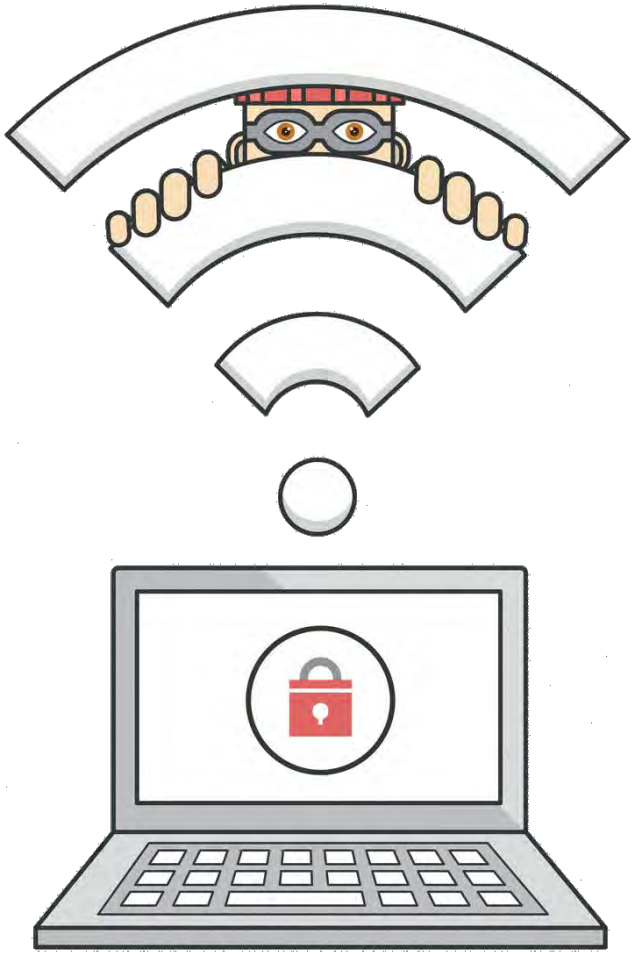
# Chellam – a Wi-Fi IDS/Firewall for Windows




**Vivek Ramachandran**
Founder & CEO
vivek@binarysecuritysolutions.com


facebook.com/ST.Trainings
twitter.com/SecurityTube
google.com/+SecurityTube
linkedin.com/company/SecurityTube

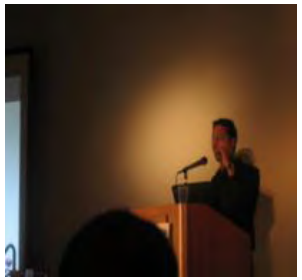
www.SecurityTube.net www.PentesterAcademy.com

# Vivek Ramachandran

B.Tech, ECE
IIT Guwahati

802.1x, Cat65k
Cisco Systems

WEP Cloaking
Defcon 19

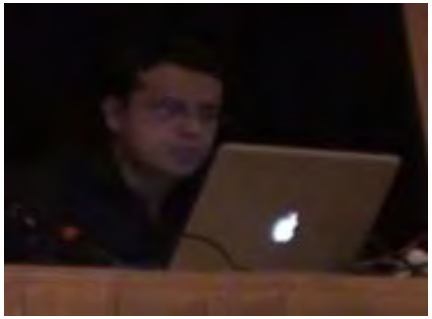


Caffe Latte Attack
Toorcon 9


Media Coverage
CBS5, BBC

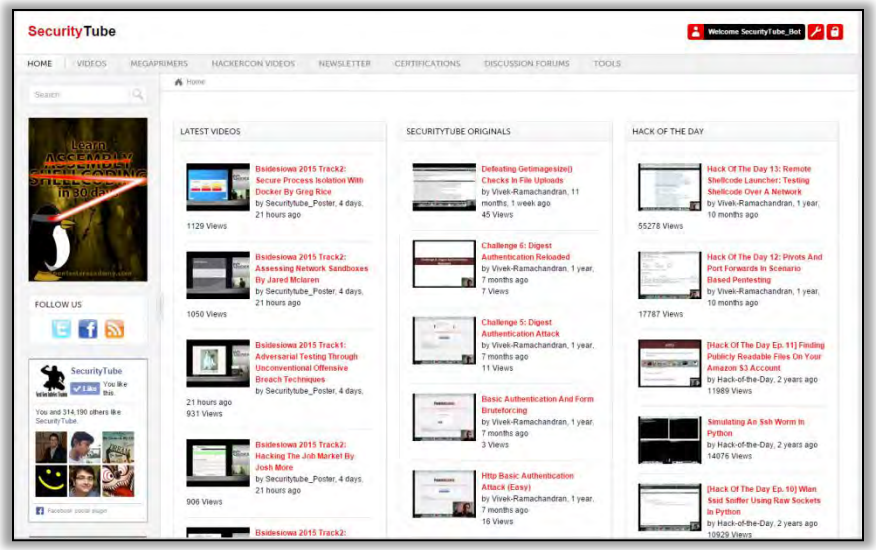

Microsoft
Security Shootout

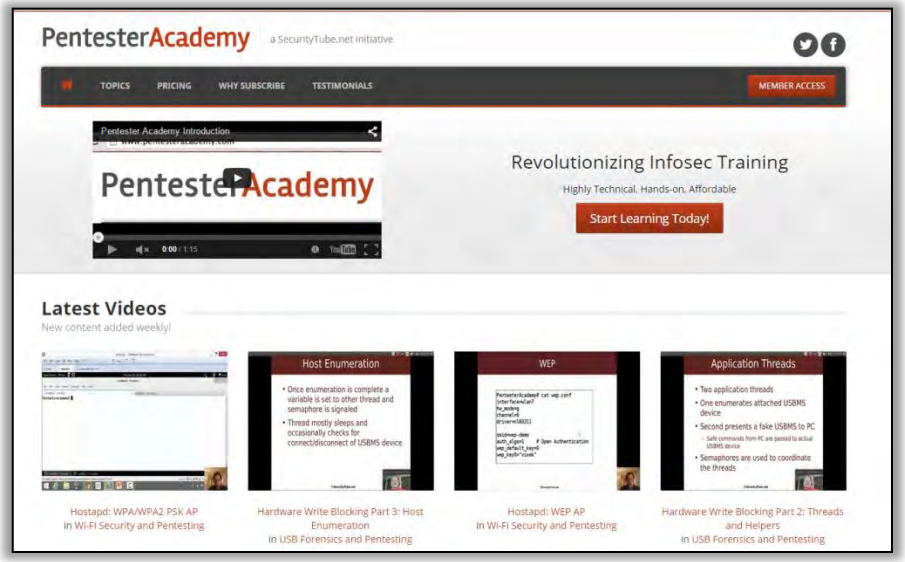
Trainer, 2011



Wi-Fi Malware, 2011

# SecurityTube and Pentester Academy

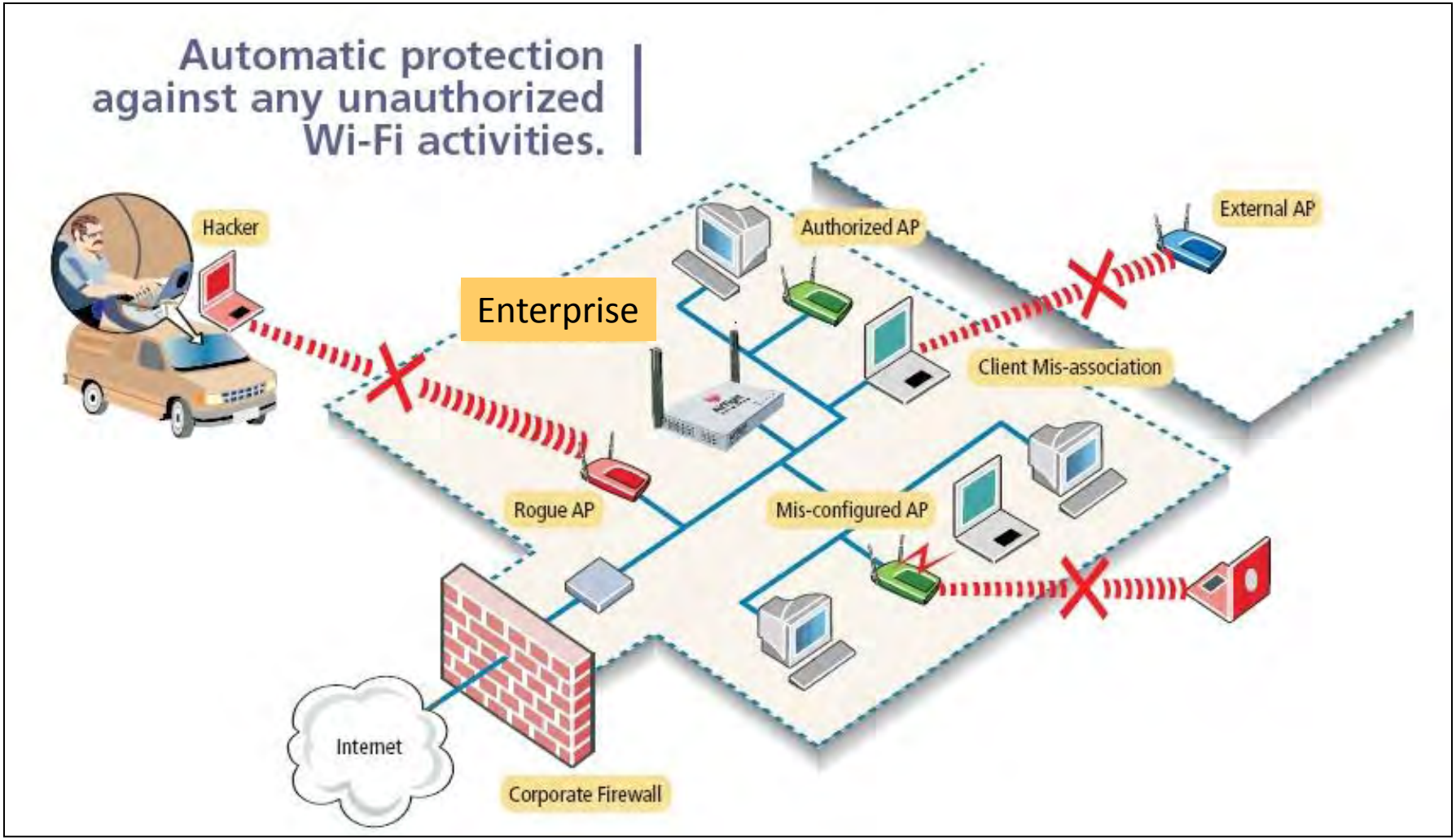


# Motivation

- Attack! Attack! Attack!
- Defense?
- Important problem?
- Solution viable?

# Enterprise Premise Focused



# Roaming Clients?


- State of current solutions
  - Lockdown Wi-Fi, Bluetooth etc.
  - Policy based on SSID
  - Not BYOD ready
  - No Attack detection
- Heterogeneous Devices
  - Varied Operating Systems
  - Non standard Wi-Fi API
  - No low level support e.g. iOS

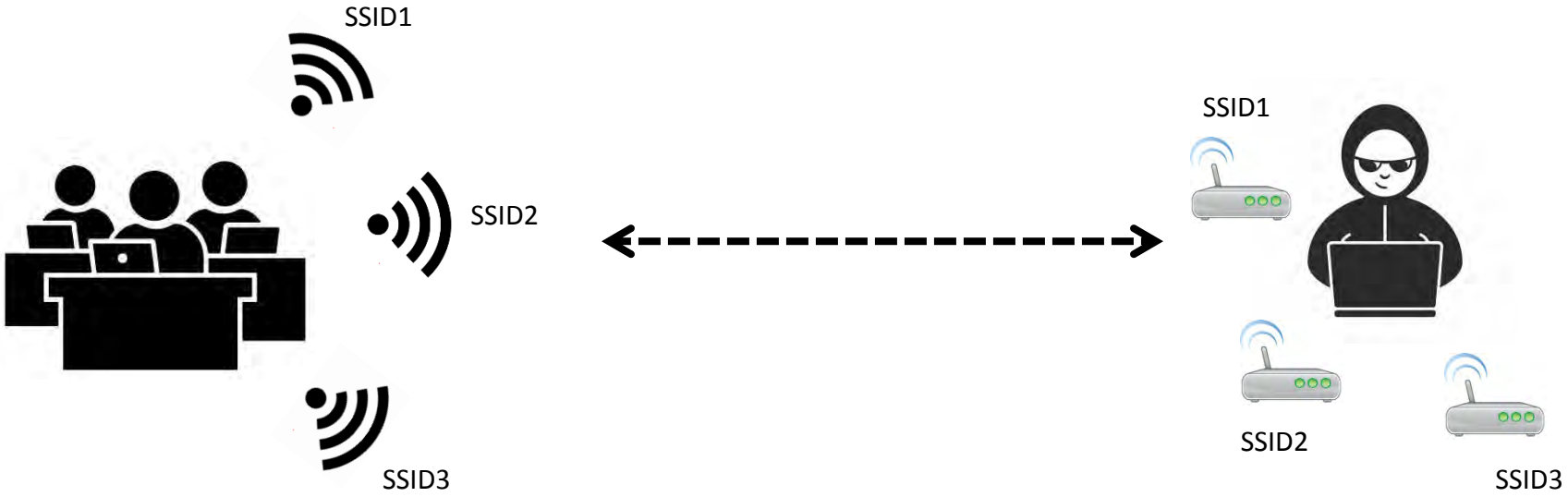
# What about the rest of us?

- World beyond Enterprise
- Millions of Personal Devices
- Every Internet capable device
- Internet Of Things (IoT)

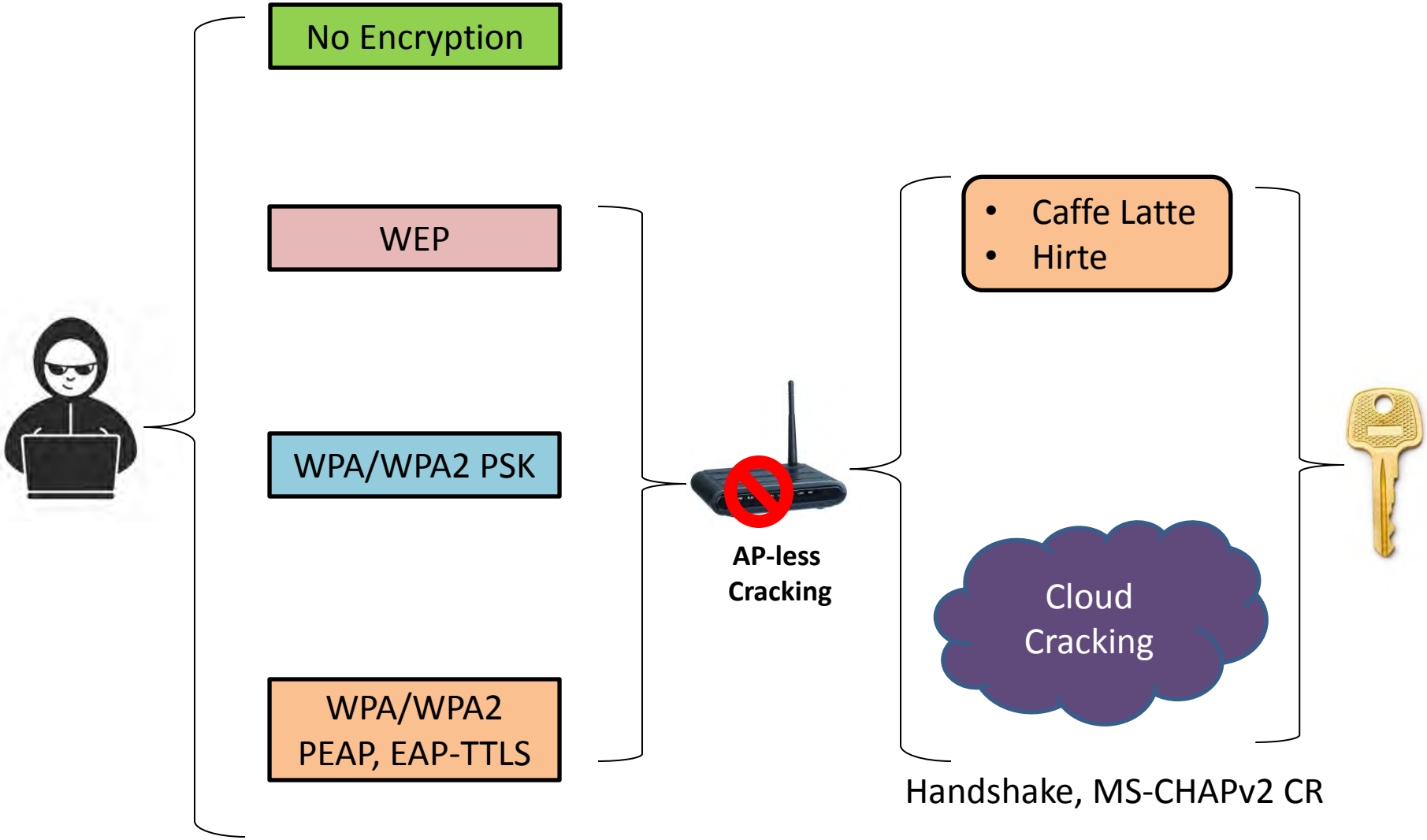
# Wi-Fi Client Attack Surface

- Honeypots
  - AP-less WEP/WPA/WPA2 Cracking
- Evil Twins
- Mis-Associations
- Hosted Network Backdoors
- …

# Typical Attack

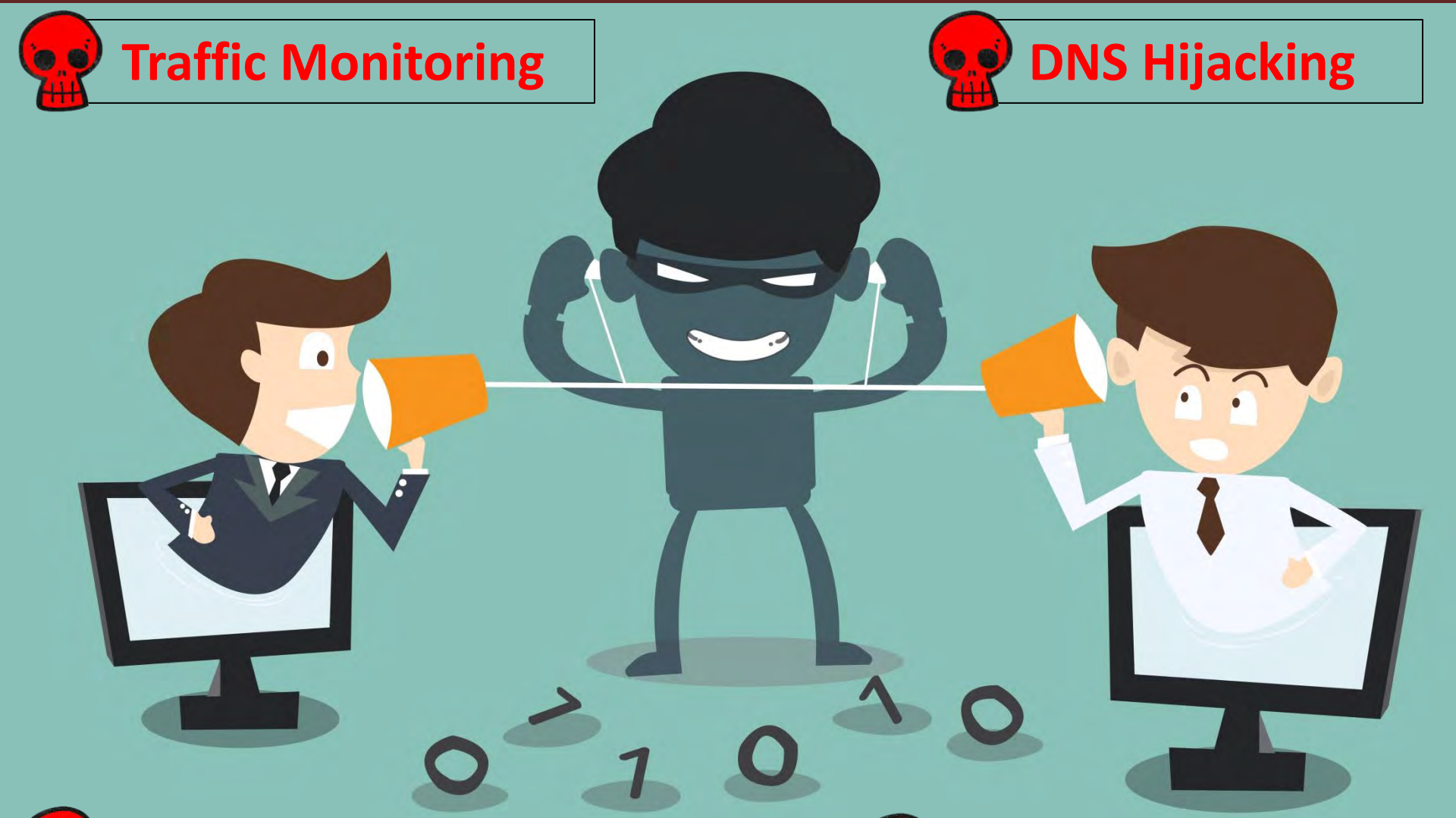


# AP-less Cracking

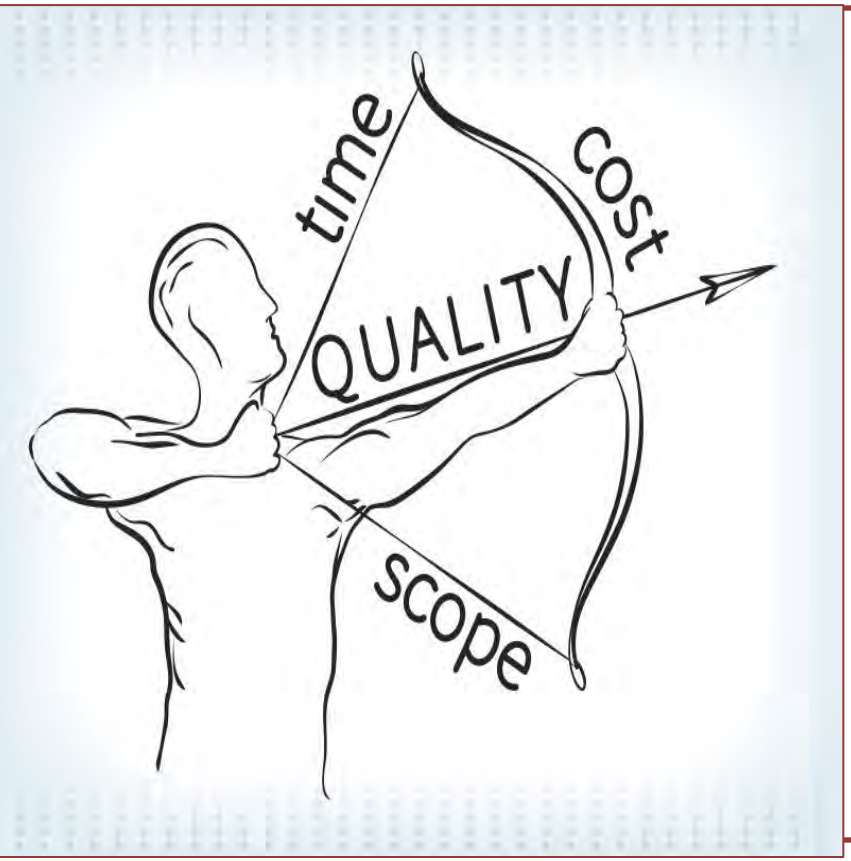


# Where are you SAFE? Nowhere!!!

# Hijack Wi-Fi == Hijack Layer 2

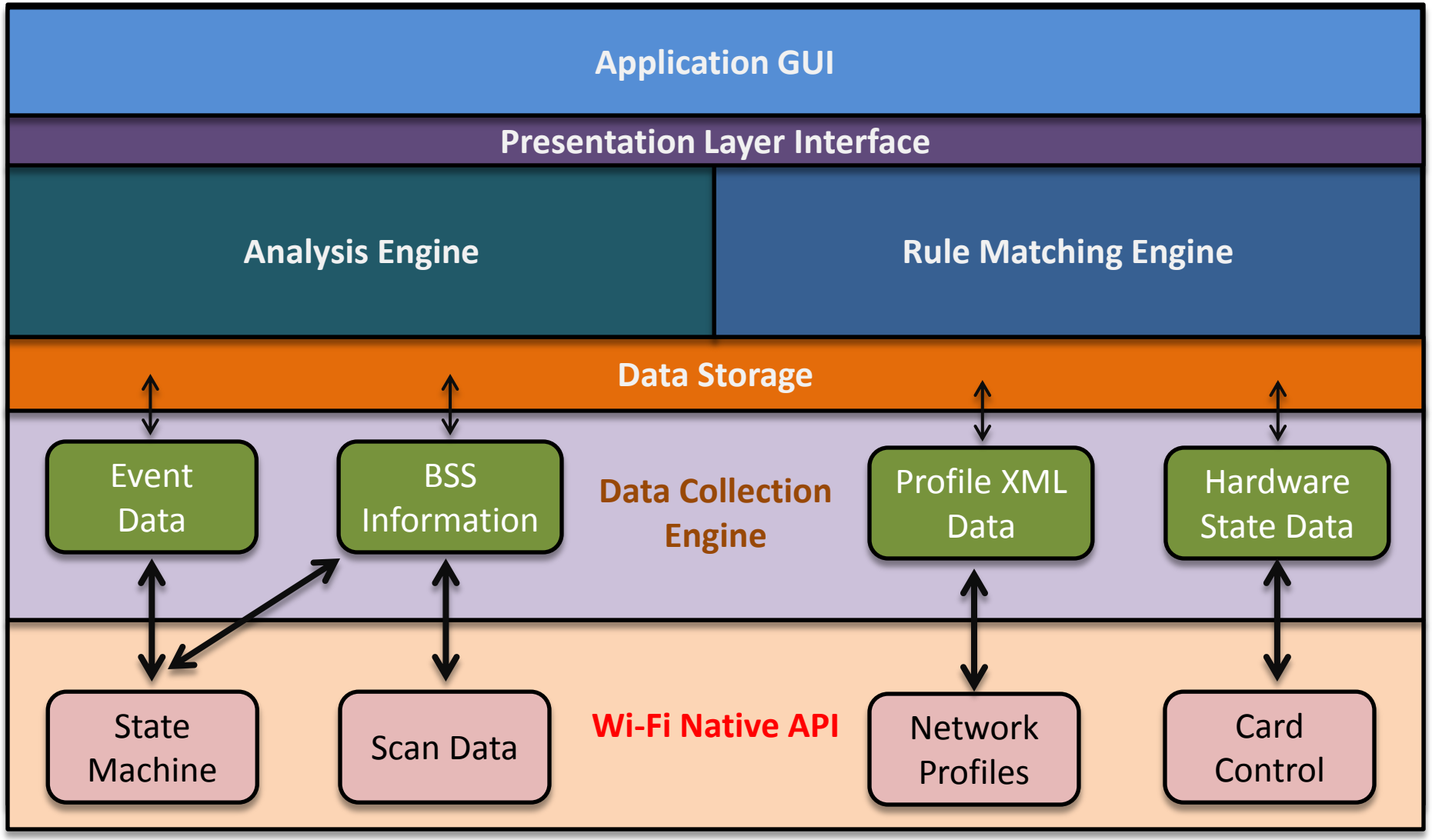


# Defining the Scope




- Windows Endpoints
  - No custom hardware or drivers
- Detect Honeypot creation Tools
- Firewall like Rule Creation
  - “Allow”, “Deny”
- Monitoring Wi-Fi state machine
- Detect Wi-Fi backdoors

# Architecture Block Diagram



# Wi-Fi Native API


| | |
|---|---|
| State Machine | 802.11 state machine per Wi-Fi card |
| Scan Data | Periodic Scan Results with BSS data |
| Network Profiles | XML network profile data |
| Card Control | Scan, Connect, Disconnect, Lock etc. |

# Technicalities

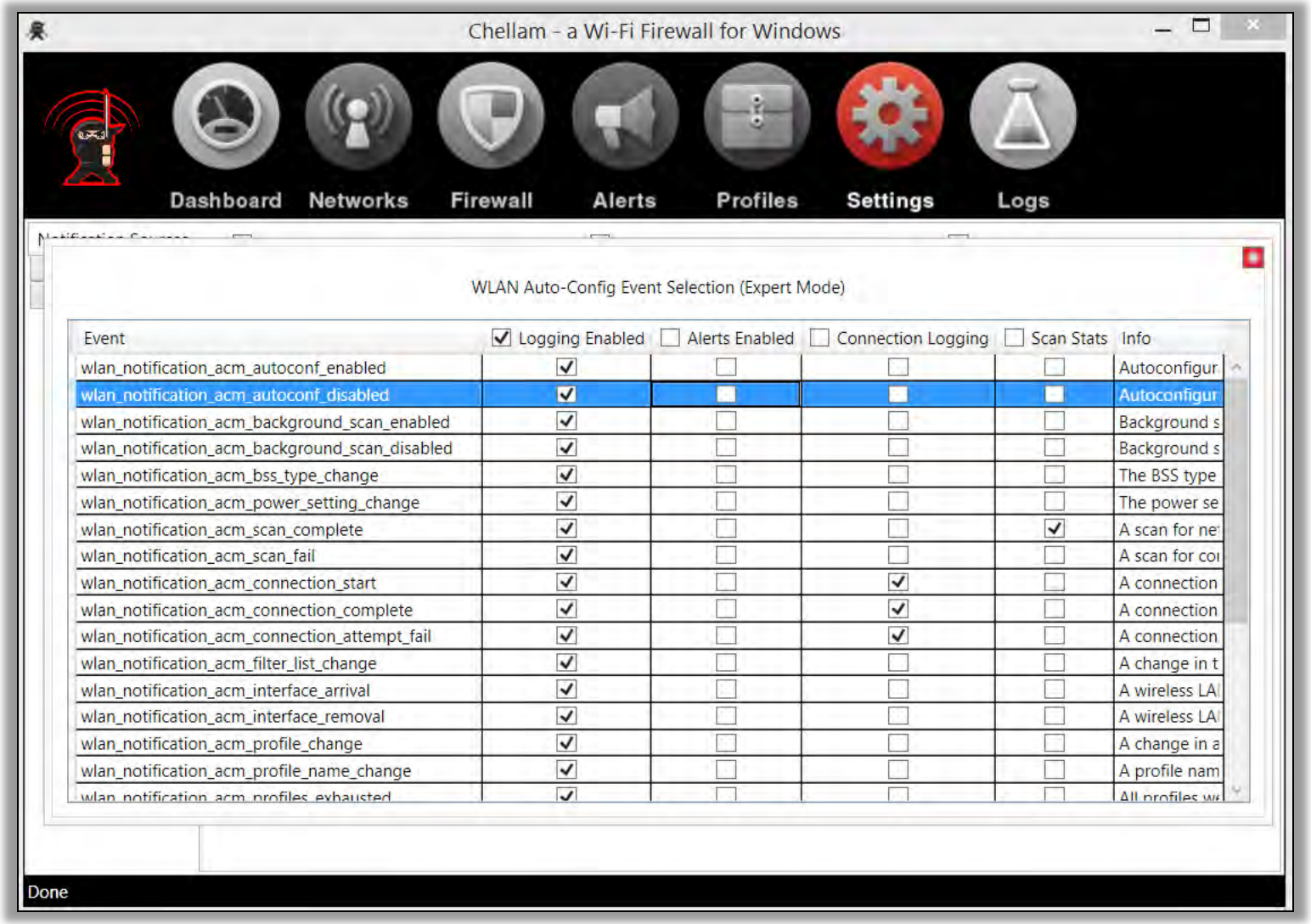
```
typedef struct _WLAN_BSS_ENTRY {
  DOT11_SSID         dot11Ssid;
  ULONG              uPhyId;
  DOT11_MAC_ADDRESS  dot11Bssid;
  DOT11_BSS_TYPE     dot11BssType;
  DOT11_PHY_TYPE     dot11BssPhyType;
  LONG               lRssi;
  ULONG              uLinkQuality;
  BOOLEAN            bInRegDomain;
  USHORT             usBeaconPeriod;
  ULONGLONG          ullTimestamp;
  ULONGLONG          ullHostTimestamp;
  USHORT             usCapabilityInformation;
  ULONG              ulChCenterFrequency;
  WLAN_RATE_SET      wlanRateSet;
  ULONG              ulIeOffset;
  ULONG              ulIeSize;
} WLAN_BSS_ENTRY, *PWLAN_BSS_ENTRY;
```

```
typedef struct _WLAN_NOTIFICATION_DATA {
  DWORD NotificationSource;
  DWORD NotificationCode;
  GUID  InterfaceGuid;
  DWORD dwDataSize;
  PVOID pData;
} WLAN_NOTIFICATION_DATA, *PWLAN_NOTIFICATION_DATA;
```

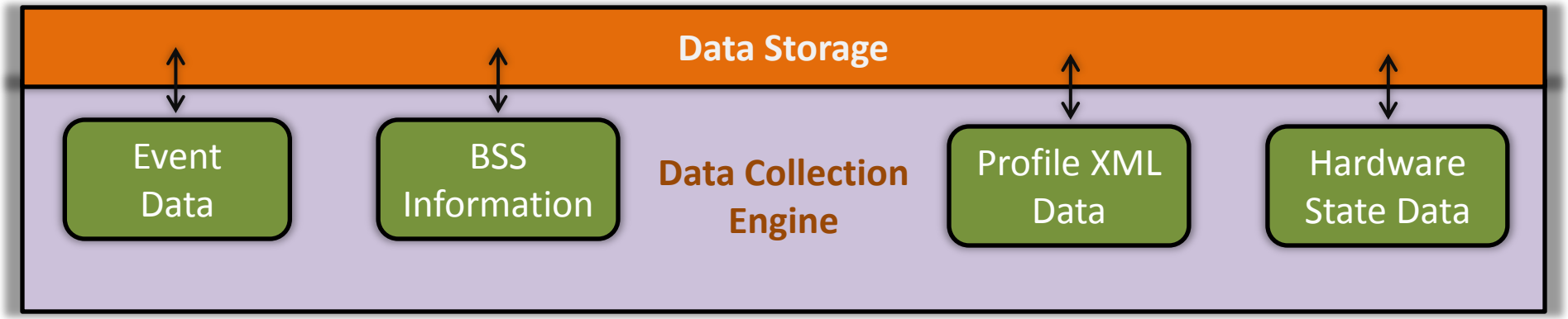
```
<?xml version="1.0" encoding="US-ASCII"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>SampleWPA2PSK</name>
    <SSIDConfig>
        <SSID>
            <name>SampleWPA2PSK</name>
        </SSID>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>auto</connectionMode>
    <autoSwitch>false</autoSwitch>
    <MSM>
        <security>
            <authEncryption>
                <authentication>WPA2PSK</authentication>
                <encryption>AES</encryption>
                <useOneX>false</useOneX>
            </authEncryption>
        </security>
    </MSM>
</WLANProfile>
```

https://msdn.microsoft.com/en-us/library/windows/desktop/ms706839(v=vs.85).aspx

# Demo – Data Sources

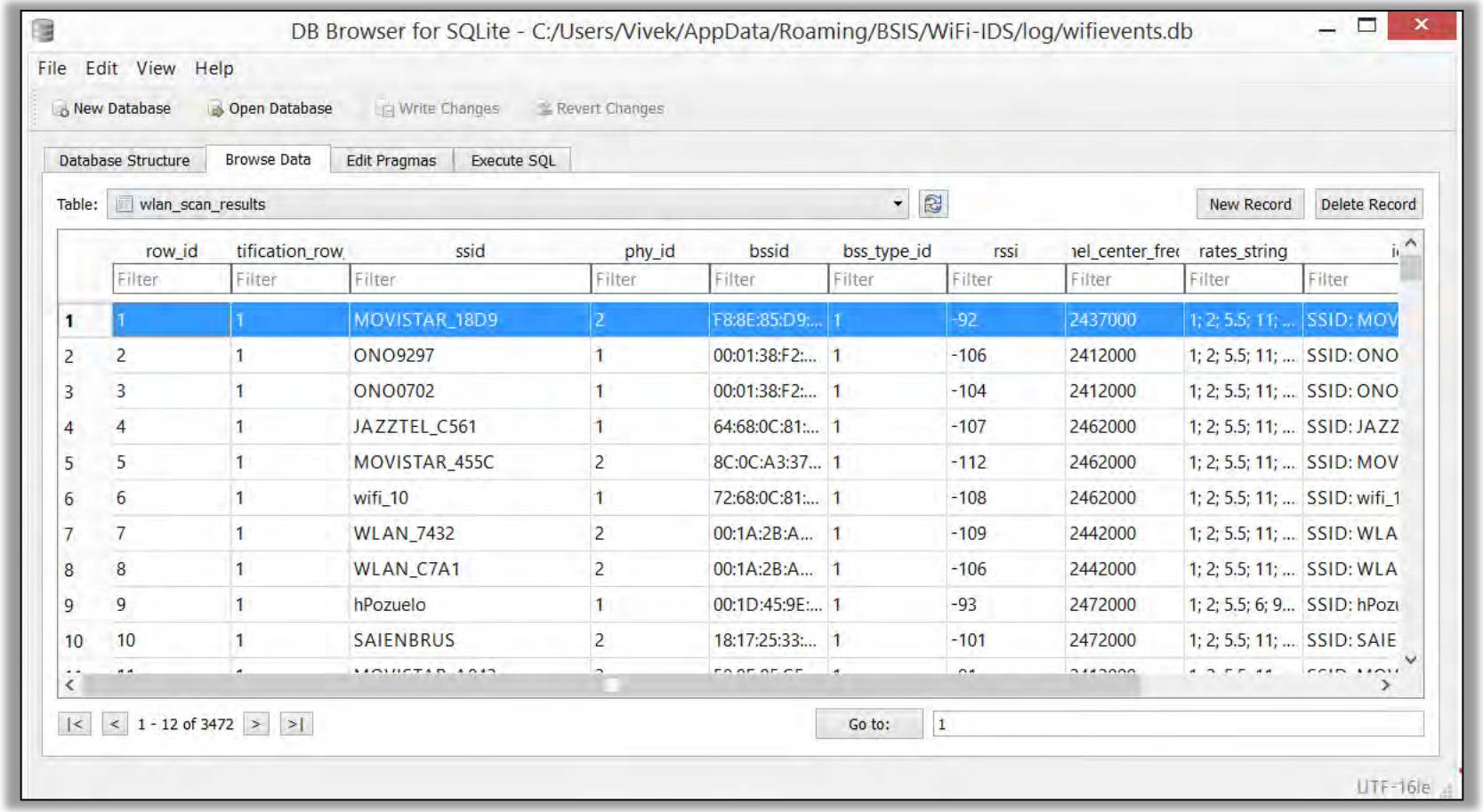


# Data Collection and Storage

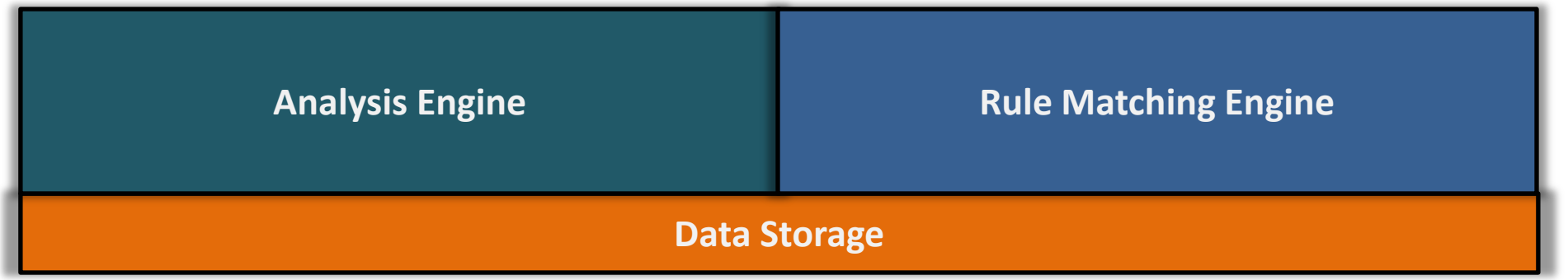



- Stored in SQLITE databases
- Makes it easy to write plugins
- 3rd party tools can use the database

# Demo – SQLITE DB Data

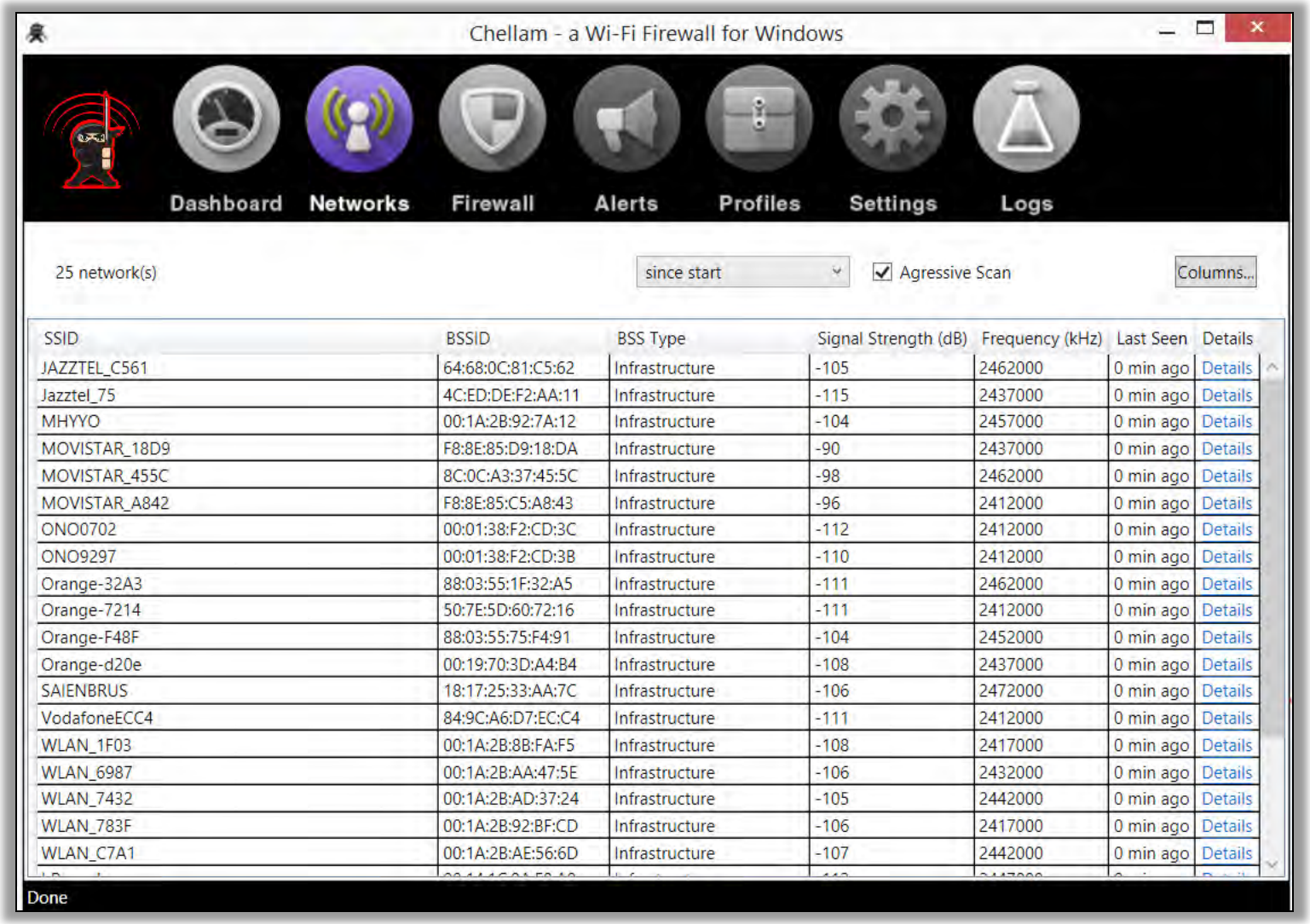


# Rule Matching and Analysis



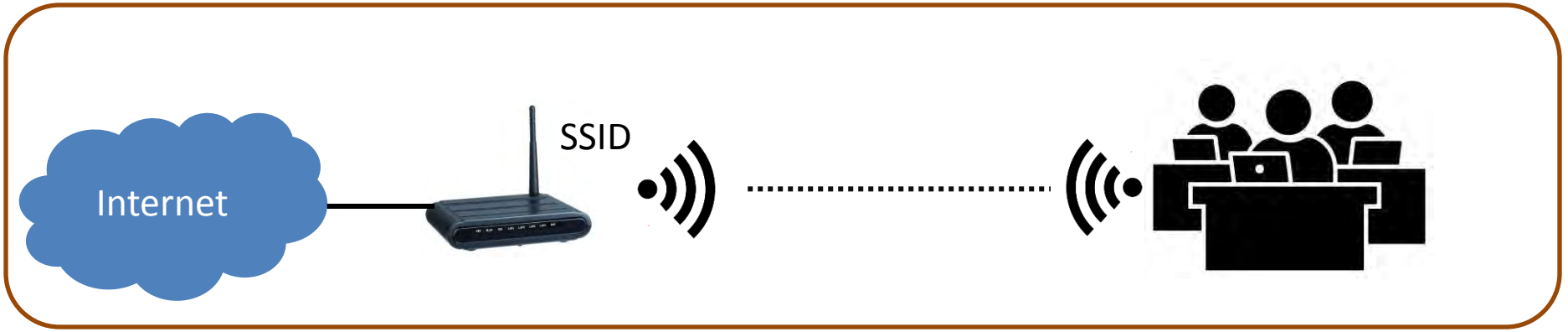

- Rules can be written to include:
  - BSSID
  - Neighboring Networks
  - Channel use patterns and frequencies
  - Information Elements in the Beacon / Probe Response
  - Access pattern based on time of day

# Demo – Monitoring and Event Detection



# Understanding Attack Detection







# Fingerprinting the Network


- BSSID(s)
- BSS type
- PHY type
- Beacon Interval
- Channel(s) & Hopping
- Rates – basic and extended
- Capability Information
- Information Element(s)

- Neighboring Access Points
- AP details as above

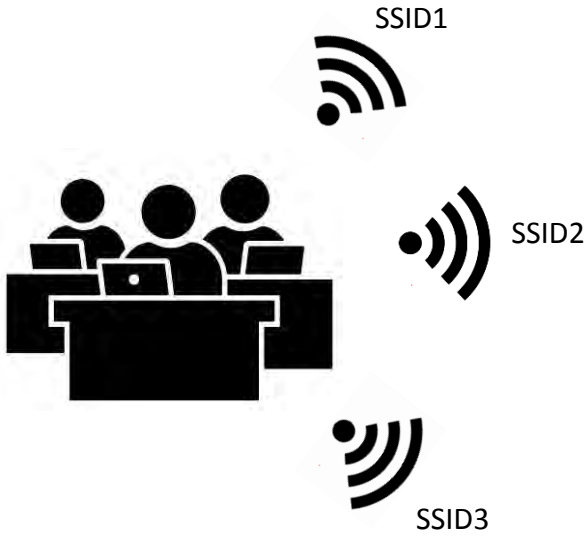
**802.11 (pre connect)**

- IP, Gateway
- DNS, ARP cache

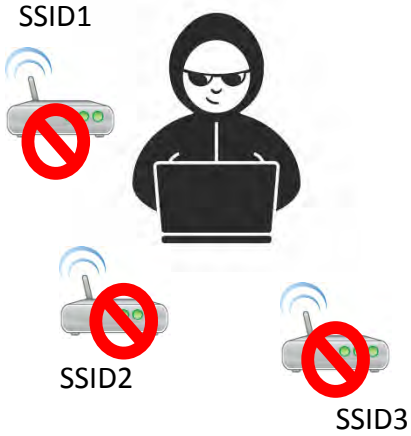
- Subnet scan
- OS and service scan

**IP & Above (post connect)**

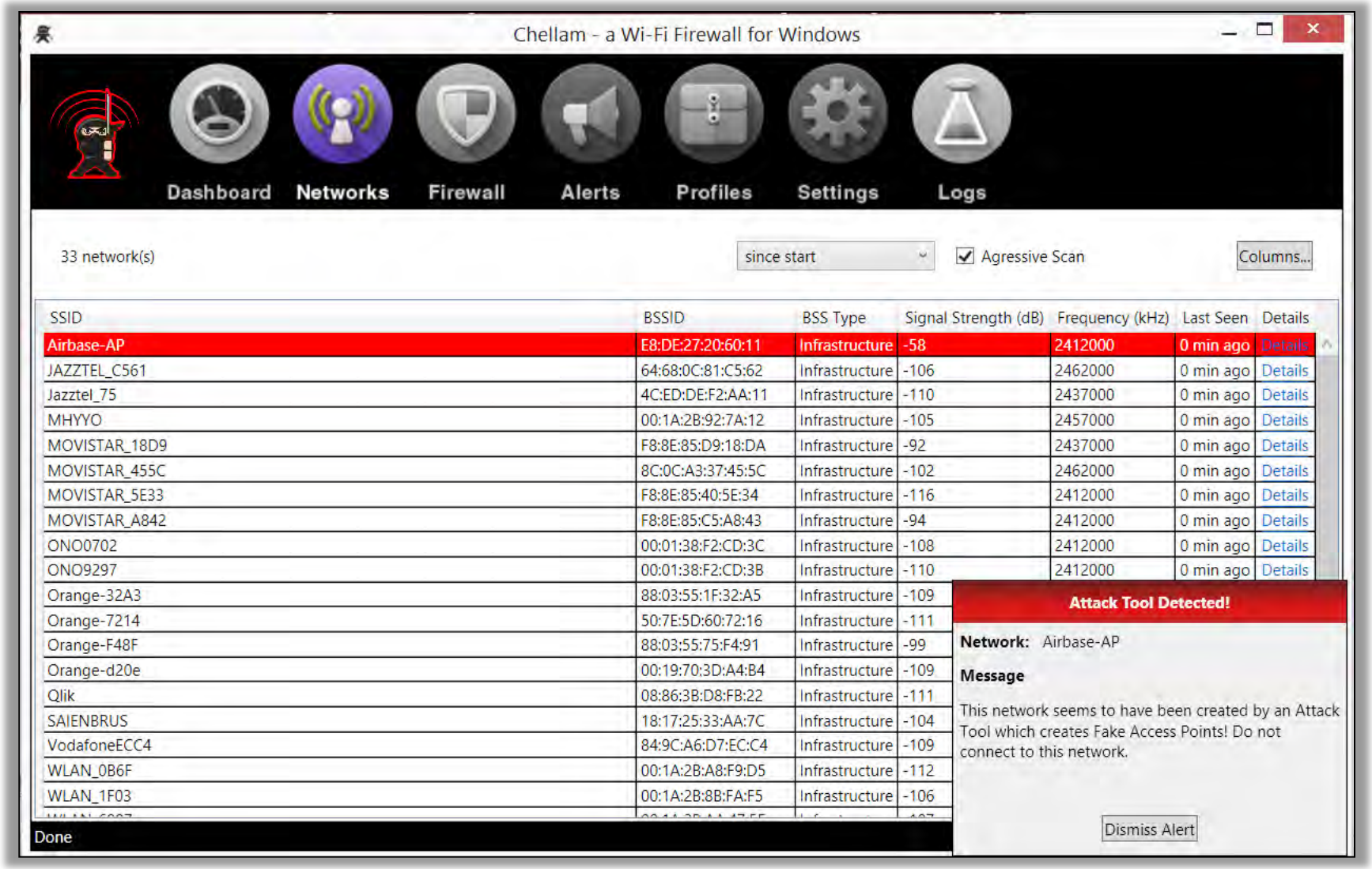
# Typical Attack Mitigation




- BSSID(s)
- Channel(s) & Hopping
- Rates – basic and extended
- Capability Information
- Information Element(s)
- Neighboring Access Points
- AP details as above



# Demo – Attack Tool Detection (Airbase)



# Why is this important?

- Attack tools will have to significantly improve
- Make it difficult to fingerprint
  - No hardcoded values, random BSSID etc.
- More features to mimic authorized networks
  - Ability to “clone” network beacons / probe responses
  - Ability to closely follow Clocks (timestamp)
  - Have to be on the right channel and band
- Very difficult to beat Whitelist approach

# Roadmap - Enhancements

- Whitelist vs Blacklist
- Plugin Architecture
  - SQL with Python
- Intrusion Prevention / Firewall with custom Driver
- Assisted and automatic learning of whitelists
- Downloadable blacklists for attack tools

# Questions?