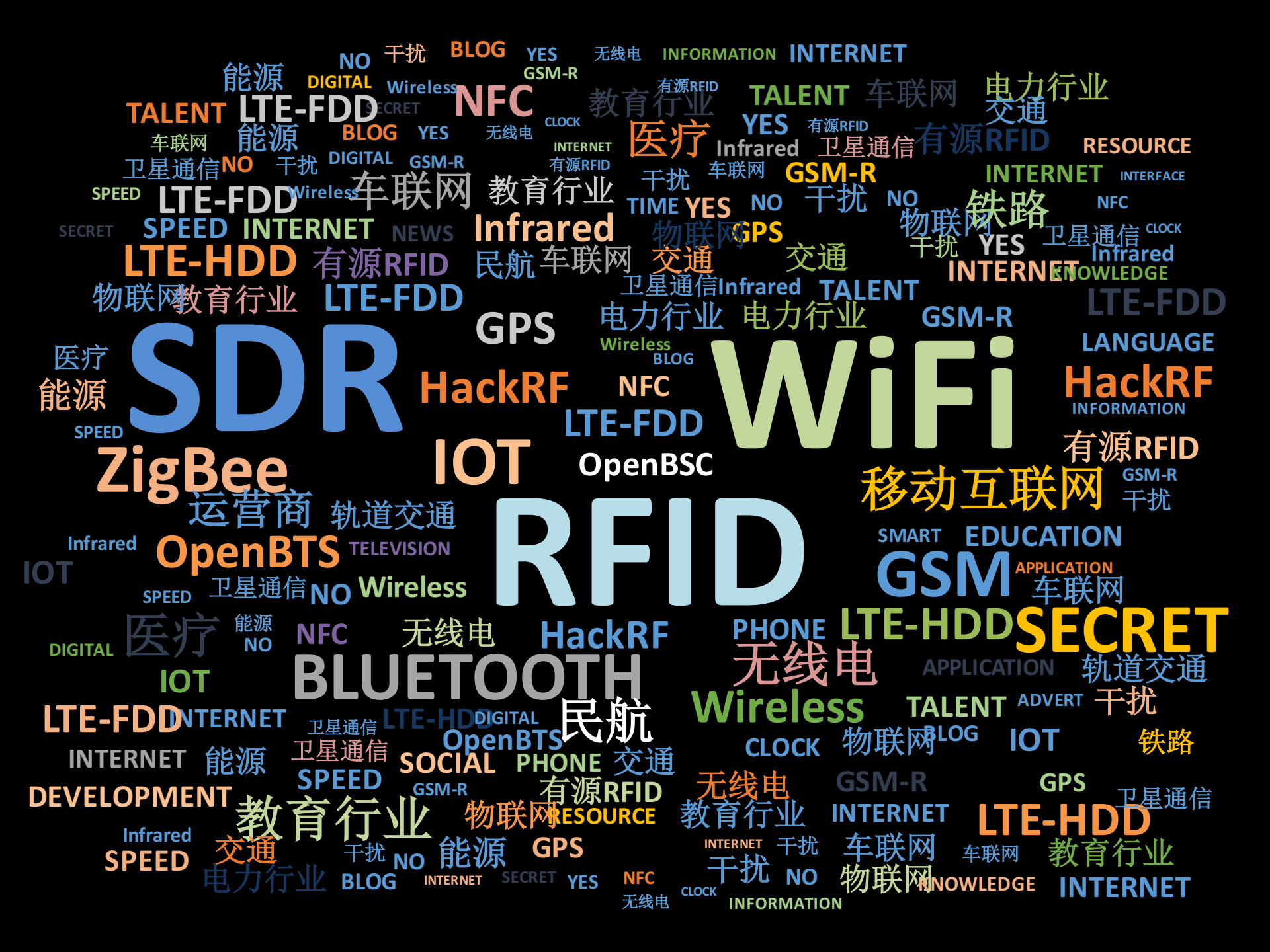
大力出奇迹の WiFi Hacking

杨　哲 (Longas)
ZerOne无线安全研究组织
ZerOne WirelessSec Research


SDR
WiFi
RFID
SECRET
BLUETOOTH
ZigBee
IOT
HackRF
OpenBTS
OpenBSC
GSM
LTE-FDD
LTE-HDD
NFC
GPS
Infrared
SPEED
INTERNET
DIGITAL
Wireless
BLOG
YES
NO
干扰
无线电
INFORMATION
GSM-R
有源RFID
TALENT
车联网
电力行业
交通
医疗
能源
卫星通信
教育行业
物联网
铁路
移动互联网
运营商
轨道交通
TELEVISION
SMART
EDUCATION
APPLICATION
PHONE
ADVERT
CLOCK
RESOURCE
INTERFACE
NEWS
TIME
SOCIAL
DEVELOPMENT
KNOWLEDGE
LANGUAGE
民航

12只猴子

- Crack WPA
- Pentest over WiFi
- Fake AP
- Air-Capture
- MITM
- WAP Tunnel
- WAPJack

WIDS / WIPS/Hotspot

- Deauth/Auth/Disco
- WiFiphisher

案例聚焦

FakeAP

空口监听

WAPJack

85%

我去WPA密码!!!!!

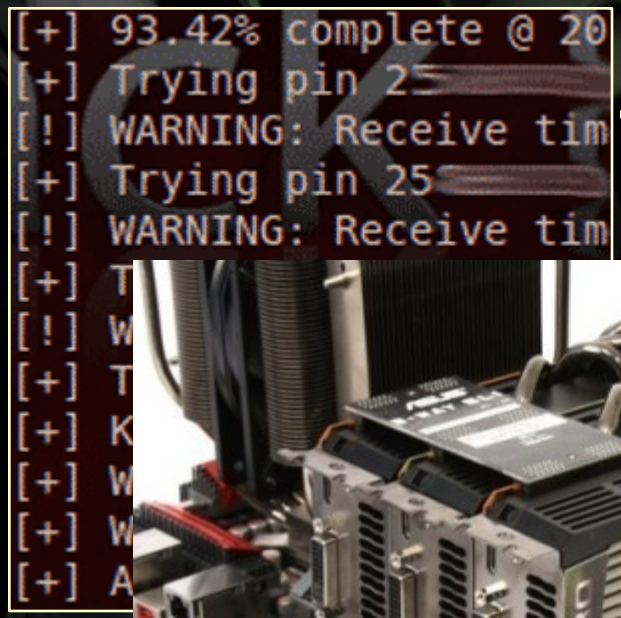
内网渗透

MITM

Deauth

Crack
#主流

- Dictionary
- WPA PMK Hash
- WPS Online / Offline
- Distributed
- GPU
- Cloud

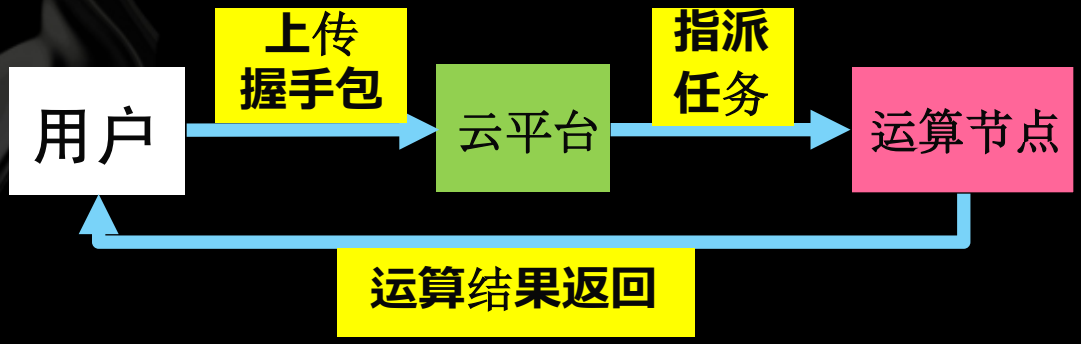


新平台
发布

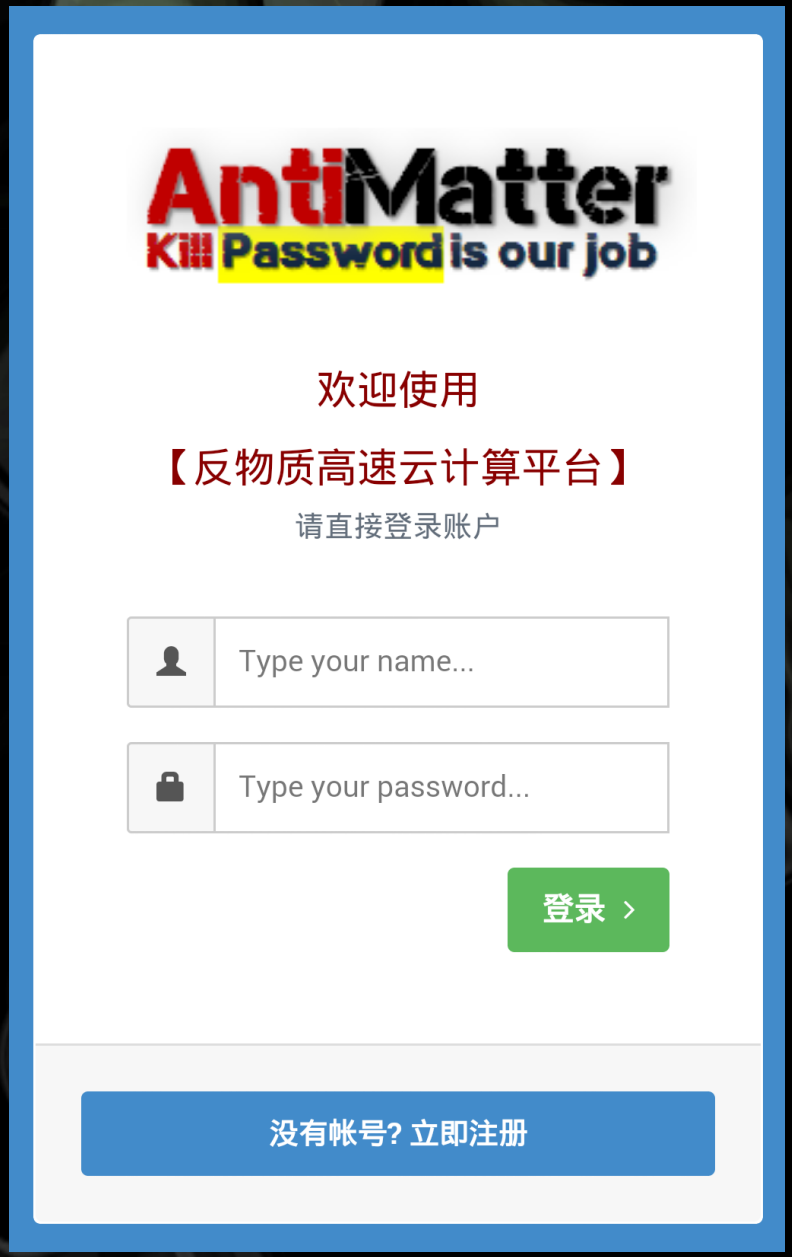
{反物质}无线安全评估云平台

AntiMatter

Kill Password is our job



初始界面


AntiMatter
Kill Password is our job
欢迎使用
【反物质高速云计算平台】
请直接登录账户
Type your name...
Type your password...
登录 >
没有帐号? 立即注册


任务中心
新建任务
任务名称 *
Type task name...
通知邮箱 *
Type your email...
上传文件 *
选择文件
未选择文件
注：文件为包含WPA/WPA2握手的数据报文，后缀名.cap
备注信息 *
Type your comment...

几个数字

40,000,000,000,000	组合
3,000	样本
300	日夜
3	公测


1qazxsw2
zxm19860412
aaron123
6666688888
01234567
888889999
1234554321
a=b?c:d;
52890301
34238817
62518915
62518913
zhouyuer
linyulong
zhangjianguo
windgame
ying123456
wireless123
46958820
GREENLEAF
tanglaoban
88990102
11759000
APPLICATION
HELLOWORLD
BLOGBLOG
RESOURCE
11223344
88776655
TOWER1234
12345678
SECRET123
TEXT
NETWORK
TOWER
susan1003
34238817
33445566
REDCLOCK
qazwsxedc
wang1104
liujiejie
sakurasakura
TOWERFUL
watashiwa
52331314
IHATEYOU
once0822
123456789
TEXTTEXT
ADVERT
wangkang
DIGITAL
DATADATA
10000008
6231565
12345679
1234567890123
3344rrff
wine888999
11112222
12345432
INFORMATION
ying12345
NETWORK123
12345679
FOLLOWME
ECONOMIC
19751023
02961756
82729336
87654321
34238817
qwerasdf
110110110
TALENT
RISK
IMPROVE2
19830405
xa_123456!
11112222
1122334455
0127h0p0d
87654321
SPEED
zxcvbnm67989989

词根？！

LYP82NLF

DEPPON%2B*%40147

1z2x3k4l5q6y

ACC2C7AHSU

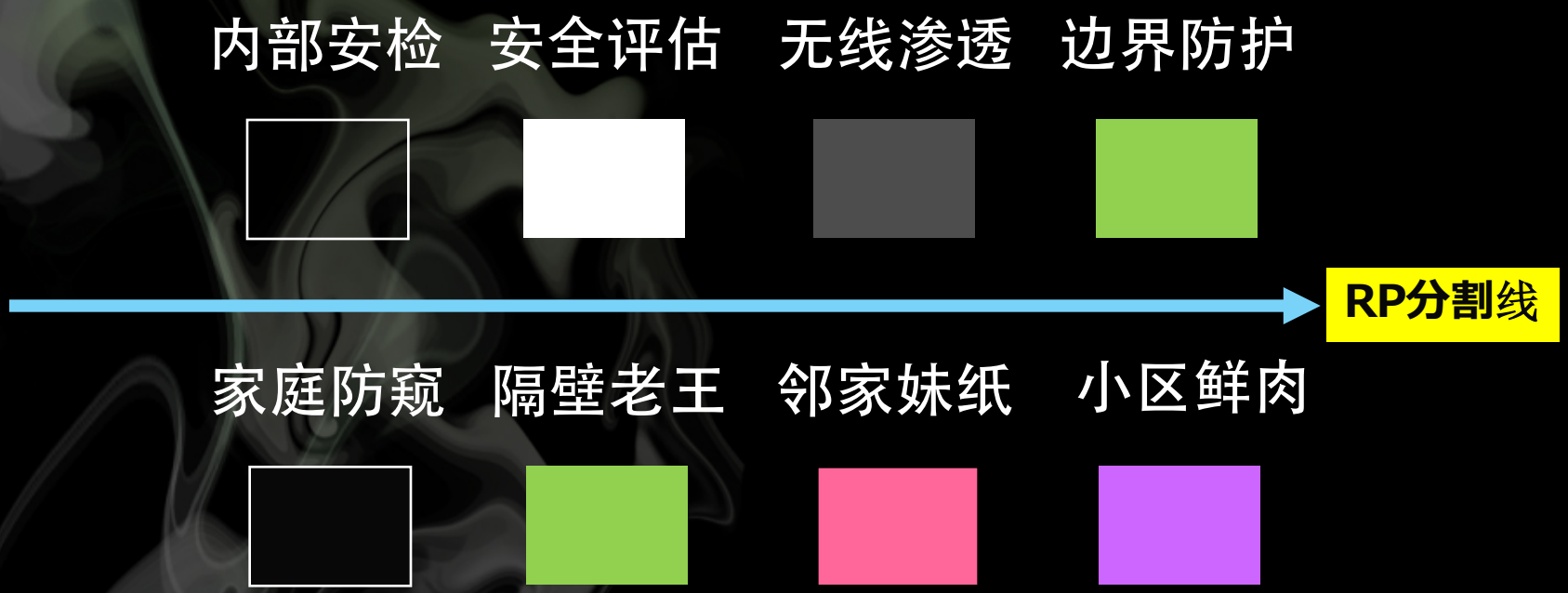
状态	结果	WPA1/2密码	总耗时
运行中	第 1 轮-未破解	未知	1:17:3
已完成	第 1 轮-已破解	13600096327	0:05:1
已完成	第 1 轮-未破解	未知	0:56:3
已完成	第 1 轮-已破解	11173336	0:01:3
已完成	第 1 轮-已破解	xuehua76	1:11:4
已完成	第 1 轮-已破解	abcd123.com	0:29:3
已完成	第 2 轮-未破解	未知	1:21:0
已完成	第 2 轮-未破解	未知	1:22:3
已完成	第 2 轮-未破解	未知	1:20:4
已完成	第 1 轮-已破解	1985100119851001	0:00:0
已完成	第 2 轮-已破解	qwer@asdf	0:00:1
已完成	第 1 轮-已破解	1qaz2wsx	0:00:1
已完成	第 1 轮-已破解	hastings	0:00:1

运算界面

```
 [0:08:09] listening for handshake...
 [0:00:11] handshake captured! saved as "hs/nossid_78-44-76-
F5-E6-82.cap"

 [+] 1 attack completed:

 [+] 1/1 WPA attacks succeeded
        nossid (78:44:76:F5:E6:82) handshake captured
        saved as hs/nossid_78-44-76-F5-E6-82.cap

 [+] starting AntiMatter Cloud Compute on 1 handshake
 [!] Now activating handshake upload process....
 [*] 2 - Upload capfile now
 [*] 1 - Upload and upload other Failed capfile --- wait for
 :)
 [*
[*]

 [*
OK
 [*
 [*]                    /hs/nossid_78-44-76-F5-E6-82.cap
[*] Upload Done:  /hs/nossid_78-44-76-F5-E6-82.cap
```

Num	邀请码 free.wpapass.com
01	7659215ecbb8977597ad913e0f2247af
02	53c555d033c8c6a7eb759d902531b5cc
03	b78783e5171416ecbbc623260e0c5a32
04	eec71f550ce81e6a69294c8f7a7e6784
05	76f429c136532587af08f3a3399a9a3b

应用领域

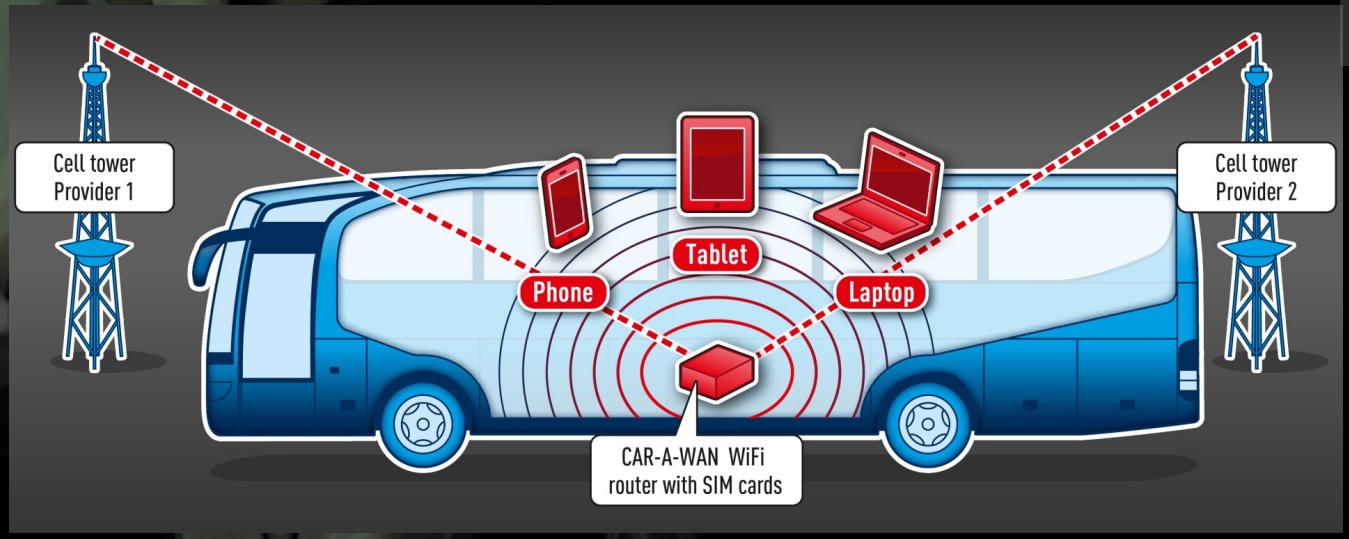


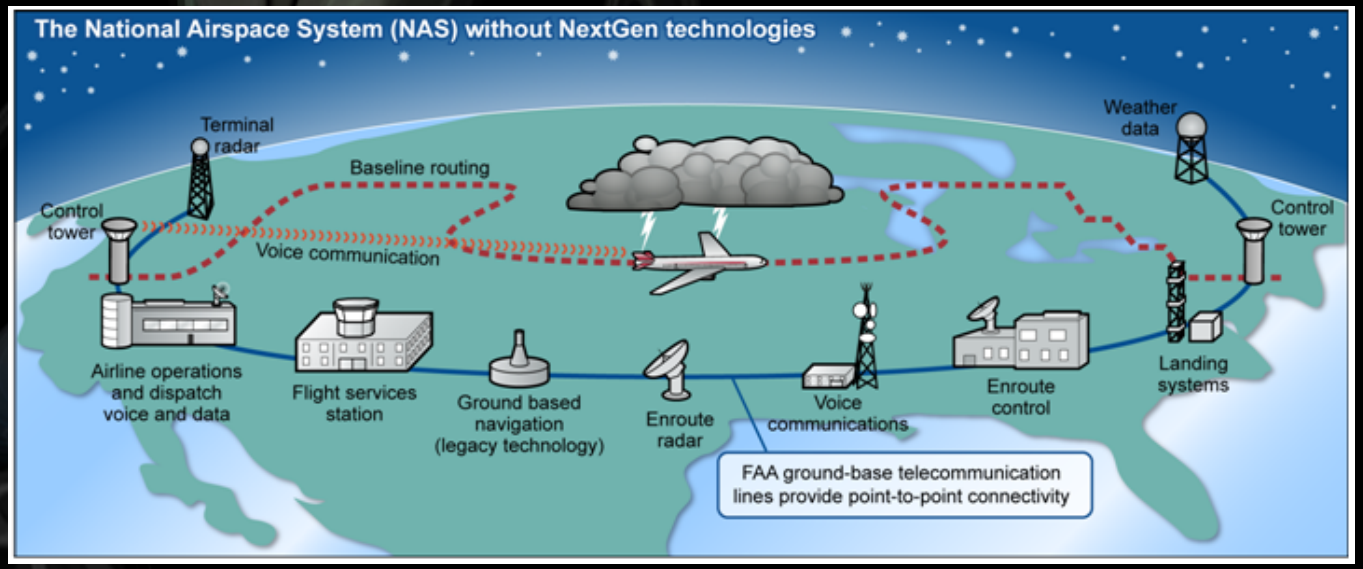
那些前浪

	平台名称	支持WPA 1/2	支持cap文件上传	支持hccap文件上传	自动提取SSID	支持中文SSID	支持多SSID	自定义任务名	任务暂停/恢复	用户自行指定字典	字典分级	历史破解任务浏览	支持外部API
1	AntiMatter	√	√		√	√	√	√	√		√	√	√
2	GPUHASH	√	√		√					√	√		
3	Cloud Cracker	√	√		√							√	√
4	HashCrack	√		√	√						√	√	
5	HashBreak	√	√		√							√	
6	Online HashCrack	√	√		√							√	
7	darkircop	√	√		√								

Amazing Race

有趣的…


Cell tower
Provider 1
Cell tower
Provider 2
Tablet
Phone
Laptop
CAR-A-WAN WiFi
router with SIM cards


The National Airspace System (NAS) without NextGen technologies
Terminal
radar
Baseline routing
Control
tower
Voice communication
Weather
data
Control
tower
Airline operations
and dispatch
voice and data
Flight services
station
Ground based
navigation
(legacy technology)
Enroute
radar
Voice
communications
Enroute
control
Landing
systems
FAA ground-base telecommunication
lines provide point-to-point connectivity

杨 哲
(Longas)
ZerOne无线安全研究组织
tec@zeronesec.com

ZerOne
WirelessSec Research

Thanks !!