

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.

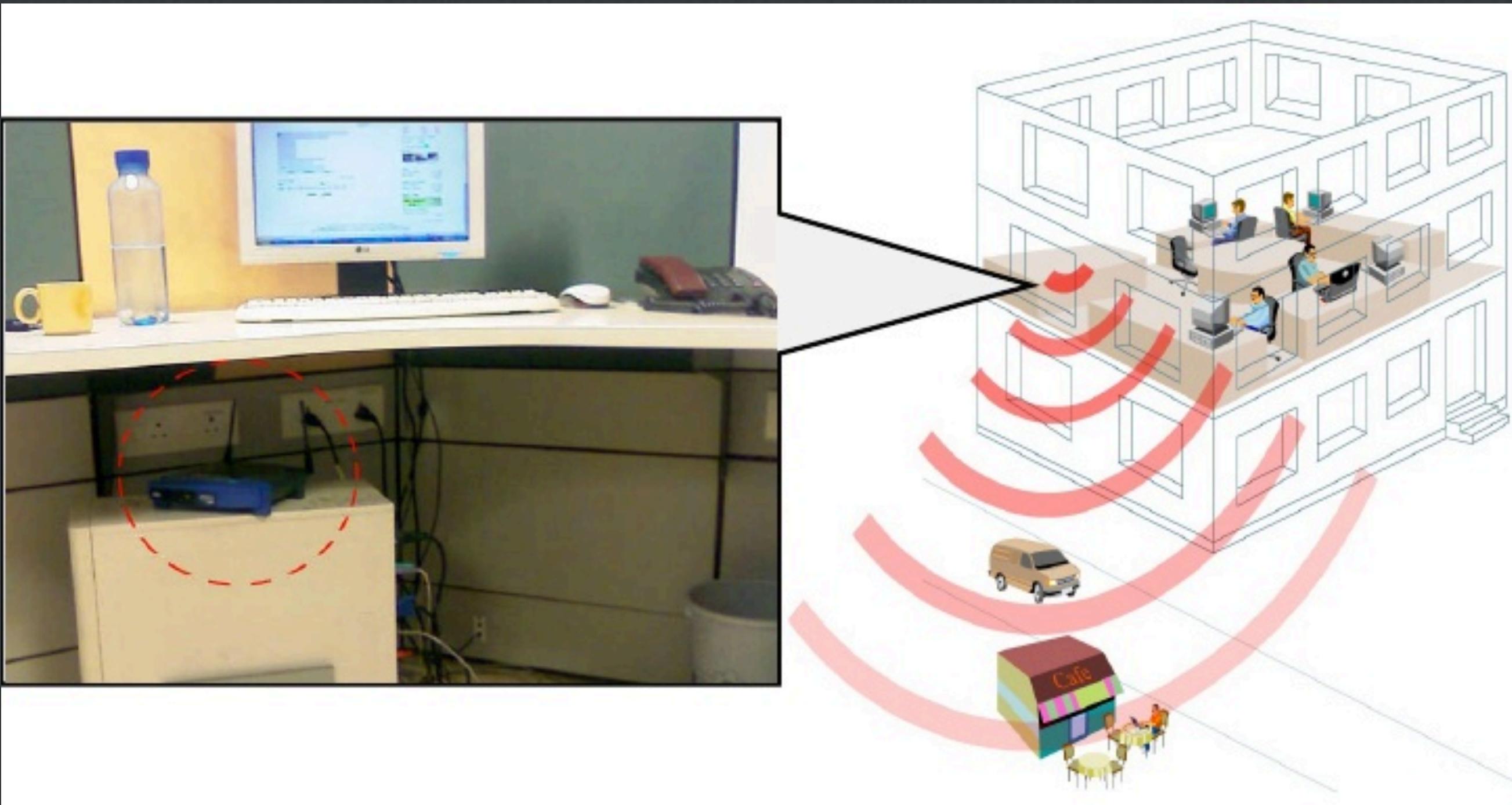


Image source: <https://pt.slideshare.net/MdSohailAhmad/rogue-ap>

* 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

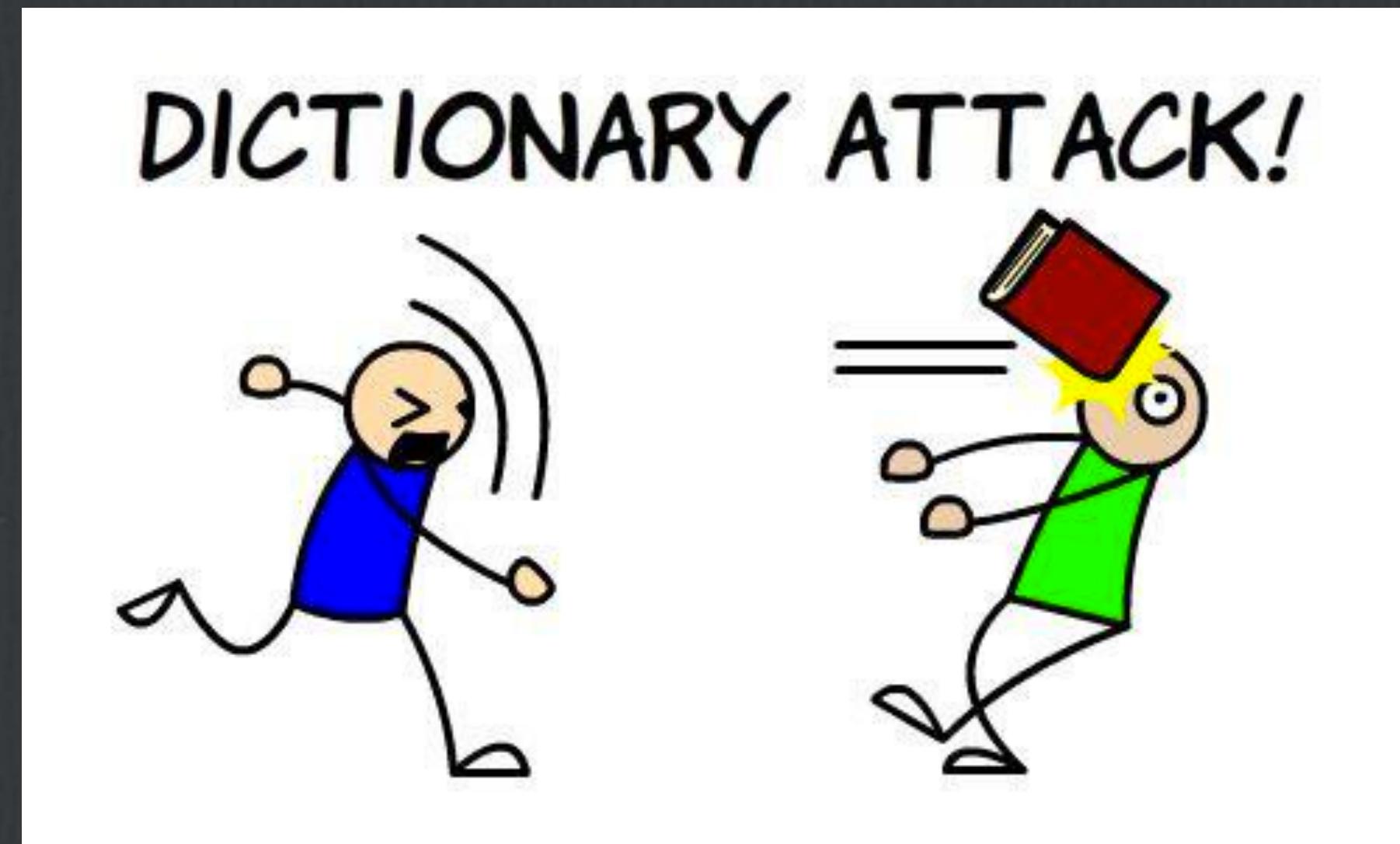
1	2	3	4	5	6	7	0
1 st half of PIN				checksum 2 nd half of PIN			

$$10^4 + 10^3 = 11000$$

```
root@N4110:~/work# reaver -i mon0 -b A8:15:4D:0F:C5:E8 -p 49312119
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffn
[+] Waiting for beacon from A8:15:4D:0F:C5:E8
[+] Associated with A8:15:4D:0F:C5:E8 (ESSID: Xiao106347)
[+] WPS PIN: '49312119'
[+] WPA PSK: '#$%19283746'
[+] AP SSID: 'Xiao106347'
root@N4110:~/work# |
```

WPS Cracking with Reaver

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



跑包 握手CAP专业跑包不成功不收费先跑后拍，不收电费 1小时出

转卖价: ￥7.00 [我要评价](#)

成色: 非全新
所在地: 广东东莞
联系方式: 叶先生/女士 1359*** 查看完整手机号
[和卖家联系](#)

交易方式: 在线交易
至 河北秦皇岛 ➔ 快递+免运费

[立即购买](#)

分享 (0) 收藏并订阅宝贝 (0)

cap 握手包 快速处理
先跑后拍 全网最低
不收电费，不出免费

- WPA/WPA2-Enterprise(802.1X)

- EAP Support

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

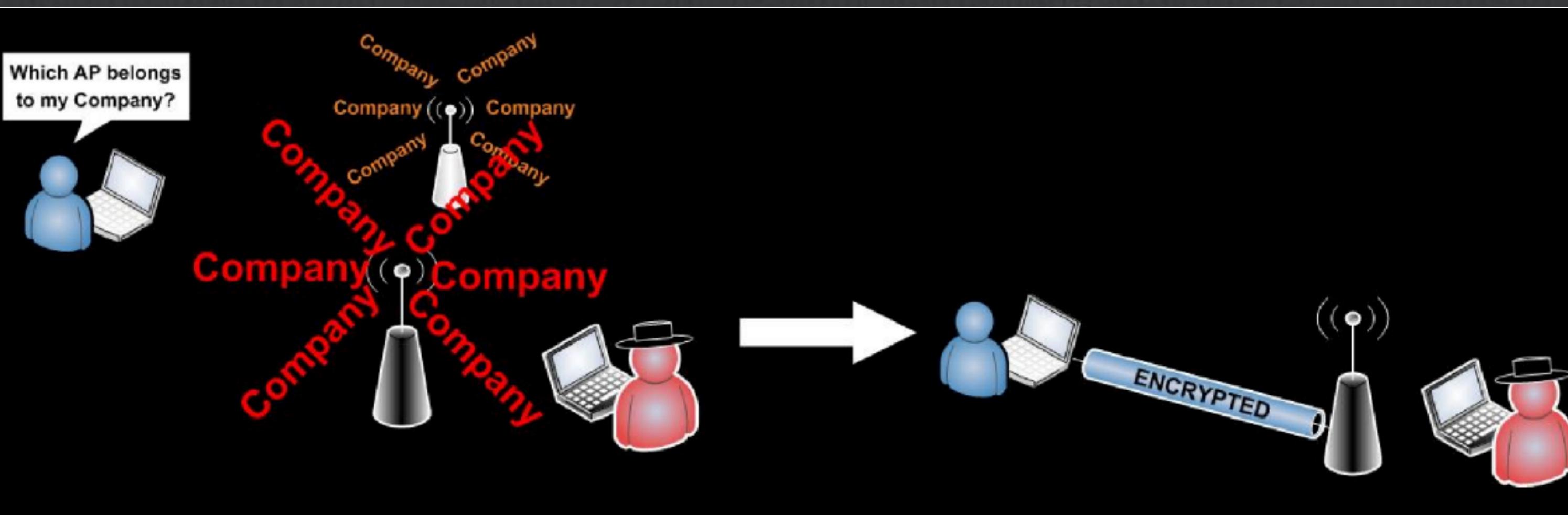
- PEAP Weakness

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



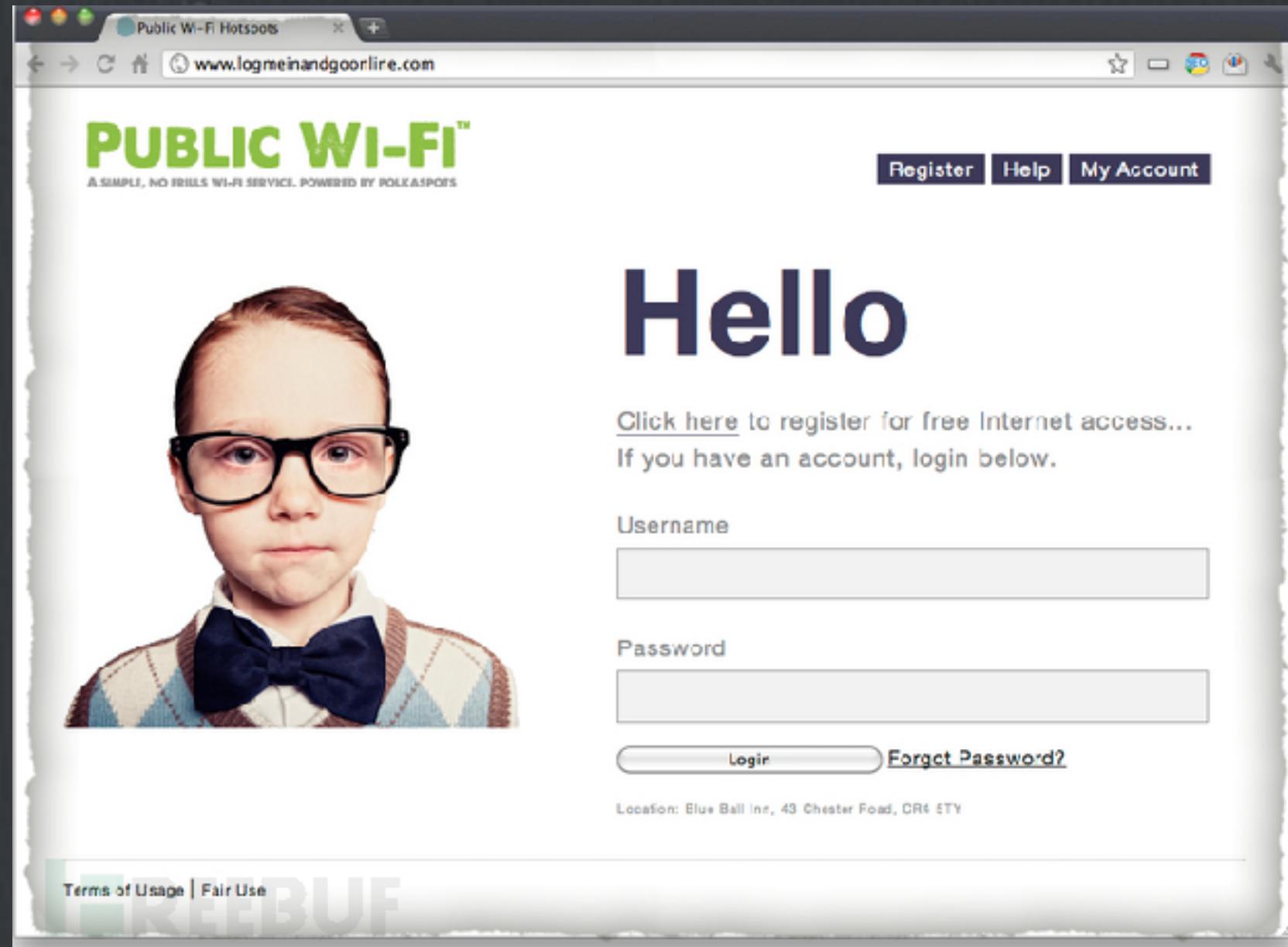
PEAP Attacks(hostapd-wpe)

- 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



校园网
Campus Network

校园网

发现校园网的"无线"精彩

连接网络

用户名	*
密码	*
<input type="checkbox"/> 记住密码	<input type="checkbox"/> 自动登录

连接

补天平台

Intruder attack 10

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

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

Brute force with default password

```
POST  
/eportal/userV2.do?method=login&param=true&wlanuserip=8dbc965aa8b5af8e9bfc5201f0724ac5&wlanacname=e5e4dd2e7ce  
f91f40562d&ssid=ce4156ea91d975f8&nasip=5bc35637b5814111504c472c8452bd32&mac=a45454e08f6a8b11bffa8:007c1ad86&  
v2&url=57c4ab3e008705d79aeffd6f798bd9c64bddbf1934486d64&username=2123 &pwd=2123 HTTP/1.1
```

补天平台

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”

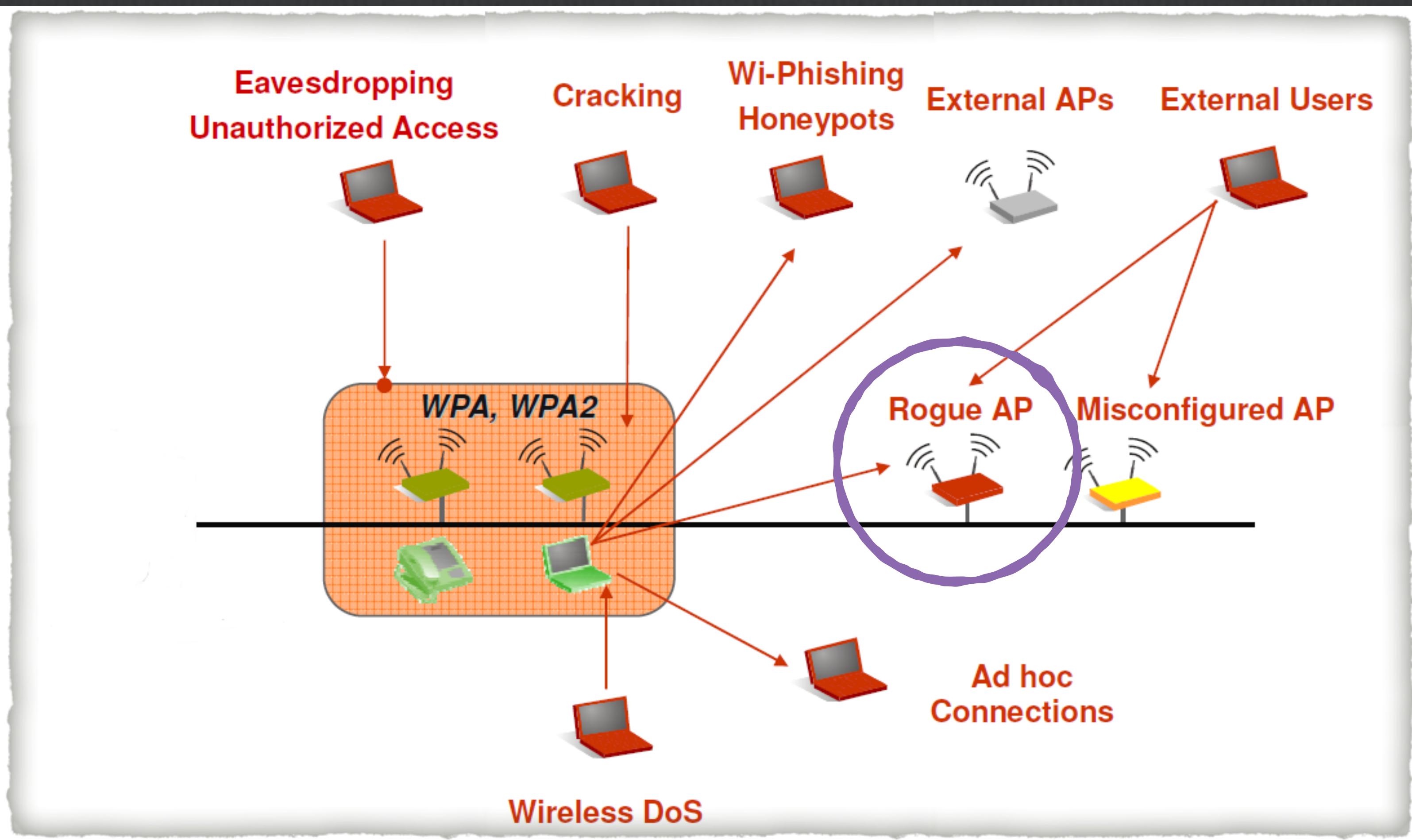


Image source: http://www.cs.ucf.edu/~czou/CNT4704-15/DSCI_Seminar.pdf

* Rogue AP

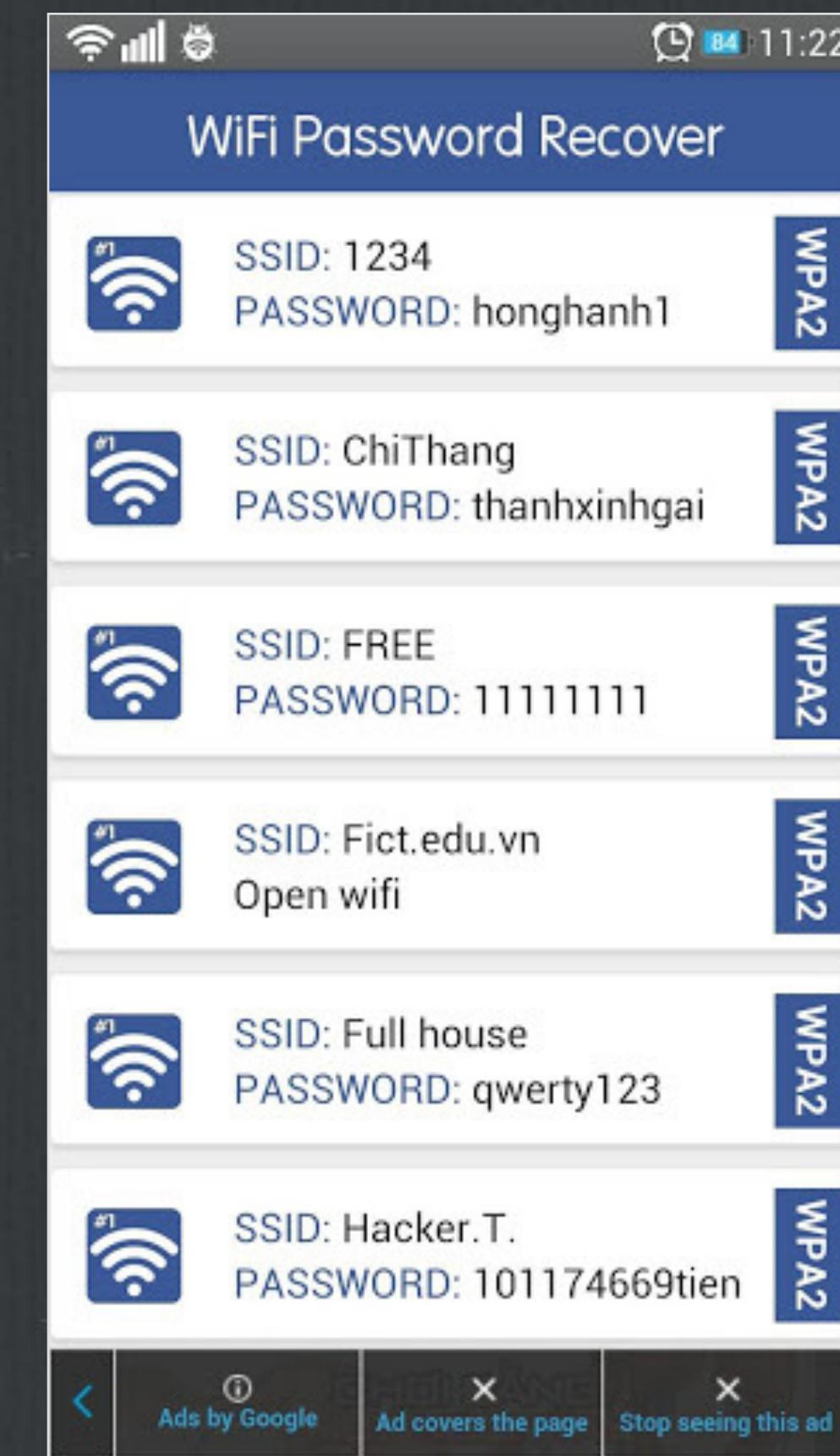
Unauthorized APs attached to enterprise network, installed with a wireless router or a USB Wi-Fi adapter.

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

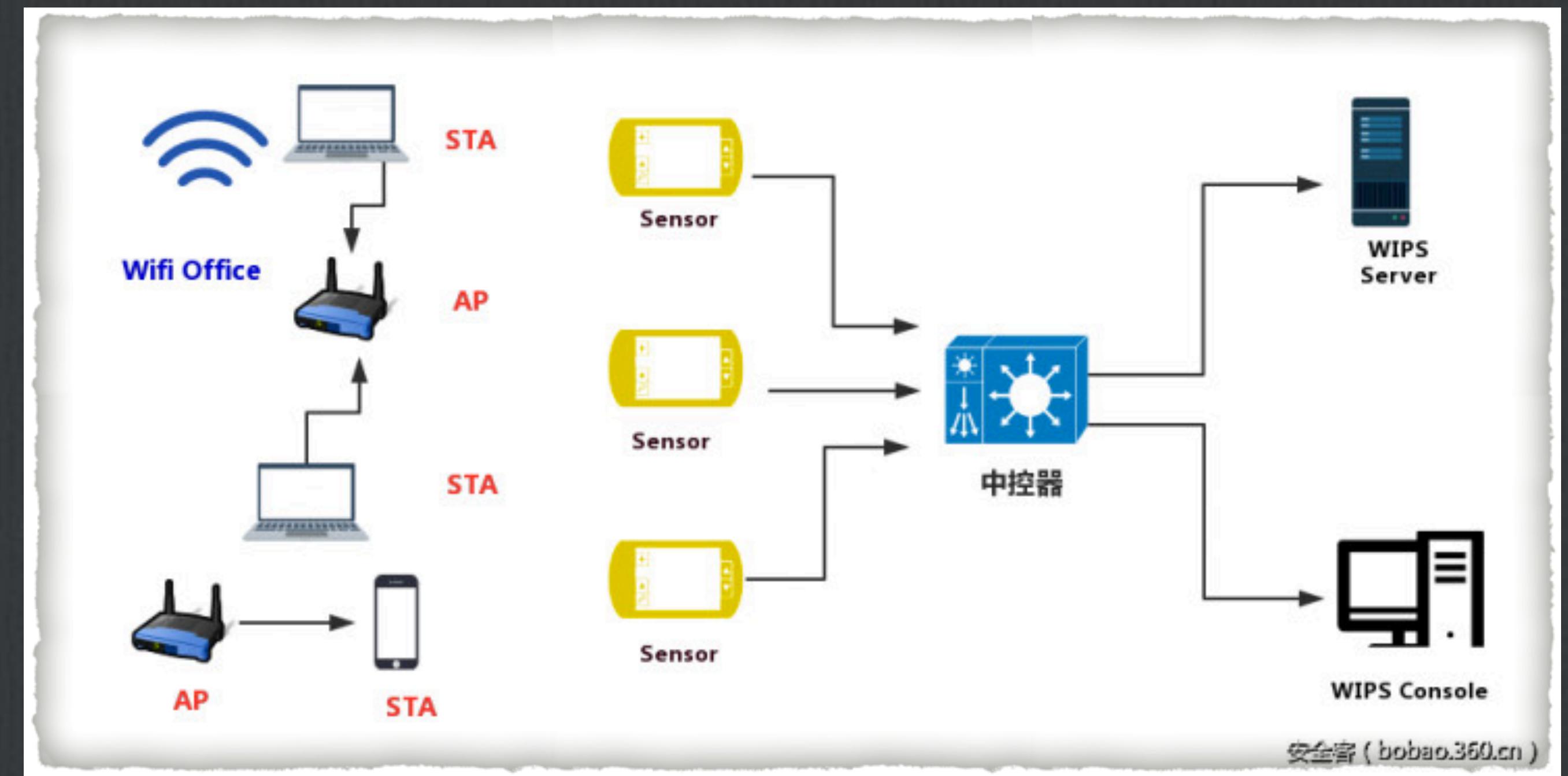


Image source: <https://www.anquanke.com/post/id/85719>

□ Discover

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

□ Attack Identification

- MAC Spoofing
- Evil-Twin Attack
- DoS Attack

*MDK3

*Aircrack-NG

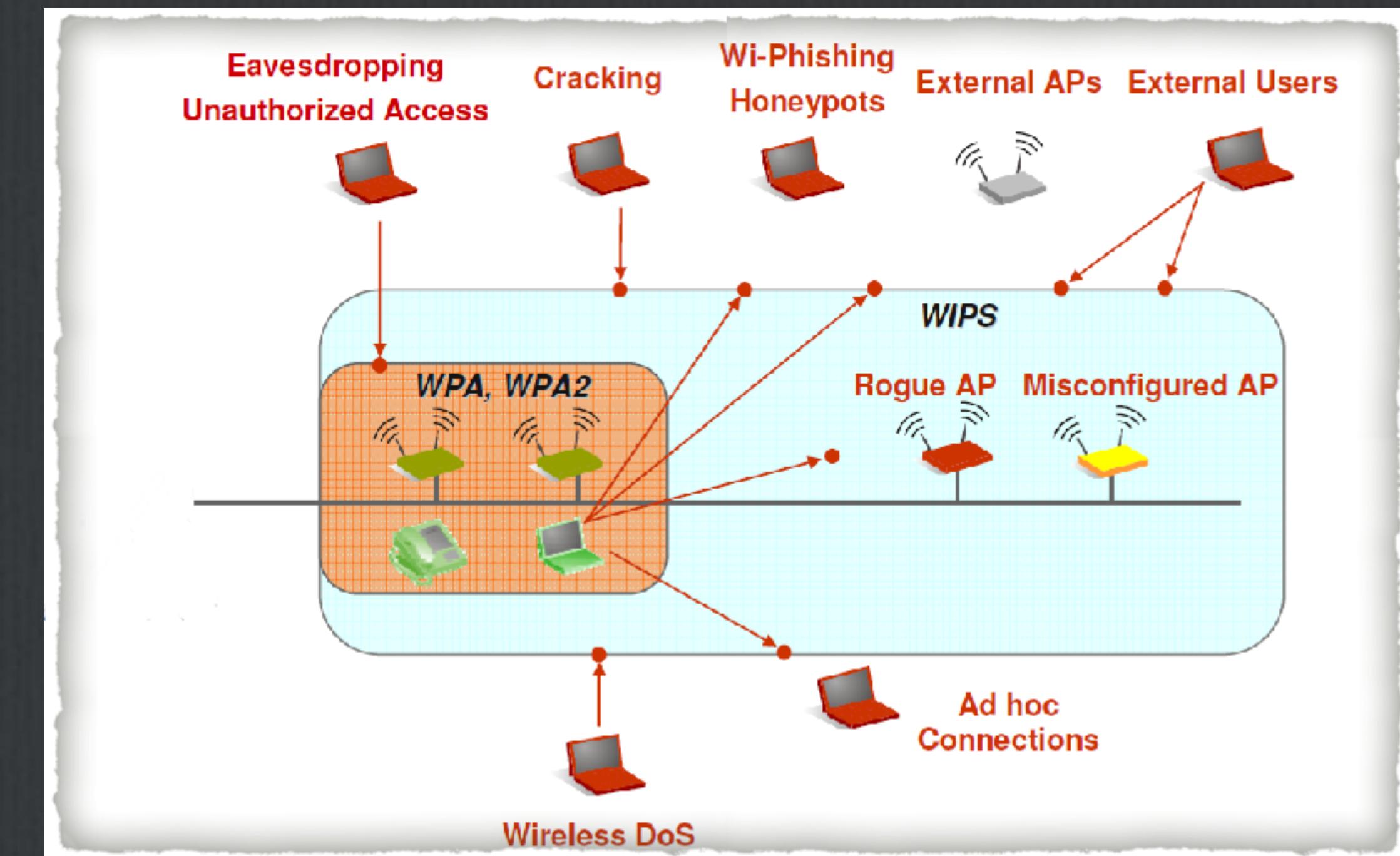


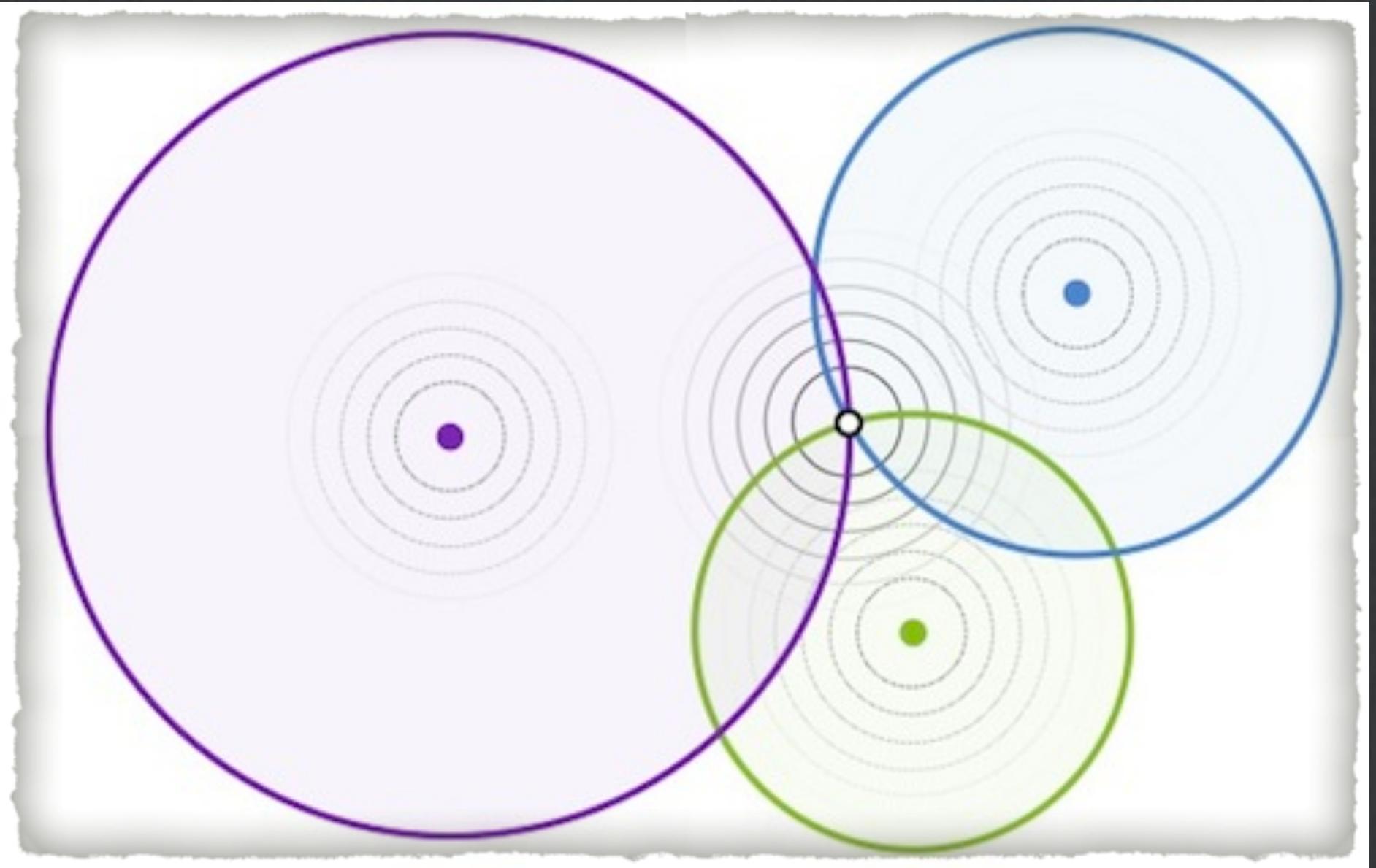
Image source: http://www.cs.ucf.edu/~czou/CNT4704-15/DSCI_Seminar.pdf

❑ 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 □ 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

可信热点分组B

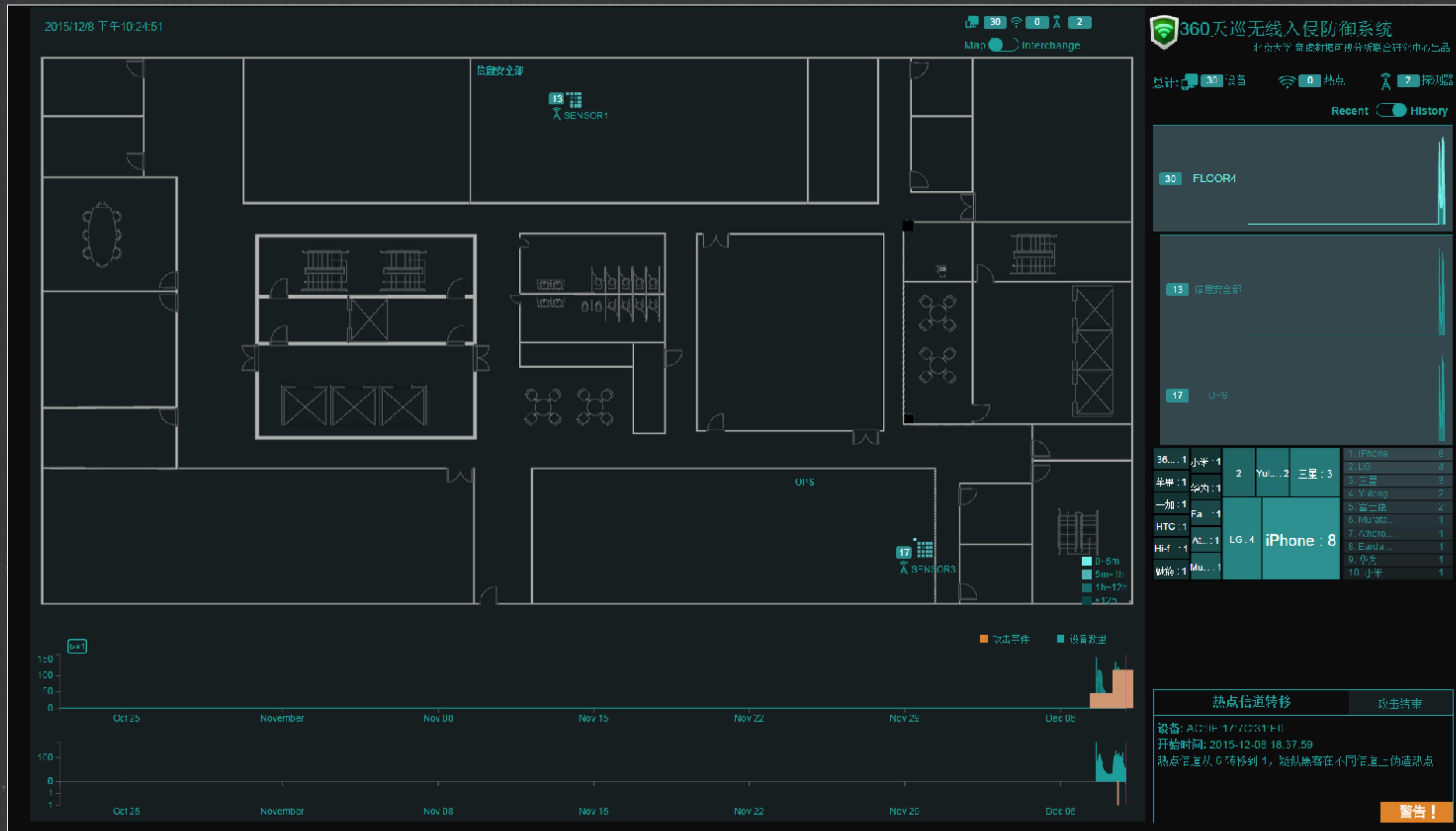
□ 恶意热点

□ 未知热点

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	锁定	● 加密方式 ● 鉴权方式 ● WPS状态 ● 隐藏热点	杭州H3C技术有限公司	3	23	活跃中 定位 2
tradecore2	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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	锁定	● 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



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"

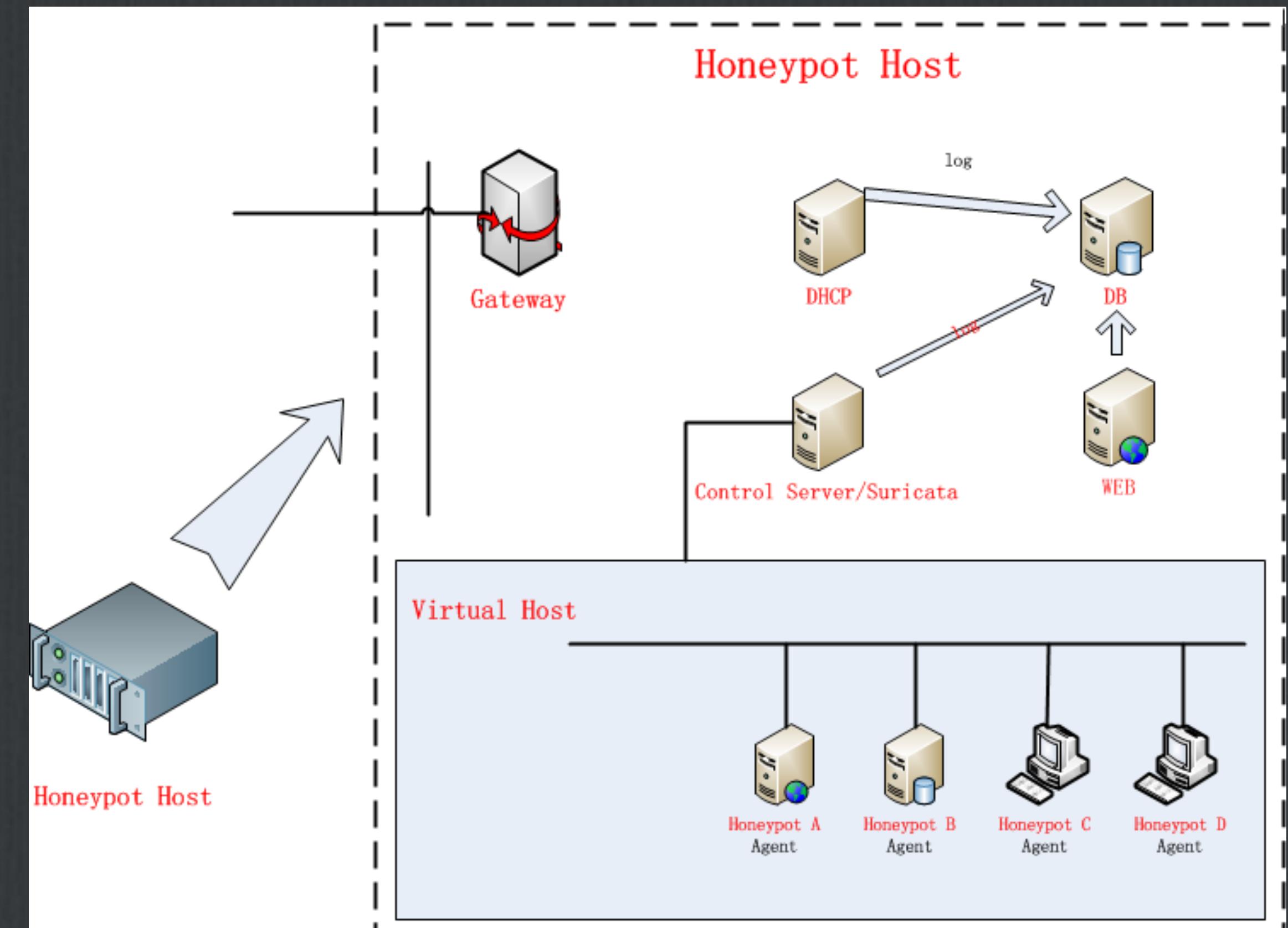
Hackers are often attacking vulnerable wireless hotspots as a **Breakthrough**. Why not use a Wireless Honeypot?

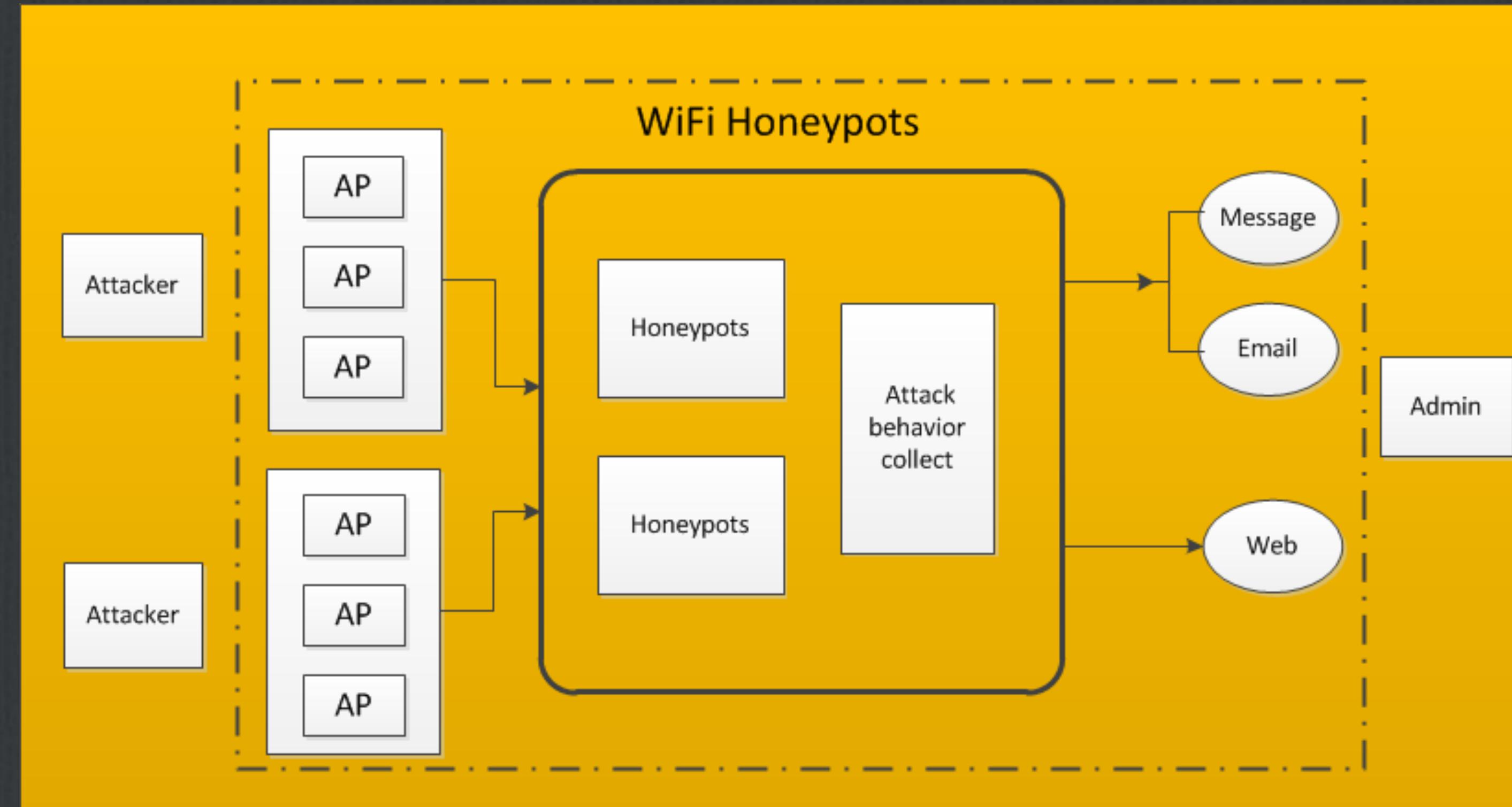
Get information about hacker:

- 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)**





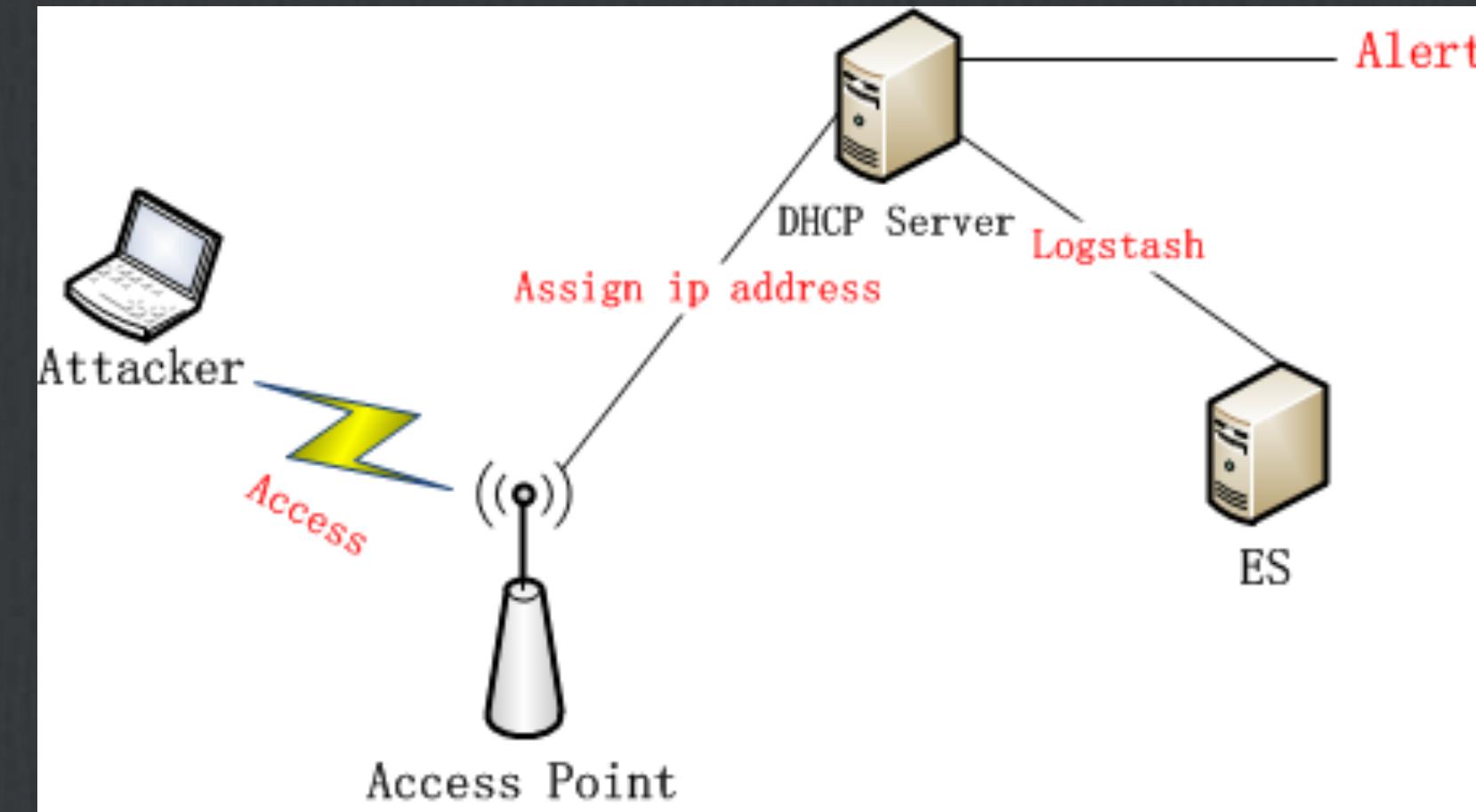
* **Wireless Access Layer**

* **Network Layer**

* **Honeypots Layer**

* Wireless Access Layer

- Set traps
 - Open
 - WEP
 - WPA with Weak Password
 - Password sharing APP

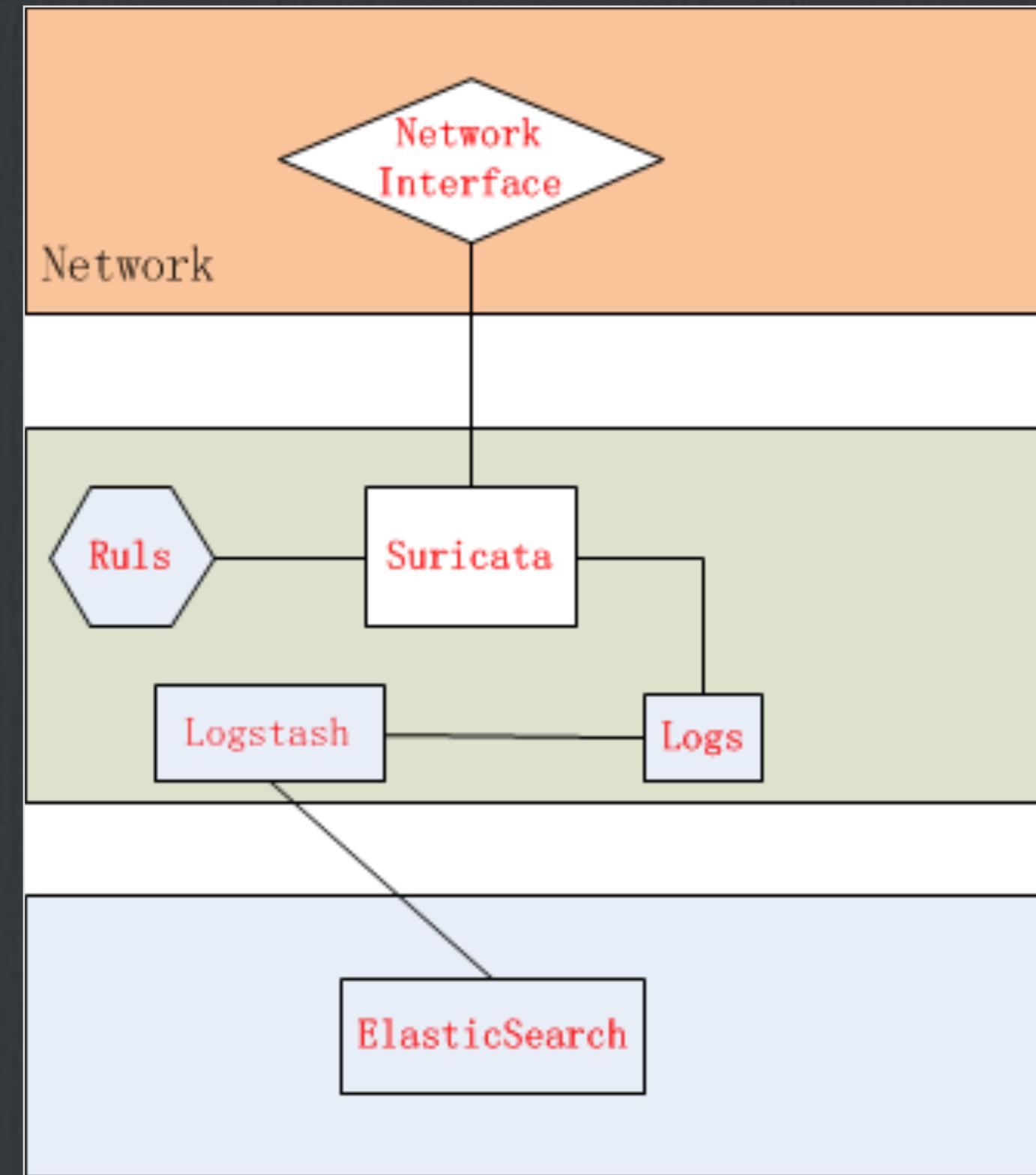


- Log connections
 - DHCP logs
 - hostname, IP address, MAC address

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)

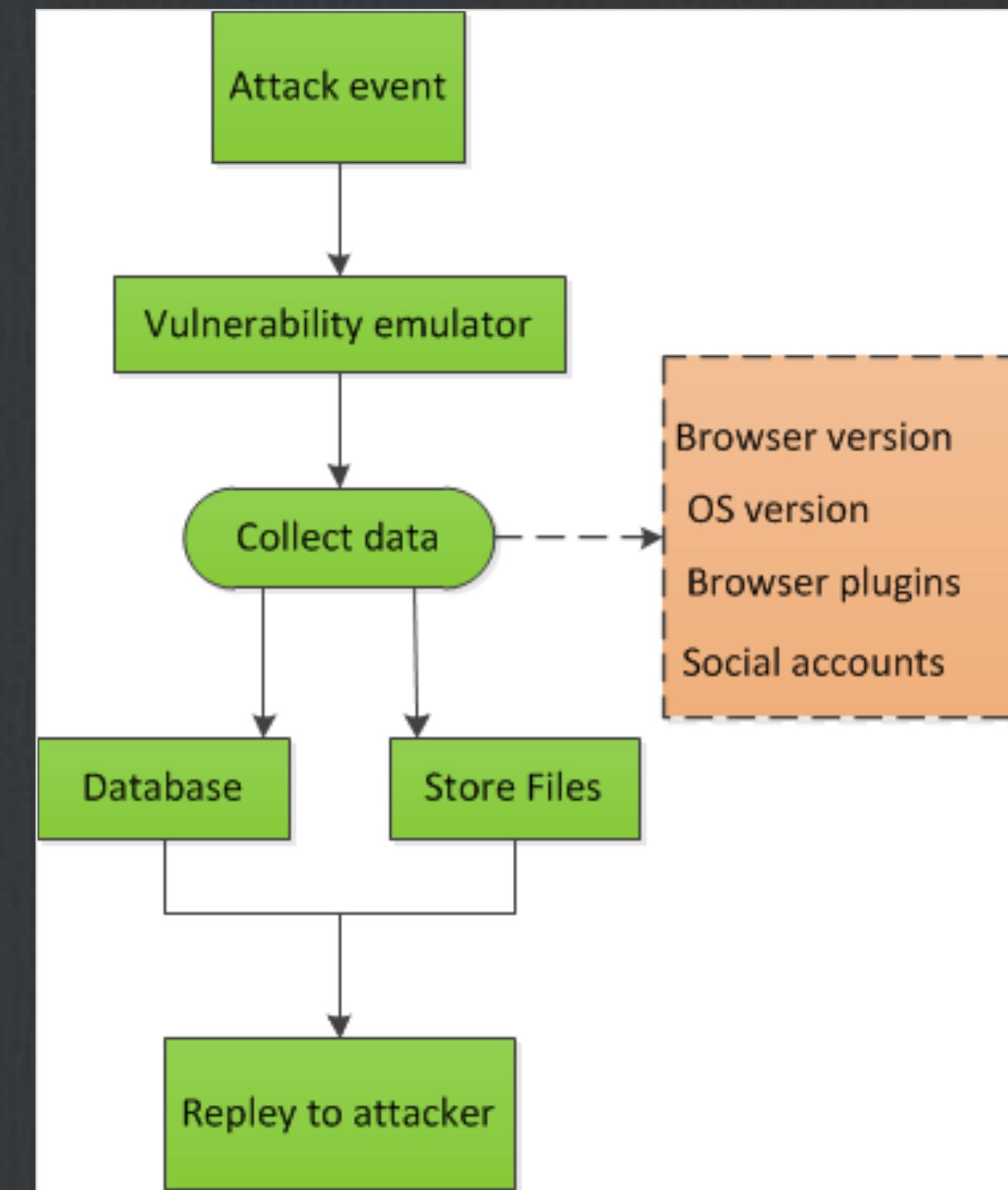
- Browser plugins

- Social accounts(**JSONP Hijacking**)

- Attacker profiling

- Set vulnerabilities

- get the access to the host



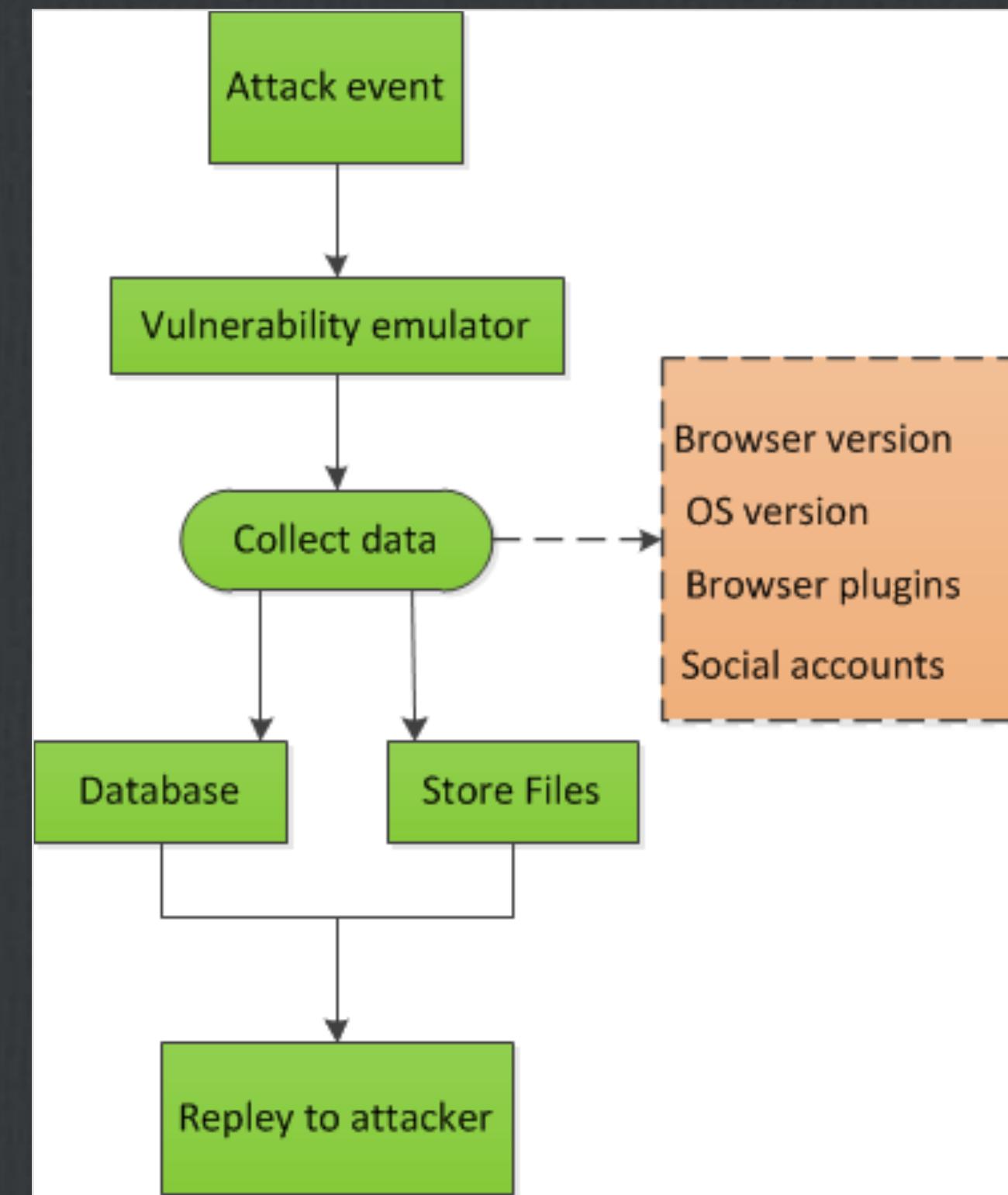
- JSONP
- make cross-domain JavaScript requests that bypass the same-origin policy
- lead to information leakage

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

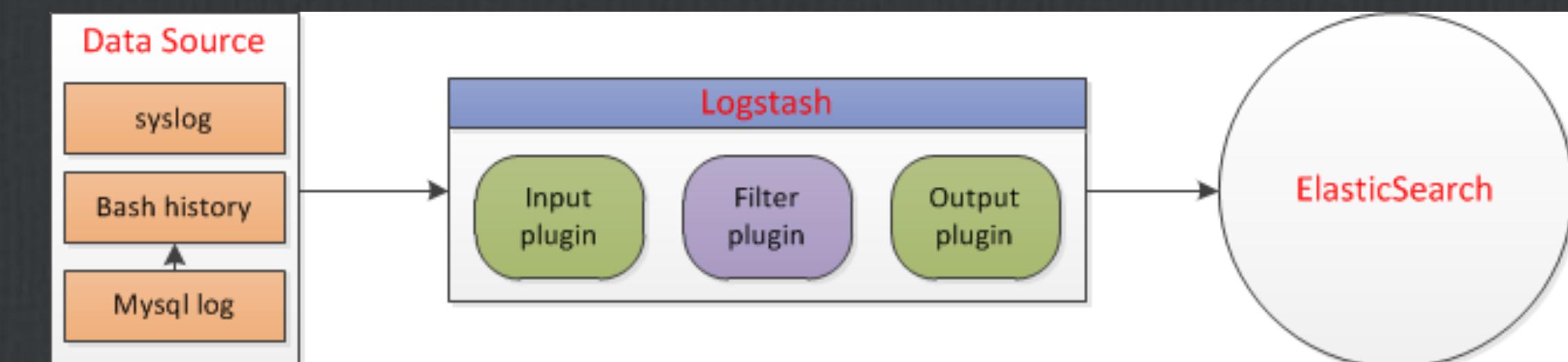
- Attack Alarm
- Monitor activities

Windows:

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

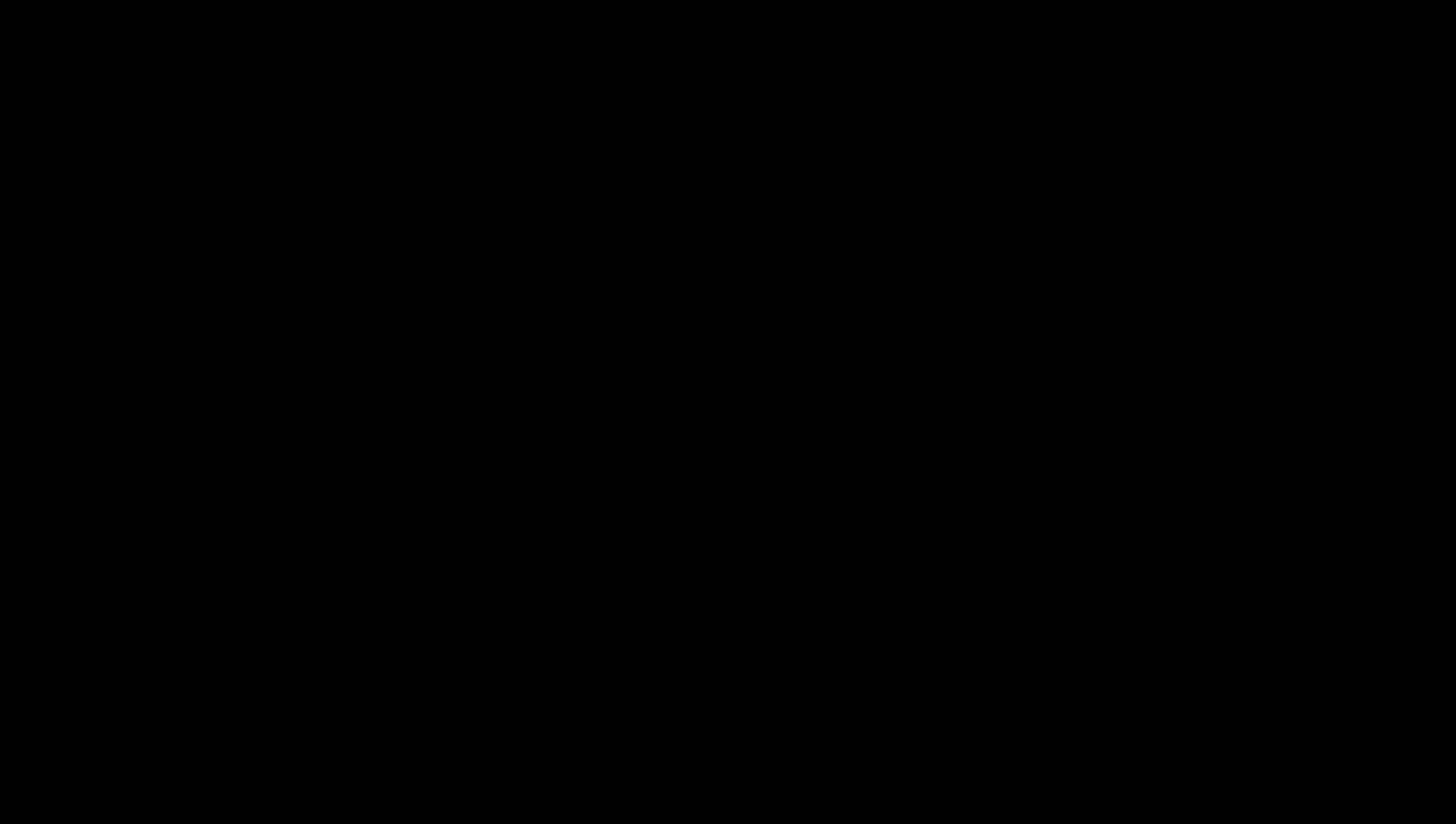
Linux:

- 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

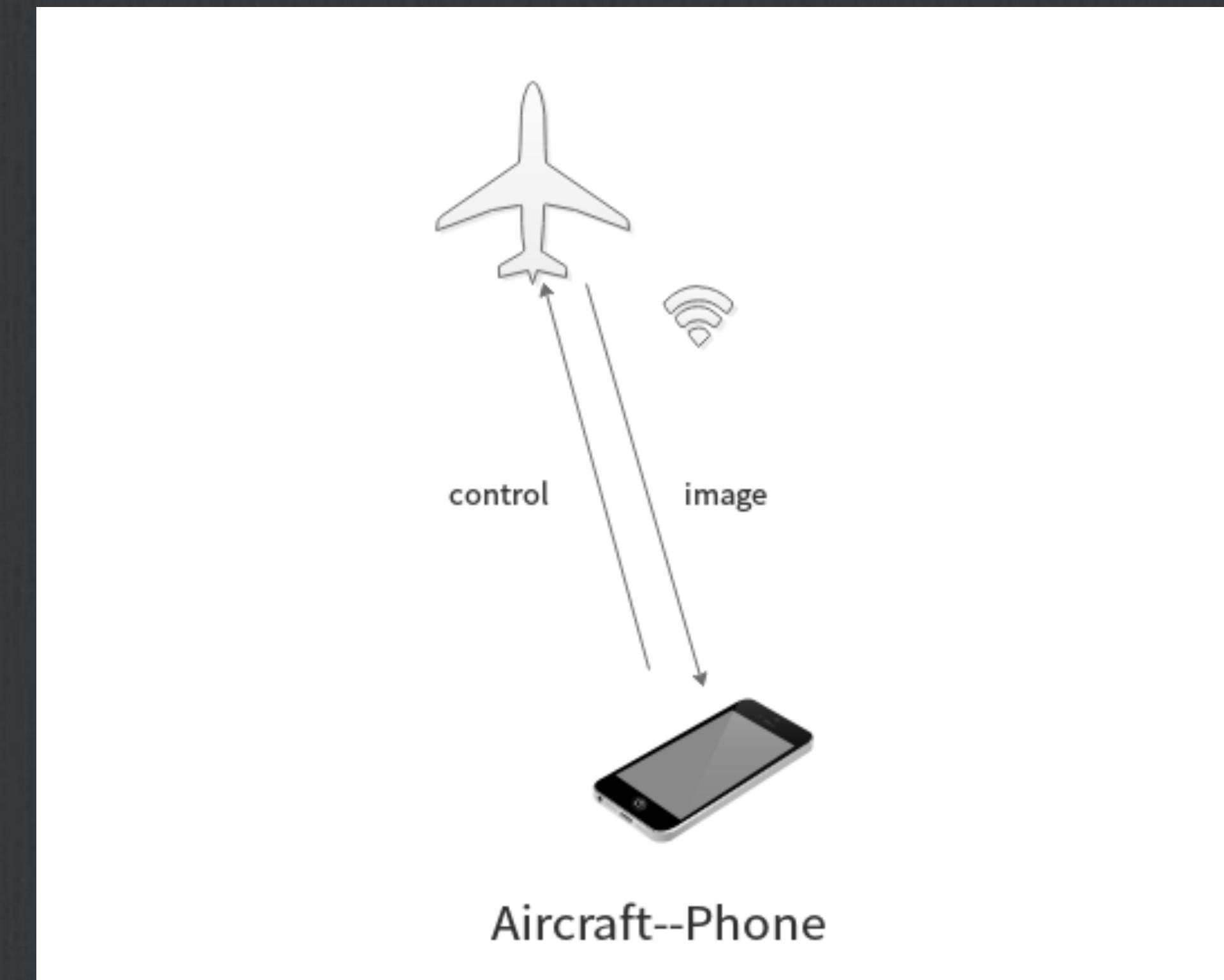
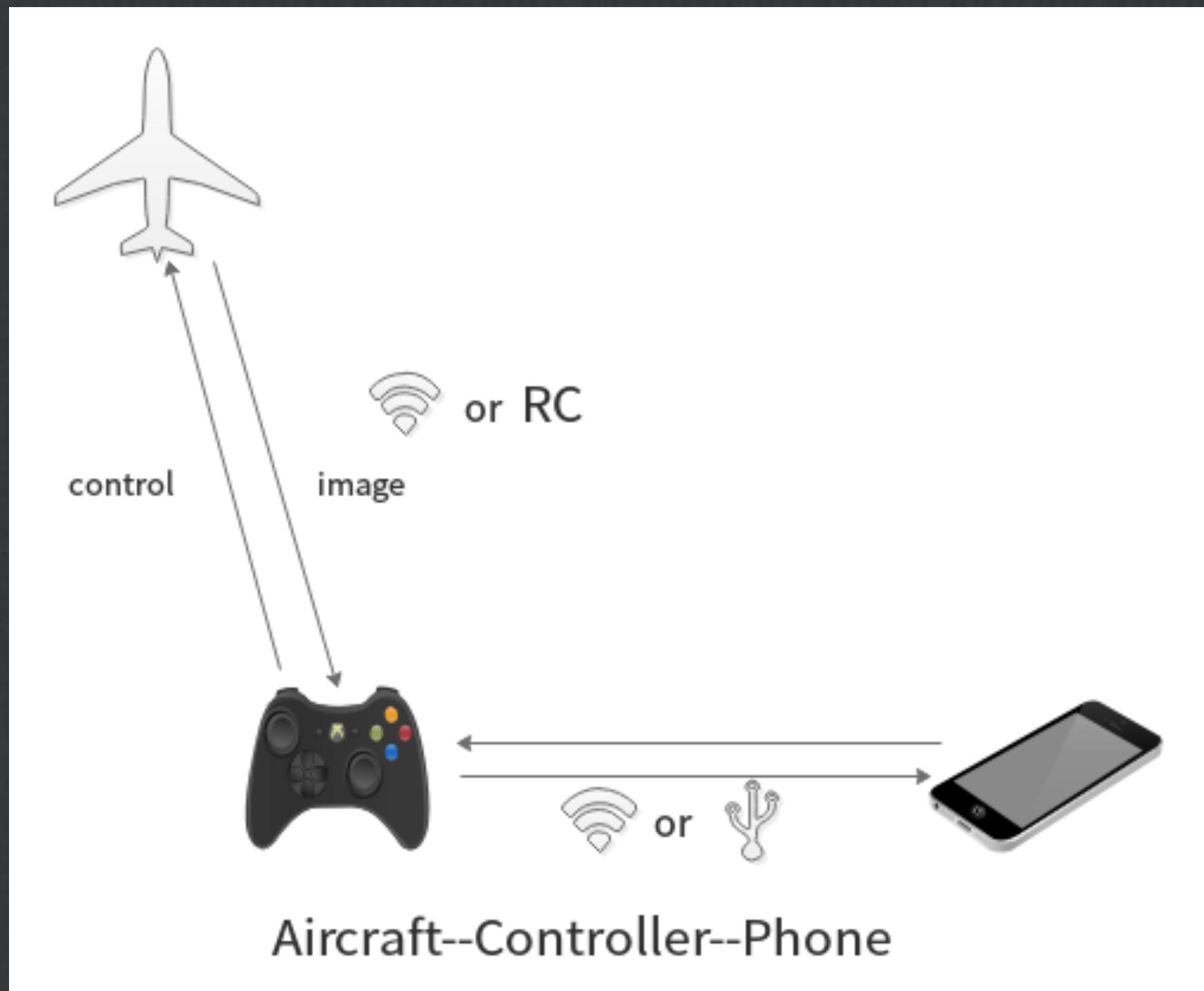




- WIPS & Wireless Honeypot
- Wireless Security Workflow
- Blocking Rogue AP
- Waiting for attackers

Others

1. Drone detector



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

30 5.455065	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11	141 QoS Data
31 5.455140	SzDjiTec_25:95:bd	SzDjiTec_25:95:bd	(... 802.11	40 Acknow
32 5.939464	SzDjiTec_25:95:bd	Broadcast	802.11	221 Beacon
33 6.042087	SzDjiTec_25:95:bd	Broadcast	802.11	221 Beacon
34 8.807052	SzDjiTec_25:95:bd	Broadcast	802.11	221 Beacon
35 8.909764	SzDjiTec_25:95:bd	Broadcast	802.11	221 Beacon
36 9.729072	SzDjiTec_25:95:bd	Broadcast	802.11	221 Beacon
37 9.751478	SzDjiTec_10:d7:46	SzDjiTec_25:95:bd	802.11	204 QoS Da
38 9.751553	SzDjiTec_10:d7:46	SzDjiTec_10:d7:46	(... 802.11	40 Acknow
20 0.750252	SzDjiTec_25:95:bd	SzDjiTec_10:d7:46	802.11	141 QoS Da

+ Frame 32: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface 0
+ Radiotap Header v0, Length 30
- 802.11 radio information
 PHY type: 802.11b (4)
 Short preamble: False
 Data rate: 1.0 Mb/s
 Channel: 3
 Frequency: 2422 MHz
 Signal strength (dBm): -64 dBm
 + [Duration: 1720 us]
+ IEEE 802.11 Beacon frame, Flags:
- IEEE 802.11 wireless LAN management frame
 + Fixed parameters (12 bytes)
 - Tagged parameters (155 bytes)
 + Tag: SSID parameter set: PHANTOM3_2595bd
 + Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]

802.1 Beacon frame from drone's AP

OUI	SSID	Drone Model
60:60:1f	PHANTOM3_xxxxxx X	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

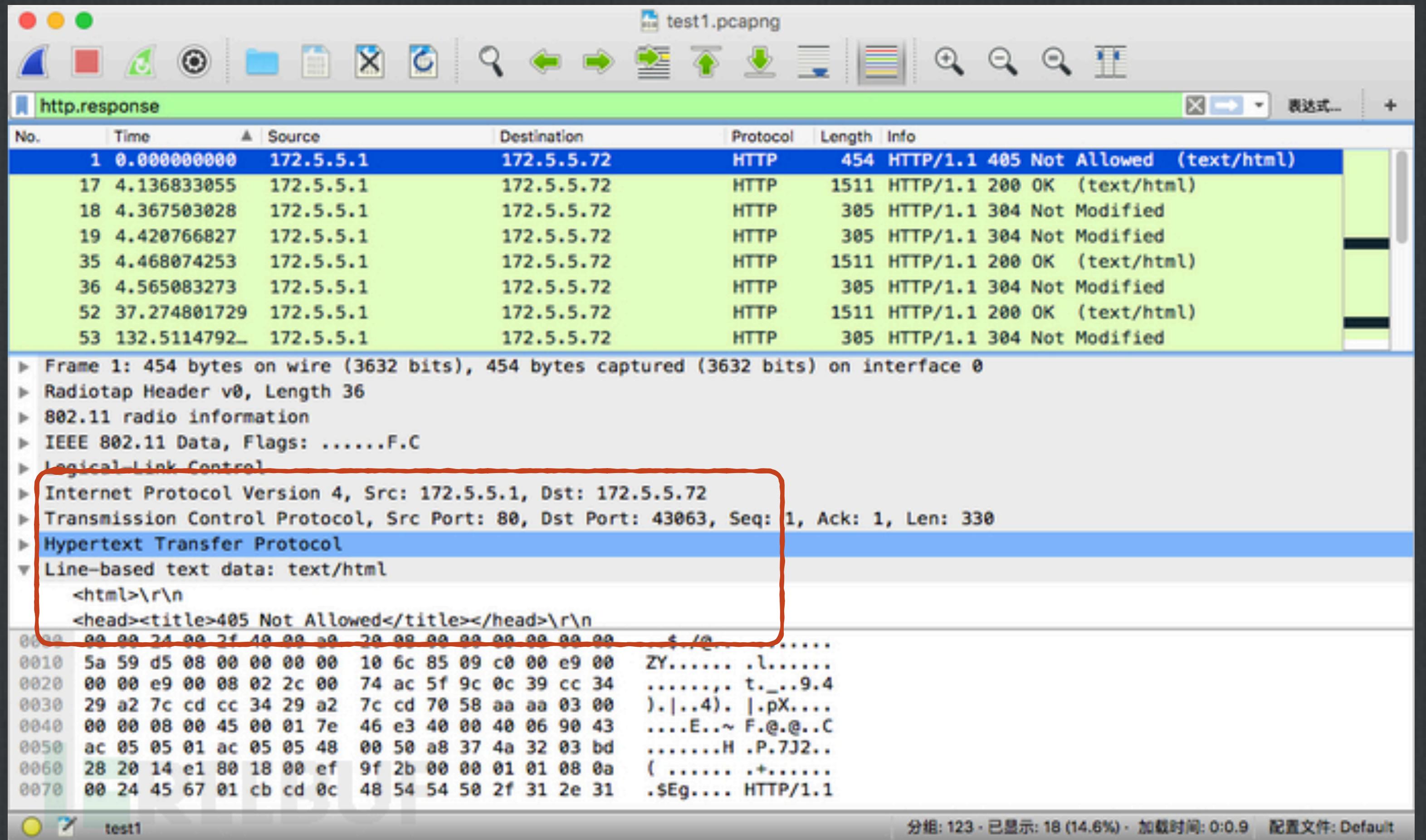
2. Wi-Fi Miner Detector



A tool for detecting Wi-Fi miner.

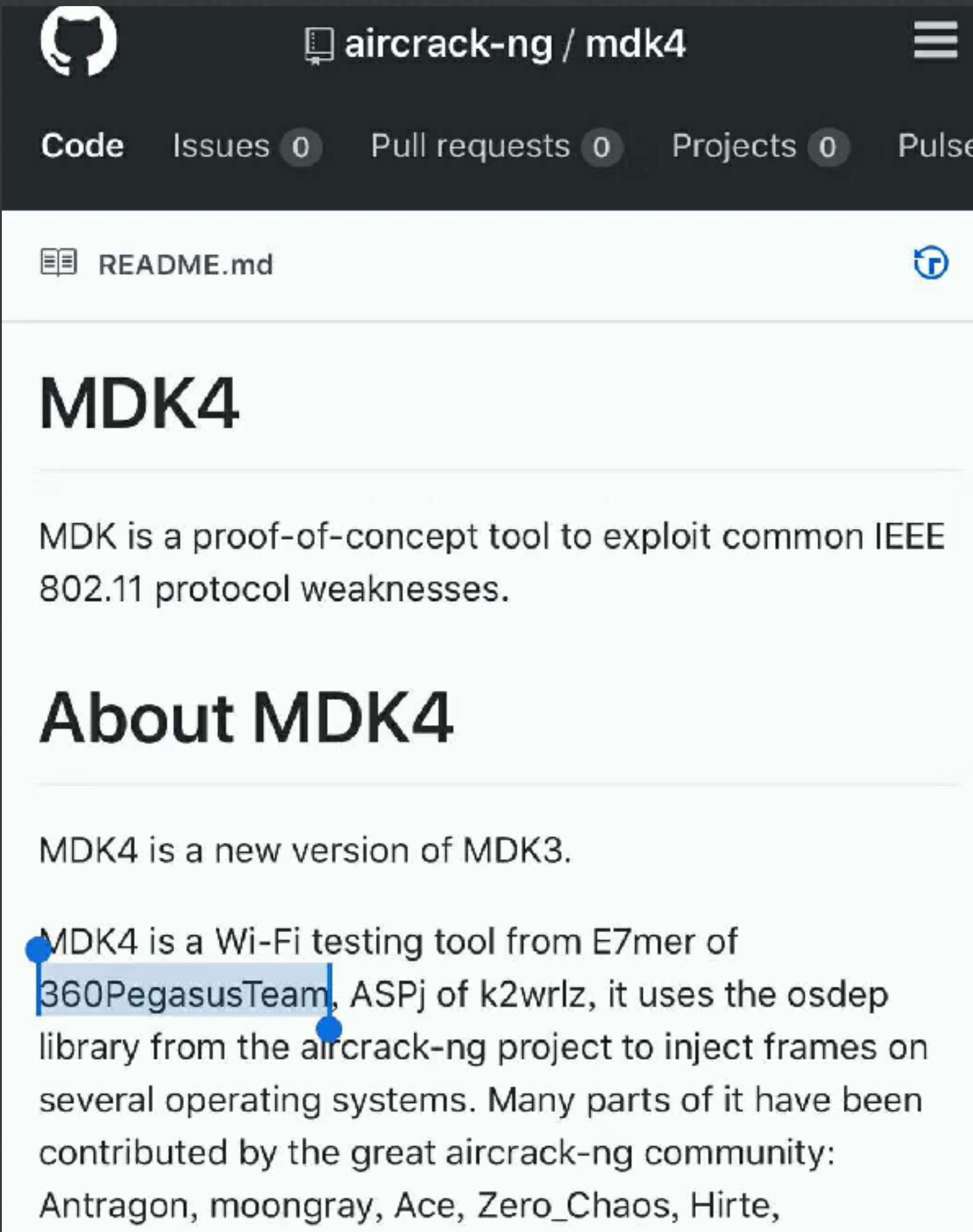
It is based on analyzing the unencrypted 802.11 Data Frame to detect mining keywords in HTTP data.

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



No connection is needed

3. MDK4



The screenshot shows the GitHub repository page for 'aircrack-ng / mdk4'. The page includes a navigation bar with links for Code, Issues (0), Pull requests (0), Projects (0), and Pulse. Below the navigation bar is a file list with 'README.md' and a 'Raw' link. The main content area features a section titled 'MDK4' with a description: 'MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses.' Below this is a 'About MDK4' section with the text: 'MDK4 is a new version of MDK3. MDK4 is a Wi-Fi testing tool from E7mer of 360PegasusTeam, ASPj of k2wrlz, it uses the osdep library from the aircrack-ng project to inject frames on several operating systems. Many parts of it have been contributed by the great aircrack-ng community: Antragon, moongray, Ace, Zero_Chaos, Hirte,'. The '360PegasusTeam' and 'k2wrlz' parts of the text are highlighted with a blue selection.

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