
出版

2013 2015

第 33 卷第 6 期
2022 年 6 月

(Ruanjian Xuebao)

杨 珉 张 超 宋 富 张 源 (1959)
C 于银菠 刘家佳 慕德俊 (1961)
TaintPoint: 方浩然 郭 帆 李航宇 (1978)
徐浩然 王勇军 黄志坚 解培岱 范书珲 (1996)
SGX2 李明煜 夏虞斌 陈海波 (2012)
Linux 谈 心 杨悉瑜 曹家俊 张 源 (2030)
Toast
凌 振 杨 彦 刘睿钊 张 悦 贾 康 杨 明 (2047)
C/C++ 李广威 袁 挺 李 炼 (2061)
杨松涛 陈凯翔 王 准 张 超 (2082)
邢 颖 钱晓萌 管 宇 章世豪 赵梦赐 林婉婷 (2097)

曹钦翔 詹博华 赵永望 (2113)
江 南 汪吕蒙 张晓曈 何炎祥 (2115)
郭 昊 曹钦翔 (2127)
Coq 石正璞 崔 敏 谢果君 陈 钢 (2150)
PPTL 王小兵 寇蒙莎 李春奕 赵 亮 (2172)
靳翠珍 张倩颖 马雨薇 李希萌 王国辉 施智平 关 永 (2189)
Coq 严 升 郁文生 付尧顺 (2208)
Coq 麻莹莹 陈 钢 (2224)
陈善言 关 永 施智平 王国辉 (2246)
张博闻 金 钊 王捍贫 曹永知 (2264)

郑 炜 王晓龙 陈 翔 夏 鑫 廖慧玲 刘程远 孙瑞阳 (2288)
李少峰 乔 磊 杨孟飞 张锦坤 马 智 刘洪标 (2312)

孙琛琛 申德荣 肖迎元 李玉坤 (2331)

张啸剑 徐雅鑫 夏庆荣 (2348)

: CN11-2560/TP*1990*m*16*405*zh+en*P*¥70*2022*22*2022-06

Journal of Software Vol.33, No.6 Jun. 2022

Contents

SPECIAL TOPIC ON SYSTEMS SOFTWARE SECURITY

1959 Preface
YANG Min, ZHANG Chao, SONG Fu, ZHANG Yuan

1961 Counterexample-guided Spatial Flow Model Checking Methods for C Codes
YU Yin-Bo, LIU Jia-Jia, MU De-Jun

1978 TaintPoint: Fuzzing Taint Flow Efficiently with Live Trace
FANG Hao-Ran, GUO Fan, LI Hang-Yu

1996 Compiler Fuzzing Test Case Generation with Feed-forward Neural Network
XU Hao-Ran, WANG Yong-Jun, HUANG Zhi-Jian, XIE Pei-Dai, FAN Shu-Hui

2012 Memory Optimization System for SGXv2 Trusted Execution Environment
LI Ming-Yu, XIA Yu-Bin, CHEN Hai-Bo

2030 Refcount Field Identification for Linux Kernel Based on Deep Learning
TAN Xin, YANG Xi-Yu, CAO Jia-Jun, ZHANG Yuan

2047 Repeating Toast Drawing Based Password Inference Attack Technique
LING Zhen, YANG Yan, LIU Rui-Zhao, ZHANG Yue, JIA Kang, YANG Ming

2061 Study of State-of-the-art Open-source C/C++ Static Analysis Tools
LI Guang-Wei, YUAN Ting, LI Lian

2082 Exploit-oriented Automated Information Leakage
YANG Song-Tao, CHEN Kai-Xiang, WANG Zhun, ZHANG Chao

2097 Cross-project Defect Prediction Method Using Adversarial Learning
XING Ying, QIAN Xiao-Meng, GUAN Yu, ZHANG Shi-Hao, ZHAO Meng-Ci, LIN Wan-Ting

SPECIAL TOPIC ON THEOREM PROVING*: *THEORY AND APPLICATIONS

2113 Preface
CAO Qin-Xiang, ZHAN Bo-Hua, ZHAO Yong-Wang

2115 Mechanized Verification of Efficient Iterative Data-flow Algorithm
JIANG Nan, WANG Lü-Meng, ZHANG Xiao-Tong, HE Yan-Xiang

2127 Semantics under Step-indexed Model and Formalization
GUO Hao, CAO Qin-Xiang

2150 Coq Formalization of Propulsion Subsystem of Flight Control System for Multicopter
SHI Zheng-Pu, CUI Min, XIE Guo-Jun, CHEN Gang

2172 Implementation of Theorem Prover for PPTL with Indexed Expressions
WANG Xiao-Bing, KOU Meng-Sha, LI Chun-Yi, ZHAO Liang

2189 Refinement-based Verification of Memory Isolation Mechanism for Trusted Execution Environment
JIN Cui-Zhen, ZHANG Qian-Ying, MA Yu-Wei, LI Xi-Meng, WANG Guo-Hui, SHI Zhi-Ping, GUAN Yong

2208 Formalization of C.T.Yang's Theorem in Coq
YAN Sheng, YU Wen-Sheng, FU Yao-Shun

2224 Coq-based Matrix Code Generation Technology
MA Ying-Ying, CHEN Gang

2246 Formalization of Collision Detection Method for Robots
CHEN Shan-Yan, GUAN Yong, SHI Zhi-Ping, WANG Guo-Hui

2264 Tool for Verifying Cloud Block Storage Based on Separation Logic
ZHANG Bo-Wen, JIN Zhao, WANG Han-Pin, CAO Yong-Zhi

SYSTEM SOFTWARE AND SOFTWARE ENGINEERING

2288 Systematic Literature Review of Duplicated Bug Report Detection Methods
ZHENG Wei, WANG Xiao-Long, CHEN Xiang, XIA Xin, LIAO Hui-Ling, LIU Cheng-Yuan, SUN Rui-Yang

2312 Verification Method of Hierarchical for Safety-critical Memory Management Systems
LI Shao-Feng, QIAO Lei, YANG Meng-Fei, ZHANG Jin-Kun, MA Zhi, LIU Hong-Biao

DATABASE TECHNOLOGY

2331 Multi-attribute Data Indexing for Query Based Entity Resolution
SUN Chen-Chen, SHEN De-Rong, XIAO Ying-Yuan, LI Yu-Kun

COMPUTER NETWORKS AND INFORMATION SECURITY

2348 Histogram Publication under Shuffled Differential Privacy
ZHANG Xiao-Jian, XU Ya-Xin, XIA Qing-Rong

ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(6):2047 2060 [doi: 10.13328/j.cnki.jos.006568]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

Toast

[1](, 211189)
[2](, 510632)
: , E-mail: yangming2002@seu.edu.cn

: 移动终端在飞速发展的同时也带来了安全问题, 其中, 口令是用户信息的第一道安全防线, 因此针对用户口令的窃取攻击是主要的安全威胁之一. 利用 Android 系统中 Toast 机制设计的缺陷, 实现了一种基于 Toast 重复绘制机制的新型口令攻击. 通过分析 Android Toast 机制的实现原理和功能特点, 发现恶意应用可利用 Java 反射技术定制可获取用户点击事件的 Toast 钓鱼键盘. 虽然 Toast 会自动定时消亡, 但是由于 Toast 淡入淡出动画效果的设计缺陷, 恶意应用可优化 Toast 绘制策略, 通过重复绘制 Toast 钓鱼键盘使其长时间驻留并覆盖于系统键盘之上, 从而实现对用户屏幕输入的隐蔽劫持. 最后, 攻击者可以通过分析用户点击在 Toast 钓鱼键盘上的坐标信息, 结合实际键盘布局推测出用户输入的口令. 在移动终端上实现该攻击并进行了用户实验, 验证了该攻击的有效性、准确性和隐蔽性, 结果表明: 当口令长度为 8 时, 攻击成功率为 89%. 发现的口令漏洞已在 Android 最新版本中得到修复.

: 口令攻击; Java 反射; Toast 重复绘制
: TP311

: , , , , , . Toast . , 2022, 33(6): 2047–2060. http://www.jos.org.cn/1000-9825/6568.htm

: Ling Z, Yang Y, Liu RZ, Zhang Y, Jia K, Yang M. Repeating Toast Drawing Based Password Inference Attack Technique. Ruan Jian Xue Bao/Journal of Software, 2022, 33(6): 2047 2060 (in Chinese). http://www.jos.org.cn/1000-9825/6568.htm

Repeating Toast Drawing Based Password Inference Attack Technique

LING Zhen[1], YANG Yan[1], LIU Rui-Zhao[1], ZHANG Yue[2], JIA Kang[1], YANG Ming[1]

[1](School of Computer Science and Engineering, Southeast University, Nanjing 211189, China)
[2](College of Cyber Security, Jinan University, Guangzhou 510632, China)

Abstract

Key words: password attack; Java reflection; repeating Toast drawing

, , . GSMA [1], 2021 4 , 78 , 51 . Android , , . Android . Android , , , . IDC [2], 2023 , 1 512 .

, . : , . : , , [3 7]; , [8,9] [10] , , ; [11 14] . , , , , . , . , , . Android Toast , Toast , , . Toast , Toast , . , Toast , Toast , . Android , , . , Java Android Toast , Toast , Toast , . Android 10 . Android 11 , Java Toast . Wang [15] Toast Overlay Android 11 , .

:

(1) Toast . Android Toast , Toast , Toast , , ;

(2) . Android : Java , Toast . , Toast , , ;

(3) . Android ; , . :

, 12 , 84.5%. , .

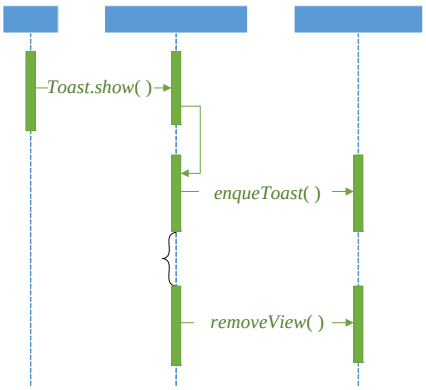
1 Toast . 2 Toast . 3 . 4 Toast . 5 . 6 .

1

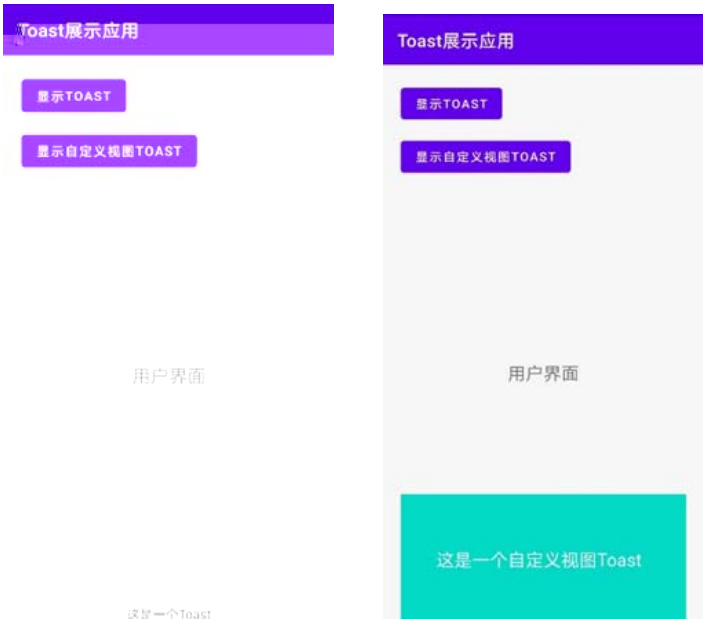
Android Toast . Toast Toast
, .

1.1 Toast

Toast Android ,
, ,
, . Toast
1 . Toast Toast.
Toast, Toast , *show*( )
. Toast *show*( ) ,
NotificationManager , *enqueueToast*( ) ,
(NotificationManager). ,
, (WindowManager),
Toast , Toast 2 s 3.5 s
.



Toast , . 1 Toast
Toast *Toast.makeText* (*context*,*text*,*duration*) Toast . *text*
Toast , *duration* Toast , :
LENGTH_LONG *LENGTH_SHORT*, 3.5 s 2 s. 2(a) ,
Toast, : “ Toast”. , Toast *setView*( )
(view), 2(b) .



(a) Toast (b) Toast

2 Toast
Toast , *removeView*( ) ,

Toast . , 500 ms , Toast
0. , , Toast . *removeView*( )
, , Toast , Toast,
Toast Toast .

1.2

Android Android ,
Android . Android ,
TalkBack, TalkBack ,
. , Android API .
, [12,16,17].
, , .
ID .
, ID,
, , . ,
, .

2

Android . Android ,
Toast , , Toast .

2.1

.

(1) , .
,
, , . Diao [18]
337 , (56.7%)
100 . Felt [19] , 17% .
Fratantonio [16] ;

(2) , .
;

(3) , ,
.

2.2

Toast , Toast .

(1) Toast , , ;

(2) Toast , . Toast ,
Toast Toast , Toast
;

(3) Toast .
Toast , Toast
. , .
Toast , Toast .

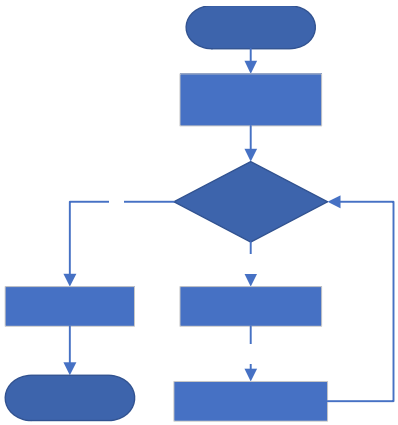
, , . ,
, Toast ,
, . , Toast , Android
, Java Toast .
. , ,
. , Toast
, . ,
.

3 Toast

Toast , ,
, , Toast ,
, .

3.1

3 , Toast 4 ,
. , ,
, . ,
, .



3 Toast

4 .

3.2

Toast .
, . ,
, .
, , .
, ,
. , EditText, ,
isPassword( ) true. , . ,
, .

3.3

, . , Toast
, , . Toast
3 : 1 Toast , 2
Toast , 3
.

3.3.1

Toast , .
. , Toast
, . , Toast , ,
, Toast . Android : Toast
Toast *mTn* *mNextView* , *mParams* ,
FLAG_NOT_TOUCHABLE[20], , 1 .

1. Toast .

```
1:  final WindowManager.LayoutParams params=mParams;
2:  params.type=WindowManager.LayoutParams.TYPE_TOAST;
3:  params.setTitle("Toast");
4:  params.flags=WindowManager.LayoutParams.FLAG_KEEP_SCREEN_ON
5:          |WindowManager.LayoutParams.FLAG_NOT_FOCUSABLE
6:          |WindowManager.LayoutParams.FLAG_NOT_TOUCHABLE;
```

Toast , Toast *show*( )
mNextView , *mParams* , *FLAG_NOT_TOUCHABLE* , , Toast
. *mTn* *mParams* public , ,
. , Java *mTn* , *mTn*
mParams , Toast , 2 .

2. Toast .

```
1:  Toast toast=new Toast(MainActivity.this);
2:  toast.setView(keyboard);  //
3:  Field f=toast.getClass( ).getDeclaredField("mTN");
4:  f.setAccessible(true);  //  Java  Toast  mTN
5:  Object mTn=f.get(toast);  //  toast  mTN
6:  Field f2=mTn.getClass( ).getDeclaredField("mParams");  //  mTn  TN  mParams

7:  f2.setAccessible(true);  //  Java  TN  mParams
8:  Object mParams=f2.get(mTn);  //  mTn  mParams
9:  mParams.flags=WindowManager.LayoutParams.FLAG_NOT_FOCUSABLE;  //
10: toast.show( );
```

3.3.2 Toast
, . Toast
3.5 s, .
, , .
.

1.1 , Toast ,
Toast . Toast, 1 Toast , Toast
Toast , Toast ,
Toast , Toast .
Toast 4 .

1. , *Toast.show*( )
Toast;

2. Toast token,
enqueueToast( ) Toast , token Toast;

3. token, Toast
. token, Toast token ,
Toast[21];

4. Toast (2 s 3.5 s) , *removeView*( )
Toast ;

5. Toast , . ,
Toast token, Toast .

D 1 5, Toast .
4 , Toast T_a, , Toast,
, . T_s, Toast
T_d, $T_s/(T_d+T_a)$ 1. Toast
Toast , $T_d/(T_d+T_a)$. : T_d , , .
4.3.2 , , Toast 3.5 s.

Toast , *D* Toast , Toast . Android Toast token , Toast , *D* , token, , Toast , . , *D* , Toast , Toast Toast , . , *D* Toast , *D* , *D* 3.4 s .

3.3.3

. ,

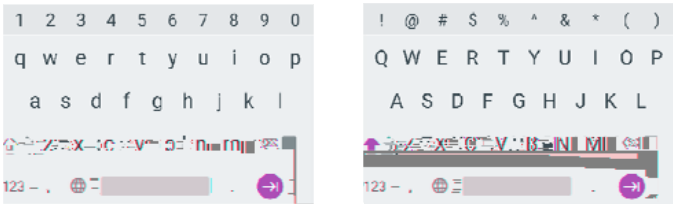
. , Toast ,

. , , , 5 ,

. , 5 .

, . Toast ,

setImageBitmap( ) Toast , .



5

, , ,

, . [22]

, , ,

. , ,

. , ,

. Pixel Gboard, ,

, Gboard .

, , , ,

.

3.4

, , .

, , ,

. Google Android Keyboard , ,

QWERTY 0 9 . [23] : *X* ,

,

, ,
. , ,
, . ,
performAction( ) , .

3.5

, . ,
, .
, Toast ,
Toast. , , ,
, 4.3.2 .
https://reurl.cc/WEzEM7. , Google Pixel 2 ,
, , , .
, Toast .
, Toast .

4

Toast . ,
; , ; ,
.

4.1

, .
, , Toast
, , .
, Google nexus6p, Android 8,
5 , Skype Instagram,
, . , .
, ,
, .
. 20 , 3
17 , 22 33 , 25 , , 20
2.

2

Samsung	s8	8
Samsung	SMG9	9
Google	nexus6p	8
Google	pixel 2xl, pixel 4	9
Vivo	v1813A, x21iA, v1816A, v1813BA	9
Oppo	PMEM00	9
Xiaomi	mi5	8
Xiaomi	mix 2s, mi6, mi8	9
Xiaomi	mix3	10
Huawei	EML-AL00, mate20	9
Huawei	nova3	9.1
Huawei	mate20 x, HMA	10

4.2

. 7 ,
. 7 , ,
10 , . 7 ,
. 3.

3

Skype	com.skype.raider	8.45.0.43
	com.facebook.katana	196.0.0.16.95
	com.evernote	8.4.1
	com.twitter.android	7.68.1
Instgram	com.instagram.android	69.0.0.10.95
	com.infonow.bofa	8.1.16
	com.eg.android.AlipayGphone	10.1.65

: , 7
. ,
. , , Toast ,
, .
, . , ,
, . ,
. , ,
, ,
, Toast .
: , Toast
.

4.3

, ,
. , Toast (2 s 3.5 s)
. , Toast
Toast .

4.3.1

, Toast 2 s (*LENGTH_SHORT*) 3.5 s (*LENGTH_LONG*) . 100
. , Toast C_t, C_p, $C_t/(C_t+C_p)$.
4 : , Toast , . :
, , Toast 3.5 s , Toast 2 s , .

4 Toast

	2 s (%)	3.5 s (%)
mix3	0	0
mix 2s	98	98
mi5	99	99
mi8	93	97

4 Toast ( )

	2 s (%)	3.5 s (%)
mi6	93	97
s8	0	0
SMG9	0	0
nova3	0	0
EML-AL00	96	99
nexus6p	98	99
mate20	98	100
HMA	0	0
mate20 x	0	0
pixel 2x1	85	93
pixel 4	96	99
v1813A	0	0
x21iA	0	0
v1816A	99	99
v1813BA	100	100
PMEM00	0	0

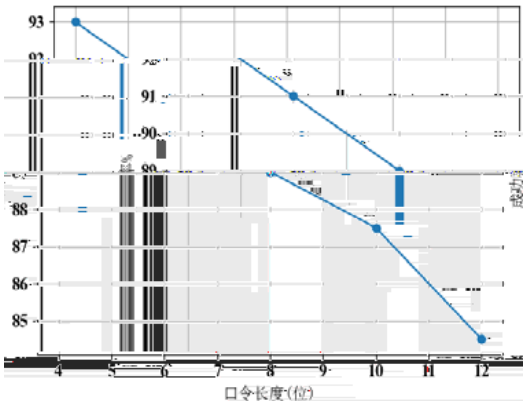
4.3.2

, Toast 3.5 s,

4 6 8 10 12 10 , . 6 .

: , . , Toast ,

. 12 , 84.5%. .



6 -

4.4

. , ,

, . : ,

. , ,

, . ,

. : , .

5

, ,

, .

, . ,

.

(1) . Maggi [3] ,
,
, . Yue [4]
, ,
, , . Xu [5]
, . Zhou [6]
, . Aviv [7] :
, .
, ,
. , , ,
;

(2) . Jung [8] : , .
, , ,
, . Aonzo [9]
, . Luman [10] Virtual App
, , ,
, . Ren [24] Android ,
. Wang [17] ActivityHijacker, Activity
, , .
,
. , Android , ;

(3) . Niemietz [12] Toast Android UI ,
. Kraunelis [13] , Android . Kalysch
[14] , Android . :
, . Fratantonio [16]
Overlay , Overlay ,
, . .
, . , Android
, .

6

Android Toast ,
. Toast, . , Java
Toast , Toast , . ,
. , ,
, .
Toast , Toast ,
, . ,
9 26 , ,
, , ; ,
, . ,
, , .

, ,
, , . ,
, .

References:

[1] GSMA. Representing the worldwide mobile communications industry. 2021. http://www.gsma.com

[2] IDC. Solid growth ahead for security products and services. 2019. https://www.idc.com/getdoc.jspcontainerId=prUS45591619

[3] Maggi F, Volpatto A, Gasparini S, Boracchi G, Zanero S. A fast eavesdropping attack against touchscreens. In: Proc. of the 7th Int'l Conf. on Information Assurance and Security (IAS). IEEE, 2011. 320 325.

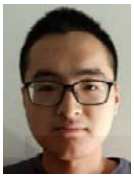
[4] Yue Q, Ling Z, Fu X, Liu B, Ren K, Zhao W. Blind recognition of touched keys on mobile devices. In: Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security. 2014. 1403

[24] Ren C, Zhang Y, Xue H, Wei T, Liu P. Towards discovering and understanding task hijacking in Android. In: Proc. of the 24th USENIX Security Symp. (USENIX Security 2015). 2015. 945 959.

(1982), , , , , CCF , , , , .

(1989), , , IoT .

(1998), , , CCF , .



(1995), , , .

(1998), , , .

(1979), , , , , CCF , , .

	/	
2022 3		, , ,
2022 4		, ,
2022 5		, , , ,
2022 6		, , ,
2022 6		, ,
2022 7		, ,
2022 8		,
2022 9		, , ,
2022 10		, , ,

R : http://www.jos.org.cn / .

Ruanjian Xuebao

(, 1990)

33 6 2022 6

Journal of Software

(monthly)

(Started in 1990)

Vol.33 No.6 Jun. 2022

Sponsored by the Chinese Academy of Sciences

Published by Institute of Software, The Chinese Academy of Sciences (ISCAS) and China Computer Fed4(Fed)-hi4oan

r4(38.2f:c)6.8 ZHAO( )6 Cen( )TJTD 017 Tc 0261 Tw Editte