h(PW_i\|ID_i)$,将 ID_i 和 HPW_i 发送给服务器.我们称此类方法为方案 V.不难看出,内部攻击者可直接通过截获的通信消息猜测出用户口令,故方案 V 未解决内部攻击问题.方案 VI 与方案 V 如出一辙,以用户生物特征替换 ID_i 来计算 HPW_i.依据第 6.1 节的实例分析,方案 VI 仍存在内部攻击威胁.此外,由于用户将生物特征发送给服务器,还可能存在隐私泄露风险.

文献[55]中,Sood 等人提出一种基于公钥密码技术的口令认证协议.在系统初始化阶段,服务器选择公私钥对,并公开公钥 *PK*.用户注册过程先选择会话密钥 *SS*,以会话密钥加密用户自主选择的身份标识和口令,再以服务器公钥 *PK* 加密会话密钥 *SS*,即用户将$\{(SS)_{PK},(ID_i)_{SS},(PW_i)_{SS}\}$发送给服务器.

此类方案有效解决了传输消息的安全性,但假设恶意内部管理员有权解密用户注册请求或监听到服务器解密及计算过程,则依然能获得用户口令.

总之,第 2 节中提到的内部攻击威胁并未引起广泛关注,文献[17,35,75]仍建议将随机数以明文保存在智能卡中.上述 7 类解决方案对内部攻击威胁有适当的缓解作用,但可能引入新的安全问题,并未从根本上解决内部攻击问题.本文将弥补这一缺陷,提出合理的解决方案抵抗内部攻击.

7.2 内部攻击解决方案

为避免服务器获得口令明文和用户隐私泄漏,采用“加盐 Hash”技术传输口令相比其他几种方式更简单、安全、高效[35].基于对 300 余个用户认证协议的分析经验,我们发现大多数采用“加盐 Hash”技术实现用户注册的

协议均无法抵抗内部攻击,这是因为这些协议均有以下两条性质.

1. RPW_i 由 ID_i,PW_i 和 r_i 确定;
2. r_i 可由用户 ID_i,PW_i 或 SC 计算出来.

其中,r_i 表示用户在注册过程中选择的随机数,SC 表示用户智能卡.以下我们将会说明,具有这两条性质的协议无法抵抗内部攻击.因此,我们称其为内部攻击的简易判断标准.

说明 1. 常见的口令存储形式有 3 种:明文、加密、哈希值.明文不可取,而加密和直接 Hash 均易被服务器还原,因此,增加一个随机盐可以有效增加口令的安全性.近年来,“加盐 Hash”技术广泛应用于现有的身份认证协议(如文献 17,19,20,35,71,75]),用户在注册阶段选择随机数 r_i,计算 $RPW_i=h(PW_i||r_i)$,将 $\{ID_i,RPW_i\}$ 发送给服务器,此类方法有助于确保服务器不能获得口令明文,且不能直接猜测用户口令.

说明 2. 假设用户登录阶段使用 RPW_i 进行验证,即智能卡无需计算出随机数 r_i,则可能存在内部攻击者仿冒用户攻击.否则,智能卡需计算出 r_i,以验证用户口令 PW_i 的正确性.此外,假设随机口令 RPW_i 与用户 ID_i,PW_i 无关,则只能与服务器主密钥相关,而服务器的目标是验证用户的合法性,若以服务器主密钥推算随机数 r_i,则服务器相当于一个预言机,将为攻击者提供仿冒用户或验证猜测口令正确性的预言机服务.

综上所述,任意协议在用户注册阶段采用了“加盐 Hash”技术传输用户口令,并且在智能卡中以某种方式保存了用户选择的随机数,该协议将无法抵抗内部攻击.针对此问题,本文提出一种新的解决方案,在此只简述用户注册过程的基本思路,协议登录、认证过程可兼容现有的用户身份认证协议.

1) 用户 U_i 选取身份标识 ID_i,口令 PW_i,生成随机数 r_i,计算 $RPW_i=h(PW_i||r_i)$.
2) $U_i\Rightarrow S$:$\{ID_i,RPW_i\}$.
3) 服务器 S 随机生成安全参数 a_i,计算 $X_i=h(h(ID_i||x)\oplus a_i)$,$F_i=h((h(ID_i)\oplus RPW_i) \bmod n)$,$D_i=X_i\oplus RPW_i$.在数据库中存储 $\{ID_i,a_i\}$;同时,将 $\{D_i,F_i,n\}$ 写入智能卡.其中,x 为系统主密钥,n 表示 (ID,PW) 池容量的整数,$2^4\leqslant n\leqslant 2^8$.
4) $S\Rightarrow U_i$:智能卡.
5) U_i 接收到智能卡,计算 $X_i=D_i\oplus RPW_i$,重新生成随机数 r_i',计算 $RPW_i'=h(PW_i\,\|\,r_i')$,$F_i'=h((h(ID_i)\oplus RPW_i') \bmod n)$,$D_i'=X_i\oplus RPW_i'$,以 D_i',F_i' 替换智能卡中的 D_i,F_i,并将 r_i' 写入智能卡.

需要指出的是:服务器接收到的 RPW_i 与智能卡中参与计算的 RPW_i' 并不相同,即使攻击者截获了注册过程中的 RPW_i,提取用户智能卡中的安全参数,也无法借助随机数 r_i' 猜测出用户口令.此外,通过引入“模糊验证因子”技术[35],如第 4.2 节和第 6.2 节所示,增加了攻击者猜测出正确口令的难度.因此,本文提出的方案可以有效解决第 2 节的内部攻击,同时允许用户自主选择口令,保护用户隐私,实现口令本地自由更新.

8 结 语

无线传感器网络的身份认证面临严峻挑战:一方面由于传感器节点计算能力和存储容量有限,无法支撑复杂密码协议;另一方面,攻击者的攻击能力不断增强,先前安全的协议在新的攻击场景下将不再安全.本文以无线传感器网络环境下的两个代表性认证协议为例,分析一种实际存在的、但未引起广泛关注的内部攻击威胁,并且给出攻击者的具体攻击过程.

具体来说,本文首先回顾 Mir 等人的协议,指出其不能抵抗内部攻击和智能卡丢失攻击,且不能实现前向安全性;然后分析 Fang 等人的协议,指出其同样不能抵抗内部攻击和智能卡丢失攻击,且未实现所宣称的前向安全性属性.针对 Mir 等人的协议和 Fang 等人的协议的具体失误之处,提出相应解决方案.本文指出一种被长期忽略的内部攻击,基于 300 余个协议分析经验,对现有尝试抵抗内部攻击的方案进行分类,指出现有解决方案的不足之处,进一步提出合理的解决方案.根据本文提出的抗内部攻击方法,设计更安全高效的用户身份认证协议,是下一步值得研究的方向.

References:

[1] Shim KA. BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Trans. on Information Forensics and Security, 2017,12(7):1545−1554.

[2] He D, Zeadally S, Wu L, *et al*. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. Computer Networks, 2017,128:154−163.

[3] Wang D, Wang P. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Computer Networks, 2014,73:41−57.

[4] Tan R, Phillips DE, Moazzami MM, *et al*. Unsupervised residential power usage monitoring using a wireless sensor network. ACM Trans. on Sensor Networks, 2017,13(3):Article No.20.

[5] Decker CJ, Reed C. The National Oceanographic Partnership Program: A Decade of Impacts on Oceanography. Oceanography, 2009,22(2):208−227.

[6] Huang H, Gong T, Ye N, *et al*. Private and secured medical data transmission and analysis for wireless sensing healthcare system. IEEE Trans. on Industrial Informatics, 2017,13(3):1227−1237.

[7] Li X, Niu J, Kumari S, *et al*. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of things environments. Journal of Network and Computer Applications, 2018,103:194−204.

[8] Shen J, Chang S, Shen J, *et al*. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems, 2018,78:956−963.

[9] United States Environmental Protection Agency. Remote sensing information gateway. 2018. http://www.epa.gov/rsig

[10] Askraba S, Paap A, Alameh K, *et al*. Laser-Stabilized real-time plant discrimination sensor for precision agriculture. IEEE Sensors Journal, 2016,16(17):6680−6686.

[11] Habib C, Makhoul A, Darazi R, *et al*. Self-adaptive data collection and fusion for health monitoring based on body sensor networks. IEEE Trans. on Industrial Informatics, 2016,12(6):2342−2352.

[12] Lamport L. Password authentication with insecure communication. Communications of the ACM, 1981,24(11):770−772.

[13] Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. IEEE Trans. on Consumer Electronics, 2004,50(2):629−631.

[14] Wong KHM, Zheng Y, Cao J, *et al*. A dynamic user authentication scheme for wireless sensor networks. In: Proc. of the IEEE Int'l Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2006. 1−8.

[15] Tseng HR, Jan RH, Yang W. An improved dynamic user authentication scheme for wireless sensor networks. In: Proc. of the IEEEGlobal Telecommunications Conf. 2007. 986−990.

[16] Das ML. Two-factor user authentication in wireless sensor networks. IEEE Trans. on Wireless Communications, 2009,8(3): 1086−1090.

[17] Wang D, Li WT, Wang P. Crytanalysis of three anonymous authentication schemes for multi-server environment. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):1937−1952 (in Chinese with English abstract). http.//www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[18] Wang D, Li WT, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. on Industrial Informatics, 2018,14(9):4081−4092.

[19] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of things notion. Ad Hoc Networks, 2014,20:96−112.

[20] Wu F, Xu L, Kumari S, *et al*. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 2017,89:72−85.

[21] Khan MK, Kim SK, Alghathbar K. Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Computer Communications, 2011,34(3):305−309.

[22] Chen TH, Shih WK. A robust mutual authentication protocol for wireless sensor networks. ETRI Journal, 2010,32(5):704−712.

[23] Yeh HL, Chen TH, Liu PC, *et al*. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 2011,11(5):4767−4779.

[24] Kumar P, Lee SG, Lee HJ. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors, 2012,12(2):1625−1647.

[25] He D, Kumar N, Chen J, *et al*. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 2015,21(1):49−60.

[26] Mir O, Munilla J, Kumari S. Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. Peer-to-Peer Networking and Applications, 2017,10(1):79−91.

[27] Fang WD, Zhang WX, Yang Y, *et al*. Biometric-based three-factor user authentication protocol for wireless sensor network. Acta Electronica Sinica, 2018,46(3):702−713 (in Chinese with English abstract).

[28] Awasthi AK, Srivastava K. A biometric authentication scheme for telecare medicine information systems with nonce. Journal of Medical Systems, 2013,37(5):Article No.9964.

[29] Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proc. of the E-Computers and Digital Techniques, 1991, 138(3):165−168.

[30] Hsu CL. Security of two remote user authentication schemes using smart cards. IEEE Trans. on Consumer Electronics, 2003,49(4): 1196−1198.

[31] Ku WC, Chen SM. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Trans. on Consumer Electronics, 2004,50(1):204−207.

[32] Dolev D, Yao A. On the security of public key protocols. IEEE Trans. on Information Theory, 1983,29(2):198−208.

[33] Kim TH, Kim C, Park I. Side channel analysis attacks using AM demodulation on commercial smart cards with SEED. Journal of Systems and Software, 2012,85(12):2899−2908.

[34] Barenghi A, Breveglieri L, Koren I, *et al*. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. Proc. of the IEEE, 2012,100(11):3056−3076.

[35] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2018,15(4):708−722.

[36] Wang D, Cheng H, Wang P, *et al*. Zipf's law in passwords. IEEE Trans. on Information Forensics and Security, 2017,12(11): 2776−2791.

[37] Wei FS, Zhang G, Ma JF, Ma CG. Privacy-preserving multi-factor authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1511−1522 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

[38] Thousands of servers password and sensitive information. 2018. https://www.solidot.org/story?sid=55915

[39] The Korean shopping website server was hacked and tens of millions of users' information was leaked. 2016. http://news.fznews.com.cn/fuzhou/20160726/5796c55702ef9.shtml

[40] Wang D, Cheng H, Wang P, *et al*. A security analysis of honeywords. In: Proc. of the 25th Network and Distributed System Security Symp. (NDSS 2018). ISOC, 2018. 1−16.

[41] Golla M, Beuscher B, Dürmuth M. On the security of cracking-resistant password vaults. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. ACM Press, 2016. 1230−1241.

[42] Juels A, Rivest RL. Honeywords: Making password-cracking detectable. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM Press, 2013. 145−160.

[43] Morris R, Thompson K. Password security: A case history. Communications of the ACM, 1979,22(11):594−597.

[44] Farash MS, Turkanović M, Kumari S, *et al*. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of things environment. Ad Hoc Networks, 2016,36:152−176.

[45] Phillip T. Github security flaw leaks user passwords to employees. 2018. https://www.dailydot.com/debug/github-bug-passwords/

[46] Agrawal P. Keeping your account secure. 2018. https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

[47] The demand of smart card, financial IC card market and industrial chain analysis in China 2017. 2018. http://www.chinaidr.com/tradenews/2018-01/117551.html

[48] Li X, Niu J, Kumari S, *et al*. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of things environments. Journal of Network and Computer Applications, 2018,103:194−204.

[49] Ma CG, Wang D, Zhao SD. Security flaws in two improved remote user authentication schemes using smart cards. Int'l Journal of Communication Systems, 2014,27(10):2215−2227.

[50] Yang JH, Chang CC. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers & Security, 2009,28(3-4):138−143.

[51] Xiao D, Liao X, Deng S. A novel key agreement protocol based on chaotic maps. Information Sciences, 2007,177(4):1136−1142.

[52] Huang X, Chen X, Li J, *et al*. Further observations on smart-card-based password-authenticated key agreement in distributed systems. IEEE Trans. on Parallel and Distributed Systems, 2014,25(7):1767−1775.

[53] Wang D, Gu Q, Cheng H, *et al*. The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proc. of the 11th ACM Asia Conf. on Computer and Communications Security (ASIACCS 2016). ACM Press, 2016. 475−486.

[54] Michael C. OPM OPM breach: What's the risk of exposed fingerprint data? 2016. https://searchsecurity.techtarget.com/answer/OPM-breach-Whats-the-risk-of-exposed-fingerprint-data

[55] Sood SK. Secure dynamic identity-based authentication scheme using smart cards. Information Security Journal: A Global Perspective, 2011,20(2):67−77.

[56] Li X, Niu J, Liao J, *et al*. Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. Int'l Journal of Communication Systems, 2015,28(2):374−382.

[57] Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. IEEE Trans. on Consumer Electronics, 2004,50(2):629−631.

[58] Chang YF, Tai WL, Chang HC. Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. Int'l Journal of Communication Systems, 2014,27(11):3430−3440.

[59] Yeh KH. A lightweight authentication scheme with user untraceability. Frontiers of Information Technology & Electronic Engineering, 2015,16(4):259−271.

[60] Li X, Niu J, Khan MK, *et al*. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 2013,36(5):1365−1371.

[61] Amin R, Kumar N, Biswas GP, *et al*. A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment. Future Generation Computer Systems, 2018,78:1005−1019.

[62] Xue K, Hong P, Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences, 2014,80(1):195−206.

[63] Madhusudhan R, Hegde M. Security bound enhancement of remote user authentication using smart card. Journal of Information Security and Applications, 2017,36:59−68.

[64] Wu F, Xu L, Kumari S, *et al*. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Systems, 2017,23(2):195−205.

[65] Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. Journal of Medical Systems, 2017,41(5):Article No.80.

[66] Xiong H, Tao J, Yuan C. Enabling telecare medical information systems with strong authentication and anonymity. IEEE Access, 2017,5:5648−5661.

[67] Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans. on Information Forensics and Security, 2015,10(9):1953−1966.

[68] Srinivas J, Mukhopadhyay S, Mishra D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks, 2017,54:147−169.

[69] Farash MS, Attari MA. An anonymous and untraceable password-based authentication scheme for session initiation protocol using smart cards. Int'l Journal of Communication Systems, 2016,29(13):1956−1967.

[70] Namasudra S, Roy P. A new secure authentication scheme for cloud computing environment. Concurrency and Computation: Practice and Experience, 2017,29(20):Article No.e3864.

[71] Wang Y, Liu J, Xiao F, *et al*. A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 2009,32(4):583−585.

[72] Amin R, Islam SKH, Biswas GP, *et al*. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Computer Networks, 2016,101:42−62.

[73] Amin R, Islam SKH, Biswas GP, *et al*. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems, 2018,80:483−495.

[74] Wu F, Xu L, Kumari S, *et al*. A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client—Server networks. Computers & Electrical Engineering, 2015,45:274−285.

[75] He D, Zeadally S, Kumar N, *et al*. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE Trans. on Information Forensics and Security, 2016,11(9):2052−2064.

附中文参考文献:

[17] 汪定,李文婷,王平.对 3 个多服务器环境下匿名认证协议的分析.软件学报,2018,29(7):1937−1952. http://www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[27] 房卫东,张武雄,杨旸,等.基于生物特征标识的无线传感器网络三因素用户认证协议.电子学报,2018,46(3):702−713.

[37] 魏福山,张刚,马建峰,马传贵.标准模型下隐私保护的多因素密钥交换协议.软件学报,2016,27(6):1511−1522. http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

[38] 数千服务器泄漏密码密钥等敏感信息.2018. https://www.solidot.org/story?sid=55915

[39] 韩购物网站服务器遭黑客攻击 千万用户信息被泄.2016. http://news.fznews.com.cn/fuzhou/20160726/5796c55702ef9.shtml

[47] 2017 年中国智能卡、金融 IC 卡市场需求及产业链分析.2018. http://www.chinaidr.com/tradenews/2018-01/117551.html

[54] Michael C.OPM 数据泄露:生物识别可以信任吗?2016. https://searchsecurity.techtarget.com.cn/11-24678/

李文婷(1990－),女,山东青岛人,博士生,CCF 学生会员,主要研究领域为公钥密码学,信息安全.

王平(1961－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为信息安全,系统软件,物联网软件.

汪定(1985－),男,博士,讲师,CCF 专业会员,主要研究领域为公钥密码学,信息安全.