

认证加密算法 SCREAM 及 iSCREAM 的新伪造攻击

田玉丹¹, 韦永壮^{2,3}

- (1. 桂林电子科技大学广西信息科学实验中心, 广西 桂林 541004;
2. 桂林电子科技大学认知无线电与信息处理省部共建教育部重点实验室, 广西 桂林 541004;
3. 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 100039)

摘 要: 认证加密算法能同时提供信息的加解密及完整性检验两个功能, 它已被广泛应用于各种网络安全系统中。最近伴随着欧洲 CAESAR 密码算法的征集活动, 认证加密算法倍受业界关注。SCREAM 算法凭借其新颖的设计理念和算法结构, 已经顺利入围 CAESAR 竞选中的第二轮候选算法。而该算法是否存在新的安全性问题是目前的研究热点之一。基于 SCREAM 参数的变化特点, 利用累加值碰撞的思想提出了一种新的伪造攻击。研究表明, 新攻击成功的概率为 1, 所需的时间复杂度及数据复杂度均可忽略; 此外该攻击同样适用于 SCREAM 的一种变体算法, 即 iSCREAM。与已有的攻击相比较, 新攻击所需的复杂度更低, 攻击范围更灵活有效。

关键词: SCREAM; iSCREAM; 伪造攻击; CAESAR; 认证

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00012

New forgery attack on the authenticated cipher SCREAM and iSCREAM

TIAN Yu-dan¹, WEI Yong-zhuang^{2,3}

- (1. Guangxi Experiment Center of Information Sciences, Guilin University of Electronic Technology, Guilin 541004, China;
2. Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China;
3. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100039, China)

Abstract: Authentication encryption algorithms have been widely used in networks security system since these algorithms can efficiently provide both privacy and integrity measurement for data transmission. Recently, authentication encryption algorithms have received attentions extensively since the event of CAESAR cipher solicitation was developed. SCREAM had been selected as one of the second-round candidates in CAESAR competition because of its novel structure and design idea. Currently, the security issue of SCREAM becomes an interesting research topic. Based on the characteristic of SCREAM variable parameters, a new forgery attack was proposed by using the basic idea of the sum collision. In particular, this attack could also be used to iSCREAM algorithm. Different to the best known attacks, the new attack requires less time and data complexities. It is shown that this new attack is more flexible and effective. Furthermore, the success probability of the forgery will be one.

Key words: SCREAM, iSCREAM, forgery attack, CAESAR, authentication

收稿日期: 2015-09-08; 修回日期: 2015-11-20。通信作者: 韦永壮, walker_wei@msn.com

基金项目: 国家自然科学基金资助项目 (No.61100185)

Foundation Item: The National Natural Science Foundation of China (No.61100185)

1 引言

认证加密算法可以同时实现信息的加解密和完整性检验两个功能, 它已被广泛应用于各种网络安全系统中。2013 年以来, 伴随着 CAESAR 征集活动^[1], 认证加密算法倍受广泛关注^[2~5]。Vincent 等基于可调认证加密模型所提出的 SCREAM 算法^[6]具有新颖的设计理念和算法结构, 并顺利入围 CAESAR 第二轮候选算法。该算法采用 LS 基本模型^[7]及 SPN 基本加密模块, 具有安全性高、加密速率快、抵抗侧信道攻击等优点。分组长度为 128 位, 明文和相关数据长度分别小于 2^{131-8n_b} (n_b 表示随机数 N 的字节长度) 和 2^{130-8n_b} 个字节, N 的长度范围在 1 到 15 个字节之间。SCREAM 和 iSCREAM 的区别在于 SPN 型结构不同。目前该算法倍受关注, 其主要分析结果如下。

Siang 等^[8]针对 SCREAM 和 iSCREAM 提出伪造攻击; 成功伪造的概率是 $\frac{1}{2^{n_b}}$ (设明文的最末分组为 n_1 个 0), 时间复杂度和数据复杂度可以忽略不计。Gregor 等^[9]针对 iSCREAM 提出“依附 S 盒不变子空间”的攻击方法, 通过寻找弱密钥恢复全部密钥。该攻击数据复杂度为 2^{32} 个选择明文, 时间复杂度为 2^{48} 。文献[10]对 SCREAM 和 iSCREAM 的基本结构进行分析, 并归了算法中的 TAE 模型及 SPN 结构。

由上可知, 文献[8]对明文要求高、攻击范围小、成功概率低; 文献[9]是基于 SPN 结构的攻击, 该攻击数据复杂度、时间复杂度都较高, 且只能攻击 iSCREAM 算法。那么, 针对 SCREAM 和 iSCREAM 能否找到一个高效的攻击, 成为当前密码学者研究的热点之一。

本文根据 SCREAM 和 iSCREAM 的可变参数 T 的计数特点提出新伪造攻击。研究表明, 新攻击可以删除明文的 $r-1$ 个分组 ($2 \leq r \leq m$), 使生成的标签 tag 不变。该攻击成功的概率为 1, 时间复杂度、数据复杂度可忽略不计。因此该攻击具有范围广、效率高等优点。

2 SCREAM 和 iSCREAM 算法介绍

通过对可调认证加密模型^[11] (TAE) 改进得

到算法 SCREAM 和 iSCREAM。SCREAM 和 iSCREAM 是 128 位加密算法, 其基本模块 $E(k)$ 的 SPN 结构包括 8 位 S 盒和 16 位 L 盒。加密过程为 $SCREAM_k(P, N, A)$, 其输入是明文 P 、128 位密钥 K 、随机数 N (建议使用 12 字节) 和相关数据 A , 输出为密文 C 和标签 tag 。解密过程为 $SCREAM_k^{-1}(C, N, A, tag)$, 输出为明文 P 和验证标签 tag^* (判断是否与 tag 匹配, 若是则返回明文 P , 否则返回空)。

SCREAM 和 iSCREAM 加密过程共分 3 个阶段, 如图 1 所示, 相关数据处理阶段、明文加密阶段、生成 tag 阶段。第一阶段, 把相关数据 A 划分为 128 位的分组, 第 i 个分组表示为 A_i 。可调分组加密器 $E(k)$ 对 A_i 进行加密, 然后将所有输出值进行异或, 便得到这一步的主要输出值 (表示为 $auth$)。如果最后一个分组长度不足 128 位, 用 1 和 0 填充, 使得最后一个分组为 128 位 (填充的数据表示为 $(10^*) := (10000 \cdots 0)$); 如果最后一个分组长度为 128 位, 那么不需要填充, 只是在加密过程中使用不同的 T_i^* 。第二阶段, 将明文 P 划分为 128 位的分组, 用加密模块 $E(k)$ 对 P_i 进行加密, 输出密文表示为 C_i 。如果明文的最末一个分组长度不足 128 位, 则对明文最后分组的位长 $|P_{m-1}|$ 加密, 将输出值截取同样长度后与明文 P_{m-1} 异或, 得到密文 C_{m-1} , 所以明文和密文长度是相同的。第三阶段, 将所有明文分组 (填充后的明文) 进行异或得到校验和 Σ , 然后对校验和进行加密, 将输出值与 $auth$ 异或得到 tag 。

在 TAE 模型中, 为了增强加密算法的安全性, 在加密不同分组时采用不同的 T 值。一般情况下, T 表示为 $(N \parallel \text{控制位} \parallel c)$, c 是明文分组计数器。具体情况如下。

相关数据处理阶段:

1) 相关数据最后一个分组除外

$$T_c^* = (N \parallel 10 \parallel c)$$

2) 相关数据最后一个分组为 128 位

$$T_c^* = (N \parallel 11 \parallel 010 \parallel 0^*)$$

3) 相关数据最后一个分组不足 128 位

$$T_c^* = (N \parallel 11 \parallel 011 \parallel 0^*)$$

明文加密阶段:

1) 明文最后一个分组除外

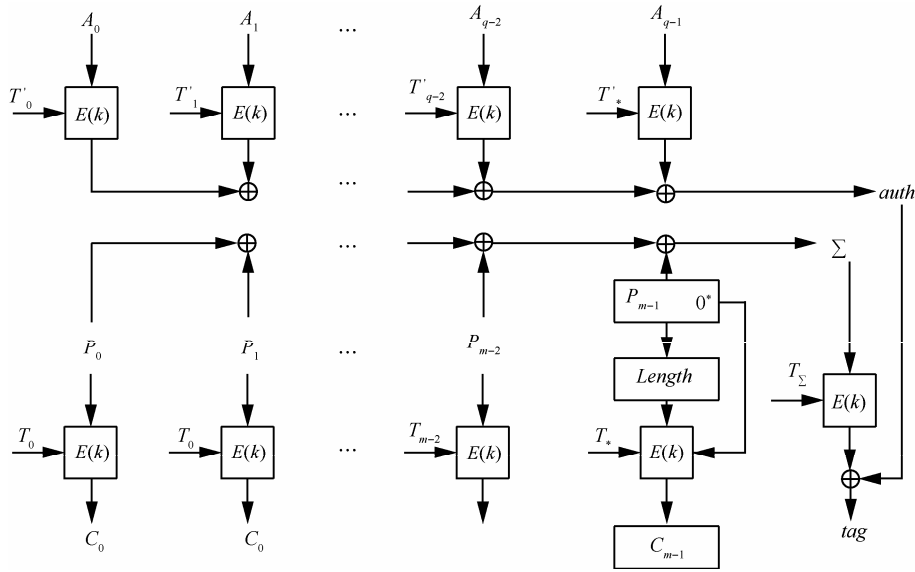


图 1 SCREAM 和 iSCREAM 的加密过程

$$T_c = (N \parallel 0 \parallel c)$$

2) 明文最后一个分组为 128 位

$$T_* = (N \parallel 11 \parallel 000 \parallel 0^*)$$

3) 明文最后一个分组不足 128 位

$$T_* = (N \parallel 11 \parallel 001 \parallel 0^*)$$

tag 标签生成阶段:

1) 明文最后一个分组为 128 位

$$T_\Sigma = (N \parallel 11 \parallel 100 \parallel 0^*)$$

2) 明文最后一个分组不足 128 位

$$T_\Sigma = (N \parallel 11 \parallel 101 \parallel 0^*)$$

引理 1 如果随机数 N 相同, 那么对应分组的 T_c 、 T_c' 相同; 如果随机数 N 相同, 且相关数据 A 相同, 那么对应的 T_* 相同; 如果随机数 N 相同, 且明文的最后一个分组长度相同, 那么对应的 T_* 、 T_Σ 相同。

证明 根据 T_c 、 T_c' 的构成原理, 这两个可变量由随机数 N 、计数器 c 和一些固定常数级联而成。如果 N 相同, 那么加密任意明文时, 对应分组 (c 相同) 的输入参数 T_c 、 T_c' 也相同。

N 和特定常数级联构成 T_* , 该常数取决于相关数据最后分组是否是 128 位。如果 N 相同且相关数据相同, 那么对应的 T_* 相同。

N 和特定常数级联构成 T_* 、 T_Σ , 该常数取决于明文的最后分组是否是 128 位。如果 N 相同且明文的最后分组长度相同, 那么对应的 T_* 、 T_Σ 相同。

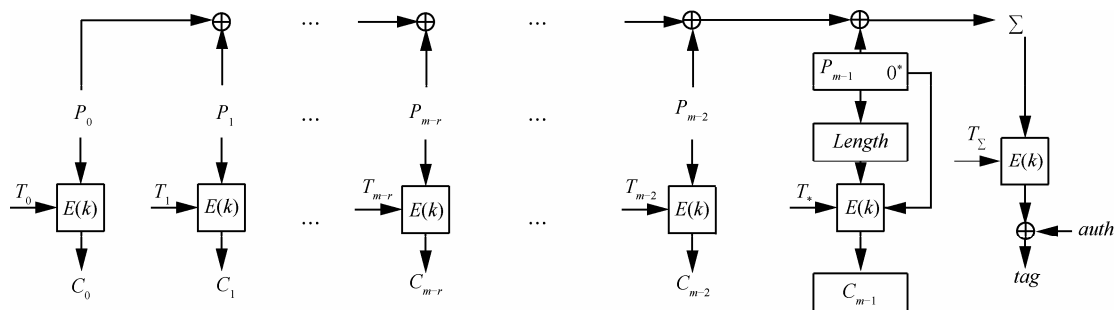
3 伪造攻击的基本思想

Brincat 等在文献[12]中提出了一种攻击方法, 即伪造攻击 (forgery attack), 这一攻击已广泛的应用到 CAESAR 算法^[13,14]的攻击当中。本文给出了 3 种形式的伪造方式, 其基本思想归纳为: 假设攻击者已经知道某一对应关系, 输入 (明文 1、公开变量 1、相关数据 1) 与输出 (密文 1、认证标签 1) 有效对应。那么, 如果能够找到另一输入 (明文 2、公开变量 2、相关数据 2) 与输出 (密文 2、认证标签 2) 有效对应, 而这一对应关系是不被密钥持有者所知晓的, 那么就称这一过程为有效的伪造攻击。

4 对 SCREAM 和 iSCREAM 的删除明文伪造攻击 (以 SCREAM 为例)

根据第 1 节对 SCREAM 的介绍, 设明文长度为 m 个分组。在 P_0 到 P_{m-2} 这 $m-1$ 个明文加密过程中, 可变参数 $T_c = (N \parallel 0 \parallel c)$ 是根据计数器 c 变化的; 当加密 P_{m-1} 时, 可变参数为常量 $T_* = (N \parallel 11 \parallel 000 \parallel 0^*)$ 或 $T_* = (N \parallel 11 \parallel 001 \parallel 0^*)$ 。根据算法的这种特性, 攻击过程如下。

步骤 1 对 m 个分组的明文 P 进行加密, 加密过程如图 2 所示。设随机数为 N , 相关数据为 A , 输入明文为 $P = (P_0 \parallel P_1 \parallel \dots \parallel P_{m-r} \parallel \dots \parallel P_{m-2} \parallel P_{m-1})$, 其中 $P_{m-r} \oplus P_{m-r+1} \oplus \dots \oplus P_{m-3} \oplus P_{m-2} = 0$ (共 $r-1$ 个分

图2 m 个分组明文的加密过程

组, $2 \leq r \leq m$)。其输出为 (C, tag) , 其中 $C = (C_0 \parallel C_1 \parallel \dots \parallel C_{m-r} \parallel \dots \parallel C_{m-2} \parallel C_{m-1})$ 。

步骤 2 保持随机数 N 、相关数据 A 与步骤 1 不变, 伪造 $m-r+1$ 个分组的明文 $P' = (P_0 \parallel P_1 \parallel \dots \parallel P_{m-r-1} \parallel P_{m-1})$ (与步骤 1 相比删除了明文中间连续的 $r-1$ 个分组), 如图 3 所示。那么, 输出值为 (C', tag) , 其中 $C' = (C_0 \parallel C_1 \parallel \dots \parallel C_{m-r-1} \parallel C_{m-1})$ 。

伪造攻击正确性分析如下。

因为步骤 1 和步骤 2 这两次加密过程随机数 N 和相关数据 A 都相同, 根据引理 1 可知, 步骤 1、步骤 2 中 T_c' 、 T_s' 对应相同, 因此两次加密过程具有相同的 $auth$ 值 (在图 1 和图 2 中将相关数据处理阶段省略, 只假设该阶段输出值为 $auth$)。步骤 1 中, 加密 m 个分组的明文 $P = (P_0 \parallel P_1 \parallel \dots \parallel P_{m-r} \parallel \dots \parallel P_{m-2} \parallel P_{m-1})$, 有 $P_{m-r} \oplus P_{m-r+1} \oplus \dots \oplus P_{m-3} \oplus P_{m-2} = 0$, 所以 $\sum P_j = \sum P_i \oplus P_{m-r} \oplus P_{m-r+1} \oplus \dots \oplus P_{m-3} \oplus P_{m-2} = \sum P_i'$, 即步骤 1 和步骤 2 得到的累加和相同。又因为步骤 1 和步骤 2 中 N 相同, 且明文的最后分组都是 P_{m-1} , 根据引理 1 可知两

次加密的 T_Σ 相同。由以上 3 个条件和 tag 的生成原理可知: $tag' = tag$, 即两次加密得到的标签相同。

根据引理 1 可知两次加密对应的 T_c 不变, P 去掉 P_{m-r} 到 P_{m-2} 这 $r-1$ 个连续的分组后得到明文 P' , 所以两次加密的前面 $m-r$ 个明文的加密过程完全没有变, 因此前 $r-1$ 个输出密文不变。 P 和 P' 的最后一个分组都为 P_{m-1} , 根据引理 1 可知 T_s 不变, 所以 P_{m-1} 的加密过程完全不变, 因此 C_{m-1} 也不变。所以图 3 中输出密文为 $C' = (C_0 \parallel C_1 \parallel \dots \parallel C_{m-r-1} \parallel C_{m-1})$ 。伪造成功的概率为 1。

5 结果分析与对比

表 1 列出了 SCREAM 和 iSCREAM 的攻击结果。由表 1 可知, 本文攻击对明文没有严格限制, 成功概率为 1, 可以删除明文的 $r-1$ 个分组 ($2 \leq r \leq m$), 而文献[8]要求明文的最后分组为全 0, 伪造成功的概率为 $\frac{1}{2^n}$, 只能伪造明文的最

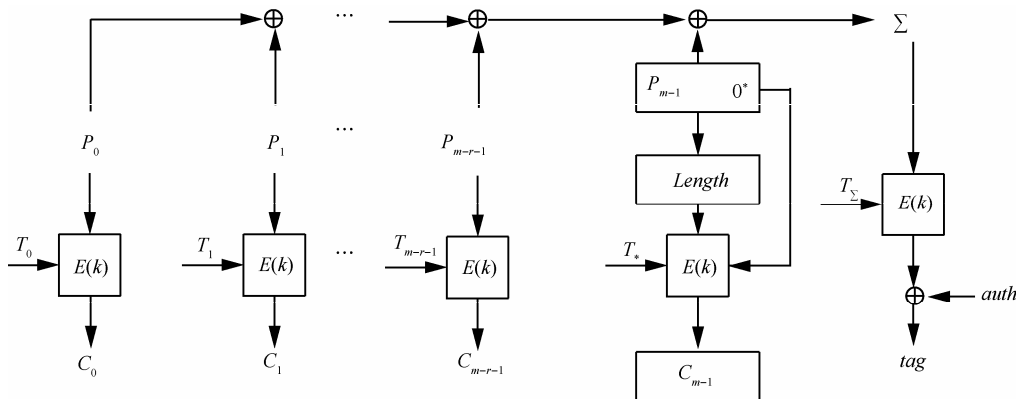
图3 $m-r+1$ 个明文分组的加密过程

表 1

SCREAM 和 iSCREAM 的攻击结果比较

攻击类型	明文要求	数据复杂度, 时间复杂度, 成功概率	攻击范围	攻击
针对最后明文分组的伪造攻击	明文的最后分组为 n_1 个 0	$(2, 2, \frac{1}{2^{n_1}})$	SCREAM 和 iSCREAM 算法中明文最后分组的 n_1 位	文献[8]
不变子空间攻击	无	$(2^{32}, 2^{48}, 1)$	只能攻击 iSCREAM	文献[9]
新伪造攻击	无	$(2, 2, 1)$	SCREAM 和 iSCREAM 算法中明文 $r-1$ 个分组	本文

后 n_1 位 (随着伪造位数 n_1 的增大, 成功概率 $\frac{1}{2^{n_1}}$ 指数倍减小)。文献[9]的时间复杂度、数据复杂度都远大于本文攻击, 且只对 iSCREAM 算法有攻击性, 并不能攻击 SCREAM 算法。因此本文提出的攻击更加实用有效。

6 结束语

认证加密是当前密码学者研究的热点和难点。本文基于认证加密算法 SCREAM 的参数特点, 利用累加值碰撞的思想寻找出新的明文、密文对应关系, 从而实现新伪造攻击。在新攻击过程中, 经过一次加解密模块访问后, 成功伪造的概率为 1。与已有的攻击相比, 新攻击所需的复杂度低、攻击范围大。该攻击同样适用于 iSCREAM (SCREAM 的变体算法)。

参考文献:

- [1] CAESAR-competition for authenticated encryption: security, applicability and robustness[DB/OL]. <http://competitions.cr.yp.to/caesar.html>.
- [2] NASOUR B, JAVAD A, MOHAMMAD R. A single query forgery on avalanche1[J]. Cryptographic Competitions Mailing List, 2014.
- [3] GUY B. Forgery on stateless cmcc[DB/OL]. <http://eprint.iacr.org/eprint-bin/search.pl>.
- [4] CHRISTOPH D, MARIA E, FLORIAN M, et al. Forgery and key recovery attacks on calico[DB/OL]. http://ascon.iaik.tugraz.at/files/analysis_calico.pdf.
- [5] THOMAS F, GAËTAN L, VALENTIN S. Forgery and key-recovery attacks on CAESAR candidate marble[DB/OL]. https://www.researchgate.net/publication/278829118_Forgery_and_key-Recovery_Attacks_on_CAESAR_Candidate_Marble.
- [6] GROSSO V, LEURENT G, STANDAERT F, et al. SCREAM & iSCREAM side-channel resistant authenticated encryption with masking[DB/OL]. <http://competitions.cr.yp.to/round1/screamv1.pdf>.
- [7] GROSSO V, LEURENT G, STANDAERT F, et al. LS-designs: bitslice encryption for efficient masked software implementa-

tions[C]// Fast Software Encryption. Berlin: Springer, c2014: 18-37.

- [8] SIANG M, LEI W. Practical forgery attacks on scream and iscream[DB/OL]. http://www1.spms.ntu.edu.sg/~syllab/m/images/b/b3/Forgery_AttackonSCREAM.pdf.
- [9] GREGOR L, BRICE M, SONDRE R. A generic approach to invariant subspace attacks: cryptanalysis of robin, iscream and zorro[DB/OL]. <http://link.springer.com/chapter/10.1007%2F978-3-662-46800-511>.
- [10] ABED F, FORLER C, LUCKS S. General Overview of the First-Round CAESAR Candidates for Authenticated Encryption[R]. 2014.
- [11] LISKOV M, RIVEST R L, WAGNER D. Wagner. Tweakable block ciphers[J]. Journal of Cryptology, 2011, 24(3): 588-613.
- [12] BRINCAT K, MITCHELL C J. New CBC-MAC forgery attacks[C]//Lecture Notes in Computer Science. c2010: 3-14.
- [13] 陈杰, 胡予濮, 韦永壮. 随机消息伪造攻击 PMAC 和 TMAC-V[J]. 计算机学报, 2007, 30(10): 1827-1832.
CHEN J, HU Y P, WEI Y Z. Random message forgery attack PMAC and TMAC-V[J]. Chinese Journal of Computers, 2007, 30(10): 1827-1832.
- [14] 晁仕德, 张绍兰, 田华, 等. 改进的 PMAC 及安全性分析[J]. 计算机工程与应用, 2009, 45(21): 77-78.
CHAO S D, ZHANG S L, TIAN H, et al. Modified PMAC and security analysis[J]. Computer Engineering and Applications, 2009, 45(21): 77-78.

作者简介:



田玉丹 (1990-), 女, 山东菏泽人, 桂林电子科技大学硕士生, 主要研究方向为认证加密。



韦永壮 (1976-), 男, 广西田阳人, 博士, 桂林电子科技大学教授, 主要研究方向为信息安全。

基于 Android 系统免 Root 主防方法的研究

刘井强, 李斌, 陈立章, 陈彬

(哈尔滨工业大学(威海)计算机科学与技术学院, 山东 威海 264209)

摘要: 为解决 Android 手机获取 Root 权限系统安全性的降低, 非 Root 授权下 Android 手机安全应用防护效果不理想的一系列问题, 研究了 ART 运行时工作原理、Java 反射机制和 AOP 原理, 设计验证了一套免 Root 主动防御机制, 避免了传统防护应用在系统内核层 Hook 系统关键函数需要 Root 授权带来的安全问题以及在应用层调用 API 效果不理想的现状, 实现了对手机应用的敏感行为拦截, 能够达到增强 Android 手机防护的效果。

关键词: Android 系统; 免 Root 主防; AOP; Hook; 行为拦截; Dalvik

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00013

Research based on the method of Android system active defense without Root permission

LIU Jing-qiang, LI Bin, CHEN Li-zhang, CHEN Bin

(College of Computer Science and Technology, Harbin Institute of Technology, (Weihai), Weihai 264209, China)

Abstract: In order to solve the problem that the system security is reduced through getting Root permission and that the security of Android smartphone is not effective without Root permission, the working principle of ART, the Java reflection mechanism and AOP principle were studied. The new mechanism was designed and implemented to avoid the security problem caused by the traditional protection application of Hooking system function in the kernel layer and the limitations with calling API in the application layer ineffectively. The interception of sensitive behavior and the protection of smartphone were both achieved.

Key words: Android system, active defense without Root, AOP, Hook, behavior interception, Dalvik

1 引言

Android 是 Google 推出的以 Linux 内核为基础的开源移动操作系统, 采用 4 层分层架构, 从上层到底层依次为应用层、应用框架层、Android 运行时和库文件层、Linux 内核层, Android 系统层次架构如图 1 所示。

近几年智能手机的普及暴露出一系列移动平台安全问题, 尤其是 Android 平台恶意应用泄露隐私的现象更是屡见不鲜^[1], Android 平台敏感行

为检测已经成为安全研究的热点^[2]。入侵检测等被动防御技术不能在系统的脆弱性方面做出预判断, 而主动防御技术能够克服这一缺点, 通过分析敏感操作预测攻击角度, 做出主动防御策略响应^[3]。通过在 Linux 内核层对服务和进程进行注入, Android 安全应用从恶意代码定义出发, Hook 系统关键函数调用, 能够对程序恶意行为做出判断, 但前提是取得 Root 授权。鉴于开放 Root 授权后会降低手机系统安全性, 手机生产厂商反对 Root 授权。安全应用厂商以漏洞利用方式获取