# The not-so-silent type Breaking network crypto in almost every popular Chinese keyboard app

Jeffrey Knockel (Citizen Lab) and Mona Wang (Princeton University)





说 会記 122 and a -----生際高電 家品 中二 回北 1 做 年二 出部 很当 开品 些二 们言后語二こ 小二 对 点雪 ala hyver 12 -10 min 三品以品 学品 一同二少世 见品 一过二月二 作 老 前篇 着 女 国 几 也 还當 先當 关篇 2 4 2016 dery 话品吗 一给二已 明母名之今 东四 机 住品 从當 可 果常 水三 电 머리 爱 问言 -120 走出五日 两智 长雪 清二 认 200 道書 字 正 事 别 次品 但意 四 覚し 车 气 644 6041 2 2 ž all. 57 山谁言笑言 书 发。第二 怎些 地 让四 经品 题 身調 师二写二方三接二提一房三 期二教二张 用雪路之 向 公認 一员二 二间 -14 2 読告 100 200 3 ---火出 Anu alter 11院:一远日语二直是衣山空部穿出部 山完前眼出务品然日喝出总部足品讲出跑出往出舞品组出贵山 场雪影点 常四离 白 哪二 而影 种智 me 每二 被品 当 又正成二者二九一七二拿二 22 Also Apport 20 上友也马品子 望 便二其之 医二带 F 妈江应照主品世品亮調変與音品阿當跳品脚品菜品停品导致每 更 边言 重要 兴 视二 位二难二千 欢無号黑万品 站無校興错二平 ting 1010 二思二男ニ 脑ニ ~ 夫之始品备二试日记 一头三岁二 八三早 星四运 像黑实品 定品 买帮 孩 如 口二感日前日 法二元二 「泉銀馬 -----使 24 条調 客之九 心山谢二界 iner No. 此黑品红雪 10 2 朋 囙 加二或言 希 业 教品 步 诉二帮罪包非室非店非愿非坏罪言此支非毛形礼-例 病二乐》饭 事该 2 化 de la 九 24 aling -• 结 一无二与 冷認 步 相二町 姐 必二 共 文 市 解二弟 Da King 物二南 赵二山 凤四久 根馬 您是 球 片言轻 极 钟言 死 游 办 照此选二言三 25 41 2. 「訪 新节 二据 部段 22 Bat 122 习 内二 满言 刚 爸品 清二 哥 指 -Z. and the second -110 wire wytowy 「须二计 调品收益 (汉)合品 光宫 交上留品 历 周篇城常注記 何品 慢語任為神話民語杯語 馆二十二受三明三 EFE 狗 4 and an \*管 终四达是海昌 北示三乎? 2900 2014 -----100 20 -----易 参 台 午 史馬差四突而白 图二故二美二许 连 卖言 查照处照将四量照并照论是尔非 响雪 2. the minut 100 - 举 左部 命器 全部 切 右四酒品婚二来習假品 取品 歌 敢出深端虽正 底 M 伯 换 鱼 级 -----2. Ľ. -1 角四急 楼上内日 够二则 至二 士品怪 ~反二居 低 香品造品失品精 雨品 林二 度二父二赛一顾 妻二 20 side head 10 miles 旅 画 担 λ 活 迎 唱 案 境 掉 消 -14 ing n.d Arr 100 eary ary 份二环 洗山银山际 新草草 \*尽 懂 联 层四 性 功 调 社 旁與纸品般 原此代二练二夏二汽二累二职二福 黄黑亲二短部借品 雪品推品 破山超四持日志山激山腿四疑山章四镜山 床口较二制 格二简二昨 阳 ton 二笔 此姓 思李 and a courty 2000 aut Mont \*休 另 静品 普 改 划 伤雪密三戏二约二 土况 山文福寺端祖当择山水四正 部緊 品随 副区場 三民 二十 pan, proty 苦品茶言 奶 - 课 蛋奶基~ 林二育二排二科二具二 東二集山止日 金山群北纪山鮮品富山 楚三观二察日 北北山 一质二律- 速二克 Ving . 200 --Paciel 山忘即費日 怀品织品努品效用值品箱四舟 研二哭言 惊点词 抱罪 铁二鸡 - 术 河 技 旧 云二列二续二 5 100 2 牛展 de. 」梦二規二 板品趣品 仅小座1 弄 31 整 传二顿三烧三剧三降二 春 灯間 众二永二八二 一否二绝 24 一开之 See. 14 - 程二猫= 谷 究 野二 供福省四甚三养品 母二招二通 价品困 标二警点季 康二绍二典二 - 杂二农业 旅 an. tell. 北一卡 按二沙岛 健二维一丽一颜 险 醒 附 责 , and 二二半 20 . 24 北国 Julyo . 2. 输 蓝王败日 盘 微言 温書 叔 掌 细二范三仍言 吸出肯非既小硬日 m 100 2.00 皮 恐 味品讨是 騎三 限 获 ÉP 态 鸟部禁止惯罪 --die Ż. 优 奖 迟言 弹 修三 秋二 概 油 挺三释 答 洲 软當 坚思 响 » <u>A</u> 食品景点饿 ARTIN 二压 undu. -240 村二替 散三鼻三 烟止精二 秀之诚 免 忠二毕 「治四篇 鞋品 袋品 桂品 折 瓜盖 聪言 骗品 俩 松 寄 14 112 ADAQ ROMADCH T 博 舒 顺品 扫 货 陪 忽 江 邮品 冬二 童 材 -Jung anto Prime NUM 航二孤 染書 啊~? 忆 爬 窗 渐 乘 國 朵二 积 沾 丢 尊二弱山 鼓 扬四 撞 寬言页二酸 胖 齐 厉 逐 三厚語 20 ------Allen . They. He. -104 sing. 中二虎 奋二党 默二 播 汤 脏 碗品 倍 抬 勇 森品 of 24 1810 200 Real Property lies ź 汗 信言 帽 渡 暂 扔 刷 闹 漫 握 啡 猪 聊書 绩 熊 污 础 100 22 100 ------...... 10 and mat and an de. 貌遊打籃吵 币 估 偶 彩言 載二 允 临 厨 蕉 泪 炼 带 他島 x 丰 拒 10.0 in. - 平肥 12 二差 - 賺 -- géo 凉 帅 耐润 暖 钢 扮 THE FIRST 1000 CHINESE CHARACTERS



## How does one type/input Chinese?

7:13 🔍 🕈	7:13 🔹 🖿	7:13 🔍 🕈
← Jeff 🥄 📞 🗄	← Jeff <b>└ :</b>	← Jeff <b>└ :</b>
		sān 👳
C Send message	C Send message	三 二 三三 三个 三天 三点>
ni'hao 😨	ni'hao 😨	×
<mark>你好</mark> 你号 泥嚎 拟好 倪好 >	<mark>你好</mark> 你敢 你号 你干 你喊 >	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	mi 1 ABC DEF 🗵	
	ni 4 5 6	o
ASDFGHJKL	● GHI JKL MNO 重输	?
	m PQRS TUV WXYZ 0	!
符 123 , _ 。 中 <sub>英</sub> ←	符 123 _ 中 <sub>英</sub> ←	设置符 123 _ 中 <sub>英</sub> ←
▼ ● ■ =	▼ ● ■ =	<b>V</b> • <b>H</b> =

## The advent of "cloud-based" prediction



## The advent of "cloud-based" prediction



## The advent of "cloud-based" prediction

Google Faces Plagiarism Questions Over Chinese Software

Posted by Zonk on Sunday April 08, 2007 @03:03PM from the i'll-just-take-a-

#### yaohua2000 writes

"Google's laboratory in China has launched its first product, a <u>Pinyin Input Method Editor</u>. The software allows the romanized characters to be translated to more traditional Chinese symbols , via entering on a QWERTY keyboard. Users soon discovered that the data Google used for the product was unusually similar to the data used by a Chinese rival, Sogou. <u>Google has evaded the</u> <u>question</u> about software similarities, reports PC World. 'The similarities, which included an error involving the name of a celebrity, were noted on a Google Labs discussion board about its Pinyin IME. Users noted that entering the Pinyin pinggong into the Google IME incorrectly produced the name of Feng Gong, an actor and comedian.'" Landscape of Chinese IMEs

## MAU of most popular IME in 2022



## Landscape of Chinese IMEs

## 2023 market share of phone manufacturers in China



## They are keyloggers



## This talk is **not** about how they are keyloggers



## Threat model

- Attacks on Sogou: Active network adversary
- All other attacks?

## All other attacks: Passive network adversary



## Adversaries

- Anyone on your network
- Your ISP
- The server's ISP
- Every network in between
- Every state actor in between



# Where is X-KEYSCORE?

### Approximately 150 sites

### Over 700 servers

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



- \* UCWeb mobile browser identification
  - \* Discovered by GCHQ analyst during DSD workshop
  - \* Chinese mobile web browser leaks IMSI, MSISDN, IMEI and device characteristics



# UCWeb – XKS Microplugin

UCWe	b													
() Help	Help Actions * Reports * View * S Map View													
0	State	10	Datetime +	Highlights	Datetime End	Browser Version	Empil Address	Handset Model	8/EI	MŞI	Global Title	Platform	Active User/T Casenotation	
1 0		1	2012-05-13 02:29:20	11	2012-05-13 02:29:23	8.0.3.107	123movies	nokiae90-1			9379900100	java	ESDHL00000M0000	
2 [	1	2	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	2123movies	nokiae90-1			9379900100	java	E9DHL00000M0000	
3	1	4	2012-05-13 19:39:11	8	2012-05-13 19:39:11	7.9.3.103		HTC A510e				android	E98DE00000000000	
4.12	1	2	2012-05-14 12:29:53	10	2012-05-14 12:29:53	8.0.4.121	Indigol	NokiaE72-1				sis	E90HL00000M0000	
5	1	5	2012-05-14 17:46:46	11 25	2012-05-14 17:46:46	8.0.4.121	amobimasti	NokiaX6-00				sis	H5H125221450000	
6		5	2012-05-15 18:28:19	11 23	2012-05-15 18:28:19	8.0.4.121	gmobimasti	NokiaX6-00			93781090013	sis	H5H125221450000	
7	6	I	2012-05-15 20:02:58	0.25	2012-05-15 20:02:58	8.0.4.121	gmobimasti	NokiaX6-00			93781090013	sis	H5H12522145000	

## Will VPNs save us?



We are **not** here to show off how clever our attacks are

• The problem is **how easy** our attacks are

• But... some of our attacks *are* cool :)

#### Legend

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

no known issues

N/A product not offered or not present on device analyzed

Keyboard developer	Android	iOS	Windows
Tencent	×	v	×
Baidu	1	1	××
iFlytek	××	~	V

#### Legend

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

#### no known issues

N/A product not offered or not present on device analyzed

Device manufacturer	Own	Sogou	Baidu	iFlytek	iOS	Windows
Samsung	××	✓*	××	N/A	N/A	N/A
Huawei	✓*	~	N/A	N/A	N/A	N/A
Xiaomi	N/A	<b>X</b> *	××	xx	N/A	N/A
OPPO	N/A	×	<b>XX</b> *	N/A	N/A	N/A
Vivo	✓*	×	N/A	N/A	N/A	N/A
Honor	N/A	N/A	<b>XX</b> *	N/A	N/A	N/A

\* Default keyboard on device

## We considered an app secure if it used TLS



## Keyboard Craptography Part 1: Sogou (The "Encrypt Wall")

- Windows
- Android
- iOS

## Sogou Windows

Untitled - Notepad	
e Edit Format View Help	
ni'hao	9 打开智能写作助手 👜
1 你好 2 你号 3 拟好 4 (**	▽`)ノノ 5 倪好 〈>
	Þ

sogou-win.pcapng															- □									
File	Edit	View	<u>G</u> o <u>C</u> a	pture	Analyze	<u>S</u> ta	tistics	Telephor	ny <u>W</u> ire	less <u>T</u> o	ols <u>H</u> elp													
		1					<b>Q</b> 🧟	ço oS	°& K	\$ 21		Ð		1										
h	ttp.req	uest.met	hod == "	POST"																	$\times \rightarrow$	🕈 🕈 Hos	at H	ITTP(2) Requ
No.		Stream	Time			Sour	rce		Destir	nation		TTL	IPID		Country		Protocol	Lengt	h H	lost				Method
	163	9	21:04	1:30.	023384	1 10.	0.2.1	5	39.1	56.16	5.32	128	3 0x6	7f	China		HTTP	6	25	get.sogou	J.COM			POST
	1681	7	21:04	1:46.	516453	3 10.	0.2.1	.5	39.1	.56.165	5.32	128	8 0x6	97	China		HTTP	7	93 0	get.sogou	J.COM			POST
	1812	12	21:04	1:59.	929873	3 10.	0.2.1	.5	39.1	56.165	5.32	128	8 0x6	9c	China		HTTP	6	89	get.sogou	J.COM			POST
1	2239	42	21:05	5:26.	744767	/ 10.	0.2.1	.5	39.1	56.165	5.32	128	8 0x6	a4	China		HTTP	6	01	get.sogou	J.COM			POST
1	2416	50	21:07	7:08.	922390	) 10.	0.2.1	.5	39.1	56.165	5.32	128	8 0x6	a9	China		HTTP	9	93	get.sogou	J.COM			POST
1	2426	51	21:07	7:10.	049447	10.	0.2.1	.5	39.1	56.165	5.32	128	8 0x6	a9	China		HTTP	9	93	get.sogou	J.COM			POST
-> :	2438	52	21:07	7:22.	749503	3 10.	0.2.1	.5	39.1	56.165	5.32	128	3 0x6	a9	China		HTTP	9	29	get.sogou	J.COM			POST
1	2448	53	21:07	7:23.	563355	5 10.	0.2.1	.5	39.1	.56.165	5.32	128	3 0x6	aa	China		HTTP	9	29	get.sogou	J.COM			POST
1	2459	54	21:07	7:49.	269127	/ 10.	0.2.1	.5	39.1	.56.165	5.32	128	3 0x6	aa	China		HTTP	9	29 9	get.sogou	J.COM			POST
1	2466	55	21:07	7:49.	573347	10.	0.2.1	.5	39.1	.56.165	5.32	128	8 0x6	aa	China		HTTP	9	29 9	get.sogou	J.COM			POST
1	2478	56	21:07	7:51.	920568	3 10.	0.2.1	.5	39.1	.56.165	5.32	128	8 0x6	ab	China		HTTP	9	29 9	get.sogou	J.COM			POST
1	2488	57	21:08	3:17.	108240	) 10.	0.2.1	.5	39.1	.56.165	5.32	128	3 0x6	ab	China		HTTP	9	29	get.sogou	J.COM			POST
1	2498	58	21:08	3:17.	417662	2 10.	0.2.1	.5	39.1	.56.165	5.32	128	3 0x6	ab	China		HTTP	9	29	get.sogou	J.COM			POST
1	2509	59	21:08	3:19.	975612	2 10.	0.2.1	.5	39.1	.56.165	5.32	128	8 0x6	ac	China		HTTP	9	29	get.sogou	J.COM			POST
1	2516	60	21:08	3:20.	282043	3 10.	0.2.1	.5	39.1	.56.165	5.32	128	3 0x6	ас	China		HTTP	9	29	get.sogou	J.COM			POST
4	1																							
	Hos	t: get	. sogou	.com	\r\n						<b>^</b>	00c0	4c	65 6	e 67	74 68	3a 20	37 32	32	0d 0a 0d	0a 6b	Lengt	h:	722 · · · · k
	Con	nectio	n: clo	se\r	\n							00d0	3d	46 4	4 68	66 4d	46 50	45 4c	37	4a 50 53	39 2b	=FDhf	MFP	EL7JPS9+
	Use	r-Agen	t: sog	jou i	me\r\n	i i						00e0	4a	5а б	ic 48	79 69	43 49	5a 53	6f	78 76 76	76 69	JZlHy	iCI	ZSoxvvvi
•	Con	tent-L	ength	722	\r\n							00f0	48	67 5	3 5a	45 6d	2b 56	6C 38	38	79 66 65	4b 4c	HgSZE	m+V	188yfeKL
	1/1/	n	-									0100	бс	75 4	d 47	35 75	5a 67	4d 39	бb	31 54 4d	74 4b	luMG5	uZg	M9k1TMtK
	[Fu	ll req	uest l	JRI:	http:/	/get	.sogo	ou.com/	q]			0110	44	6a 3	2 6e	2f 79	4a 2f	48 2f	бс	72 4c 74	39 30	Dj2n/	yJ/	H/lrLt90
	[HT	TP req	uest 1	/1]		0.00	1995	10	0.5.5.5			0120	34	74 3	7 61	67 51	2b 31	37 41	бd	75 7a 78	6b 4b	4t7ag	0+1	7AmuzxkK
	Re	sponse	in fr	ame:	2440]							0130	4a	51 6	ie 6b	63 64	79 4a	70 2f	59	47 64 37	4f 46	J0nkc	dуЈ	p/YGd70F
	Fil	e Data	: 722	byte	s							0140	63	62 7	4 42	34 41	66 50	36 50	бе	6f 52 45	73 7a	cbtB4	AfP	<b>6PnoREsz</b>
* H	TML F	FORM UF	L Enc	oded	: appl	icat	ion/x	-www-fo	orm-ur	lencod	ed	0150	69	56 7	a 68	6d 43	62 59	4e 5a	36	6d 6c 37	67 4e	iVzhm	СЬҮ	NZ6ml7gN
	For	m item	: "k"	= "F	DhfMFP	EL73	JPS9 J	JZlHyiC	IZSoxv	vviHg9	SZEm V	0160	38	6d 3	3 36	49 69	2b 4a	6b 2b	47	7a 34 47	59 79	8m36I	i+J	k+Gz4GYy
+	For	m item	: "v"	= "D	wPfg55	5i/	8dAus	JnZBnC	0akVXU	CjFjX7	Mf3HR	0170	42	71 5	7 4a	47 32	61 54	4c 37	76	49 3d 26	76 3d	BqWJG	2aT	L7vI=&v=
	For	m item	: "u"	= "9	FiFygG	R053	SCP300	fhHMA9	KMOITY	OxJfor	BrU3U	0180	44	77 5	0 66	67 35	35 2b	35 69	2f	38 64 41	75 73	DwPfg	55+	51/8dAus

0190

01a0

01b0

Þ

Form item: "u" = "9FiFygGR053cP30qfhHMA9KmQiTy0xJfogBrU3U Form item: "g" = "rbIqDIl0140zvaVexEFtiy0I4EzIQS2G0pLu pq" Form item: "p" = "8XbsCmnQFu70Bb/oaInQAb1g5xxpm1s5a5TLlFf

Packets: 2544 · Displayed: 23 (0.9%)

4a 6e 5a 42 6e 43 30 61 6b 56 58 55 43 6a 46 6a

58 5a 4d 66 33 48 52 4c 45 55 57 4e 7a 65 59 53

51 51 57 31 4b 76 38 44 63 33 70 43 6a 61 66 75

Profile: Default

7 Text item (text), 174 bytes

No.

4 0 Host HTTP(2) Request

JnZBnC0a kVXUCjFj

XZMf3HRL EUWNzeYS

00W1Kv8D c3pCjafu

\*

## Sogou Craptography for Windows

- K-AES key
- V IV
- U tunneled URL
- G tunneled GET params
- P tunneled POST params

## Sogou Craptography for Windows

- K AES key *k* (encrypted with 1024-bit public RSA key)
- V IV v (encrypted with 1024-bit public RSA key)
- U tunneled URL (encrypted with k and v)
- G tunneled GET params (encrypted with k and v)
- P tunneled POST params (encrypted with *k* and *v*)

- Padding oracle?
- Distinct responses for good/bad padding





Cipher Block Chaining (CBC) mode decryption



Chaining (CBC) mode decryption

## XOR algebra

Since  $X \oplus X = 0...$ 

- 1. ciphertext<sub>*n*-1</sub>  $\oplus$  Decrypt(ciphertext<sub>*n*</sub>) = plaintext<sub>*n*</sub>
- 2. ciphertext<sub>*n*-1</sub>  $\oplus$  Decrypt(ciphertext<sub>*n*</sub>)  $\oplus$  plaintext<sub>*n*</sub> = 0
- 3. Decrypt(ciphertext<sub>n</sub>) = ciphertext<sub>n-1</sub>  $\oplus$  plaintext<sub>n</sub>

# $ciphertext_{n-1} \oplus Decrypt(ciphertext_n) = plaintext_n$

Find byte *b* such that

 $b \oplus \text{Decrypt}(\text{ciphertext}_n)[15] == 0x01 \Rightarrow \text{Decrypt}(\text{ciphertext}_n)[15] == b \oplus 0x01$ To recover plaintext\_n[15]

 $plaintext_n[15] = ciphertext_{n-1}[15] \oplus b \oplus 0x01$ 

Set

```
ciphertext<sub>n-1</sub>[15] = b \oplus 0x01 \oplus 0x02
```

Find *b* such that

```
b \oplus \text{Decrypt}(\text{ciphertext}_n)[14] == 0x02
```

- Problem 1: IV encrypted with RSA key
- Problem 2: plaintext is zlib-compressed



Cipher Block Chaining (CBC) mode decryption

- The beginning of the URL field "U" is predictable during typing
- Same key, IV used for U, G, and P
- Set IV = all zeros
- Attack first block per normal, yielding plaintext<sub>1</sub>  $\oplus$  IV
- We know plaintext<sub>1</sub> (!)
- We can recover the IV
```
{
1:
2
  ł
  1
    2: "1111_sogou_pinyin_guanwang_13.4e_1111"
3: "13.4.0.7561"
    5: 3
    7:1
    8: "13.4.0.7561"
  }
  7: "nihaohaohaohaohaohaozdaasdfffaahellocanyoureadthis"
  16:11
  17
     ł
    3
      1: 2
      2: 1
    9:1
    10:1
  }
  19
    4: "0"
```

#### Sogou Android



- K AES key *k* (encrypted with 1024-bit public RSA key)
- V IV v (not encrypted this time)
- U tunneled URL (encrypted with k and v)
- G tunneled GET params (encrypted with k and v)
- P tunneled POST params (encrypted with *k* and *v*)

- K AES key *k* (encrypted with 1024-bit public RSA key)
- V IV v (not encrypted this time)
- U tunneled URL (encrypted with k and v)
- G tunneled GET params (encrypted with k and v)
- P tunneled POST params (encrypted with *k* and *v*)
- $R k \oplus$  another AES key r
- $S k \oplus (s \text{ encrypted with } r \text{ and } \text{``EscowDorisCarlos''})$
- $E k \oplus (e \text{ encrypted with } r \text{ and } \text{``EscowDorisCarlos''})$
- $F k \oplus (f \text{ encrypted with } r \text{ and } \text{``EscowDorisCarlos''})$



- Let 256-bit k = 128-bit  $k_1 \parallel 128$ -bit  $k_2$
- After attack, first plaintext blocks of S, E, F:
- $k_2 \oplus s$
- $k_2 \oplus e$
- $k_2 \oplus f$
- s is predictable
- We can recover  $k_2$
- We can recover e, f, and  $r_2$

```
1
  {
     "com.android.messaging"
  1:
  2: "11.20"
  4:1
  6: "android_sweb"
  8: "Google"
  10: "android_sweb"
  11: "11.20"
  14: "30"
  18: "-1"
  22: "5682b3aa4fa7bd40d776c93a35a77c6d"
}
2
  1: 0xbff000000000000
  2: 0xbff000000000000
  3: "-1"
}
3:
   "<mark>canyoureadthis</mark>"
4:
11
  1: "onekeyimageenable"
  2: "1"
}
```

# Sogou Craptography for iOS?

- Key generation?
- Key from Unix time in seconds
- If you know the time, you know the key
- IV from Unix time in seconds
- Key likely to be IV
- The IV is transmitted unencrypted!

```
void __cdecl +[DataEncryptor randomizeAesKeyIv:keyLen:iv:ivLen:](
        id a1,
        SEL a2,
        unsigned int8 *key,
        ssize t key len,
        unsigned int8 *iv,
        ssize t iv len)
  unsigned int8 *iv ; // x20
  unsigned int8 *key ; // x22
  unsigned int key seed; // w0
  unsigned int iv seed; // w0
  if ( key )
    iv = iv;
    if (iv)
      key = key;
      key seed = time(0LL);
      srand(key_seed);
      if ( key len >= 1 )
      {
        do
          *key ++ = rand();
          --key len;
        while ( key_len );
      iv seed = time(0LL);
      srand(iv seed);
      if ( iv len \geq 1 )
        do
          *iv ++ = rand();
          --iv len;
        while ( iv len );
```

# Sogou Craptography for iOS?

• BUT, all of this is wrapped in TLS!

```
void __cdecl +[DataEncryptor randomizeAesKeyIv:keyLen:iv:ivLen:](
        id a1,
       SEL a2,
       unsigned int8 *key,
        ssize_t key_len,
       unsigned int8 *iv,
        ssize_t iv_len)
 unsigned int8 *iv ; // x20
  unsigned int8 *key ; // x22
  unsigned int key_seed; // w0
  unsigned int iv seed; // w0
  if ( key )
  {
    iv = iv;
   if (iv)
      key = key;
      key seed = time(0LL);
     srand(key_seed);
     if (key len >= 1)
      {
        do
          *key ++ = rand();
          --key len;
       while ( key_len );
      iv seed = time(0LL);
      srand(iv seed);
      if ( iv_len >= 1 )
       do
          *iv ++ = rand();
          --iv len;
        while ( iv_len );
```

# Keyboard Craptography Part 2: iFlytek

- Android
- iOS
- Windows

#### iflytek-typing.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help 📶 🔳 🖉 😳 🚞 🛅 🕱 🙆 🍳 < 🔈 🔈 📂 考 📃 📃 🔍 Q. Q. 🏦

#### http.request.method == "POST"

🖾 🗔 🔹 🔶 Host HTTP(2) Request

r	No. Sti	ream Time	Source	Destination	TTL	IPID	Country	Protocol	Length	Host			Method	-
	251	1 13:53:19.94715	10.42.0.123	183.192.161.22		64 0x3d5	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	253	2 13:53:20.04955	10.42.0.123	183.192.161.22		64 0xb63	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	257	1 13:53:20.35535	10.42.0.123	183.192.161.22		64 0x3d5	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	261	2 13:53:20.81590	10.42.0.123	183.192.161.22		64 0xb63	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	263	1 13:53:21.11744	10.42.0.123	183.192.161.22		64 0x3d5	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	265	2 13:53:21.15016	10.42.0.123	183.192.161.22		64 0xb63	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	271	2 13:53:21.64774	10.42.0.123	183.192.161.22		64 0xb64	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	274	7 13:53:21.74995	10.42.0.123	183.192.161.22		64 0xe5a	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	276	1 13:53:21.97310	10.42.0.123	183.192.161.22		64 0x3d5	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	281	2 13:53:22.21112	10.42.0.123	183.192.161.22		64 0xb64	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	286	1 13:53:22.51204	10.42.0.123	183.192.161.22		64 0x3d6	China	HTTP	378	pinyin	.voicecloud	.cn	POST	
1	317	2 13:53:23.36951	10.42.0.123	183.192.161.22		64 0xb64	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
	319	1 13:53:23.70060	10.42.0.123	183.192.161.22		64 0x3d6	China	HTTP	378	pinyin	.voicecloud	l.cn	POST	
-	► 323	2 13:53:23.90291	10.42.0.123	183.192.161.22		64 0xb64	China	HTTP	378	pinyin	.voicecloud	.cn	POST	
	329	1 13:53:24.21863	10.42.0.123	183.192.161.22		64 0x3d6	China	HTTP	378	pinyin	.voicecloud	.cn	POST	*
4	•												•	
	Accep	t-Encoding: identity	\r\n	1	008	0 2e 31	34 39 38	33 20 48	54 54 50	2f 31	2e 31 0d	.14983 H	TTP/1.1.	*
	Conte	nt-Length: 104\r\n			009	0 0a 41	63 63 65	70 74 2d	45 6e 63	6f 64	69 6e 67	·Accept-	Encoding	
	Host:	pinyin.voicecloud.cr	n/r/n		00a	0 3a 20	69 64 65	6e 74 69	74 79 0d	0a 43	6f 6e 74	: identi	tyCont	
	Conne	ction: Keep-Alive\r\r	n		006	0 65 6e	74 2d 4c	65 6e 67	74 68 3a	20 31	30 34 0d	ent-Leng	th: 104.	
	User-	Agent: okhttp/3.12.3	\r\n	-	000	0 0a 48	6f 73 74	3a 20 70	69 6e 79	69 6e	2e 76 6f	·Host: p	inyin.vo	
	\r\n				000	0 69 63	65 63 6c	6f 75 64	2e 63 6e	0d 0a	43 6f 6e	icecloud	.cnCon	
	[Full	request URI: http://	/pinyin.voiceclo	ud.cn/?time=1694	00e	0 6e 65	63 74 69	of 6e 3a	20 4b 65	65 70	2d 41 6c	nection:	Keep-Al	
	[HTTP	request 10/13]	sing s		001	0 69 76	65 0d 0a	55 73 65	72 2d 41	67 65	6e 74 3a	iveUse	r-Agent:	
	[Prev	request in frame: 31	17]		010	0 20 6f	6b 68 74	74 70 2f	33 2e 31	32 2e	33 0d 0a	okhttp/	3.12.3	
	Resp	onse in frame: 328]	1.2		011	0 0d 0a	a8 0e 32	ff 5f ba	68 d7 e3	78 9c	67 bd 28	····2·_·	h··x·g·(	
	Next	request in frame: 33	31		012	0 5b 2e	fd e0 7f	d0 1c e0	5f c2 ba	c6 bb	af 3a c9	L		
	File	Data: 104 bytes			013	0 81 88	fd 4b c3	19 a5 27	35 ab 98	21 65	1d 9c 4f	· · · K · · · ·	5!e0	
1	▼ Data	(104 bytes)			014	0 b3 af	30 75 35	a8 b8 d3	b1 03 0e	2C d2	80 94 fc	•••0{5••••	••••	
	Dat	a: a80e32ff5fba68d7e.	3789c67bd285b2e1	de0/td01ce05tc2b	015	0 01 a7	30 75 00	38 bd 6c	0a 03 78	44 61	e2 5f 54	••=u•8•L	··xDa·_T	
	LLe	ingth: 104]		-	016	10 1C 1a	a9 0b 1e	87 75 1a	82 51 d2	79 4c	DC 95 19	·····u·	·Q·yL···	
	(			•	017	0 40 e7	80 36 75	e0 b3 d3	Te fo			@··6U···	1.1	-

07 Data (data.data), 104 bytes Packets: 344 · Displayed: 24 (7.0%)

Profile: Default

#### iflytek-typing.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help 📶 🔳 🧟 🕲 🚞 🖹 🐹 🙆 🍳 🎸 🗲 🛸 🖊 📃 🔍 Q, Q, 🏋

#### http.request.method == "POST"

🖾 📼 🔹 🔶 Host HTTP(2) Request

N	o.	Stream	Time	Source	Destination	TTL	IPID	Country	Protoco	l Length	Host	Method
	251	1	13:53:19.94715	. 10.42.0.123	183.192.161.22	64	1 0x3d5	China	HTTP	378	pinyin.voicecloud.cn	POST
	253	2	13:53:20.04955	. 10.42.0.123	183.192.161.22	64	1 0xb63	China	HTTP	378	pinyin.voicecloud.cn	POST
	257	1	13:53:20.35535	10.42.0.123	183.192.161.22	64	4 0x3d5	China	HTTP	378	pinyin.voicecloud.cn	POST
	261	2	13:53:20.81590	10.42.0.123	183.192.161.22	64	4 0xb63	China	HTTP	378	pinyin.voicecloud.cn	POST
	263	1	13:53:21.11744	10.42.0.123	183.192.161.22	64	1 0x3d5	China	HTTP	378	pinyin.voicecloud.cn	POST
	265	2	13:53:21.15016	10.42.0.123	183.192.161.22	64	1 0xb63	China	HTTP	378	pinyin.voicecloud.cn	POST
	271	2	13:53:21.64774	10.42.0.123	183.192.161.22	64	4 0xb64	China	HTTP	378	pinyin.voicecloud.cn	POST
	274	7	13:53:21.74995	10.42.0.123	183.192.161.22	64	4 0xe5a	China	HTTP	378	pinyin.voicecloud.cn	POST
	276	1	13:53:21.97310	10.42.0.123	183.192.161.22	64	4 0x3d5	China	HTTP	378	pinyin.voicecloud.cn	POST
	281	2	13:53:22.21112	10.42.0.123	183.192.161.22	64	1 0xb64	China	HTTP	378	pinyin.voicecloud.cn	POST
	286	1	13:53:22.51204	10.42.0.123	183.192.161.22	64	1 0x3d6	China	HTTP	378	pinyin.voicecloud.cn	POST
+	317	2	13:53:23.36951	. 10.42.0.123	183.192.161.22	64	1 0xb64	China	HTTP	378	pinyin.voicecloud.cn	POST
	319	1	13:53:23.70060	. 10.42.0.123	183.192.161.22	64	4 0x3d6	China	HTTP	378	pinyin.voicecloud.cn	POST
	<ul> <li>323</li> </ul>	2	13:53:23.90291	. 10.42.0.123	183.192.161.22	64	1 0xb64	China	HTTP	378	pinyin.voicecloud.cn	POST
1	329	1	13:53:24.21863	. 10.42.0.123	183.192.161.22	64	1 0x3d6	China	HTTP	378	pinyin.voicecloud.cn	POST 🔻
4												•
•	Frame	323: 3	78 bytes on wire	e (3024 bits), 3	78 bytes capturec*	0040	00 16	50 4f 5	3 54 20 2f	3f 74 69	6d 65 3d 31 36	POST / ?time=16 📤
E	Ether	net II,	Src: HTC_86:1a	:8a (40:4e:36:86	:1a:8a), Dst: Hor	0050	39 34	31 30 3	9 32 30 36	31 34 36	26 70 72 6f 74 941	109206 146 <mark>&amp;prot</mark>
F	Inter	net Pro	tocol Version 4	, Src: 10.42.0.1	23, Dst: 183.192.	0060	6f 3d	32 2e 3	0 26 61 70	70 5f 69	64 3d 31 30 30 o=2	2.0≈ p_id=100
Þ	Trans	nission	Control Protoco	ol, Src Port: 37	704, Dst Port: 80	0070	49 4d	45 26 6	3 6c 69 5f	76 65 72	3d 31 32 2e 31 IME	&cli_ ver=12.1
*	Hyper	text Tr	ansfer Protocol			0080	2e 31	34 39 3	8 33 20 48	54 54 50	2f 31 2e 31 0d .14	1983 H TTP/1.1.
	<ul> <li>POS</li> </ul>	T /?ti	me=1694109206146	&proto=2.0&app_i	d=100IME&cli_ver	0090	0a 41	63 63 6	5 70 74 2d	45 6e 63	6f 64 69 6e 67 ·Ac	ccept- Encoding
	Þ. [	Expert	Info (Chat/Sequ	uence): POST /?ti	ime=1694109206146	00a0	3a 20	69 64 6	5 6e 74 69	74 79 00	0a 43 6f 6e 74 : i	identi tyCont
	F	Request	Method: POST			00b0	65 6e	74 2d 4	c 65 6e 67	74 68 3a	20 31 30 34 0d ent	t-Leng th: 104.
	- F	Request	URI: /?time=169	94109206146&proto	p=2.0&app_id=100I	0000	0a 48	6f 73 7	4 3a 20 70	69 6e 79	69 6e 2e 76 6f ·Ho	ost: p inyin.vo
		Reque	est URI Path: /			00d0	69 63	65 63 6	c 6f 75 64	2e 63 6e	e Od Oa 43 6f 6e ice	cloud .cnCon
	8	<ul> <li>Reque</li> </ul>	est URI Query: t	ime=169410920614	6&proto=2.0&app_i	00e0	6e 65	63 74 6	9 6f 6e 3a	20 4b 65	65 70 2d 41 6c nec	tion: Keep-Al
		Re	quest URI Query	Parameter: time=	1694109206146	00f0	69 76	65 0d 0	a 55 73 65	72 2d 41	67 65 6e 74 3a ive	e··Use r-Agent:
		Re	quest URI Query	Parameter: proto	=2.0	0100	20 6f	6b 68 7	4 74 70 2f	33 2e 31	. 32 2e 33 0d 0a ok	<pre>khttp/ 3.12.3</pre>
		Re	quest URI Query	Parameter: app_i	d=100IME	0110	0d 0a	a8 0e 3	2 ff 5f ba	68 d7 e3	78 9c 67 bd 28 ···	··2·_· h··x·g·(
		Re	quest URI Query	Parameter: cli_v	er=12.1.14983	0120	5b 2e	fd e0 7	f d0 1c e0	5f c2 ba	c6 bb af 3a c9 [	
		enuest	Version HTTP/1	1		0130	81 88	fd 4b c	3 19 a5 27	35 ab 98	21 65 1d 9c 4f ···	K····' 5··!e··0

○ Z HTTP Request-URI Query Parameter (http.request.uri.query.parameter), 18 bytes

Packets: 344 · Displayed: 24 (7.0%)

Profile: Default

- 🗆 ×

#### iFlytek craptography for Android

• Encrypted using DES key *k* in ECB mode.

#### iFlytek craptography for Android

- Encrypted using DES key *k* in ECB mode.
- How is *k* derived?

```
__int64 generate_key_seed()
```

return now\_nanoseconds() / 1000000;

```
[...]
```

```
if ( ptr && length )
{
    v17 = (_DWORD)length + 8;
    output = malloc((int)length + 8);
    memset(output, 0, v17);
    sprintf((char *)key, "%08llu", (key_seed % 0x5F5E100) ^ 0x1001111);
    v19 = DES_ECB_Encrypt(ptr, (__int64)output, key, (unsigned int)length);
    free(ptr);
```

#### iFlytek craptography for Android

- Encrypted using DES key *k* in ECB mode.
- How is *k* derived?

*k* = b'%08u' % ((*s* % 0x5F5E100) ^ 0x1001111)

where s is the current Unix time in milliseconds.

## iFlytek craptography for Android

- Who can decrypt everything you type?
- Anyone who knows the time
- Just in case you don't know the time, they tell you the time for you...

```
1:0
2: 0
3: 49
4: "xxxxx"
5: 0
7 {
    1: "app_id"
    2: "100IME"
}
7 {
    1: "uid"
    2: "230817031752396418"
}
7 {
    1: "cli_ver"
    2: "12.1.14983"
}
7 {
    1: "net_type"
    2: "wifi"
}
7
  {
    1: "OS"
    2: "android"
}
8:8
```

#### iFlytek craptography for iOS and Windows?

• Same problems but... wrapped in TLS



# Keyboard Craptography Part 3: Baidu

- Samsung
- Windows
- Android
- iOS

et	tings	Q	<	Preloaded apps	:
2	Screen time • App time	rs	du	Baidu IME	
0	Smart Manager Storage • Memory • De protection	evice		Best weather	
	My Files		+- ×÷	Calculator	
	Analyze storage	•	3	Calendar	
3	Apps Default apps + App set	tings	0	Clock	
				Editor Lite	
	General management Language and keyboard		Solary Shop	Galaxy Shop	
			8×	Gaming Hub	
3	TalkBack * Mono audio Assistant menu	. •	-57	Google Calendar Sync	
			٥	Microsoft Office	
	Software update Download and install		•	Outlook	
D	User manual Learn more		*;	Photo Editor	
)	About tablet Status • Legal informat	ion •	<b>~</b>	Samsung Editing Assets	
	Tablet name		f	Samsung Flow	
>	Developer options	6	0	Samsung Kids	
		3			<

\$ 98%

20:21 Wed, Jan 3

samsung-baidu-typing.pcapng



#### udp.dstport == 4040

🛛 🗔 🔹 🔶 Host HTTP(2) Request

No	D.	Stream	Time	Source	Destin	ation	TTL	IPID	Country	y Protoc	ol Length	Host		Method	^
	1		19:59:03.01713	. 10.42.0.1	23 163.1	77.18.42	64	0xfc1	China	UDP	282				
	2		19:59:03.01718	. 10.42.0.1	163.1	77.18.42	64	0xfe0	China	UDP	282	2			
	3		19:59:03.10600	. 10.42.0.1	23 163.1	77.18.42	64	0xfe0	China	UDP	282	2			
	7		19:59:03.43030	. 10.42.0.1	163.1	77.18.42	64	0xfe1	China	UDP	282	2			
	9		19:59:03.72659	. 10.42.0.1	23 163.1	77.18.42	64	0xfe2	China	UDP	282	2			
	11		19:59:04.01770	. 10.42.0.1	23 163.1	77.18.42	64	0xfe7	China	UDP	282	2			
	13		19:59:04.36315	. 10.42.0.1	163.1	77.18.42	64	0xfe8	China	UDP	282	2			
	15		19:59:04.65400	. 10.42.0.1	163.1	77.18.42	64	Oxfeb	China	UDP	282	2			
	17		19:59:05.23373	. 10.42.0.1	23 163.1	77.18.42	64	0xfec	China	UDP	282	2			
	19		19:59:06.03824	. 10.42.0.1	163.1	77.18.42	64	0xff8	China	UDP	282	2			
	21		19:59:06.45497	. 10.42.0.1	163.1	77.18.42	64	0xffb	China	UDP	282	2			
	23		19:59:06.76345	. 10.42.0.1	163.1	77.18.42	64	0xffe	China	UDP	282	2			
	- 25	ř.	19:59:07.34328	. 10.42.0.1	23 163.1	77.18.42	64	0x007	China	UDP	282				Ŧ
•														•	
•	Frame	25: 28	2 bytes on wire	(2256 bits	;), 282 bytes	captured	( 0020	12 2a	9b 37 0	of c8 00 f8	fe 4e 03	01 00 00 00	0 00 .*.7	• N • • • • • •	*
1	Ether	net II,	Src: HTC_86:1a	:8a (40:4e	36:86:1a:8a	, Dst: Ask	e 0030	78 ec	39 be 0	00 e4 01 00	02 00 e4	00 00 00 b	4 00 x·9····		
1	Inter	net Pro	tocol Version 4	, SFC: 10.4	12.0.123, Dst	: 163.177.	1 0040	00 00	08 00 0	00 00 21 8a	5e t8 05		0 00/.	<b>^</b>	
÷	Data	(240 by	m Protocol, Src	POIL: 397.	s, DSC PORT	4040	0050		01 01 0		74 02 80		d da	+	
-	Dat	a Itru	ncated1: 0301000	0000078ec3	9be00e401000	200e400000	0070	e0 e0	8e 9e a	a9 c2 7c 0a	d5 99 52	27 88 18 f	7 b8 ••••••	· · R ' · · · ·	
	[Le	ength: 2	240]				0080	7c 68	44 04 t	o2 d2 52 5b	25 bf do	cf c1 3d a	0 64  hD···R[	% • • • • = • d	
	-	-	-				0090	ad 7c	5b 23 9	91 a9 5d 1b	62 82 51	24 6b 46 50	d 41 • [#••]•	b\$kF]A	
							00a0	bb 24	8b 03 1	10 f5 5d df	6f 86 21	36 92 45 10	0 81 •\$••••]•	0.10.E.	
							0060	31 17	80 d1 7	7f c0 5a d0	fd 99 co	df 77 2c 2	$2 41 1 \cdots Z$	••••w,"A	
							0000	a8 99	a7 a4 0	14 14 33 ae	9e 6a 30	) fb 6c f4 9	b af3.	· j0 · L · · ·	
							0000	er 39	ce ad 1	LO 84 22 8D	ba ad 51	TD 02 al C	5 90 .9	Q	
							0000		00 db 0					A	
							00e0 00f0	95 5T	e0 d5 d	ad f9 34 21	5e 5d ft d2 92 ac	dz 1a c7 50 90 45 0b 4	a 17	^]VC	
							00e0 00f0 0100	95 5f c4 b4 ea ff	e0 d5 d e3 f9 e 9c 3b 7	ed f9 34 21 7d 78 ce 17	5e 5d ft d2 92 ac 50 31 ce	dz 1a c7 50 90 45 0b 40 e2 f6 1c 41	a 17 ·····4! f 24 ····;}x··	^]VC E.J. P10\$	

Packets: 26 · Displayed: 13 (50.0%)

Profile: Default

- 🗆 x

```
1 signed int fastcall GA10 aesv1 encrypt(struct s cloud tool *cloud tool, int *plain crypt buf, int crypt len)
  2 {
   3
     struct s cloud tool *cloud tool ; // r5@1
     int *plain crypt buf ; // r4@1
     int plain len ; // r7@1
     signed int result; // r002
     int uninit1; // r2@4
     int uninit2; // r3@4
      int i; // r2@5
 10
      unsigned int8 fixed key[16]; // [sp+4h] [bp-2Ch]@6
 11
• 12
      cloud tool = cloud tool;
• 13
      plain crypt buf = plain crypt buf;
     plain len = crypt len;
• 14
15
      GA60(cloud tool);
16
     if ( !cloud tool
 17
        [] (unsigned int8)plain crypt buf & 3
 18
        [] get crypt len((int)cloud tool , *plain crypt buf ) != plain len )
 19
      {
0 20
       return -1;
 21
• 22
      GA61 generate key(cloud tool , plain crypt buf , uninit1, uninit2);
23
      GB02 encrypt(
 24
       cloud tool ->aes,
 25
        (unsigned int *)plain crypt buf + 5,
 26
        *plain crypt buf ,
 27
        (unsigned int8 *)plain crypt buf + 4);
0 28
      i = (unsigned int8)plain_crypt_buf_ & 3;
 29
      do
 30
        fixed key[i] = ~( BYTE)i ^ ((unsigned int)(1937 * i) >> (i & 3)) * (i + 11);
31
• 32
        ++1;
 33
      }
34
      while ( i != 16 );
• 35
      GB02 encrypt(cloud tool ->aes, (unsigned int *)plain crypt buf + 1, 16, fixed key);
36
     result = 0:
      *plain crypt buf ^= plain crypt buf [4] ^ plain crypt buf [1] ^ plain crypt buf [2] ^ plain crypt buf [3];
• 37
0 38
     return result;
• 39 }
```

- Randomly generate "AES" key  $k_1$
- "Generate" "AES" key k<sub>2</sub>
- "AES"-encrypt  $k_1$  with  $k_2$
- Encrypt message with  $k_1$
- Transmit encrypted  $k_1$  and encrypted message

• How does recipient know  $k_2$ ?

```
void __cdecl generate_static_key(unsigned __int8 *output, bool flag)
{
    unsigned int i; // eax
    unsigned int v3; // edi
    unsigned int v4; // edx
    i = 0;
    v3 = 0;
    do
    {
        v4 = v3;
        v3 += !flag + 1937;
        butput[i] = ~(_BYTE)i ^ ((i + 11) * (v4 >> (i & 3)));
        ++i;
     }
     while ( i < 16 );
}</pre>
```

- "AES"?
- Modified AES with additional permutations...
- Security through obscurity...



```
[800,
{0:
    1276,
     10,
     0,
     '92F8EE78F1DDCBE74CFEB1166F70883D%7C0',
     'a1|SM-T220-gta7litewifi|320',
     '8.5.20.4'
     'com.android.settings.intelligence',
     '1012497q',
     b''
     ['2你好惨又热大腿'],
     b''],
1: [0, b'',
            'nihaocanyoureadthis']}
```

### Baidu craptography for Windows

- Mostly cosmetic differences versus Baidu on Samsung
- "AES"v2
- Instead of additional permutations...
- One fewer round

```
[...]
2 {
    1: "nihaocanyoureadthis"
    5: 3407918
  }
3
    1: 107
    2: 10
    5: 1
4
    1: "1133d4c64afbf1feda85d3c497dd6164|0"
    2: "wn1||0"
    3: "6.0.3.44"
    4: "notepad.exe"
  }
[...]
```

• Uses an upgraded protocol

baidu-more-typing.pcapng



#### udp.dstport == 4040

🛛 🗔 🔹 🌵 Host HTTP(2) Request

- 🗆 ×

r	lo.	Stream	Time	Source	Destination	TTL	IPID	Country	Protocol	Length	Host		Method	*
	9		11:09:50.52747	10.42.0.123	183.232.232.201	64	1 0x7e2	China	UDP	315	;			
	11		11:09:50.98372	10.42.0.123	183.232.232.201	64	1 0x7e6	China	UDP	324	ł			
	12		11:09:51.30070	10.42.0.123	183.232.232.201	64	1 0x7e9	China	UDP	326				
	13		11:09:51.62529	10.42.0.123	183.232.232.201	64	1 0x7ea	China	UDP	326	i			
	14		11:09:52.11269	10.42.0.123	183.232.232.201	64	1 0x7eb	China	UDP	333	1			
	15		11:09:52.72995	10.42.0.123	183.232.232.201	64	4 0x7ed	China	UDP	334	ł			
	16		11:09:52.96285	10.42.0.123	183.232.232.201	64	4 0x7f0	China	UDP	341				
	19		11:09:53.10463	10.42.0.123	183.232.232.201	64	4 0x7f1	China	UDP	346	i .			
	22		11:09:53.85170	10.42.0.123	183.232.232.201	64	4 0x7fd	China	UDP	353	1			
	23		11:09:54.24071	10.42.0.123	183.232.232.201	64	4 0x7fd	China	UDP	357	,			
	26		11:09:54.63822	10.42.0.123	183.232.232.201	64	4 0x803	China	UDP	361				
	L 27		11:09:54.95330	10.42.0.123	183.232.232.201	64	1 0x807	China	UDP	365				
													Þ	-
	Eramo	27. 36	5 bytes on wire	(2020 bits) 365	bytes captured	0020	02 80	he ds of ce	2 01 /h	03 25 0/	00 f5 00 82	46K	. %	-
	Ether	net II.	Src: HTC 86:1a	:8a (40:4e:36:86:	(1a:8a). Dst: Hone	0030	61 6a	ed 62 4d 41		2a 98 02	be 19 1a 0c	95 ai.bMA.	70	
	Inter	net Pro	tocol Version 4	. Src: 10.42.0.12	23. Dst: 183.232.2	2 0040	bb 6e	d5 d0 9b 85	5 c3 63	5f 27 e1	09 c7 a7 70	27 • n • • • • • c	'p'	_
	User I	Datagra	m Protocol, Src	Port: 47317, Dst	t Port: 4040	0050	f2 65	9c 68 0c 6a	a 25 ff	7b 02 47	de 9c 23 a1	a6 •e•h•j%•	•G••#••	
	• Data	(323 by	rtes)			0060	d6 09	77 16 3e 94	1 2c 99	21 29 26	dc 1c ea 06	02	)&	
	Dat	a [tru	ncated]: 0400f50	e8246616aed624d4	118162a9802be191a	0070	b8 8d	24 2f b4 59	08 45	e5 13 73	39 97 6e 7d	2a ••\$/•Y•E	• s9•n}*	
	[Le	ngth:	323]			0080	51 86	c9 f3 d5 ec	10 f0	99 6f 53	64 89 cb fc	da Q·····	oSd	
						0090	96 9d	d3 85 a5 11	92 56	57 fd 08	a5 08 9b 35	9† ·····V I	1	
						0000	20 D7			TE 91 88	0a 39 95 0D			
						0000		35 10 D3 03		25 30 20	30 d9 24 TD	18 ······D 7	a;,0·>··	
						0000	h9 4d	c1 6d 70 8f	F a0 a3	58 ca 20				
						00e0	03 45	20 b8 86 64	1 9f 68	35 af 27	87 7e d8 ba	43 • E • • d • h	5	
						00f0	9a f8	ec 07 f2 ca	09 76	fc d7 28	15 0d fd 3f	d7v	(?.	
						0100	50 67	a1 4d 6b 58	3 21 de	d9 19 22	41 1f f1 7c	5f Pg·MkX! ·	· · "A · · ]	
						0110	7c 3c	e8 aa 10 84	1 36 bc	96 ca fe	c1 ca 5a 55	60  <···6·	•••••ZU`	
														T

Packets: 28 · Displayed: 18 (64.3%)

Profile: Default

- "AES"v3
- Uses modified CTR mode



• Modified CTR mode fails to have cryptographic diffusion

Block								Ρ	laiı	nte	xt													Ci	phe	erte	ext						
0	00	0	0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	e2	d4	00	1c	с6	5d	80	33	0c	b9	48	7d	d5	27	72	7a
1	01	0	0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	e2	d4	00	1c	с6	5d	80	33	0c	b9	48	7d	d5	27	72	7a

• IV and key re-use: plaintexts with same first N blocks will encrypt to the same first N ciphertext blocks

- Static elliptic-curve Diffie-Hellman! But...
- IV and key are re-used across application lifetime
- No forward secrecy (pinned static server key)
- Lack of message integrity (only CRC32)
- Modified CTR mode fails to have cryptographic diffusion

# Keyboard Craptography Part 4: Samsung IME

59 Sun, Dec 3	ন্থি 57
Samsung Keyboard	
Languages and types 简体中文, English (US)	
Chinese input options	
Smart typing	
Predictive text	
Suggest emojis English (US)	
Suggest stickers while typing Emoji pairs, Preloaded and downloaded stickers	
Auto replace 简体中文, English (US)	
Suggest text corrections No languages selected	
Text shortcuts	
More typing options	
Style and layout	
Keyboard toolbar	
High contrast keyboard	
Theme Light	
	•

# Keyboard Craptography Part 4: Samsung IME

Chinese input options	
Insert next word with space key	
Fuzzy pinyin input	
Simplified Chinese	
Detailed word databases	
Hot words and Kaomojis by Sogo Only use through WLAN	DU
Cloud input by Sogou Only use through WLAN	
Suggest rare words	
Suggest trad. Chinese	
Manage Shuangpin keyboard	
Link to Contacts Show predicted contacts that start with the of Touch and hold contact's name to view their i	characters just tapped.

₸ 57%

02:58 Sun, Dec 3

####
Wireshark · Follow HTTP Stream (tcp.stream eq 1) · samsung.pcapng

- 🗆 ×

1602841941J.POST /web_ime/mo	bile_pb.php?dur	tot=327&h=8f2bc	112-bbec-3f96-	86ca-652e98	316ad8&r
=android_oem_samsung_open&v:	8.13.10038.4131	/3&S=&e=&l=&TC=	=U&Dase=dW5rDM9	3DISWLJAFMC	.4w&ext_v
Content-Type: application/x	www-form-urlence	oded			
User-Agent: Dalvik/2.1.0 (L	nux; U; Android	13; SM-T220 Bu	ild/TP1A.22062	4.014)	
Host: shouji.sogou.com					
Connection: Keep-Alive					
Accept-Encoding: gzip					
content-Length. 107					
x					
\ \$8f2bc112-bbec-3f96-86ca-65	e98316ad8 andr	nid oem samsund	00en 8 13 10	038 413173"	8 1000
".com.tencent.mobilegg:.nih	ocanvoureadthis	· ·		050.415175	
(.H					
.0".327HTTP/1.1 200 OK					
Date: Sat, 07 Oct 2023 19:10	:13 GMT				
Content-Type: application/od	tet-stream				
Content-Length: 200					
connection: keep-ative					
i2V					
.`0}Y.`fTr.e.a.d.t.h.i.s	.us				
h:.					
.`0}Y.`fTr.e.a.d.t.h.i.s	D				
Kf[					
Kf[,	"				
1602841941J.					
2 <mark>client</mark> pkts, 12 server pkts, 23 turns.					
Entire conversation (11 kB)	*	Show data as	ASCII	•	Stream 1
ind:					Find Ne
					1

### Is it even craptography?

If there is no cryptography?



### Generalizing attacks

Discussed attacks can generally also be applied to...

- incoming data
- spoofing data
- modifying data

### "Please do not make it public"

#### Comment



#### tsrc审核

2023-06-25 17:10:23

Thank you for your interest in Tencent security. There is no low or low security risk for this issue. We look forward to your next more exciting report.



#### tsrc审核

2023-06-26 11:52:30

Sorry, my previous reply was wrong, we are dealing with this vulnerability, please do not make it public, thank you very much for your report

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

no known issues

N/A product not offered or not present on device analyzed

Keyboard developer	Android	iOS	Windows
Tencent	×	v	×
Baidu	1	1	××
iFlytek	××	~	V

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

no known issues or all known issues fixed

N/A product not offered or not present on device analyzed

Keyboard developer	Android	iOS	Windows
Tencent	v	<b>v</b>	~
Baidu	1	1	1
iFlytek	~	~	~

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

#### no known issues

N/A product not offered or not present on device analyzed

Device manufacturer	Own	Sogou	Baidu	iFlytek	iOS	Windows
Samsung	××	✓*	××	N/A	N/A	N/A
Huawei	✓*	~	N/A	N/A	N/A	N/A
Xiaomi	N/A	<b>X</b> *	××	xx	N/A	N/A
ОРРО	N/A	×	<b>XX</b> *	N/A	N/A	N/A
Vivo	✓*	×	N/A	N/A	N/A	N/A
Honor	N/A	N/A	<b>XX</b> *	N/A	N/A	N/A

\* Default keyboard on device

**XX** working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers

**X** working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper

weaknesses present in cryptography implementation

no known issues or all known issues fixed

N/A product not offered or not present on device analyzed

Device manufacturer	Own	Sogou	Baidu	iFlytek	iOS	Windows
Samsung	~	✓*	1	N/A	N/A	N/A
Huawei	✓*	V	N/A	N/A	N/A	N/A
Xiaomi	N/A	✓*	1	~	N/A	N/A
OPPO	N/A	V	!*	N/A	N/A	N/A
Vivo	✓*	V	N/A	N/A	N/A	N/A
Honor	N/A	N/A	<b>XX</b> *	N/A	N/A	N/A

\* Default keyboard on device

#### Let's zoom out a bit!

### Most downloaded apps in 2023?



### Most downloaded apps in 2023?

1 WeChat	1012	7	TikTok	654
2 Alipay	901	8	QQ	583
3 Taobao	795	9	Facebook	553
4 Pinduoduo	728	10	Baidu	491
5 Instagram	696	11	Kuaishou	480
6 Douyin	695	12	WhatsApp	475

#### Most Popular Apps Key Statistics

 Instagram was the most downloaded app globally in 2023, with 696 million downloads



#### **HTTPS Is Actually Everywhere**

SEPTEMBER 21, 2021



### How many always use HTTPS/TLS?

WeChat	1012	TikTok	654
Alipay	901	QQ	583
Taobao	795	Facebook	553
Pinduoduo	728	Baidu	491
Instagram	696	Kuaishou	480
Douyin	695	WhatsApp	475

### How many always use HTTPS/TLS?

X WeChat	1012	$\checkmark$	TikTok	654
🗙 Alipay	901	X	QQ	583
🗙 Taobao	795	$\checkmark$	Facebook	553
X Pinduoduo	728	X	Baidu	491
🔽 Instagram	696	X	Kuaishou	480
V Douyin	695	$\checkmark$	WhatsApp	475

\*but they're also **not not** encrypting...

many of them are using proprietary cryptography

## Uh-oh



So far, researchers have mostly been conducting one-off studies analyzing proprietary cryptography in individual apps

Can we measure this **systematically**?





**91%** of top 45 apps exclusively used standard encryption (QUIC, TLS) to transmit data



**4%** of top 44 apps exclusively used standard encryption

**54%** used proprietary cryptography



• Are these backdoors?

- Are these backdoors?
  - **No**

# **Success Stories**

- \* UCWeb mobile browser identification
  - \* Discovered by GCHQ analyst during DSD workshop
  - \* Chinese mobile web browser leaks IMSI, MSISDN, IMEI and device characteristics

# UCWeb – XKS Microplugin

UCWeb	1.1												
🕜 Help	Help Actions * Reports * View * SMap View												
	State	ID	Datetime 🔺	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform Active User/	Casenotation
1	-1	1	2012-05-13 02:29:20	8	2012-05-13 02:29:23	8.0.3.107	2123movies	nokiae90-1	والمناجعة والمتحاد الملكو		9379900100	java	E9DHL00000M0000
2	-	3	2012-05-13 06:00:59	8	2012-05-13 06:01:00	8.0.3.107	2123movies	nokiae90-1			9379900100	java	E9DHL00000M0000
3	-1	4	2012-05-13 19:39:11	8	2012-05-13 19:39:11	7.9.3.103		HTC A510e				android	E9BDE00000M0000
4	1	2	2012-05-14 12:29:53	8	2012-05-14 12:29:53	8.0.4.121	⊉djgol	NokiaE72-1				sis	E9DHL00000M0000
5		5	2012-05-14 17:46:46	6 44	2012-05-14 17:46:46	8.0.4.121	gmobimasti	NokiaX6-00	A States Inc.			sis	H5H125221450000
6	-1	<u>6</u>	2012-05-15 18:28:19	6 23	2012-05-15 18:28:19	8.0.4.121	gmobimasti	NokiaX6-00			93781090013	sis	H5H125221450000
7		Z	2012-05-15 20:02:58	04	2012-05-15 20:02:58	8.0.4.121	gmobimasti	NokiaX6-00			93781090013	sis	H5H1252214500C

# Why is this happening?

- Many of these applications became massively popular around the early 2010s
  – before TLS was de-facto standard
- Anti-scraping/competition
- Inertia
- ???

## How do we stop it from being bad?

- 1. Find the problems
  - Security researchers should pay more attention to these **massively popular** but understudied apps
  - Any researcher that even looked at this traffic in Wireshark would know there is a problem

## How do we stop it from being bad?

- 2. Report the problems
  - Many did switch to TLS when we reported severe vulns, some did not
  - We need to better engage with these companies and put pressure on them to design better products

## How do we stop it from being bad?

- 3. Prevent future problems?
- Can platforms, app store enforcement, etc. impose restrictions on the nature of app's network access?
- "Don't roll your own crypto" how do we spread this message?

For our full report...

https://citizenlab.ca/2024/04/vulnerabilities/

