Software Engineering and Applications 软件工程与应用, **2018, 7(1), 1-12**
Published Online February 2018 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2018.71001

Research on AES Cache Attack Technology Based on ARM Processor

Bo Li

School of Computer and Engineering, Beihang University, Beijing
Email: leborn@buaa.edu.cn

Received: Feb. 6th, 2018; accepted: Feb. 18th, 2018; published: Feb. 24th, 2018

Abstract

Cache attack is a powerful attack tool that can access the user's private information based on the memory access mode revealed by the Cache, such as the user's keyboard input, encryption keys, etc. On Intel x86 platform, there have been Cache attack implementations aiming at AES, DES encryption algorithm, but on the Android platform, the structure of the Cache, instruction Set and Cache replacement strategy have a lot of differences from that of Intel x86, so Cache attack on mobile devices is difficult. This paper reduces the impact of random error of the experimental results on the Android platform by introducing hypothesis testing, eventually getting all AES key bytes. Then this paper explores the asynchronous attack mode.

Keywords

Cache Attack, AES Attack, AES Cache

基于ARM处理器的AES缓存攻击技术研究

李　勃

北京航空航天大学，北京
Email: leborn@buaa.edu.cn

收稿日期：2018年2月6日；录用日期：2018年2月18日；发布日期：2018年2月24日

摘　要

Cache攻击是一种强大的攻击工具，能够根据Cache泄露的内存访问模式获取用户的私密信息，比如用户的键盘输入、加密的密钥等。在Intel x86平台上，已经有针对AES、DES加密算法的Cache攻击实现，但是在Android平台上，由于Cache结构、指令集、Cache替换策略等与Intel x86有很多差别，因此攻击难

文章引用: 李勃. 基于 ARM 处理器的 AES 缓存攻击技术研究[J]. 软件工程与应用, 2018, 7(1): 1-12.
DOI: 10.12677/sea.2018.71001