The not-so-silent type

Vulnerabilities in Chinese IME Keyboards' Network Security Protocols

Jeffrey Knockel*, Mona Wang†, and Zoë Reichert*

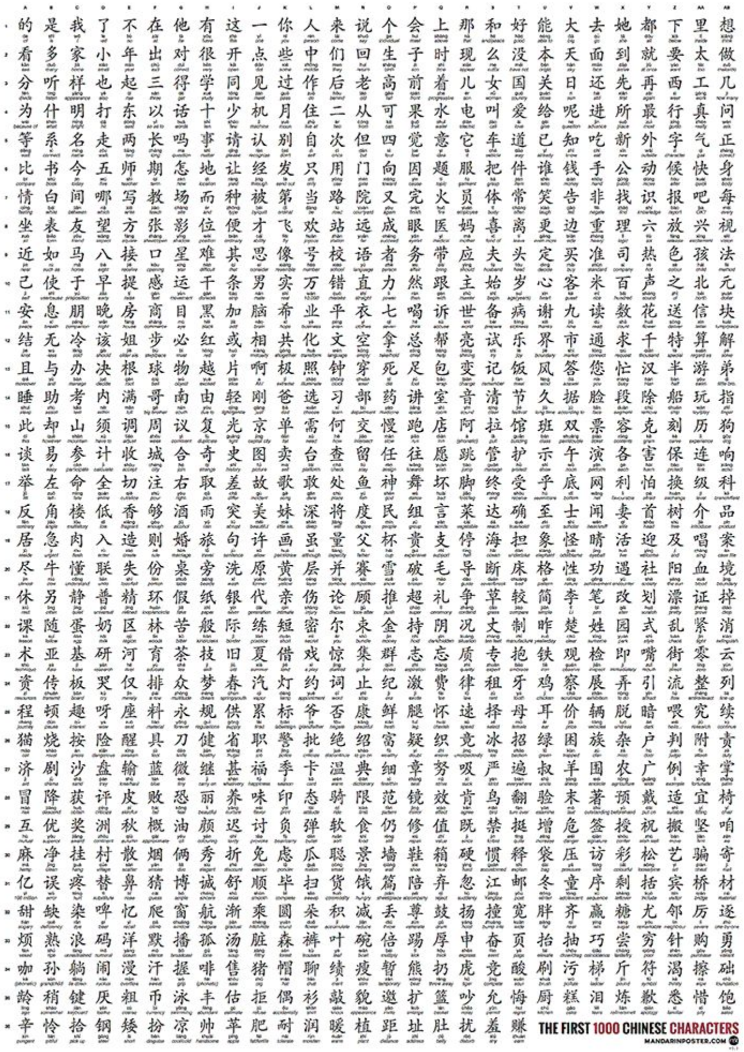
* Citizen Lab, University of Toronto
† Princeton University

What’s a Chinese IME?

26 keys, 26 letters

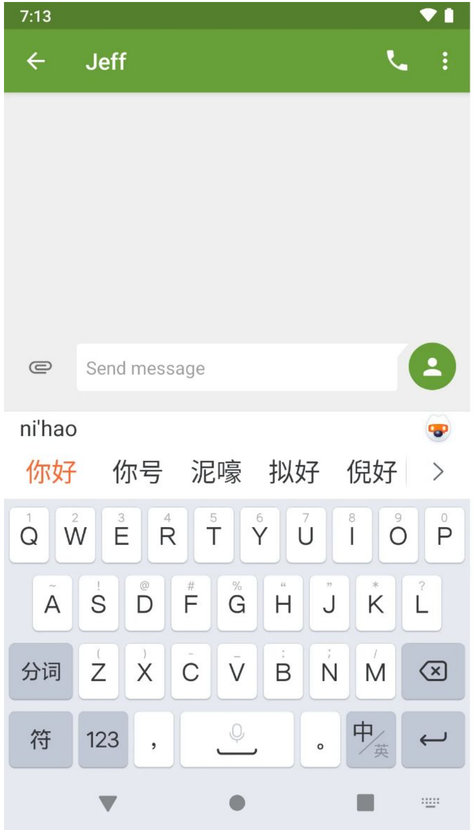
What’s a Chinese IME?

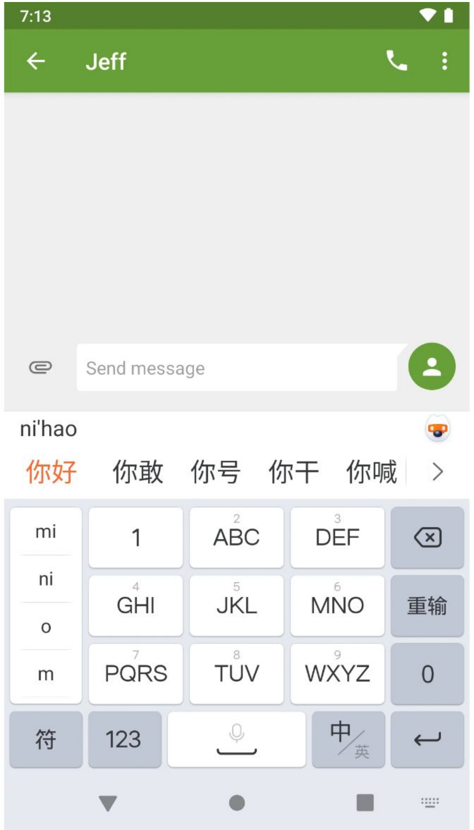
1,000s of characters?

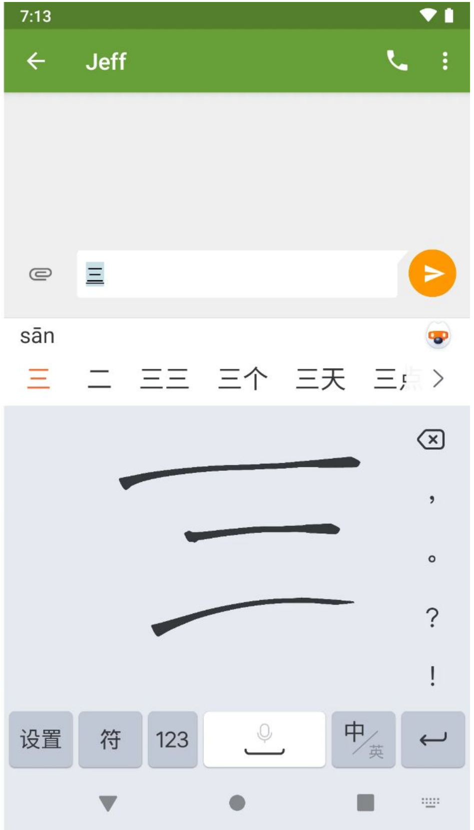

THE FIRST 1000 CHINESE CHARACTERS
MANDARINPOSTER.COM

What’s a Chinese IME?

How does one type/input Chinese?



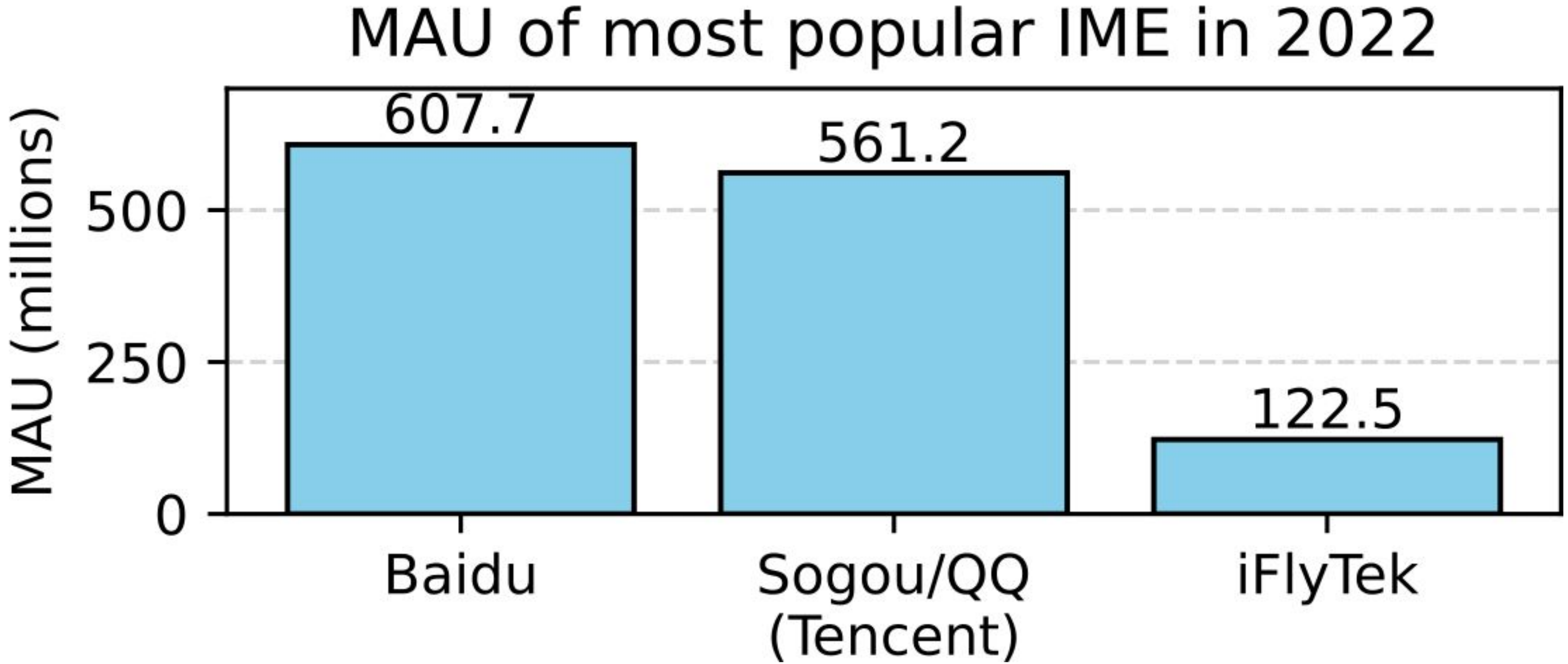




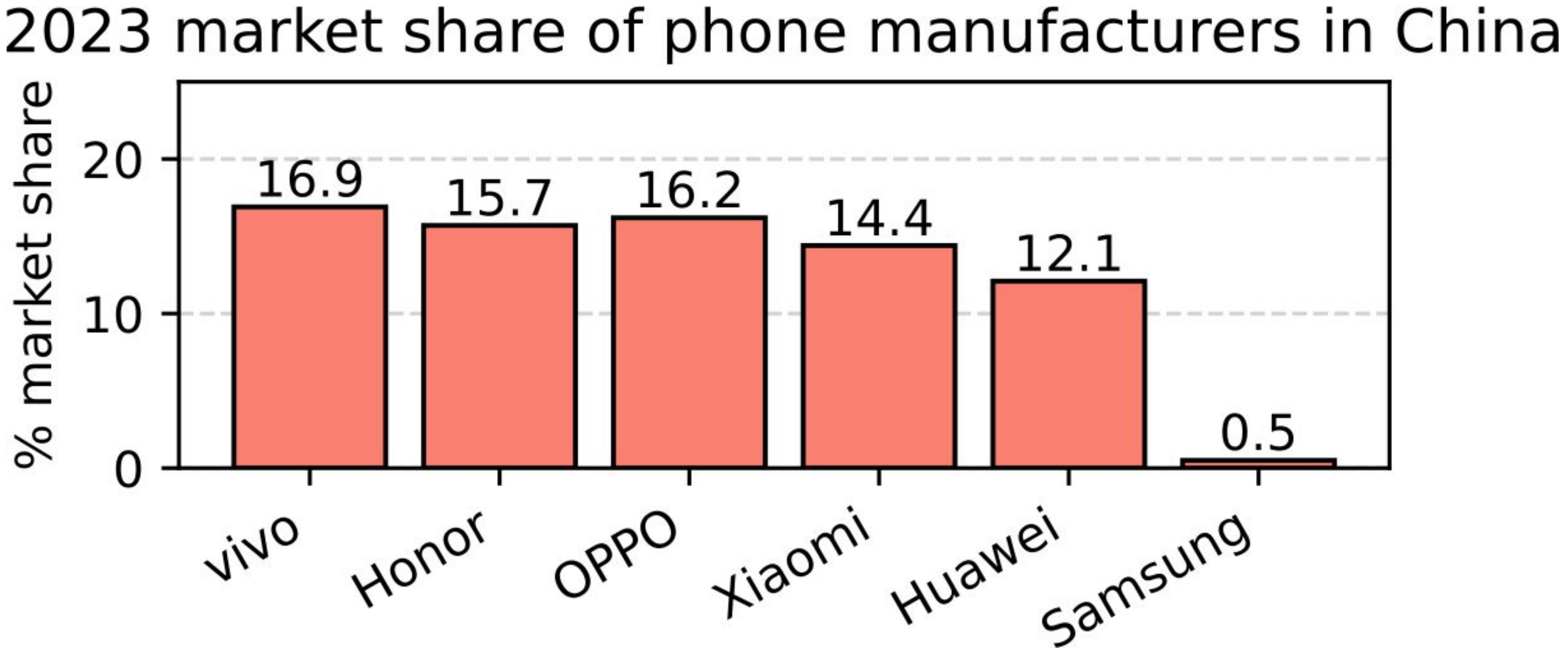
What’s a Chinese IME?

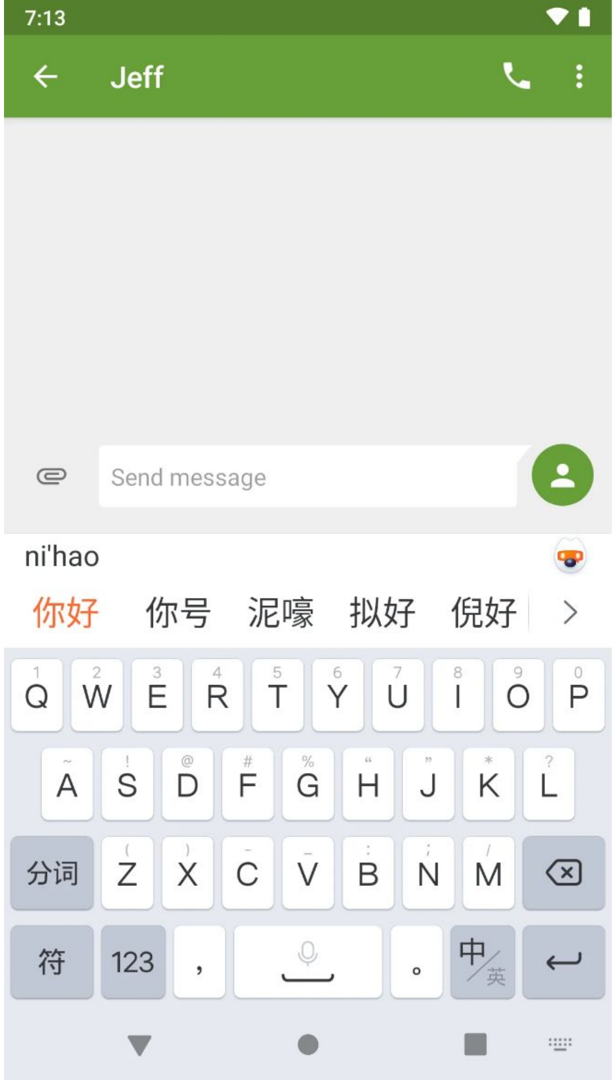
9 buttons, 26 letters!?

Landscape of Chinese IMEs



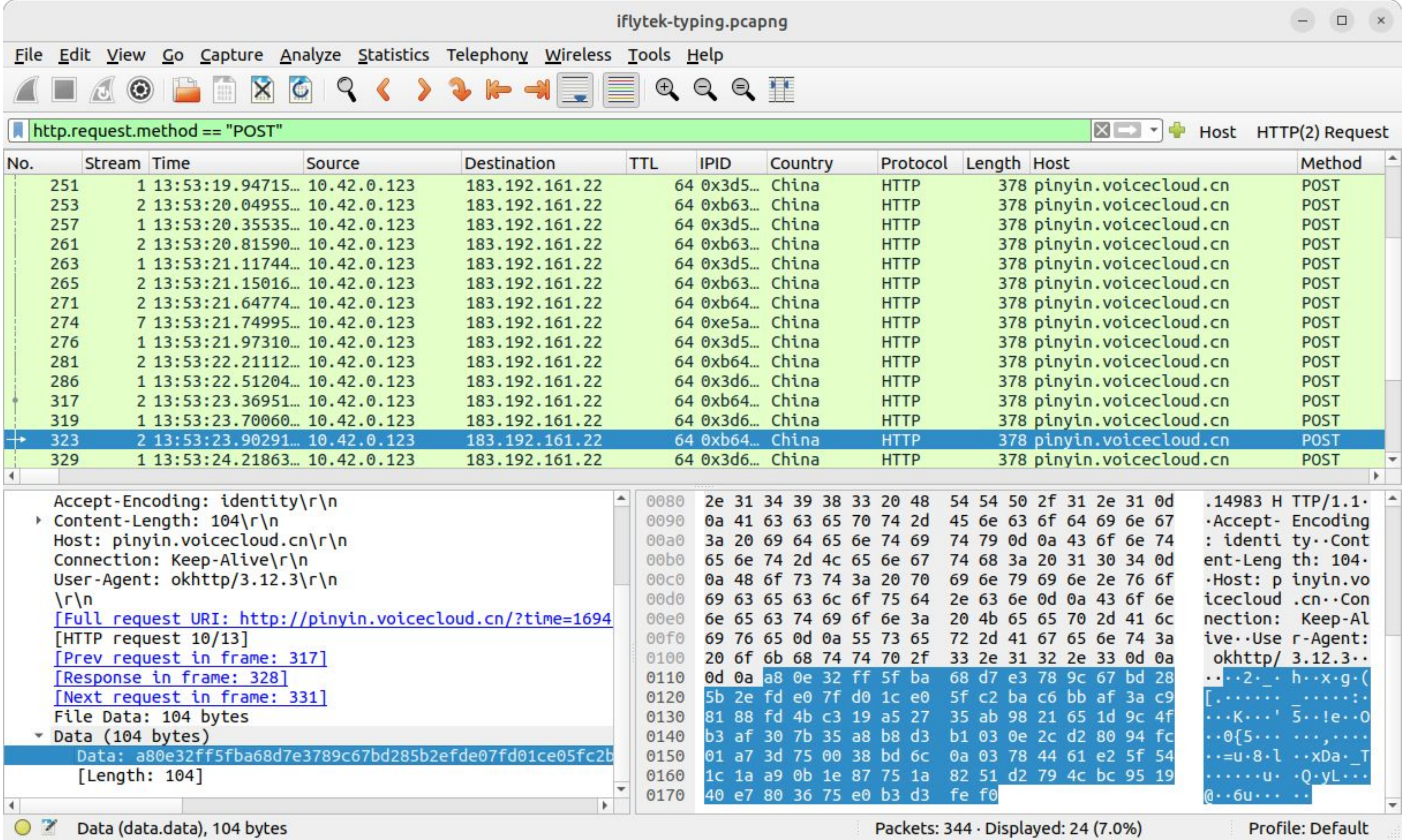
Landscape of Chinese IMEs





ni'hao

7:13
Jeff
Send message
你好
你号
泥嚎
拟好
倪好
1 Q 2 W 3 E 4 R 5 T 6 Y 7 U 8 I 9 O 0 P
~ A ! S @ D # F % G " H " J * K ? L
分词 (Z) X - C _ V : B ; N / M
符
123
，
。
中/英


iflytek-typing.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Host
HTTP(2) Request

```
http.request.method == "POST"
```

```
No.  Stream 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.cn  POST
 253      2 13:53:20.04955… 10.42.0.123  183.192.161.22    64 0xb63…  China   HTTP       378 pinyin.voicecloud.cn  POST
 257      1 13:53:20.35535… 10.42.0.123  183.192.161.22    64 0x3d5…  China   HTTP       378 pinyin.voicecloud.cn  POST
 261      2 13:53:20.81590… 10.42.0.123  183.192.161.22    64 0xb63…  China   HTTP       378 pinyin.voicecloud.cn  POST
 263      1 13:53:21.11744… 10.42.0.123  183.192.161.22    64 0x3d5…  China   HTTP       378 pinyin.voicecloud.cn  POST
 265      2 13:53:21.15016… 10.42.0.123  183.192.161.22    64 0xb63…  China   HTTP       378 pinyin.voicecloud.cn  POST
 271      2 13:53:21.64774… 10.42.0.123  183.192.161.22    64 0xb64…  China   HTTP       378 pinyin.voicecloud.cn  POST
 274      7 13:53:21.74995… 10.42.0.123  183.192.161.22    64 0xe5a…  China   HTTP       378 pinyin.voicecloud.cn  POST
 276      1 13:53:21.97310… 10.42.0.123  183.192.161.22    64 0x3d5…  China   HTTP       378 pinyin.voicecloud.cn  POST
 281      2 13:53:22.21112… 10.42.0.123  183.192.161.22    64 0xb64…  China   HTTP       378 pinyin.voicecloud.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
 317      2 13:53:23.36951… 10.42.0.123  183.192.161.22    64 0xb64…  China   HTTP       378 pinyin.voicecloud.cn  POST
 319      1 13:53:23.70060… 10.42.0.123  183.192.161.22    64 0x3d6…  China   HTTP       378 pinyin.voicecloud.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
```

```
    Accept-Encoding: identity\r\n
  ▸ Content-Length: 104\r\n
    Host: pinyin.voicecloud.cn\r\n
    Connection: Keep-Alive\r\n
    User-Agent: okhttp/3.12.3\r\n
    \r\n
    [Full request URI: http://pinyin.voicecloud.cn/?time=1694
    [HTTP request 10/13]
    [Prev request in frame: 317]
    [Response in frame: 328]
    [Next request in frame: 331]
    File Data: 104 bytes
  ▾ Data (104 bytes)
      Data: a80e32ff5fba68d7e3789c67bd285b2efde07fd01ce05fc2b
      [Length: 104]
```

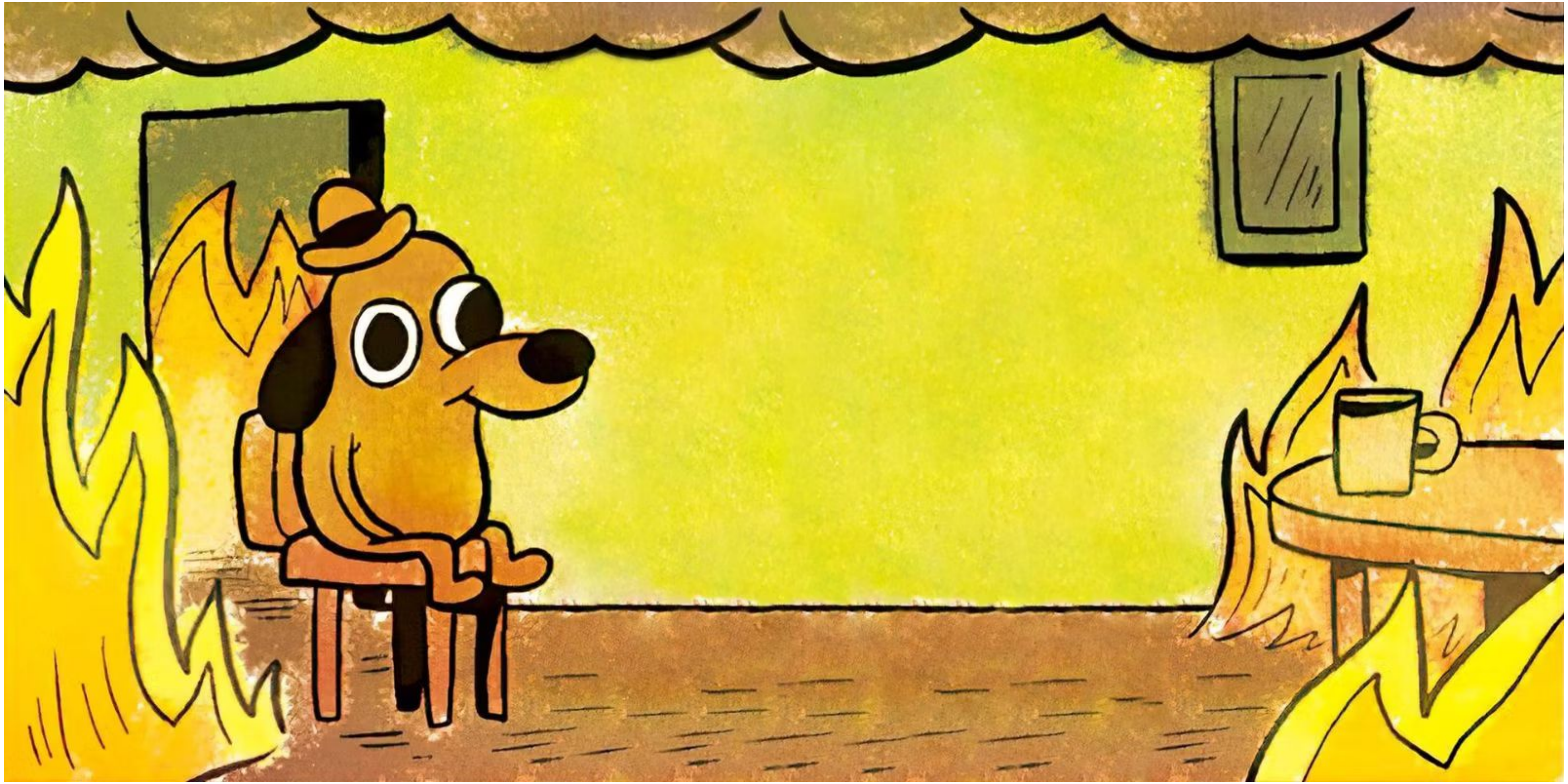
```
0080  2e 31 34 39 38 33 20 48  54 54 50 2f 31 2e 31 0d   .14983 H TTP/1.1·
0090  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   ·Accept- Encoding
00a0  3a 20 69 64 65 6e 74 69  74 79 0d 0a 43 6f 6e 74   : identi ty··Cont
00b0  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 31 30 34 0d   ent-Leng th: 104·
00c0  0a 48 6f 73 74 3a 20 70  69 6e 79 69 6e 2e 76 6f   ·Host: p inyin.vo
00d0  69 63 65 63 6c 6f 75 64  2e 63 6e 0d 0a 43 6f 6e   icecloud .cn··Con
00e0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00f0  69 76 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ive··Use r-Agent:
0100  20 6f 6b 68 74 74 70 2f  33 2e 31 32 2e 33 0d 0a    okhttp/ 3.12.3··
0110  0d 0a a8 0e 32 ff 5f ba  68 d7 e3 78 9c 67 bd 28   ····2·_· h··x·g·(
0120  5b 2e fd e0 7f d0 1c e0  5f c2 ba c6 bb af 3a c9   [.······ _·····:·
0130  81 88 fd 4b c3 19 a5 27  35 ab 98 21 65 1d 9c 4f   ···K···' 5··!e··O
0140  b3 af 30 7b 35 a8 b8 d3  b1 03 0e 2c d2 80 94 fc   ··0{5··· ···,····
0150  01 a7 3d 75 00 38 bd 6c  0a 03 78 44 61 e2 5f 54   ··=u·8·l ··xDa·_T
0160  1c 1a a9 0b 1e 87 75 1a  82 51 d2 79 4c bc 95 19   ······u· ·Q·yL···
0170  40 e7 80 36 75 e0 b3 d3  fe f0                     @··6u··· ··
```

Data (data.data), 104 bytes

Packets: 344 · Displayed: 24 (7.0%)

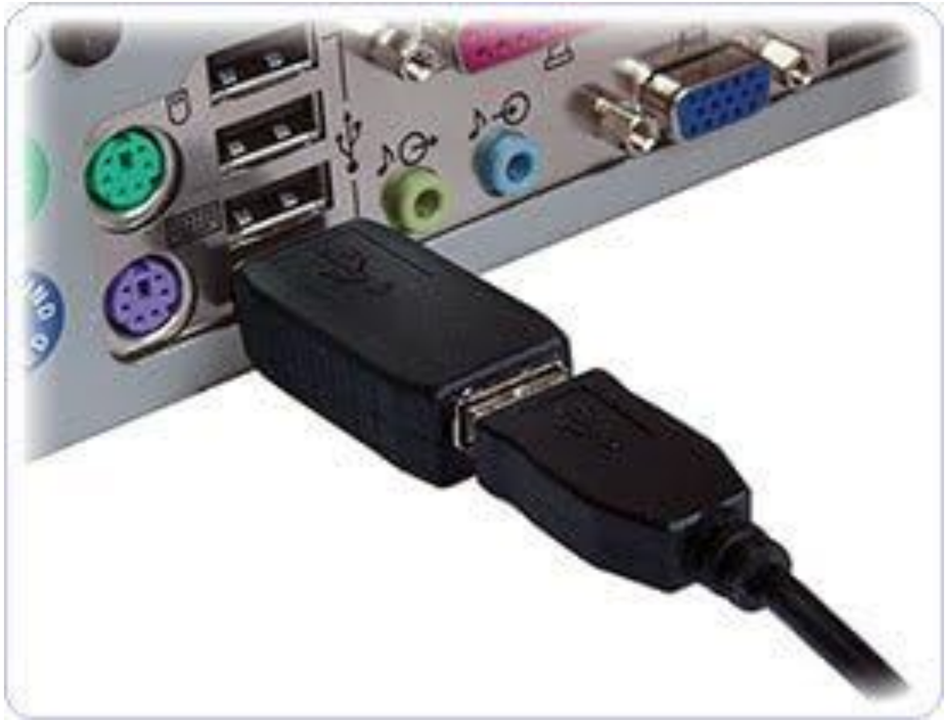
Profile: Default

Uh oh



See, e.g.: You Shouldn’t Collect My Secrets: Thwarting Sensitive Keystroke Leakage in Mobile IME Apps (Chen et al.) USENIX Security 2015

They are keyloggers



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

Threat model

- Attacks on Tencent’s: CBC padding oracle
- All other attacks? **Passively decryptable.**

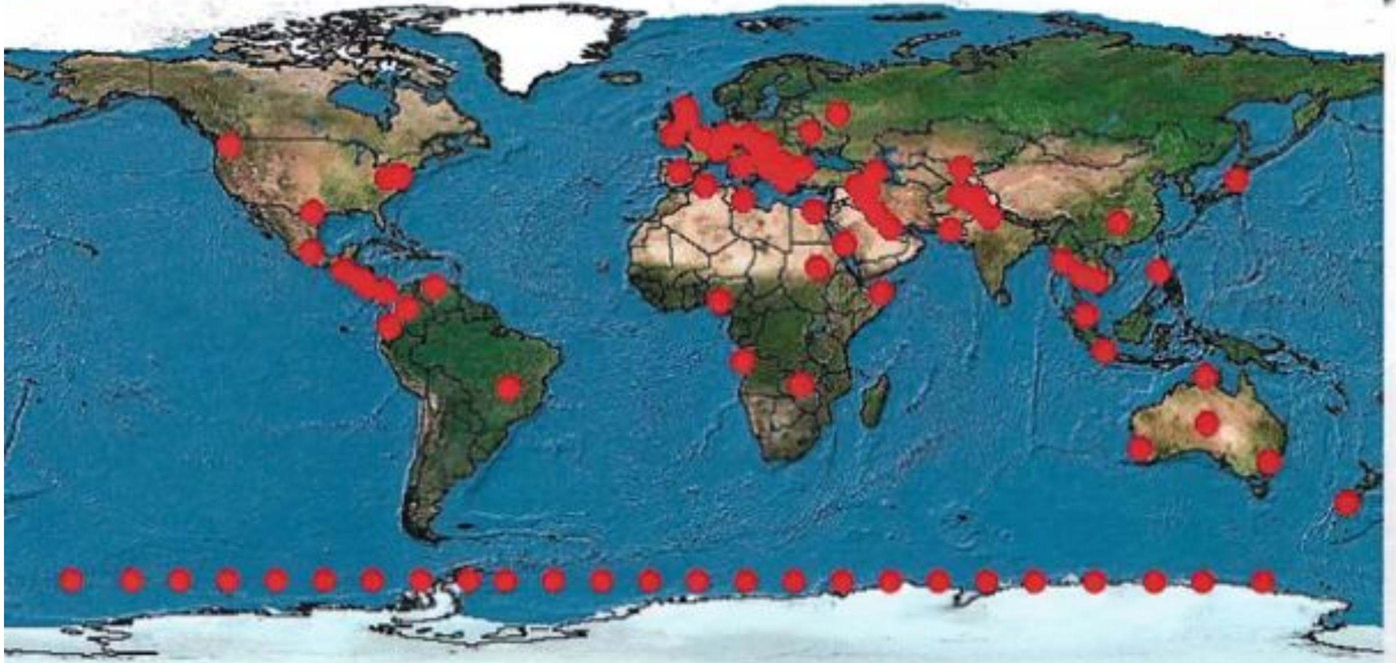
Success Stories

- UCWeb mobile browser identification
  - Discovered by GCHQ analyst during DSD workshop

  - Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics

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

Where is X-KEYSCORE?

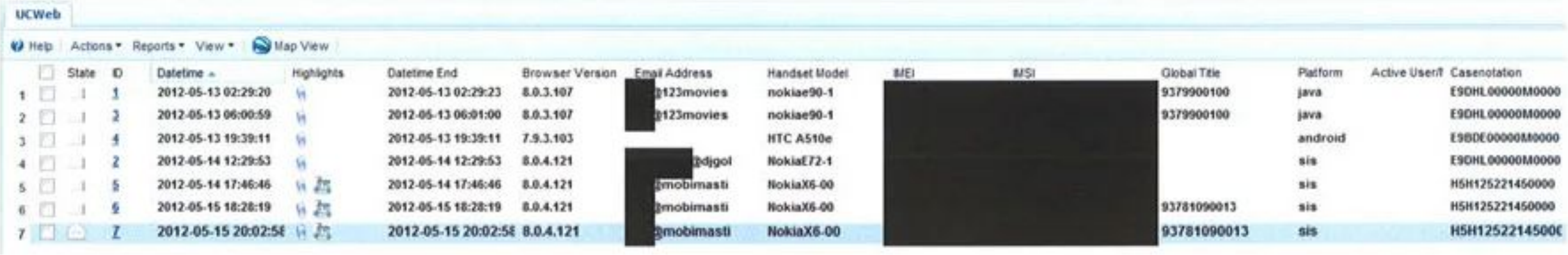


Approximately 150 sites

Over 700 servers

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

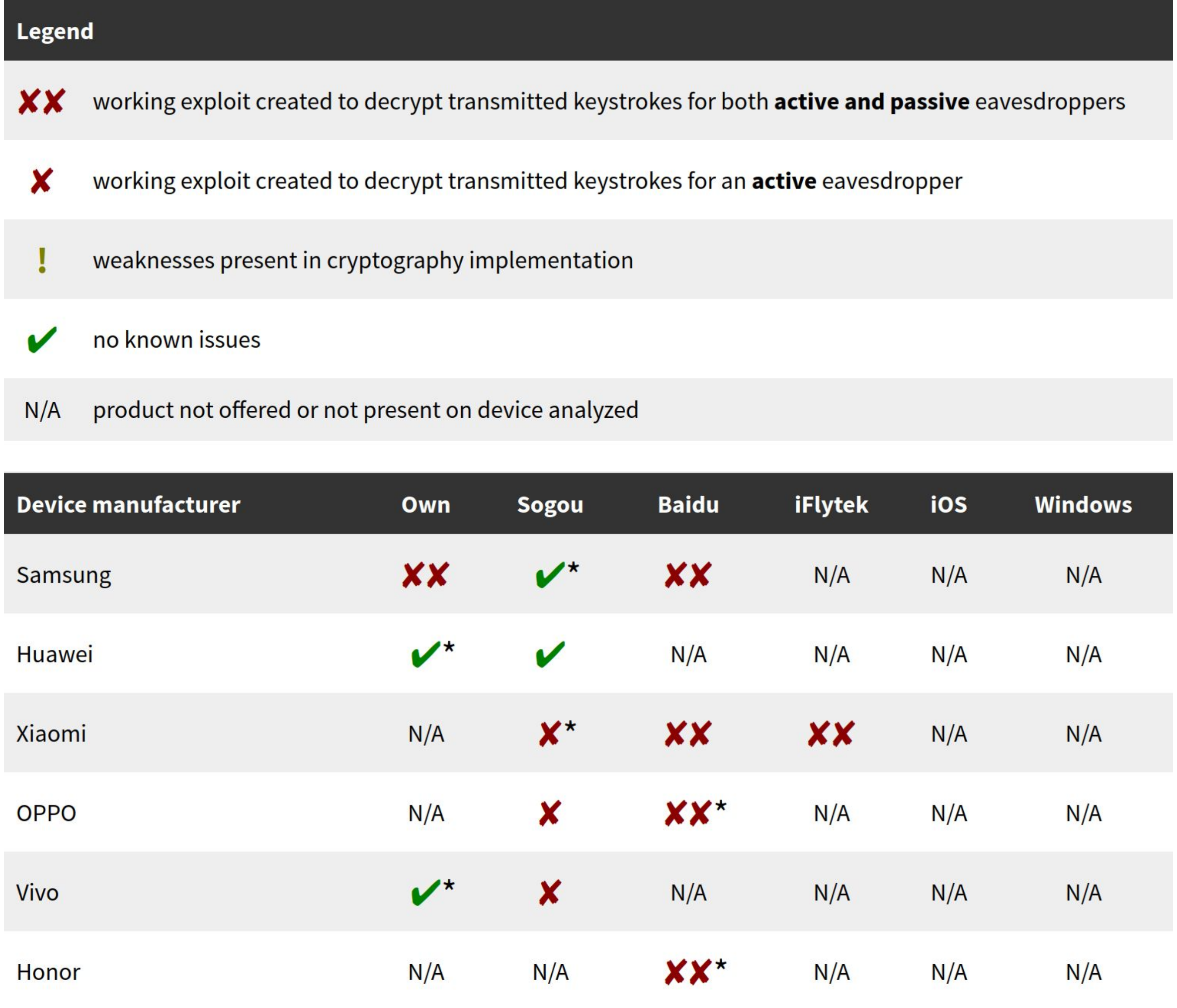
UCWeb – XKS Microplugin



	□	State	ID	Datetime ▲	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform	Active User/I	Casenotation
1	□		1	2012-05-13 02:29:20		2012-05-13 02:29:23	8.0.3.107	[redacted]@123movies	nokiae90-1	[redacted]	[redacted]	9379900100	java		E9DHL00000M0000
2	□		3	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	[redacted]@123movies	nokiae90-1	[redacted]	[redacted]	9379900100	java		E9DHL00000M0000
3	□		4	2012-05-13 19:39:11		2012-05-13 19:39:11	7.9.3.103		HTC A510e	[redacted]	[redacted]		android		E9BDE00000M0000
4	□		2	2012-05-14 12:29:53		2012-05-14 12:29:53	8.0.4.121	[redacted]@djgol	NokiaE72-1	[redacted]	[redacted]		sis		E9DHL00000M0000
5	□		5	2012-05-14 17:46:46		2012-05-14 17:46:46	8.0.4.121	[redacted]@mobimasti	NokiaX6-00	[redacted]	[redacted]		sis		H5H12522145000
6	□		6	2012-05-15 18:28:19		2012-05-15 18:28:19	8.0.4.121	[redacted]@mobimasti	NokiaX6-00	[redacted]	[redacted]	93781090013	sis		H5H12522145000
7	□		7	2012-05-15 20:02:5		2012-05-15 20:02:5	8.0.4.121	[redacted]@mobimasti	NokiaX6-00	[redacted]	[redacted]	93781090013	sis		H5H1252214500

Legend	
✘✘	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✘	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	✘	✔	✘
Baidu	!	!	✘✘
iFlytek	✘✘	✔	✔

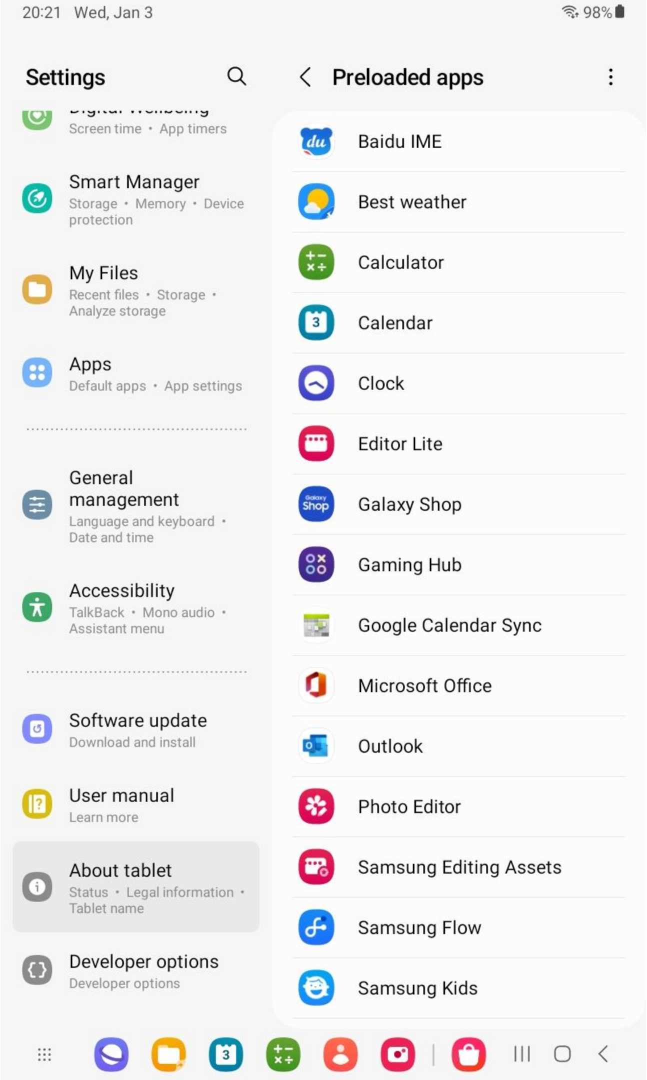


Legend	
✗✗	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✗	working exploit created to decrypt transmitted keystrokes for an **active** eavesdropper
!	weaknesses present in cryptography implementation
✓	no known issues
N/A	product not offered or 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	✗*	✗✗	✗✗	N/A	N/A
OPPO	N/A	✗	✗✗*	N/A	N/A	N/A
Vivo	✓*	✗	N/A	N/A	N/A	N/A
Honor	N/A	N/A	✗✗*	N/A	N/A	N/A

* Default keyboard on device

Baidu for Android (Preloaded onto Samsung)



20:21 Wed, Jan 3 98%

Settings

Digital Wellbeing
Screen time • App timers

Smart Manager
Storage • Memory • Device protection

My Files
Recent files • Storage • Analyze storage

Apps
Default apps • App settings

General management
Language and keyboard • Date and time

Accessibility
TalkBack • Mono audio • Assistant menu

Software update
Download and install

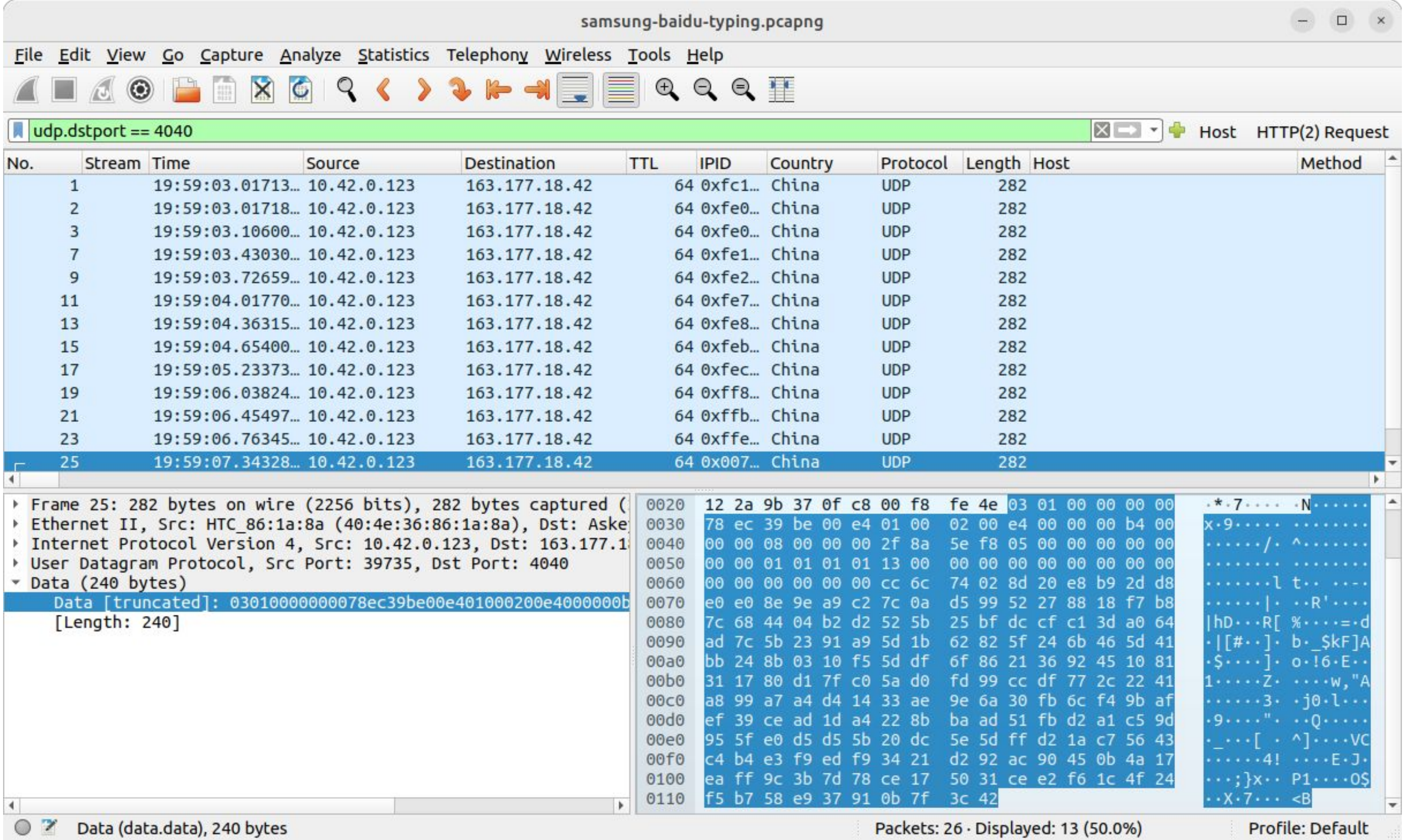
User manual
Learn more

About tablet
Status • Legal information • Tablet name

Developer options
Developer options

Preloaded apps

- Baidu IME
- Best weather
- Calculator
- Calendar
- Clock
- Editor Lite
- Galaxy Shop
- Gaming Hub
- Google Calendar Sync
- Microsoft Office
- Outlook
- Photo Editor
- Samsung Editing Assets
- Samsung Flow
- Samsung Kids


samsung-baidu-typing.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Host
HTTP(2) Request

```
udp.dstport == 4040
```

No.	Stream	Time	Source	Destination	TTL	IPID	Country	Protocol	Length	Host	Method
1		19:59:03.01713…	10.42.0.123	163.177.18.42	64	0xfc1…	China	UDP	282		
2		19:59:03.01718…	10.42.0.123	163.177.18.42	64	0xfe0…	China	UDP	282		
3		19:59:03.10600…	10.42.0.123	163.177.18.42	64	0xfe0…	China	UDP	282		
7		19:59:03.43030…	10.42.0.123	163.177.18.42	64	0xfe1…	China	UDP	282		
9		19:59:03.72659…	10.42.0.123	163.177.18.42	64	0xfe2…	China	UDP	282		
11		19:59:04.01770…	10.42.0.123	163.177.18.42	64	0xfe7…	China	UDP	282		
13		19:59:04.36315…	10.42.0.123	163.177.18.42	64	0xfe8…	China	UDP	282		
15		19:59:04.65400…	10.42.0.123	163.177.18.42	64	0xfeb…	China	UDP	282		
17		19:59:05.23373…	10.42.0.123	163.177.18.42	64	0xfec…	China	UDP	282		
19		19:59:06.03824…	10.42.0.123	163.177.18.42	64	0xff8…	China	UDP	282		
21		19:59:06.45497…	10.42.0.123	163.177.18.42	64	0xffb…	China	UDP	282		
23		19:59:06.76345…	10.42.0.123	163.177.18.42	64	0xffe…	China	UDP	282		
25		19:59:07.34328…	10.42.0.123	163.177.18.42	64	0x007…	China	UDP	282		

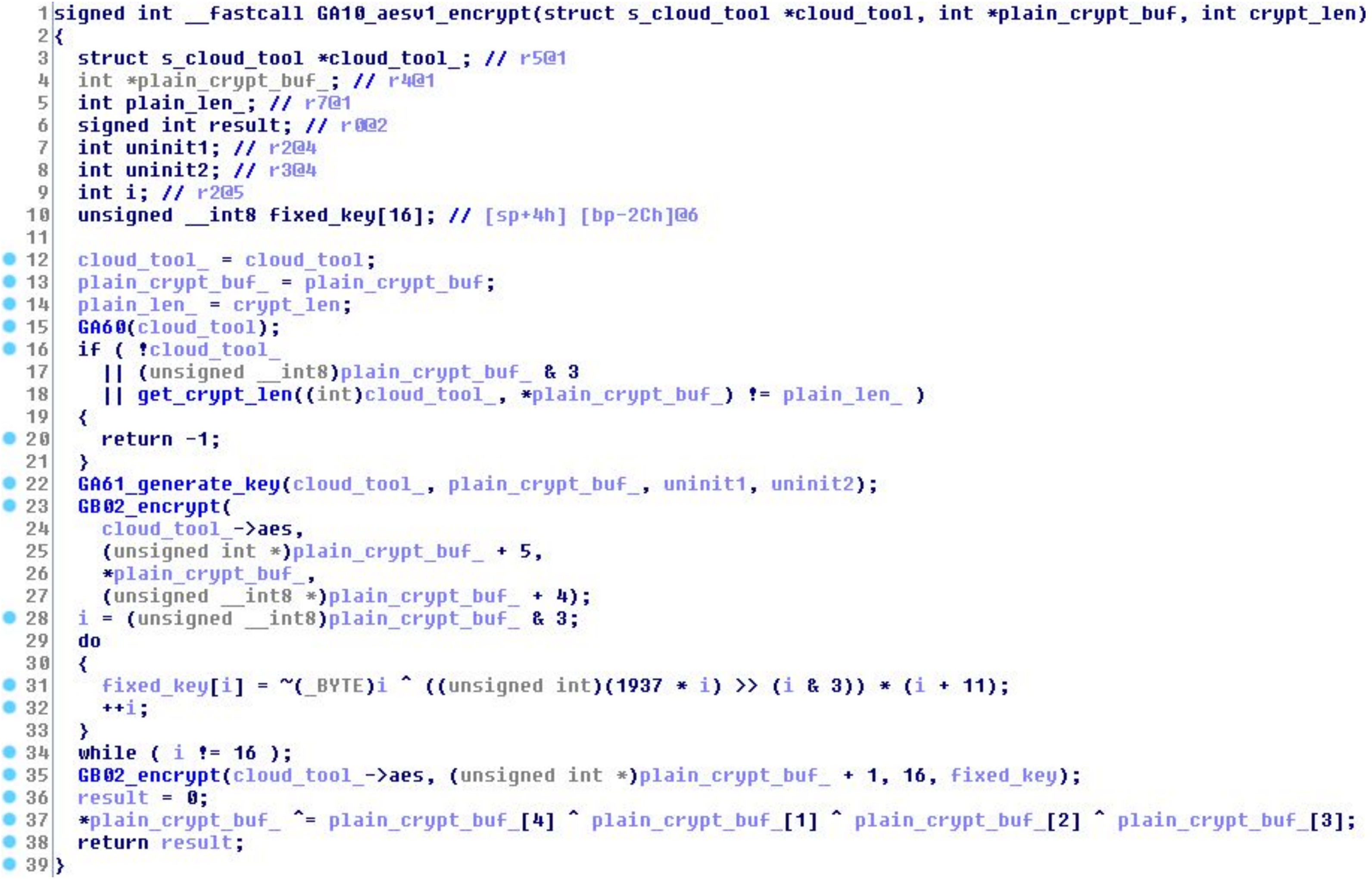
```
▸ Frame 25: 282 bytes on wire (2256 bits), 282 bytes captured (
▸ Ethernet II, Src: HTC_86:1a:8a (40:4e:36:86:1a:8a), Dst: Aske
▸ Internet Protocol Version 4, Src: 10.42.0.123, Dst: 163.177.1
▸ User Datagram Protocol, Src Port: 39735, Dst Port: 4040
▾ Data (240 bytes)
    Data [truncated]: 0301000000078ec39be00e401000200e4000000b
    [Length: 240]
```

```
0020  12 2a 9b 37 0f c8 00 f8  fe 4e 03 01 00 00 00 00   ·*·7···· ·N······
0030  78 ec 39 be 00 e4 01 00  02 00 e4 00 00 00 b4 00   x·9····· ········
0040  00 00 08 00 00 00 2f 8a  5e f8 05 00 00 00 00 00   ······/· ^·······
0050  00 00 01 01 01 01 13 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 cc 6c  74 02 8d 20 e8 b9 2d d8   ·······l t·· ··-·
0070  e0 e0 8e 9e a9 c2 7c 0a  d5 99 52 27 88 18 f7 b8   ······|· ··R'····
0080  7c 68 44 04 b2 d2 52 5b  25 bf dc cf c1 3d a0 64   |hD···R[ %····=·d
0090  ad 7c 5b 23 91 a9 5d 1b  62 82 5f 24 6b 46 5d 41   ·|[#··]· b·_$kF]A
00a0  bb 24 8b 03 10 f5 5d df  6f 86 21 36 92 45 10 81   ·$····]· o·!6·E··
00b0  31 17 80 d1 7f c0 5a d0  fd 99 cc df 77 2c 22 41   1·····Z· ····w,"A
00c0  a8 99 a7 a4 d4 14 33 ae  9e 6a 30 fb 6c f4 9b af   ······3· ·j0·l···
00d0  ef 39 ce ad 1d a4 22 8b  ba ad 51 fb d2 a1 c5 9d   ·9····"· ··Q·····
00e0  95 5f e0 d5 d5 5b 20 dc  5e 5d ff d2 1a c7 56 43   ·_···[ · ^]····VC
00f0  c4 b4 e3 f9 ed f9 34 21  d2 92 ac 90 45 0b 4a 17   ······4! ····E·J·
0100  ea ff 9c 3b 7d 78 ce 17  50 31 ce e2 f6 1c 4f 24   ···;}x·· P1····O$
0110  f5 b7 58 e9 37 91 0b 7f  3c 42                     ··X·7··· <B
```

Data (data.data), 240 bytes

Packets: 26 · Displayed: 13 (50.0%)

Profile: Default



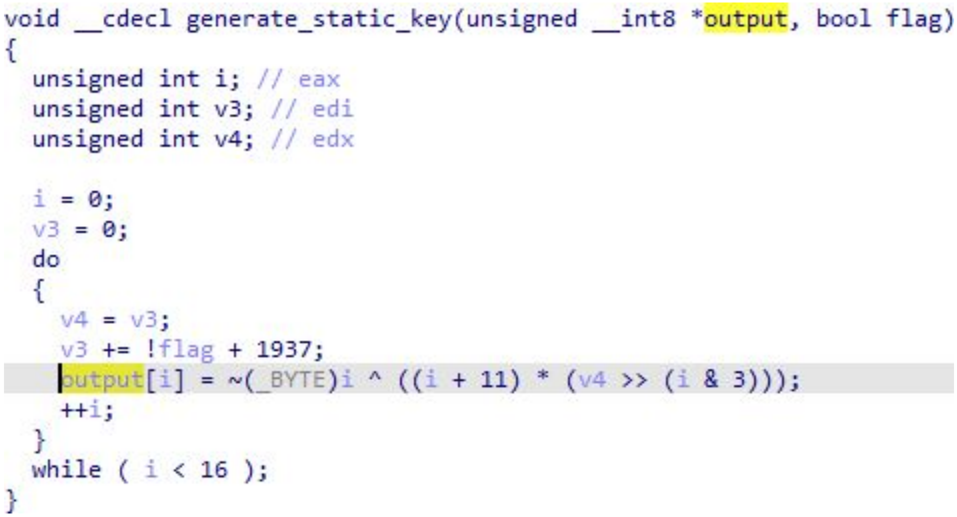
```
signed int __fastcall GA10_aesv1_encrypt(struct s_cloud_tool *cloud_tool, int *plain_crypt_buf, int crypt_len)
{
  struct s_cloud_tool *cloud_tool_; // r5@1
  int *plain_crypt_buf_; // r4@1
  int plain_len_; // r7@1
  signed int result; // r0@2
  int uninit1; // r2@4
  int uninit2; // r3@4
  int i; // r2@5
  unsigned __int8 fixed_key[16]; // [sp+4h] [bp-2Ch]@6

  cloud_tool_ = cloud_tool;
  plain_crypt_buf_ = plain_crypt_buf;
  plain_len_ = crypt_len;
  GA60(cloud_tool);
  if ( !cloud_tool_
    || (unsigned __int8)plain_crypt_buf_ & 3
    || get_crypt_len((int)cloud_tool_, *plain_crypt_buf_) != plain_len_ )
  {
    return -1;
  }
  GA61_generate_key(cloud_tool_, plain_crypt_buf_, uninit1, uninit2);
  GB02_encrypt(
    cloud_tool_->aes,
    (unsigned int *)plain_crypt_buf_ + 5,
    *plain_crypt_buf_,
    (unsigned __int8 *)plain_crypt_buf_ + 4);
  i = (unsigned __int8)plain_crypt_buf_ & 3;
  do
  {
    fixed_key[i] = ~(_BYTE)i ^ ((unsigned int)(1937 * i) >> (i & 3)) * (i + 11);
    ++i;
  }
  while ( i != 16 );
  GB02_encrypt(cloud_tool_->aes, (unsigned int *)plain_crypt_buf_ + 1, 16, fixed_key);
  result = 0;
  *plain_crypt_buf_ ^= plain_crypt_buf_[4] ^ plain_crypt_buf_[1] ^ plain_crypt_buf_[2] ^ plain_crypt_buf_[3];
  return result;
}
```

Baidu for Android (Preloaded onto Samsung)

- Randomly generate “AES” key k_1
- “Generate” “AES” key k_2
- “AES”-encrypt k_1 with k_2
- Encrypt message with k_1
- Transmit encrypted k_1 and encrypted message

“Generate”?

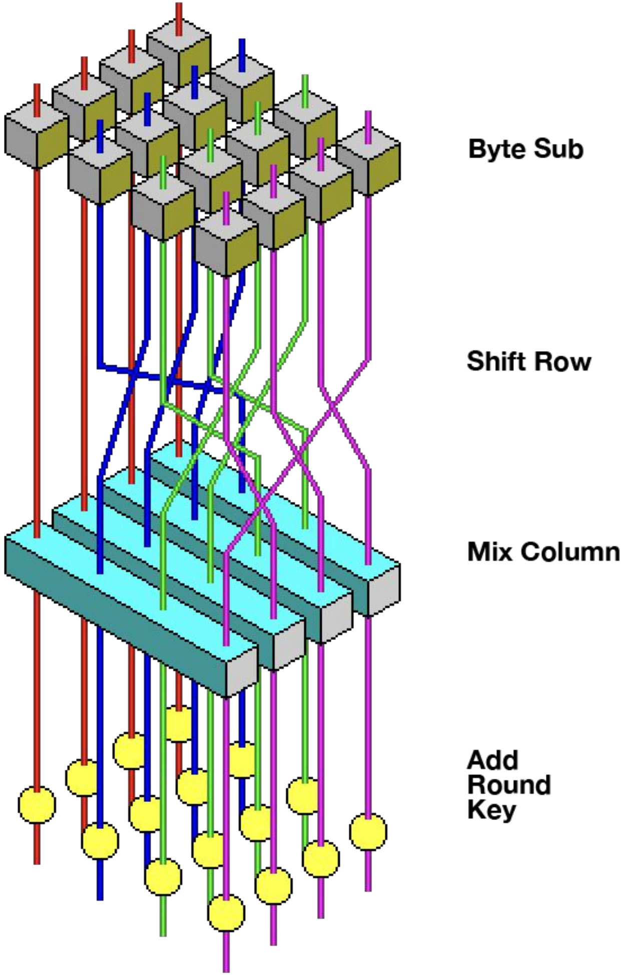
- How does recipient know k_2?
- **Effectively a hard-coded key**



```
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;
    output[i] = ~(_BYTE)i ^ ((i + 11) * (v4 >> (i & 3)));
    ++i;
  }
  while ( i < 16 );
}
```

“AES”?

- Modified AES with additional permutations…
- Security through obscurity…



```
{0: [800,
     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 cryptography 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"
  }
[...]
```

Generalizing attacks

Attacks can generally be extended to…

- decrypting incoming data
- spoofing data
- modifying data

Legend	
✘✘	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✘	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	✘	✔	✘
Baidu	!	!	✘✘
iFlytek	✘✘	✔	✔

Legend	
✗✗	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✗	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	✓	✓	✓
Baidu	!	!	!
iFlytek	✓	✓	✓

Legend	
✗✗	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✗	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	✗*	✗✗	✗✗	N/A	N/A
OPPO	N/A	✗	✗✗*	N/A	N/A	N/A
Vivo	✓*	✗	N/A	N/A	N/A	N/A
Honor	N/A	N/A	✗✗*	N/A	N/A	N/A

* Default keyboard on device

Legend	
✗✗	working exploit created to decrypt transmitted keystrokes for both **active and passive** eavesdroppers
✗	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	✓	✓*	!	N/A	N/A	N/A
Huawei	✓*	✓	N/A	N/A	N/A	N/A
Xiaomi	N/A	✓*	!	✓	N/A	N/A
OPPO	N/A	✓	!*	N/A	N/A	N/A
Vivo	✓*	✓	N/A	N/A	N/A	N/A
Honor	N/A	N/A	✗✗*	N/A	N/A	N/A

* Default keyboard on device

Let’s zoom out a bit!

Most downloaded apps in 2023?

1		
2		
3		
4		
5		
6		

7		
8		
9		
10		
11		
12		

Source: https://www.businessofapps.com/data/most-popular-apps/ (1/30/2024)

Most downloaded apps in 2023?

1	WeChat	1012
2	Alipay	901
3	Taobao	795
4	Pinduoduo	728
5	Instagram	696
6	Douyin	695

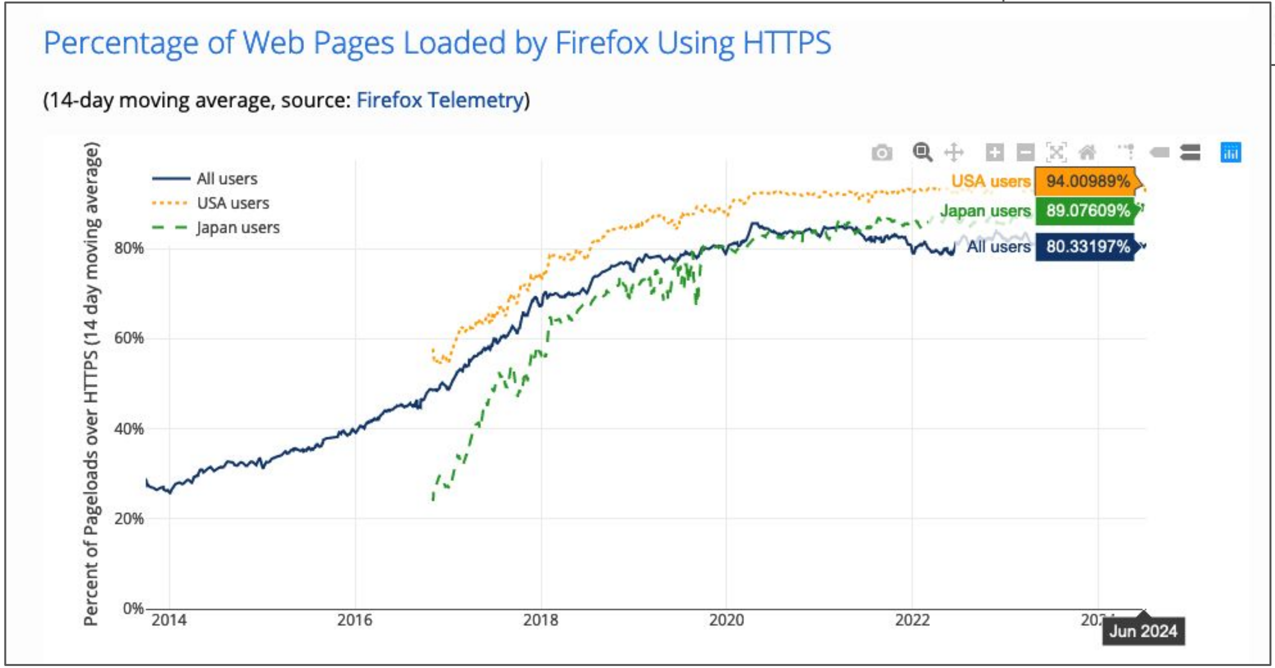
7	TikTok	654
8	QQ	583
9	Facebook	553
10	Baidu	491
11	Kuaishou	480
12	WhatsApp	475

Source: https://www.businessofapps.com/data/most-popular-apps/ (1/30/2024)

ELECTRONIC FRONTIER FOUNDATION

HTTPS Is Actually Everywhere

SEPTEMBER 21, 2021



Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

How many always use HTTPS/TLS?

	WeChat	1012
	Alipay	901
	Taobao	795
	Pinduoduo	728
	Instagram	696
	Douyin	695

	TikTok	654
	QQ	583
	Facebook	553
	Baidu	491
	Kuaishou	480
	WhatsApp	475

Source: https://www.businessofapps.com/data/most-popular-apps/ (1/30/2024)

How many always use HTTPS/TLS?

❌	WeChat	1012
❌	Alipay	901
❌	Taobao	795
❌	Pinduoduo	728
✅	Instagram	696
✅	Douyin	695

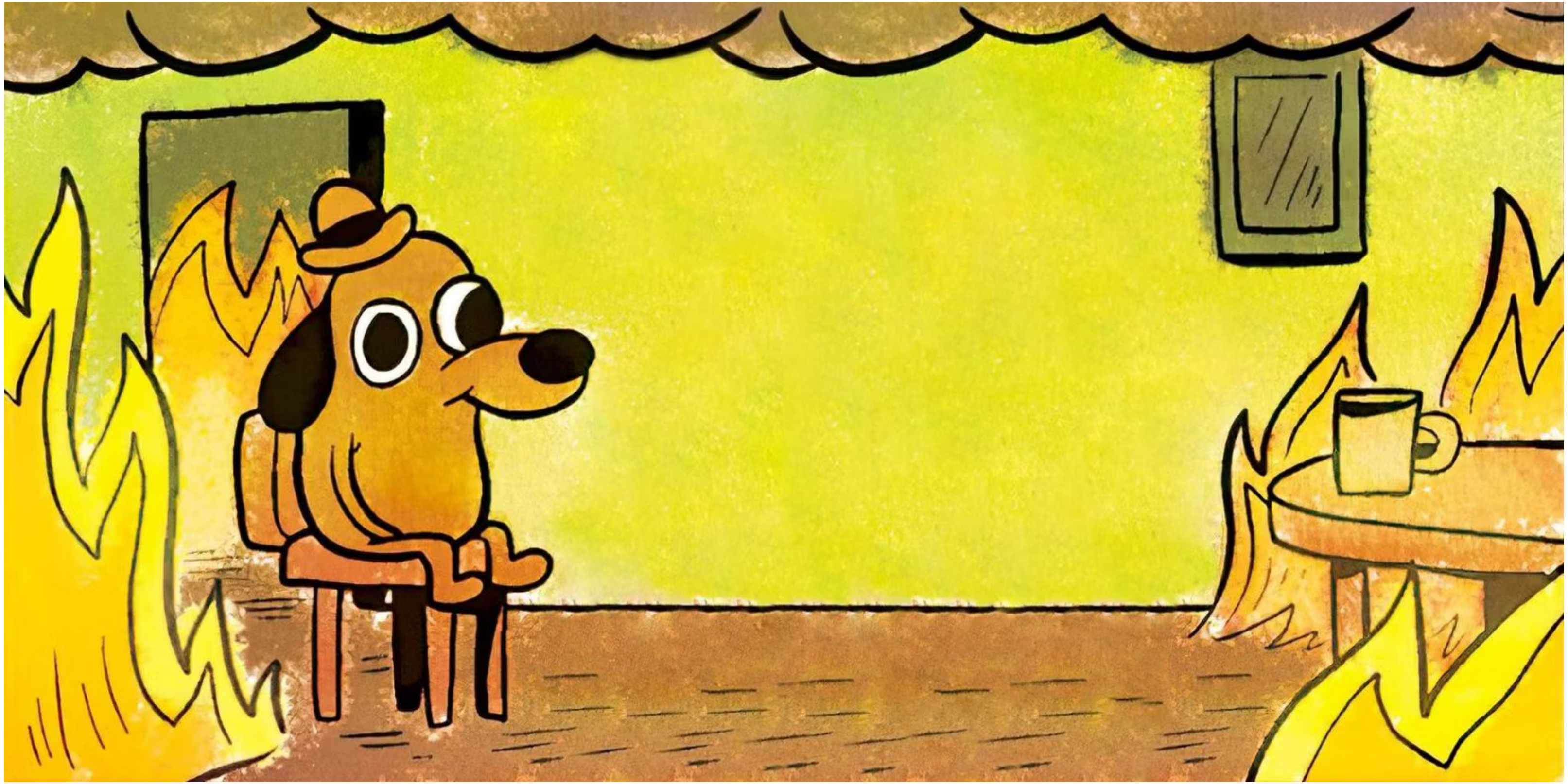
✅	TikTok	654
❌	QQ	583
✅	Facebook	553
❌	Baidu	491
❌	Kuaishou	480
✅	WhatsApp	475

*but they’re also **not not** encrypting…

many of them are **using proprietary cryptography**

Source: https://www.businessofapps.com/data/most-popular-apps/ (1/30/2024)

Oh no



Growing body of evidence

- Chinese browsers [1]
- Prominent Latin American apps [2]
- LINE [3]

[1] Privacy and Security Issues in BAT Web Browsers. (Knockel at al.)
[2] Analyzing Prominent Mobile Apps in Latin America. (Kujath et al.)
[3] Analysis of end-to-end encryption in the LINE messaging application. (Espinoza et al.)

Conclusions

- Large, understudied app ecosystems **still** have serious and easily exploited vulnerabilities in their cryptosystems
- These vulnerabilities may be under active exploitation
- More work is needed to further characterize the “shape” of this class of apps so that we can better predict which apps still need our attention and help fix them

Thank you!

Tons more details in the paper!

Questions?