Drosera

Protect your wireless network using honeypot

Yunfei Yang(@qingxp9)
PegasusTeam, 360 Technology

Who We Are

360 Security Technology is a leading Internet security company in Asia. Our core products are anti-virus security software for PC and cellphones.

PegasusTeam was founded in 2015. We focus on the wireless security and wireless pentesting.

Agenda

- [ ] Wi-Fi Attack Surfaces
- [ ] Wireless Intrusion Prevention System
- [ ] Wireless Honeypot

Wi-Fi Attack Surfaces

- Physical Properties
- DoS Attacks
- Weak Encryption and Authentication
- Rogue APs

Image source: http://www.quick-dk.com/el-nuevo-modelo-de-capacitacion-en-la-generacion-conectada/

✳ Physical Properties

- Do not need any physical connection
- RF signal spillage may expose the network to unauthorized users.

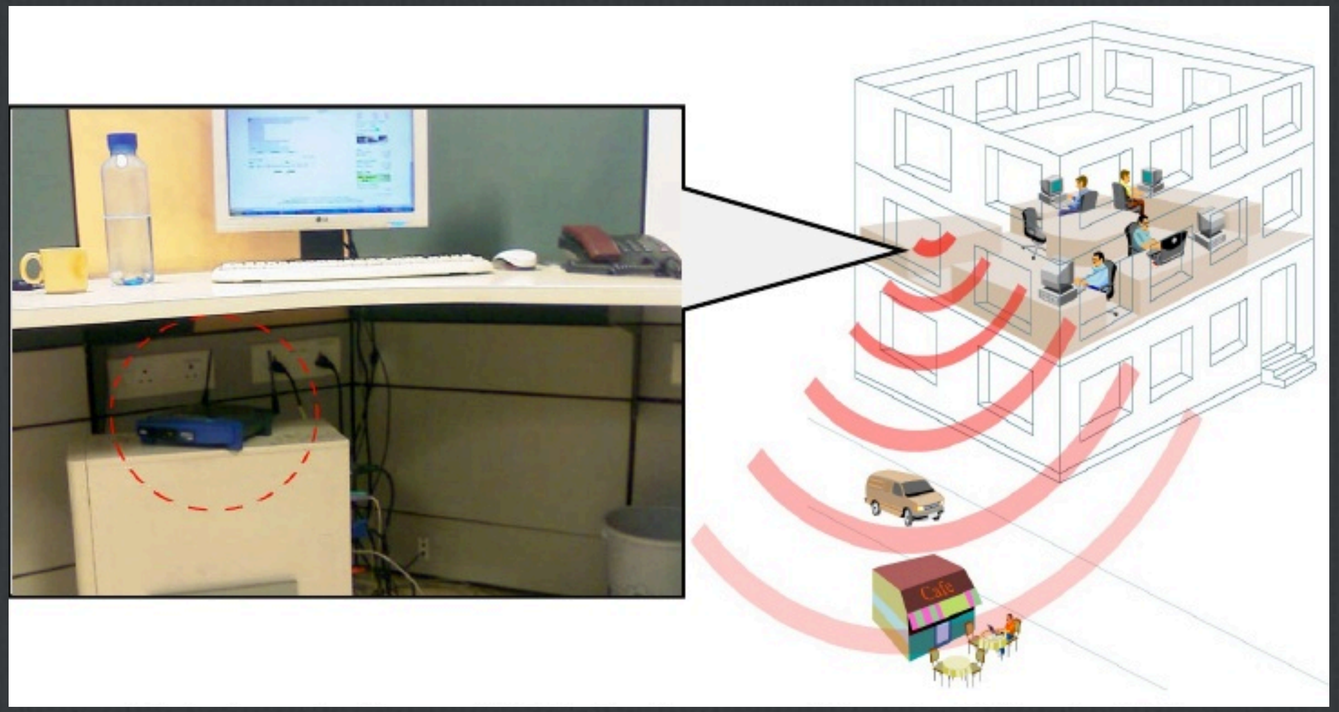


Image source: https://pt.slideshare.net/MdSohailAhmad/rogue-ap

✳ DoS Attacks

- Beacon Flood
- Authentication Flood
- Association Flood
- Deauthentication Flood
- Disassociation Flood
- …

MDK3

b Beacon Flood Mode

- show many fake APs at clients.

d Deauth/Disassoc Amok Mode

- kick all clients from AP.

✳ Weak Encryption and Authentication

- WEP
- Wi-Fi Protected Setup(WPS)
- WPA/WPA2-PSK(Pre-shared Key)
- WPA/WPA2-Enterprise(802.1X)
- OPEN with Captive Portal

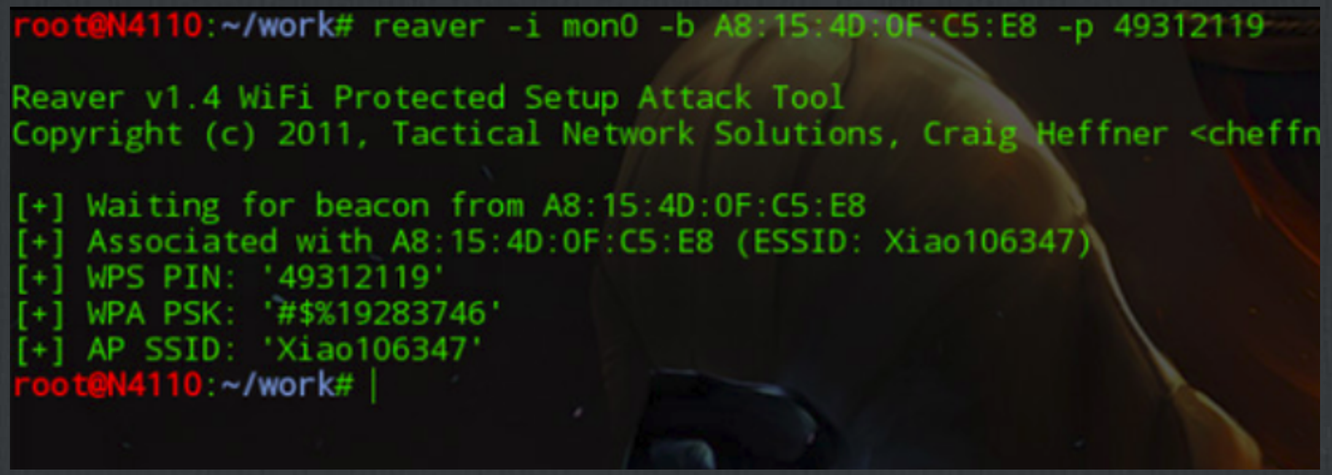
Push Button Mode

• Wi-Fi Protected Setup

PIN Mode

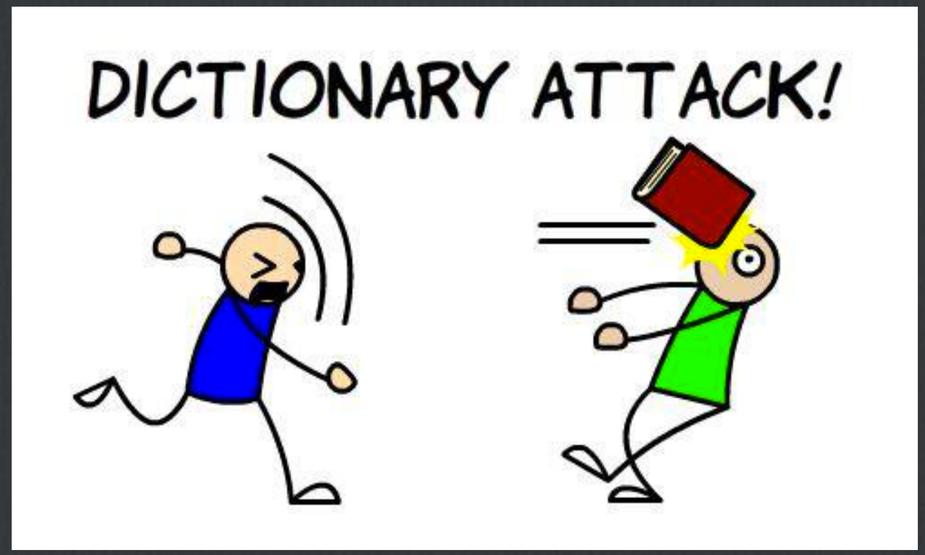
1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

10^4 + 10^3 = 11000



WPS Cracking with Reaver

- WPA/WPA2-PSK(Pre-shared Key)



- WPA/WPA2-Enterprise(802.1X)

EAP Support

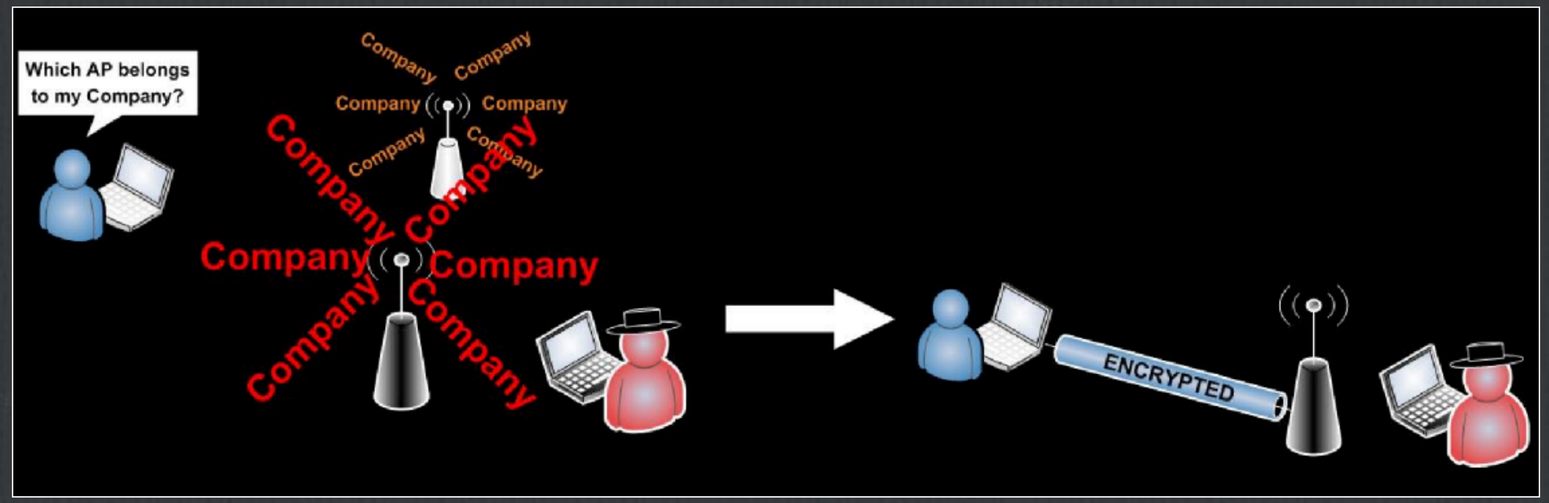
- Windows XP(sp3+)
  - EAP-TLS
  - PEAP
- Android/iOS
  - EAP-SIM
  - EAP-TLS
  - PEAP
  - LEAP
  - EAP-FAST
- ...

PEAP Weakness

- PEAP deploy with untrusted certificate.
- Users make the decision to trust/reject network.
- Anyone can impersonate the RADIUS server

□ PEAP Attacks(hostapd-wpe)

- Fake AP + RADIUS Server
- Always Return EAP-Success
- Logs authentication credentials (challenge/response,password, username
- Credential cracking with fixed challenge



- OPEN with Captive Portal

- [ ] Data unencrypted
- [ ] EvilTwin Attack
- [ ] Attack Portal Web Server
- [ ] MAC Spoofing

Intruder attack 10

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Time...	Length
1	2143201	200			803
6	2143206	200			803
8	2143208	200			803
10	2143210	200			803
11	2143211	200			803
12	2143212	200			803
17	2143217	200			803
20	2143220	200			803
30	2143230	200			803
0		200			814
2	2143202	200			814
3	2143203	200			814
4	2143204	200			814
5	2143205	200			814
7	2143207	200			814

Brute force with default password

```
POST
/eportal/userV2.do?method=login&param=true&wlanuserip=8dbc965aa8b5af8e9bfc5201f0724ac5&wlanacname=e5e4dd2e7ce
f91f40562d&ssid=ce4156ea91d975f8&nasip=5bc35637b5814111504c472c8452bd32&mac=a45454e08f6a8b11bffea8
v2&url=57c4ab3e008705d79aeffd6f798bd9c64bddbf1934486d64&username=2123[redacted]&pwd=2123[redacted] HTTP/1.1
```


User and Password in the request are not encrypted

Many portal service had remote-code execution vulnerabilities in the Struts 2

“WPA2 is Essential, But Not Enough”

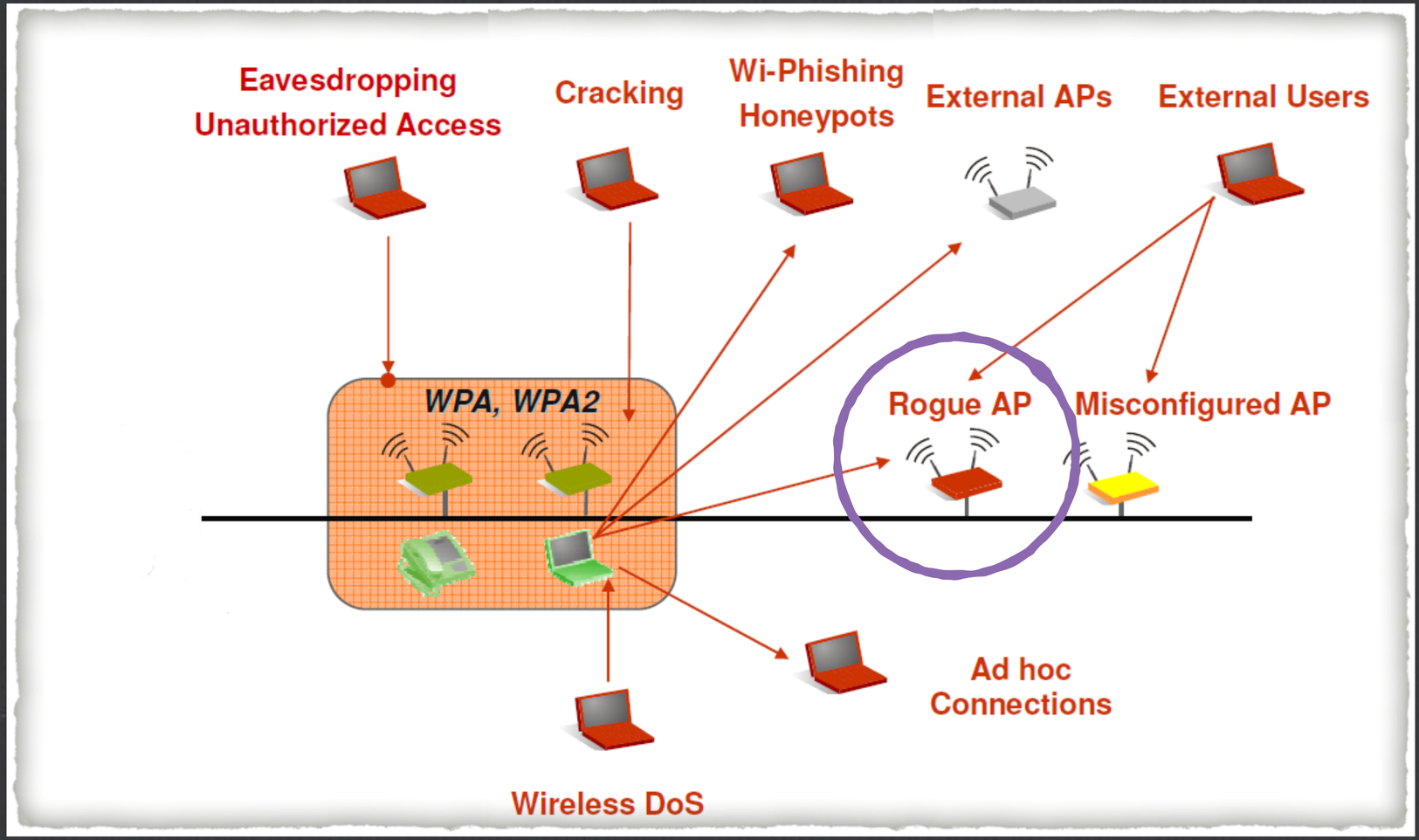


Image source: http://www.cs.ucf.edu/~czou/CNT4704-15/DSCI_Seminar.pdf

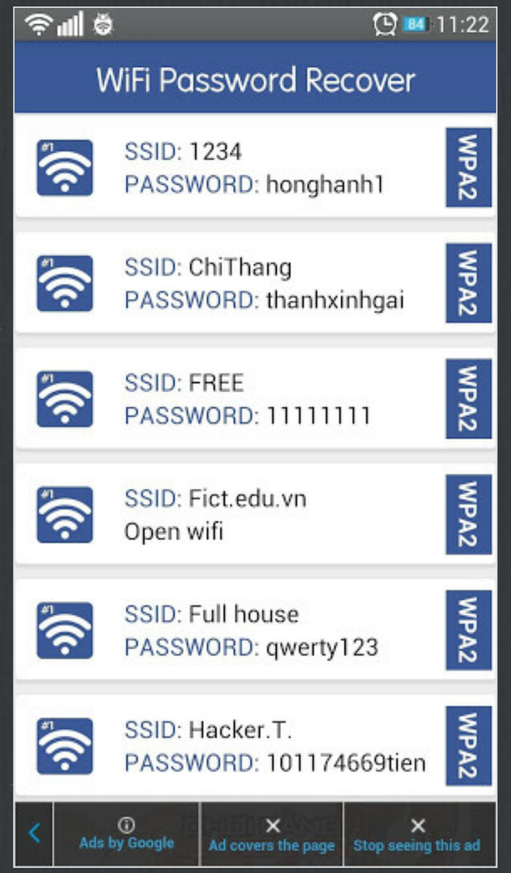
✳ Rogue AP

Unauthorized APs attached to enterprise network, installed with a wireless router or a USB Wi-Fi adapter.

May configured with poor security by naive users.

A supercomputer was invaded through a Rogue AP

Password Sharing APP



Wireless Intrusion Prevention System (WIPS)

- Three Components
  - Sensors — Scan for wireless packets
  - Server — Analyzes packets
  - Console — User interface

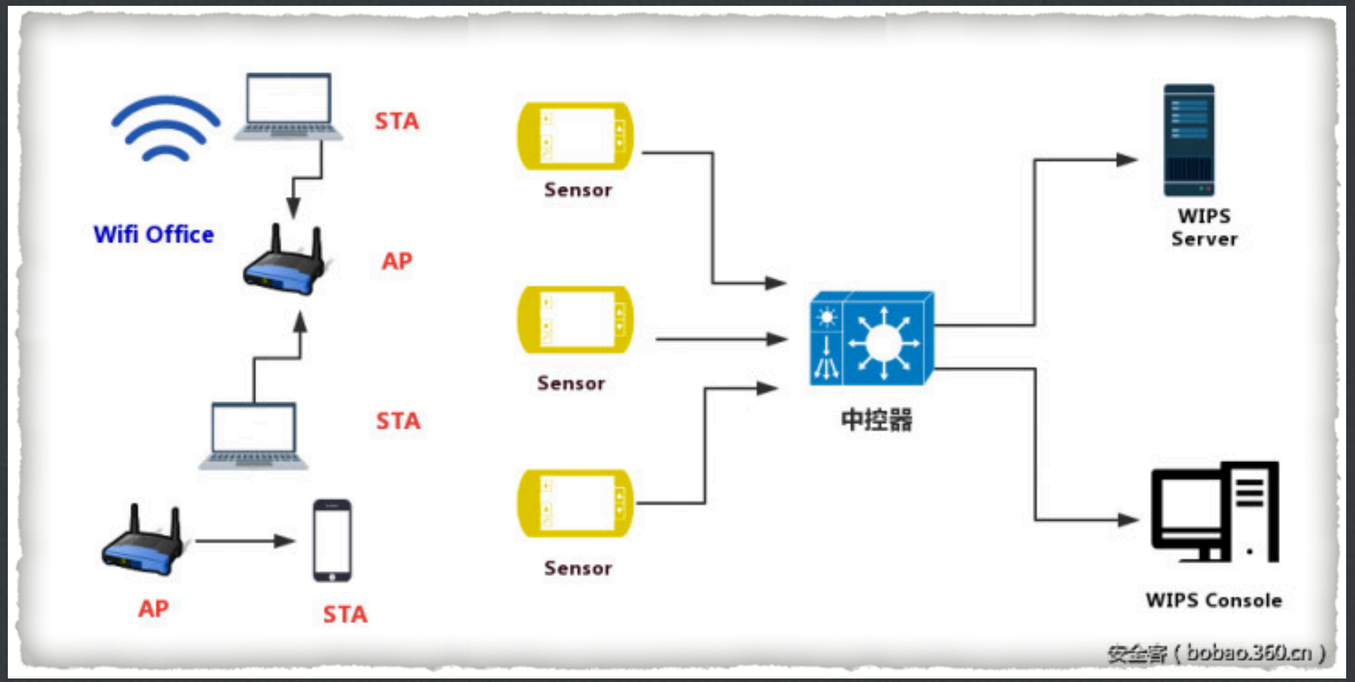


Image source: https://www.anquanke.com/post/id/85719

- Discover
  - Access Points (BSSID、ESSID、PWR、OUI)
  - Wireless Clients (MAC、PWR、OUI)

- Attack Identification
  - MAC Spoofing
  - Evil-Twin Attack
  - DoS Attack
    - ✳MDK3
    - ✳Aircrack-NG

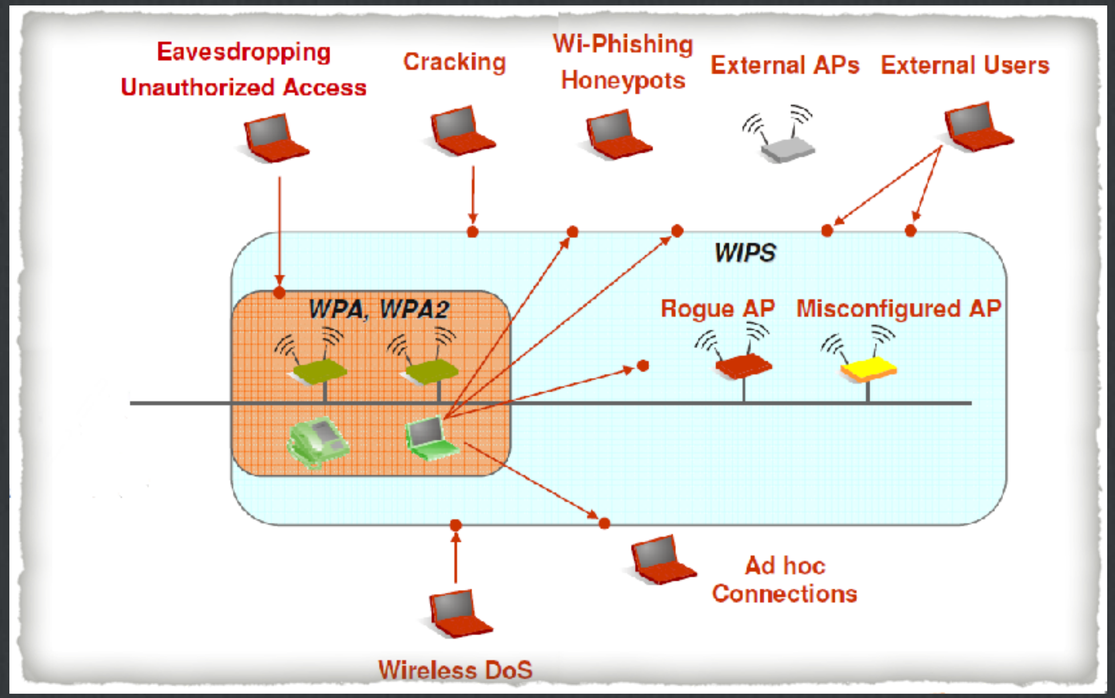
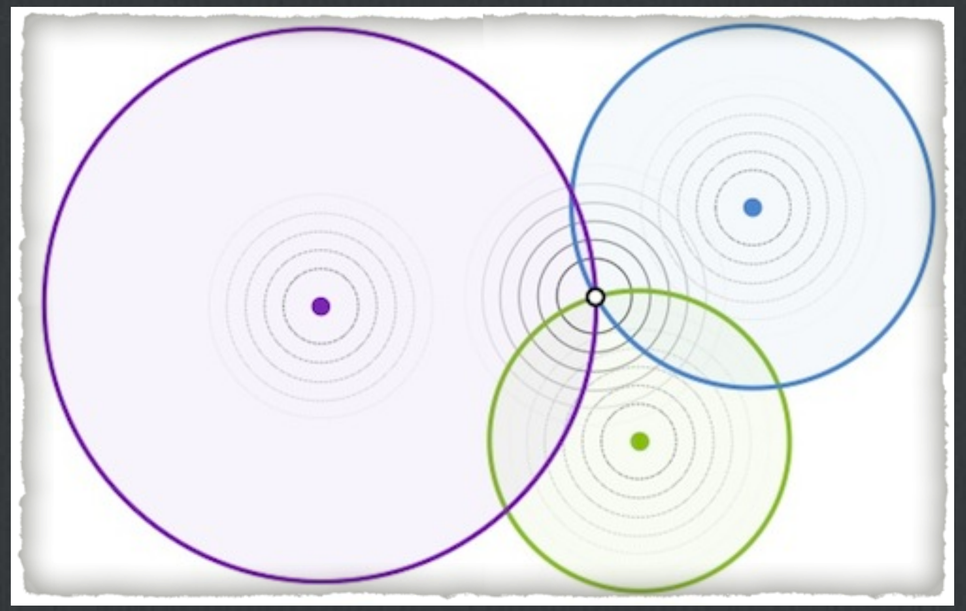


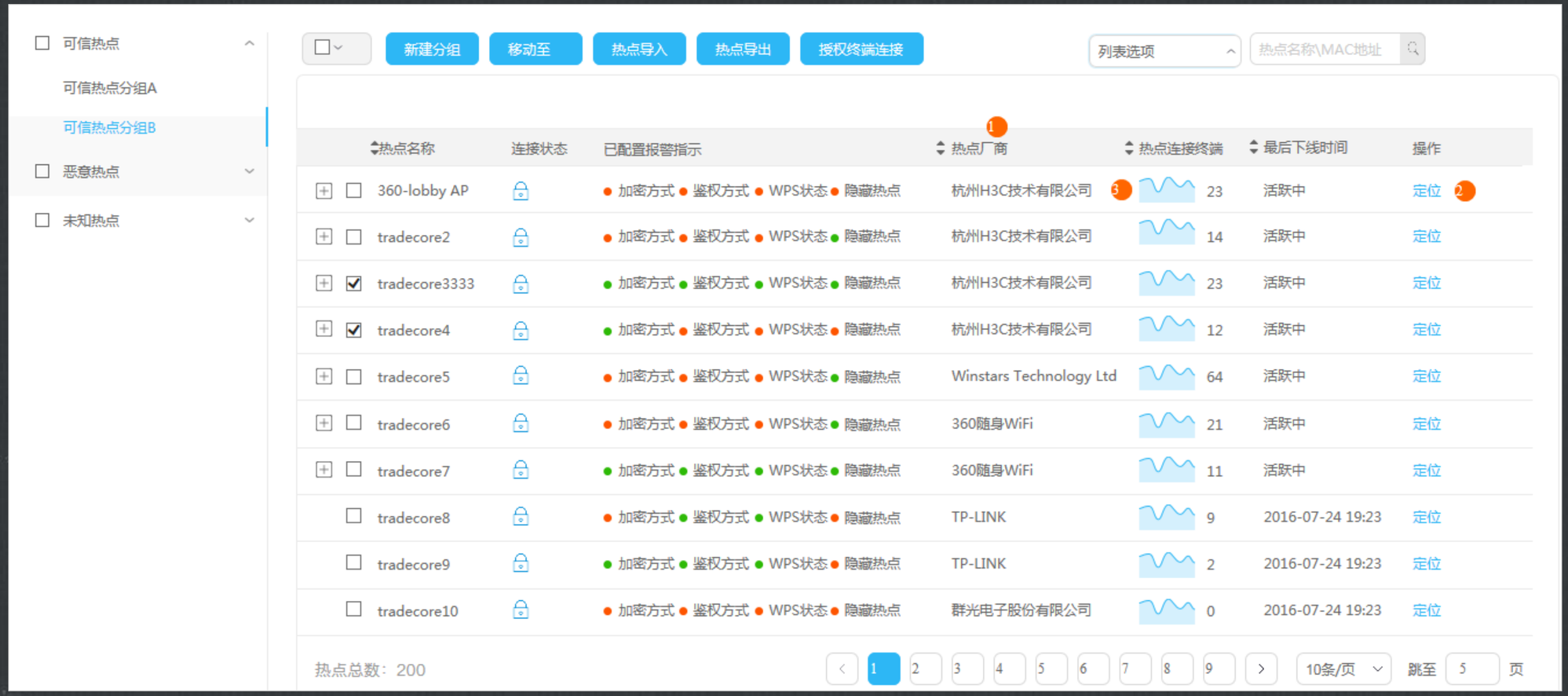
Image source: http://www.cs.ucf.edu/~czou/CNT4704-15/DSCI_Seminar.pdf

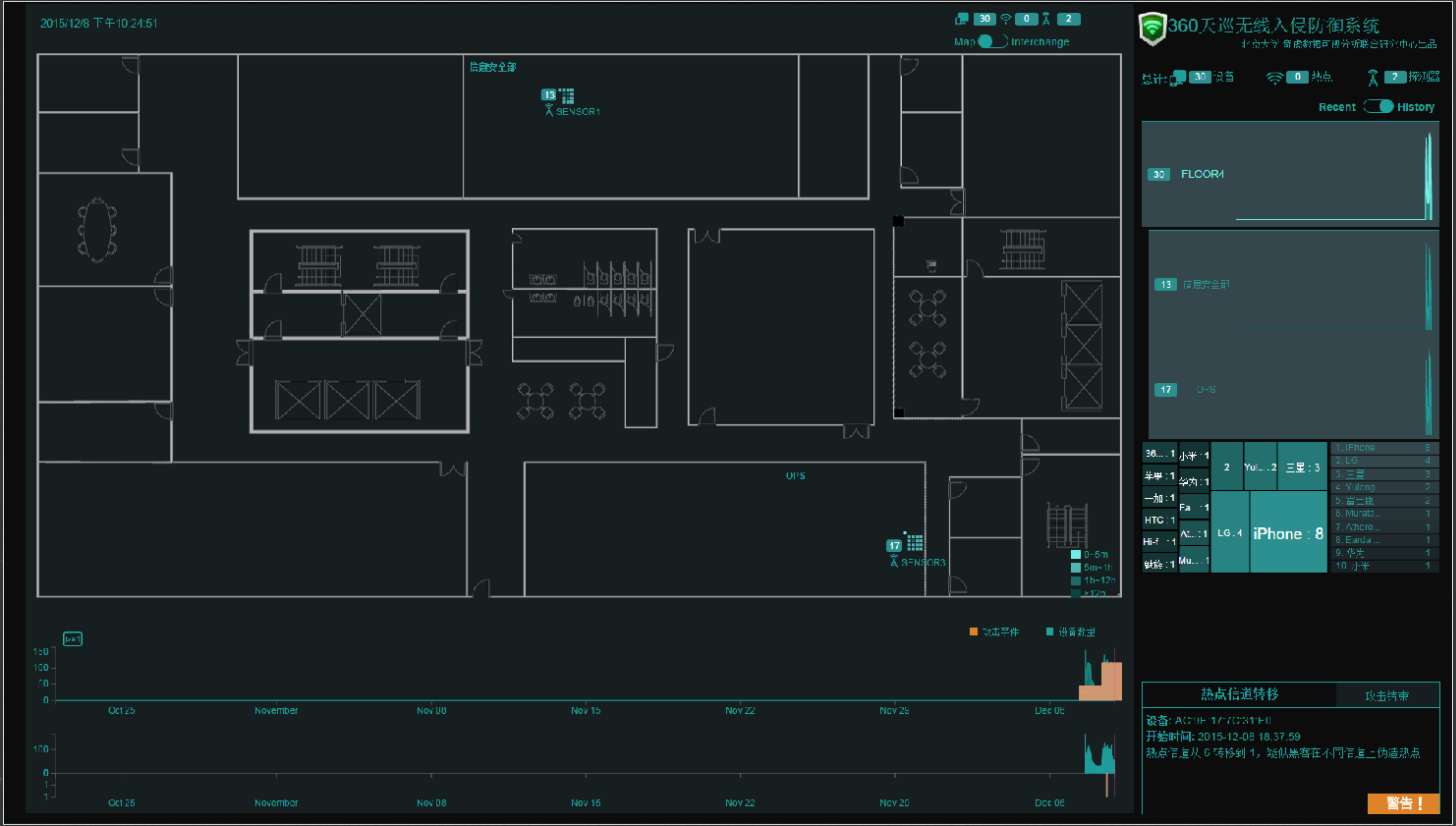
- Locate
  - APs
  - Clients
  - Attackers



- Block
  - Rogue AP Block
    - Blocked APs cannot work properly.
  - Client Block
    - Blocked clients are unable to connect with APs.

Dashboard


可信热点
可信热点分组A
可信热点分组B
恶意热点
未知热点
新建分组
移动至
热点导入
热点导出
授权终端连接
列表选项
热点名称\MAC地址
热点名称
连接状态
已配置报警指示
热点厂商
热点连接终端
最后下线时间
操作
360-lobby AP 加密方式 鉴权方式 WPS状态 隐藏热点 杭州H3C技术有限公司 23 活跃中 定位
tradecore2 加密方式 鉴权方式 WPS状态 隐藏热点 杭州H3C技术有限公司 14 活跃中 定位
tradecore3333 加密方式 鉴权方式 WPS状态 隐藏热点 杭州H3C技术有限公司 23 活跃中 定位
tradecore4 加密方式 鉴权方式 WPS状态 隐藏热点 杭州H3C技术有限公司 12 活跃中 定位
tradecore5 加密方式 鉴权方式 WPS状态 隐藏热点 Winstars Technology Ltd 64 活跃中 定位
tradecore6 加密方式 鉴权方式 WPS状态 隐藏热点 360随身WiFi 21 活跃中 定位
tradecore7 加密方式 鉴权方式 WPS状态 隐藏热点 360随身WiFi 11 活跃中 定位
tradecore8 加密方式 鉴权方式 WPS状态 隐藏热点 TP-LINK 9 2016-07-24 19:23 定位
tradecore9 加密方式 鉴权方式 WPS状态 隐藏热点 TP-LINK 2 2016-07-24 19:23 定位
tradecore10 加密方式 鉴权方式 WPS状态 隐藏热点 群光电子股份有限公司 0 2016-07-24 19:23 定位
热点总数：200
1 2 3 4 5 6 7 8 9
10条/页
跳至 5 页



2015/12/8 下午10:24:51
Map
Interchange
SENSOR1
OPS
SENSOR3
360天巡无线入侵防御系统
总计: 30 设备
0 热点
2 探测器
Recent
History
30 FLOOR4
13
17
iPhone : 8
LG : 4
1. iPhone
2. LG
热点信道转移
攻击结束
开始时间: 2015-12-08 18.37.59
警告！
Oct 25
November
Nov 08
Nov 15
Nov 22
Dec 06

WIPS Not Enough

When an attacker get a valid user credentials, the boundary is broken.

- ☐Who initiated the attack?
- ☐When?
- ☐What did he do?
- ☐What tools did he use?

Solutions must support：

- Real-time alarm
- Track attacker activity
- Attacker profiling
- Locating the attacker

Wireless Honeypot "Drosera"

Hackers are often attacking vulnerable wireless hotspots as a B**reakthrough**. Why not use a Wireless Honeypot?

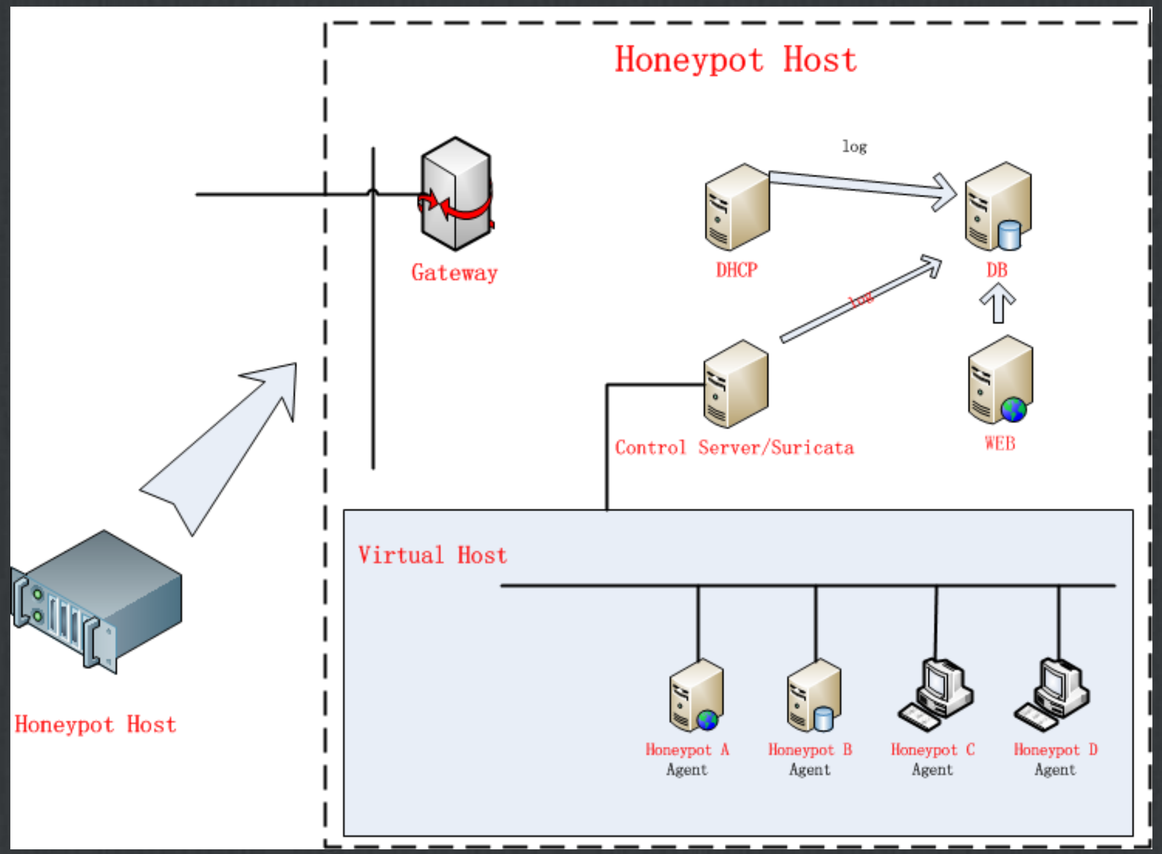
Get information about hacker：

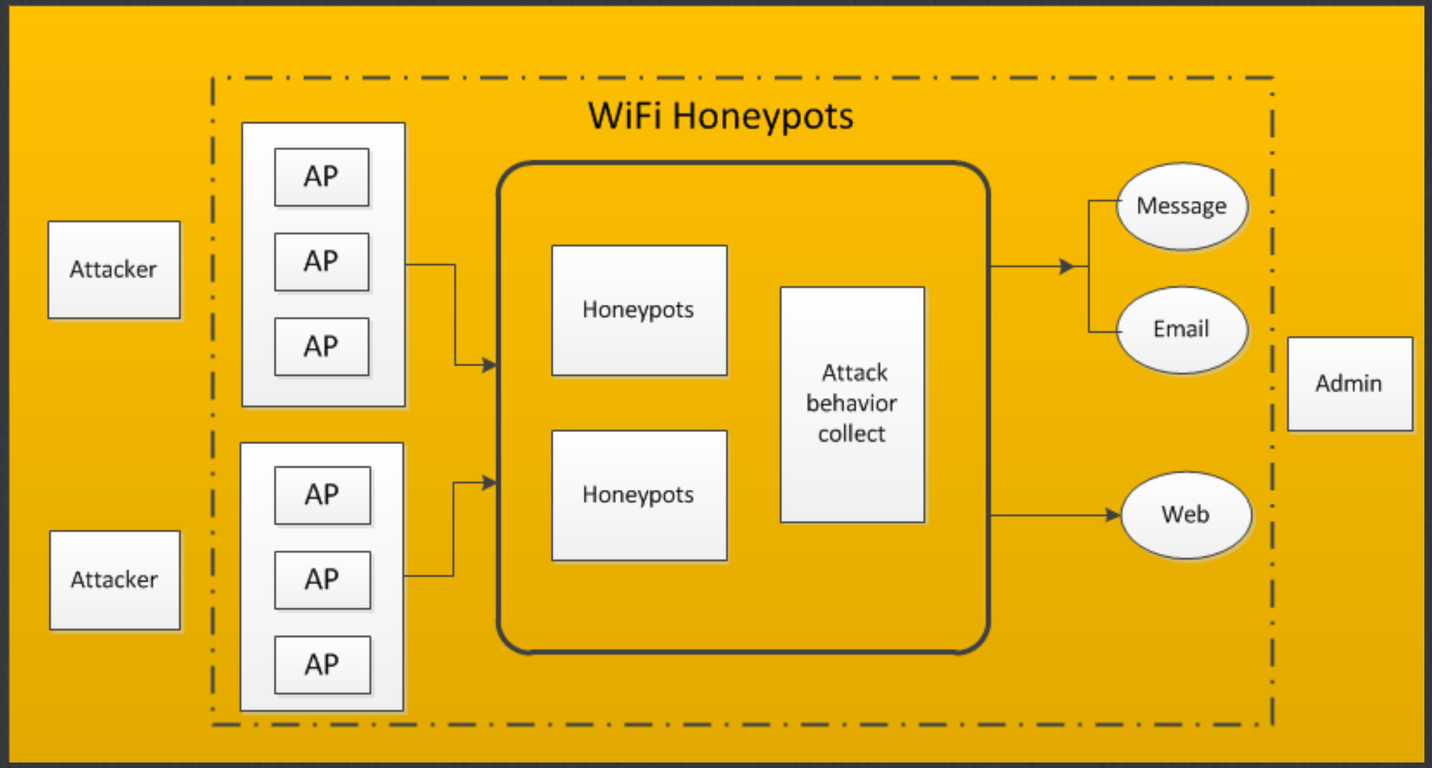
- Skill level
- Goals
- Methods
- Tools

Architecture of Honeypot Platform

- ☐ Gateway(DHCP, DNS)
- ☐ Honeypots based on virtualization technologies

- Network traffic inspection(Suricata)
- Data collection(ELK)
- Attack Alarm(Email, SMS)

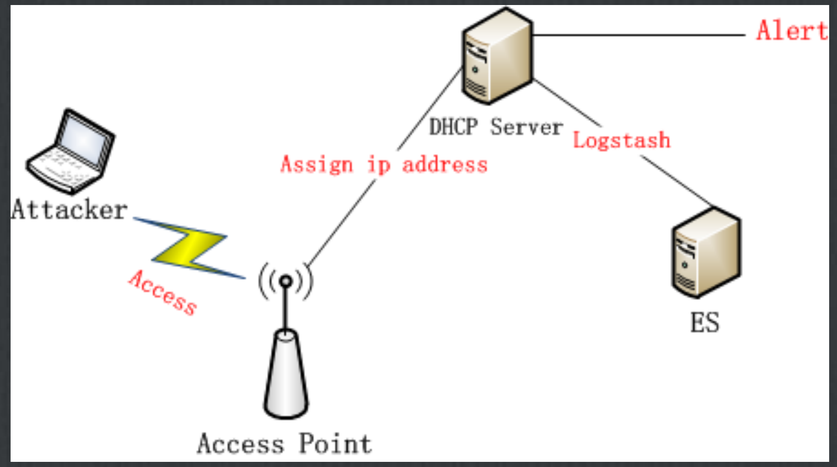




- Wireless Access Layer
- Network Layer
- Honeypots Layer

✳ Wireless Access Layer

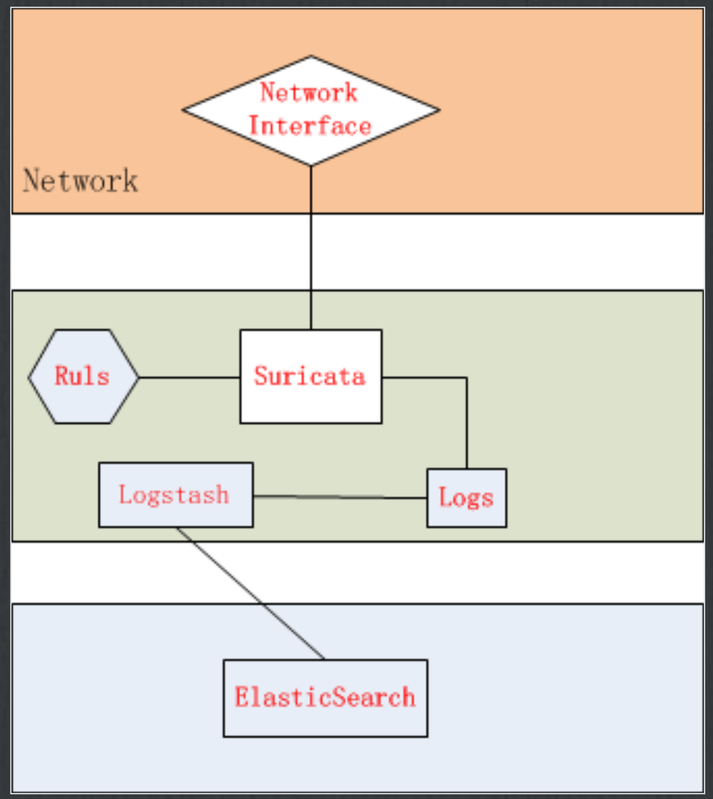
- ☐ **Set traps**
  - **Open**
  - **WEP**
  - **WPA with Weak Password**
  - **Password sharing APP**
- ☐ **Log connections**
  - **DHCP logs**
    - **hostname, IP address, MAC address**



Attack will be monitor once connect to the network

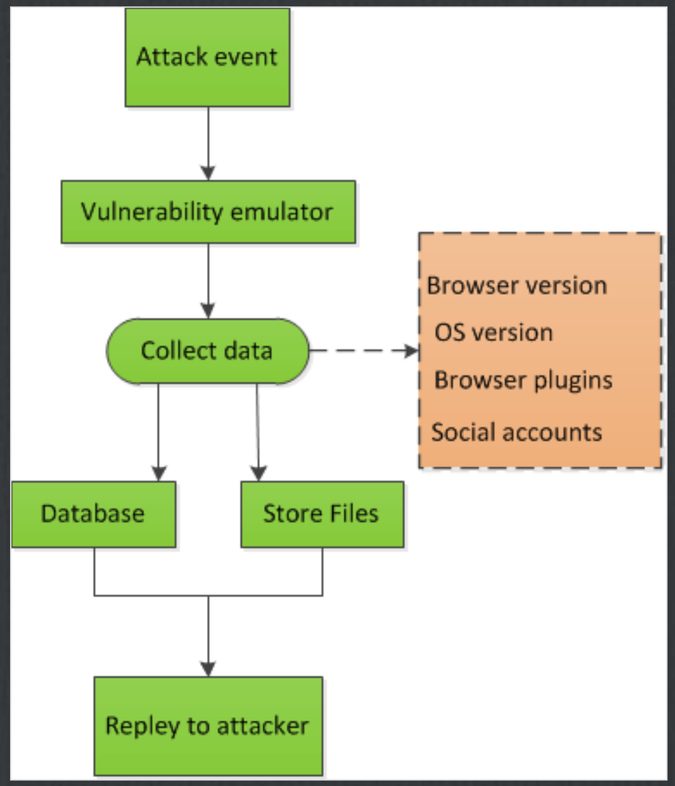
Network Layer

- Honeypots connected via Bridge mode
- Inspect network traffic(Suricata)
  - Scanning(Nmap, sqlmap, WVS)
  - Host Login Activity
  - Request to Services(SSH, Database, HTTP, ICMP)
- Alarm



✳ Honeypots Layer

- ☐ **Web Honeypot**
  - **Data Collection**
    - **User-Agent(OS, Browser)**
    - **Browser plugins**
    - **Social accounts(JSONP Hijacking)**
  - **Attacker profiling**
  - **Set vulnerabilities**
    - **get the access to the host**



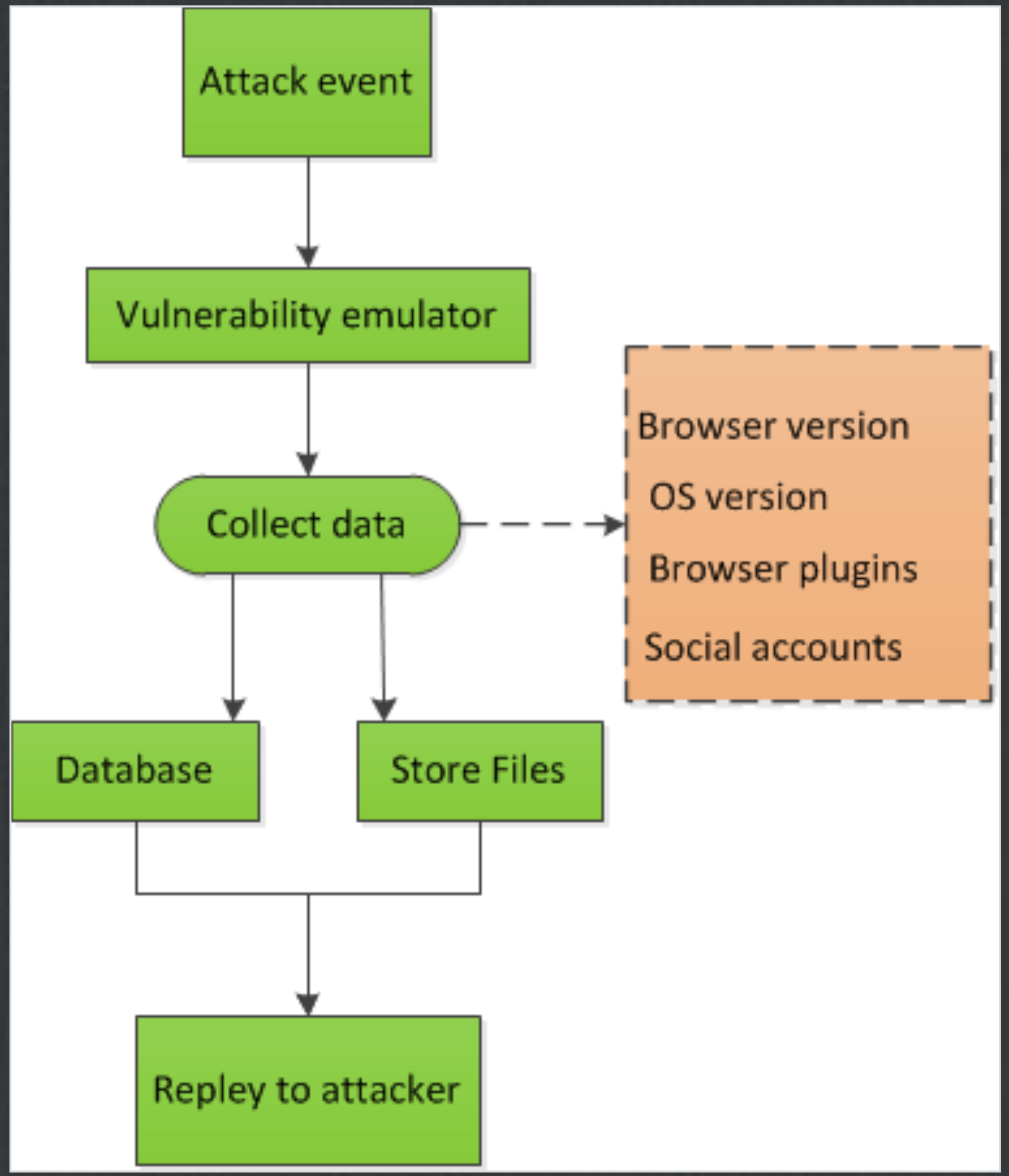
- JSONP
  - make cross-domain JavaScript requests that bypass the same-origin policy
  - lead to information leakage

Website	Global Rank	Rank in China	Information leaked
baidu.com	5	1	username
taobao.com	9	2	MemberId, Nickname, Mobile Phone Number, LoginId
qq.com	10	3	UserId
sina.com.cn	13	4	UserId
sohu.com	34	8	Nickname, PassportID (mail service)
360.cn	54	9	Profile name, profile ID
tianya.cn	65	11	UserId
163.com	75	18	UserId
youku.com	92	19	Username UserId
jd.com	94	20	UserId
alipay.com	96	22	MemberId, Nickname, Mobile Phone Number, LoginId
ifeng.com	197	32	Username, UserId
gome.com.cn	350	73	LoginName, LoginID
58.com	492	87	Username, email, userid, nickname
suning.com	925	134	UserId
ctrip.com	1153	167	UserId, Phone number
renren.com	727	177	UserId, Real Name, Username, birthday, sex
qunar.com	1501	196	Userid, NickName

✺ Honeypots Layer

☐ Web Honeypot

- Data Collection
  - User-Agent(OS, Browser)
  - Browser plugins
  - Social accounts(Jsonp hijacking)
- Attacker profiling
- Set vulnerabilities
  - get the access to the host



☐ High-interaction honeypots

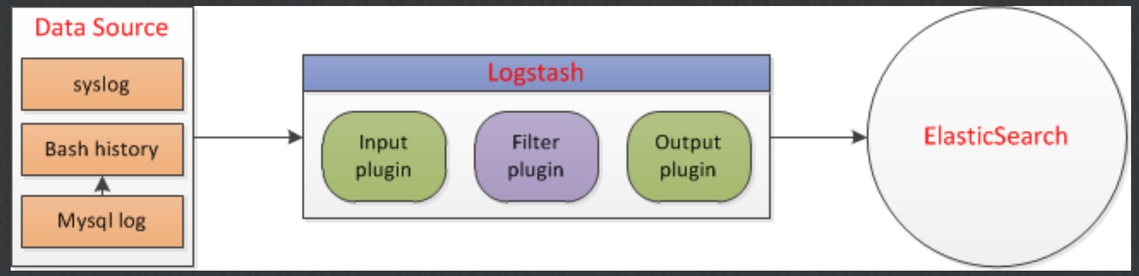
- Attack Alarm
- Monitor activities

Windows:

- Monitor Files, Process, Registry, Services
- Capture samples and analysis with Sandbox(Cuckoo).

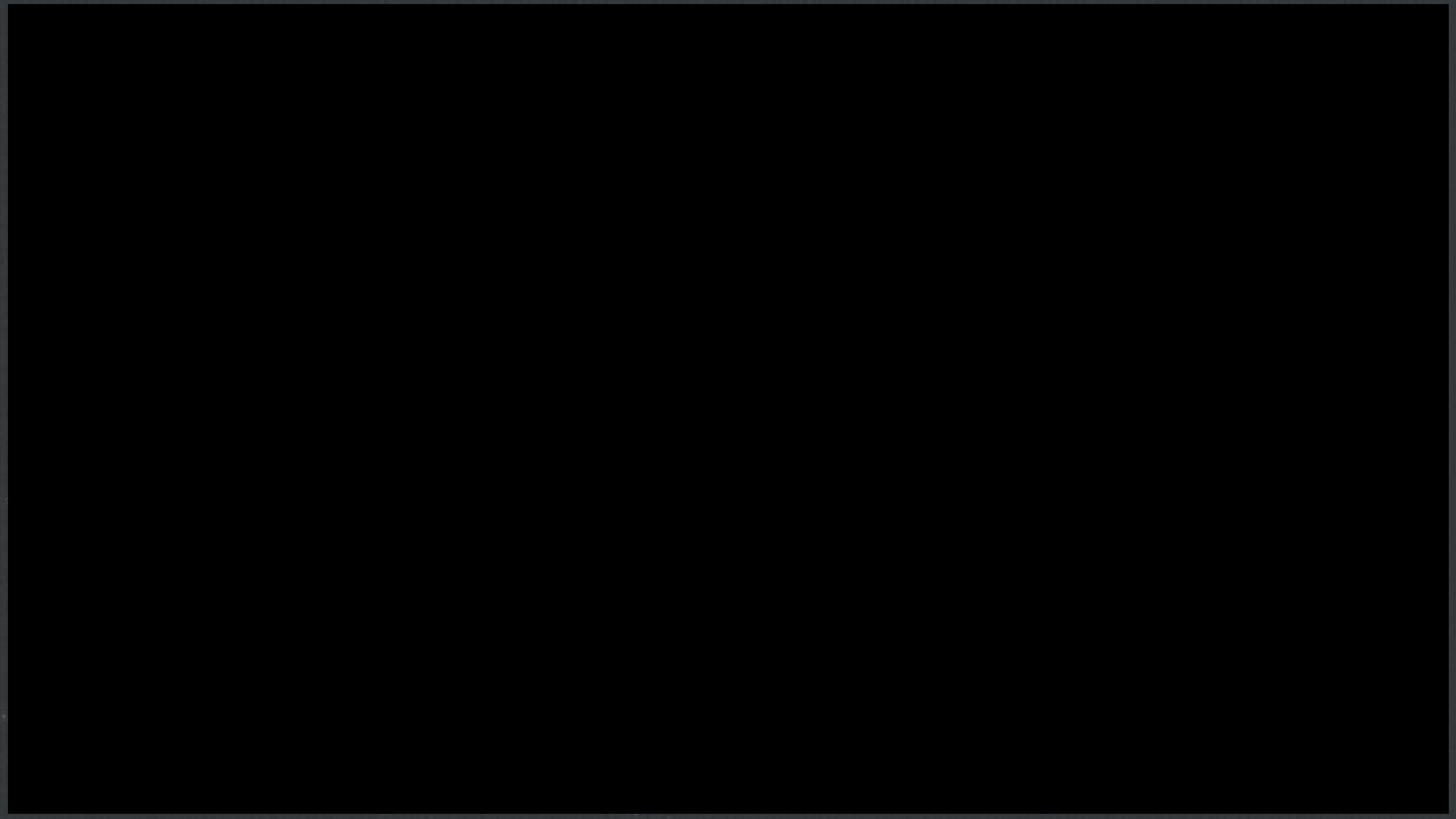
Linux:

- Bash history
- Services Log: Mysql, SSH, Apache
- Monitor sensitive Files and Directories



- Hide virtual machine fingerprint features
- Timing recovery

Windows honeypot Demo



Collaborative Defense

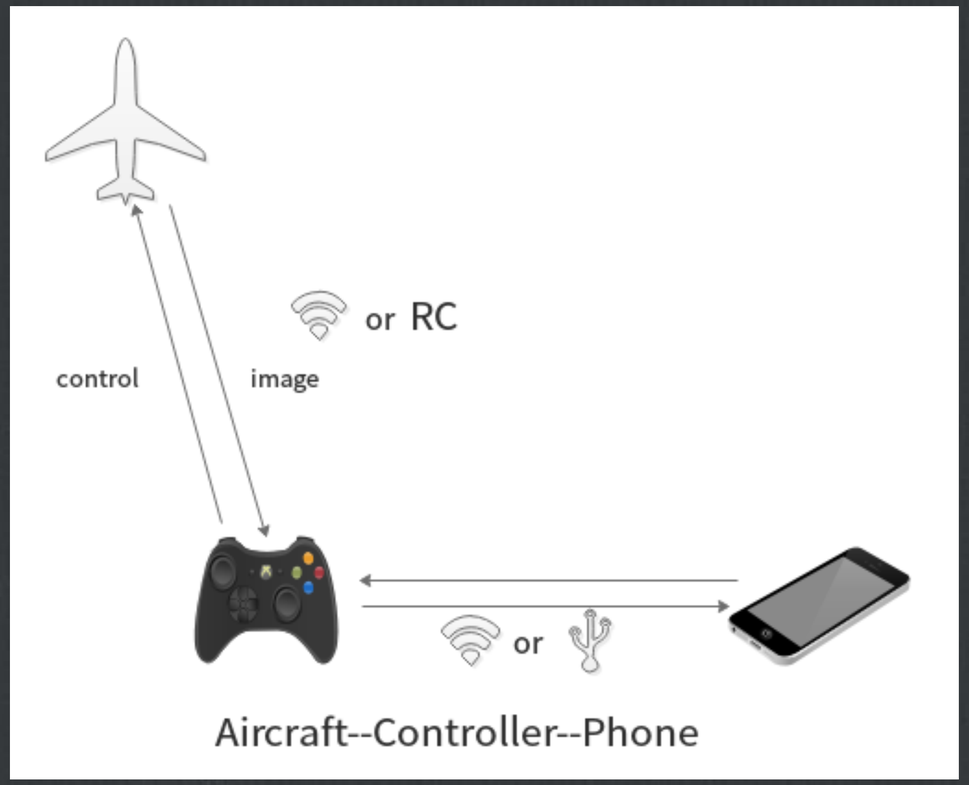
The combination of WIPS and honeypot can be very effective to detect and prevent wireless attack.

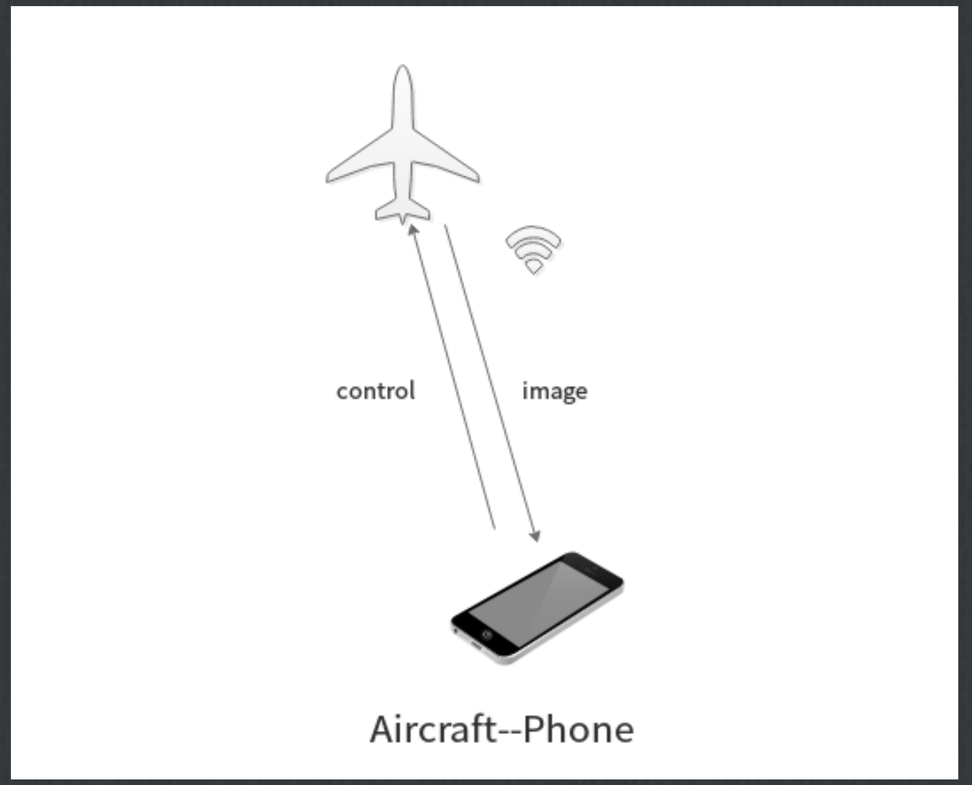
- Forensic analysis
  - Who
  - When
  - How
- Emergency processing
  - Stop attacking(block the device)
  - Locate the attacker

- WIPS & Wireless Honeypot
- Wireless Security Workflow
- Blocking Rogue AP
- Waiting for attackers

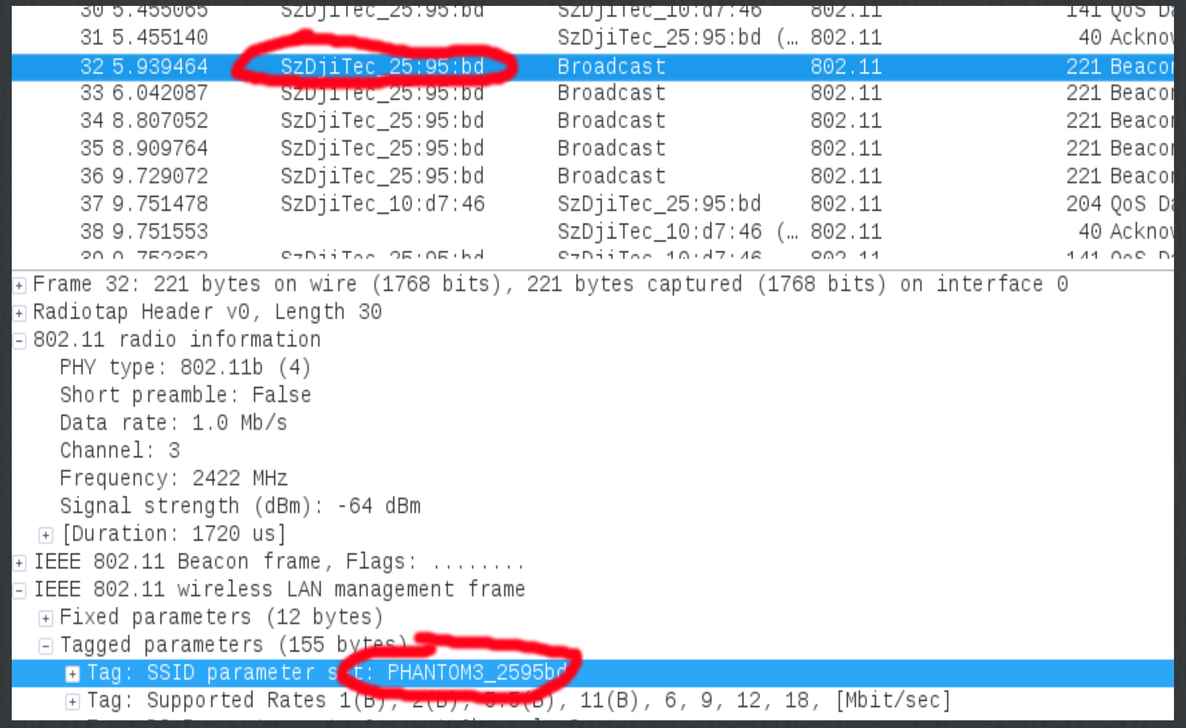
Others

1. Drone detector





Consumer-grade drones mostly use Wi-Fi to transmit control, picture between aircraft and cellphones.

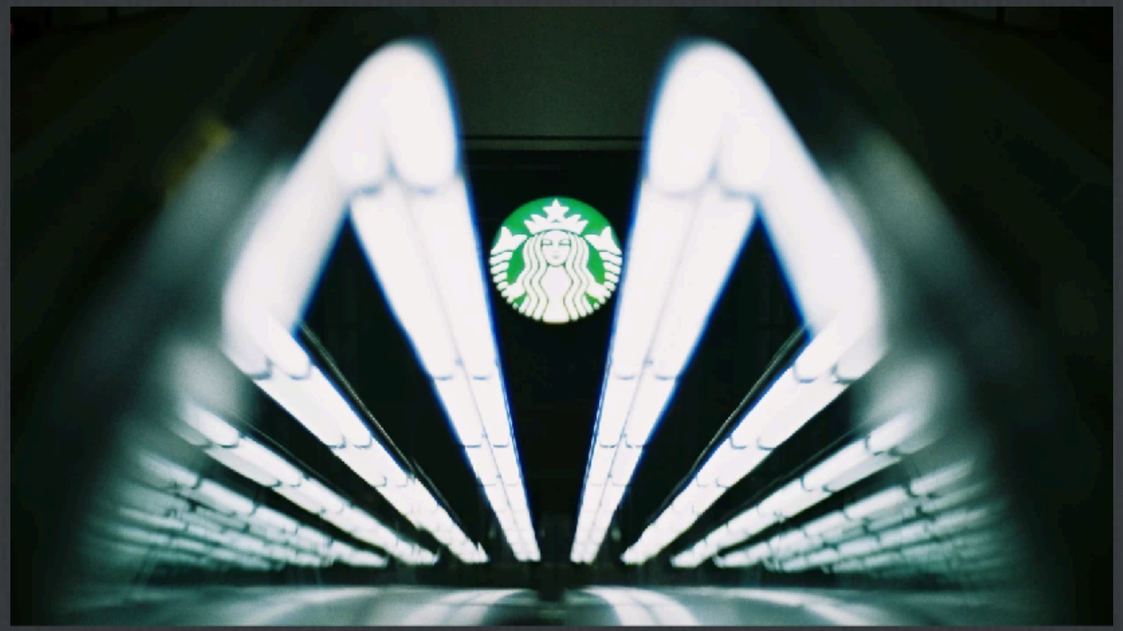


802.1 Beacon frame from drone's AP

OUI	SSID	Drone Model
60:60:1f	PHANTOM3_xxxxxx	PHANTOM3
60:60:1f	Mavic-xxxxxx	MAVIC
e4:12:18	XPLORER_xxxxxx	XPLORER
	KONGYING-xxxxxx	KONGYING
	MiRC-xxxxxx	XiaoMi

OUI, SSID and Drone Model Mapping Table

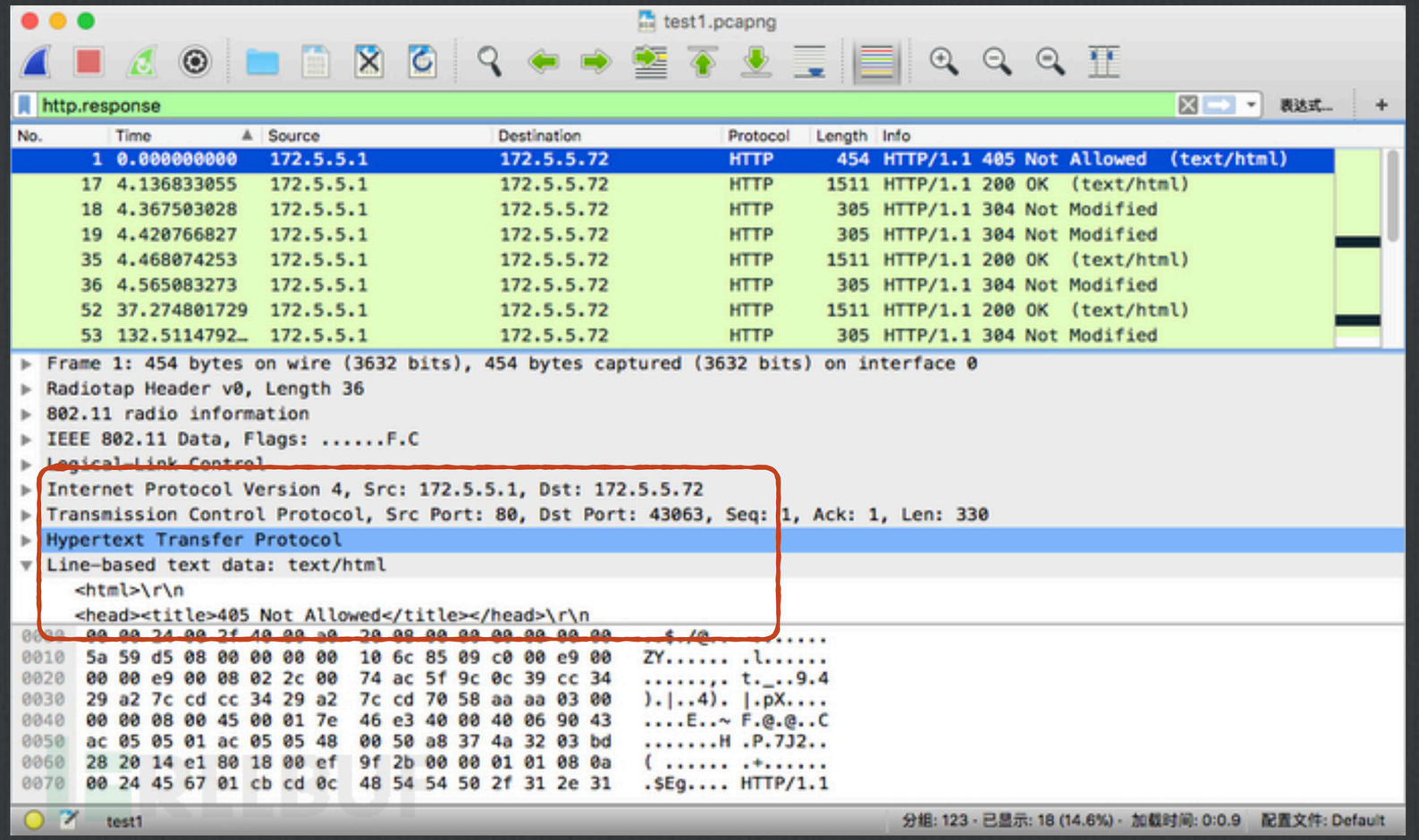
2. Wi-Fi Miner Detector



A tool for detecting Wi-Fi miner.

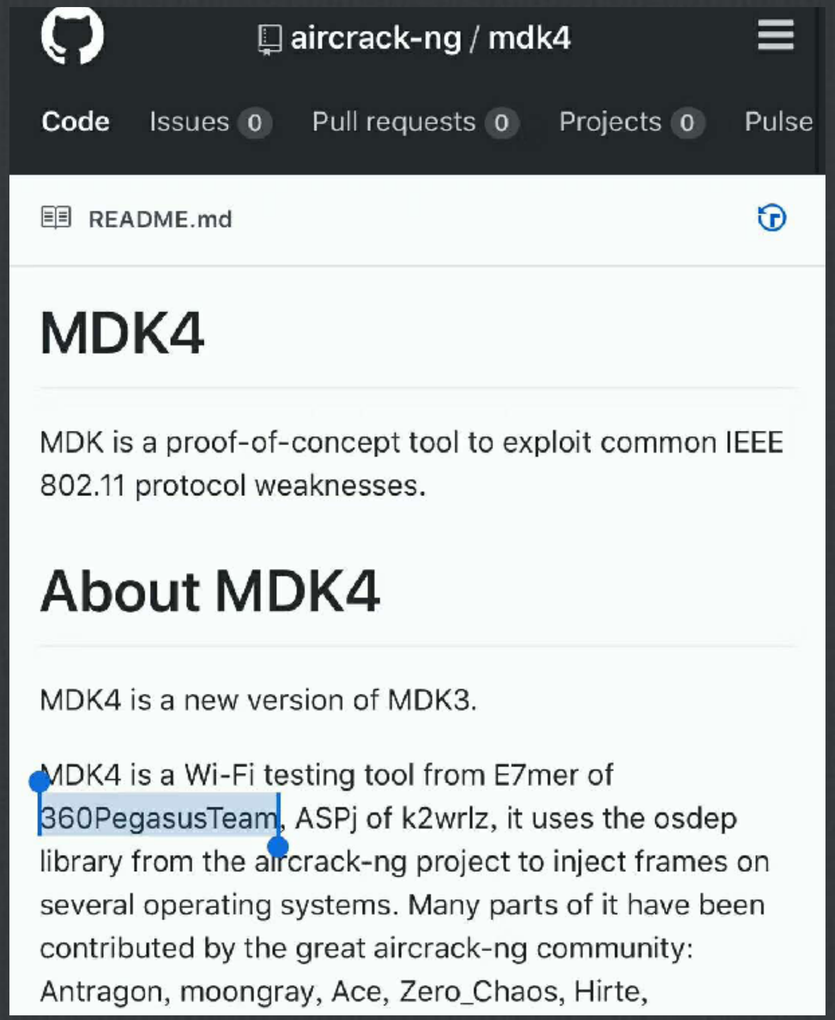
It is based on analyzing the unencrypted 802.11 Data Frame to detect mining keywords in HTTP data.

"Starbucks Wi-Fi Hijacked People's Laptops to Mine Cryptocurrency"



No connection is needed

3. MDK4



New features:

- ☐ support both 2.4Ghz and 5Ghz
- ☐ support blocking special devices in command options
- ☐ support packets fuzzing
- ☐ ...

https://github.com/aircrack-ng/mdk4

Thanks

@qingxp9