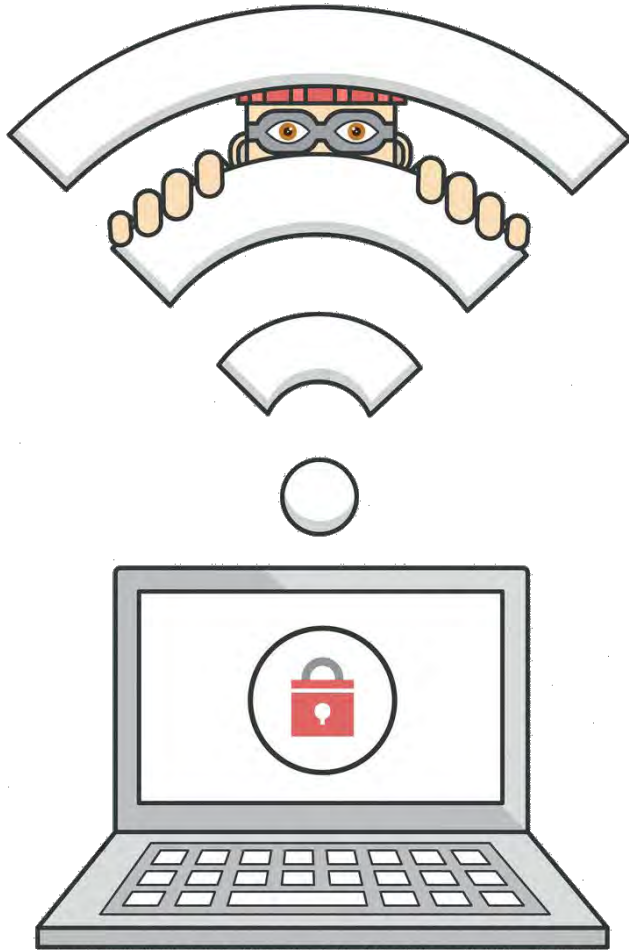


# Chellam – a Wi-Fi IDS/Firewall for Windows



<b>Vivek Ramachandran</b> Founder & CEO	<a href="mailto:vivek@binarysecuritysolutions.com">vivek@binarysecuritysolutions.com</a>
 <a href="https://facebook.com/ST.Trainings">facebook.com/ST.Trainings</a>	
 <a href="https://twitter.com/SecurityTube">twitter.com/SecurityTube</a>	
 <a href="https://google.com/+SecurityTube">google.com/+SecurityTube</a>	
 <a href="https://linkedin.com/company/SecurityTube">linkedin.com/company/SecurityTube</a>	
<a href="http://www.SecurityTube.net">www.SecurityTube.net</a>	<a href="http://www.PentesterAcademy.com">www.PentesterAcademy.com</a>

# Vivek Ramachandran



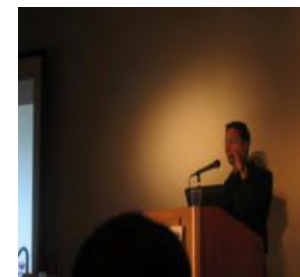
B.Tech, ECE  
IIT Guwahati



802.1x, Cat65k  
Cisco Systems



WEP Cloaking  
Defcon 19



Caffe Latte Attack  
Toorcon 9



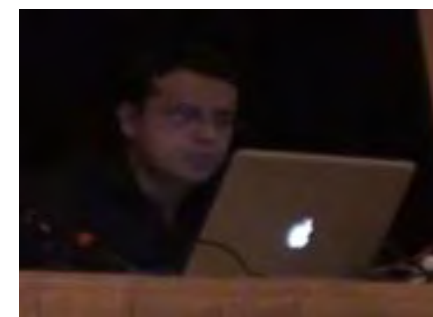
Media Coverage  
CBS5, BBC



Microsoft  
Security Shootout



Trainer, 2011



Wi-Fi Malware, 2011

# SecurityTube and Pentester Academy

The screenshot shows the SecurityTube website homepage. At the top, there is a navigation bar with links for HOME, VIDEOS, MEGAPRIMERS, HACKERCON VIDEOS, NEWSLETTER, CERTIFICATIONS, DISCUSSION FORUMS, and TOOLS. A search bar is located on the left. The main content area is divided into three columns: LATEST VIDEOS, SECURITYTUBE ORIGINALS, and HACK OF THE DAY. Each column contains several video thumbnails with titles and view counts. For example, the first video in the LATEST VIDEOS column is titled 'Bideslowa 2015 Track: Secure Process Isolation With Docker By Greg Rice' and has 1129 views. The HACK OF THE DAY section features a video titled 'Hack Of The Day 13: Remote Shellcode Launcher: Testing Shellcode Over A Network' with 55278 views.

The screenshot shows the Pentester Academy website homepage. At the top, there is a navigation bar with links for TOPICS, PRICING, WHY SUBSCRIBE, TESTIMONIALS, and a MEMBER ACCESS button. A search bar is located on the left. The main content area features a large video player with the title 'Pentester Academy Introduction' and a play button. To the right of the video player, there is a headline 'Revolutionizing Infosec Training' and a sub-headline 'Highly Technical, Hands-on, Affordable'. Below the headline, there is a 'Start Learning Today!' button. The bottom section is titled 'Latest Videos' and contains four video thumbnails with titles and descriptions. The first video is 'Hostapd: WPA/WPA2 PSK AP In Wi-Fi Security and Pentesting'. The second is 'Hardware Write Blocking Part 3: Host Enumeration in USB Forensics and Pentesting'. The third is 'Hostapd: WEP AP in Wi-Fi Security and Pentesting'. The fourth is 'Hardware Write Blocking Part 2: Threads and Helpers in USB Forensics and Pentesting'.

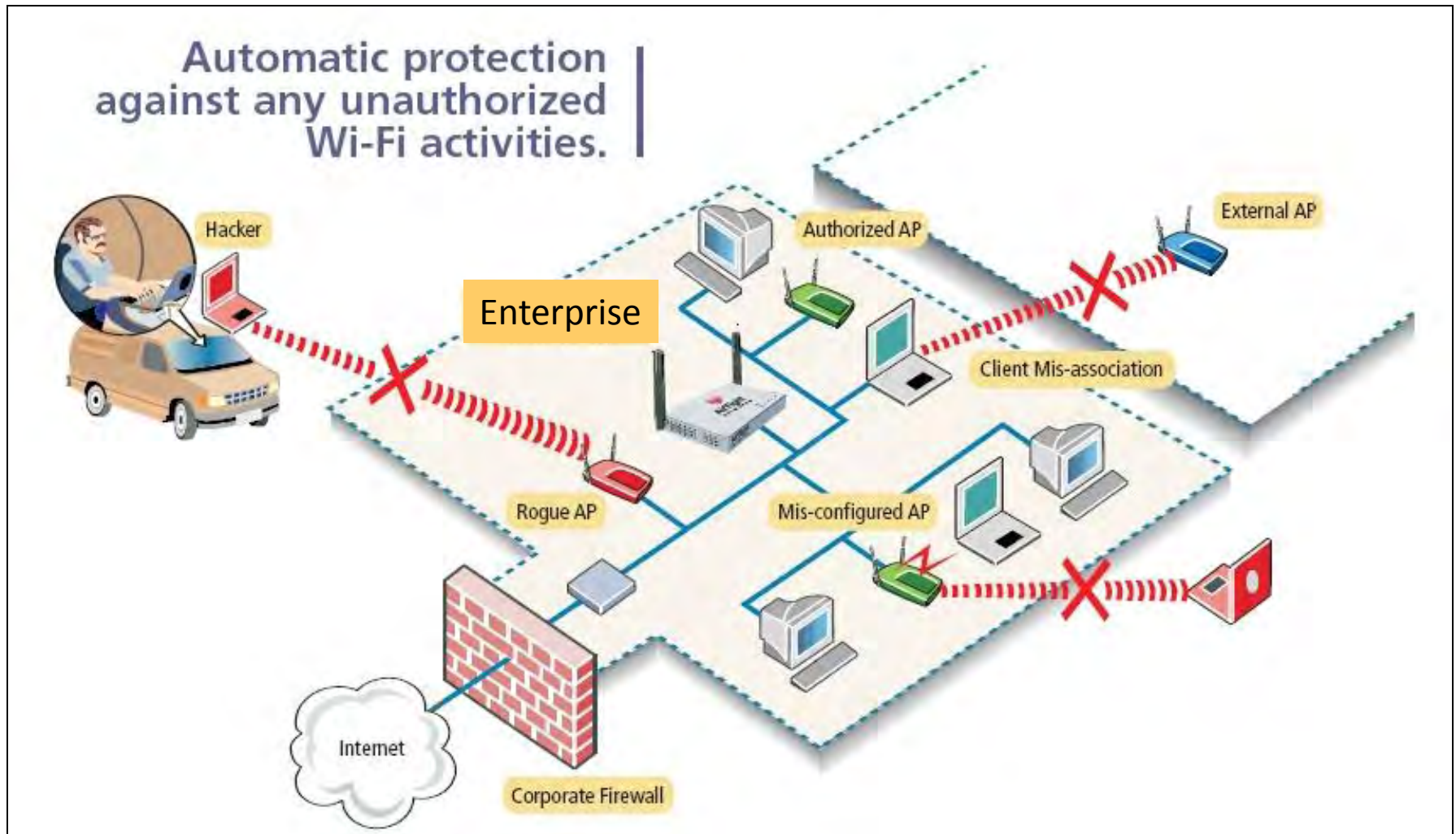
# Motivation



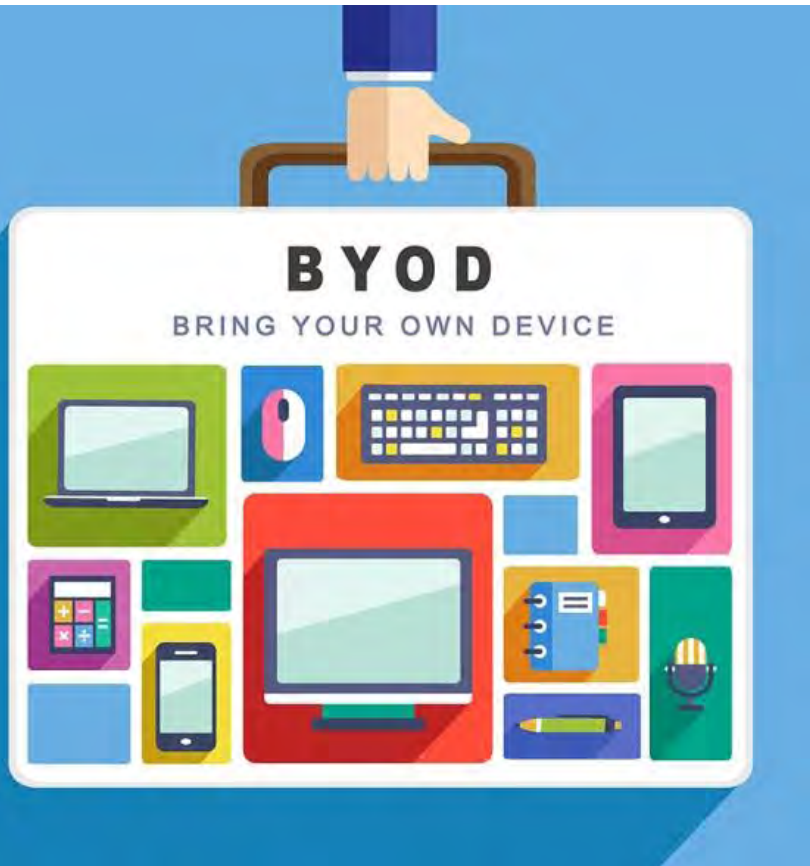
- Attack! Attack! Attack!
- Defense?
- Important problem?
- Solution viable?



# 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)

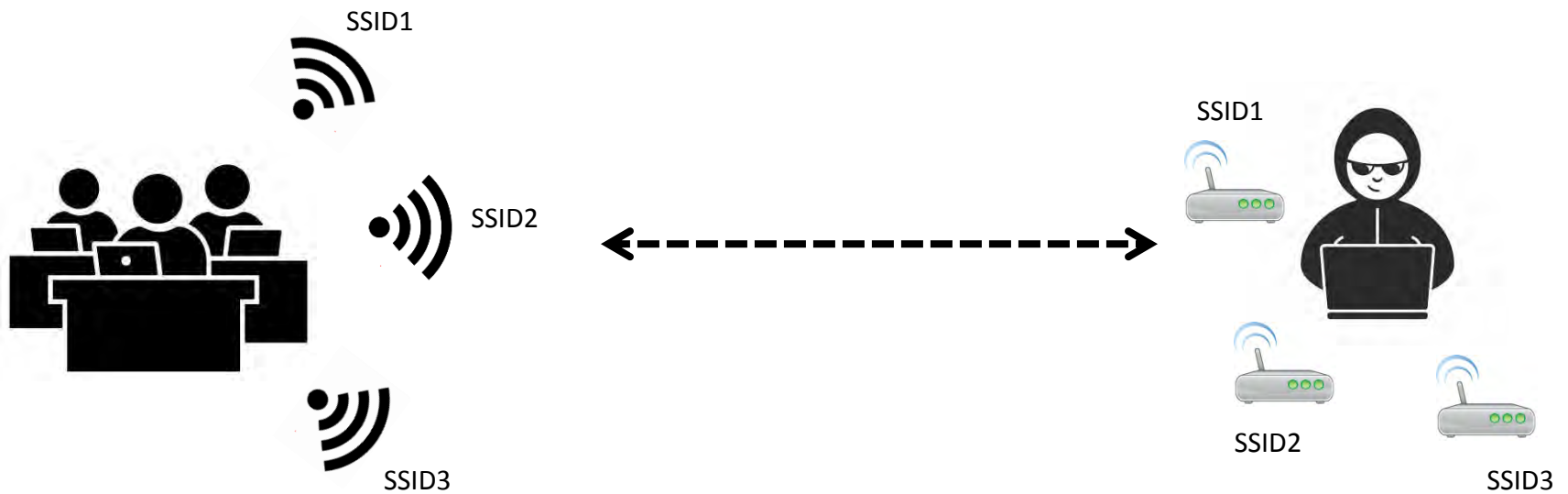
# Wi-Fi Client Attack Surface



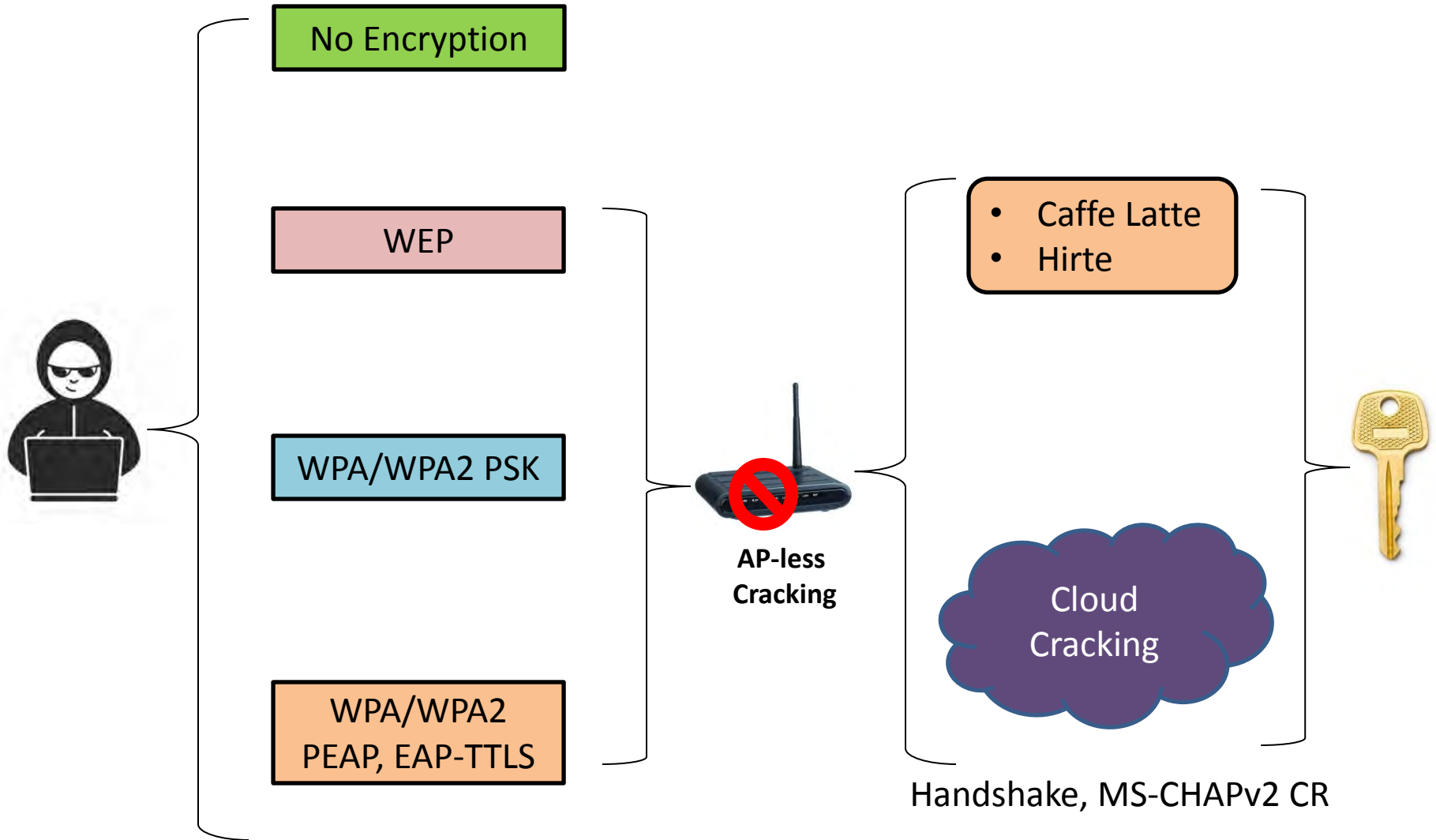
- Honeypots
  - AP-less WEP/WPA/WPA2 Cracking
- Evil Twins
- Mis-Associations
- Hosted Network Backdoors
- ...



# Typical Attack



# AP-less Cracking



# Where are you SAFE? Nowhere!!!



# Hijack Wi-Fi == Hijack Layer 2



**Traffic Monitoring**



**DNS Hijacking**



**SSL MITM**



**Application Attacks**

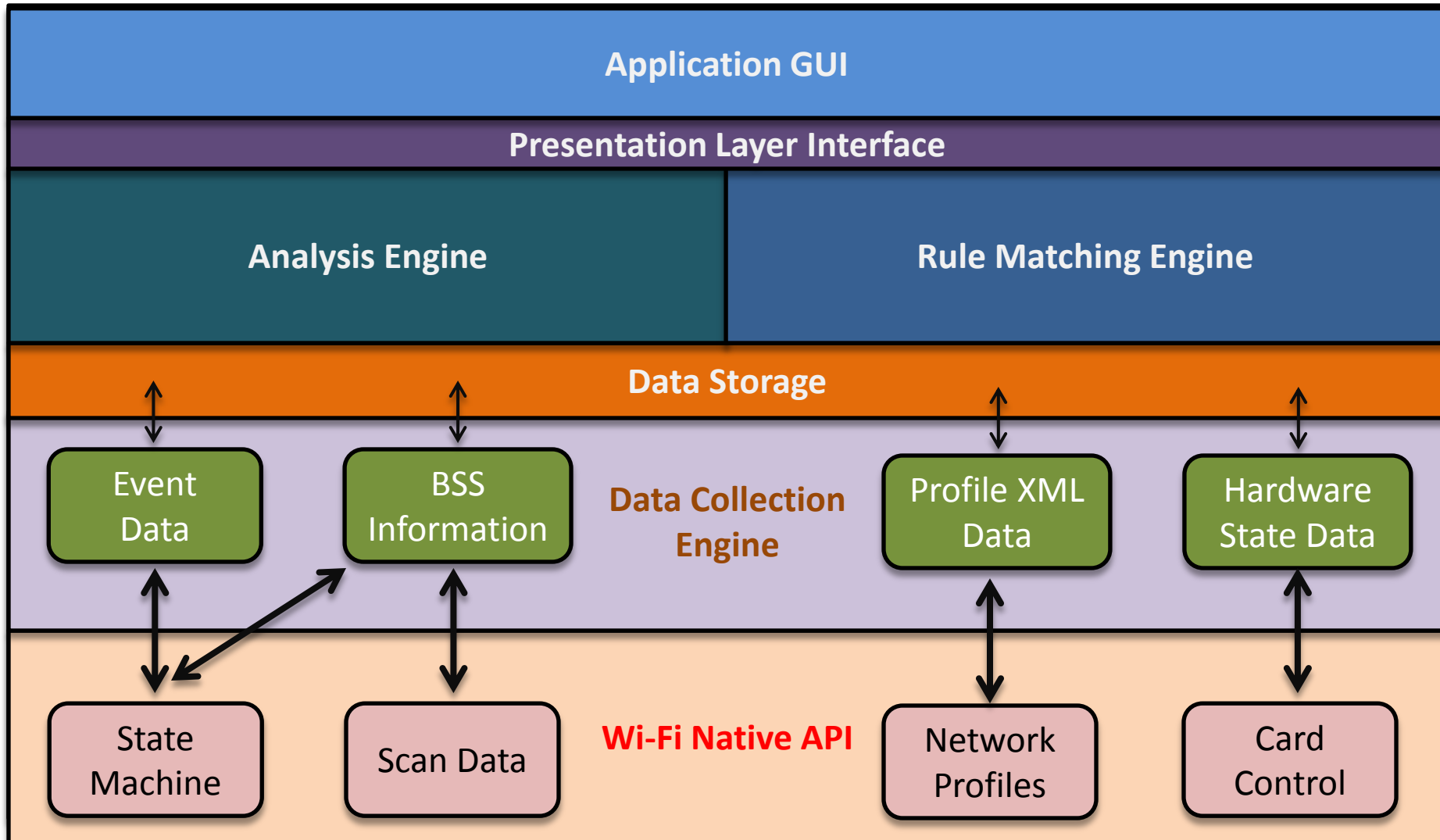


# Defining the Scope

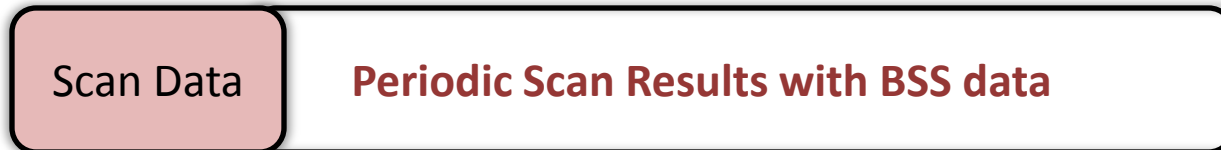


- Windows Endpoints
  - No custom hardware or drivers
- Detect Honeypot creation Tools
- Firewall like Rule Creation
  - “Allow”, “Deny”
- Monitoring Wi-Fi state machine
- Detect Wi-Fi backdoors

# Architecture Block Diagram



# Wi-Fi Native API



# 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>
```



# Demo – Data Sources

Chellam - a Wi-Fi Firewall for Windows

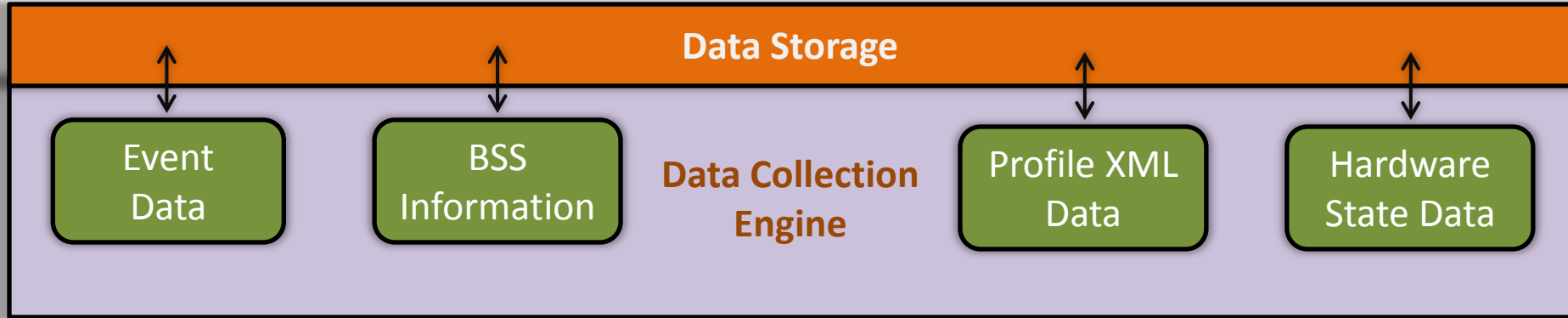
Dashboard Networks Firewall Alerts Profiles Settings Logs

WLAN Auto-Config Event Selection (Expert Mode)

Event	<input checked="" type="checkbox"/> Logging Enabled	<input type="checkbox"/> Alerts Enabled	<input type="checkbox"/> Connection Logging	<input type="checkbox"/> Scan Stats	Info
wlan_notification_acm_autoconf_enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Autoconfigur
wlan_notification_acm_autoconf_disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Autoconfigur
wlan_notification_acm_background_scan_enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Background s
wlan_notification_acm_background_scan_disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Background s
wlan_notification_acm_bss_type_change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The BSS type
wlan_notification_acm_power_setting_change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The power se
wlan_notification_acm_scan_complete	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A scan for ne
wlan_notification_acm_scan_fail	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A scan for coi
wlan_notification_acm_connection_start	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A connection
wlan_notification_acm_connection_complete	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A connection
wlan_notification_acm_connection_attempt_fail	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A connection
wlan_notification_acm_filter_list_change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A change in t
wlan_notification_acm_interface_arrival	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A wireless LA
wlan_notification_acm_interface_removal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A wireless LA
wlan_notification_acm_profile_change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A change in a
wlan_notification_acm_profile_name_change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A profile nam
wlan_notification_acm_profiles_exhausted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All profiles w

Done

# Data Collection and Storage



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

# Demo – SQLITE DB Data

The screenshot shows the DB Browser for SQLite application window. The title bar indicates the database path: C:/Users/Vivek/AppData/Roaming/BSIS/WiFi-IDS/log/wifievts.db. The interface includes a menu bar (File, Edit, View, Help) and a toolbar with options like 'New Database', 'Open Database', 'Write Changes', and 'Revert Changes'. The main area is divided into tabs: 'Database Structure', 'Browse Data', 'Edit Pragas', and 'Execute SQL'. The 'Browse Data' tab is active, showing a table named 'wlan\_scan\_results'. The table has 11 columns: row\_id, tification\_row, ssid, phy\_id, bssid, bss\_type\_id, rssi, nel\_center\_frec, rates\_string, and i. The first row is highlighted in blue. Below the table, there are navigation controls including 'Go to:' and a text input field containing '1'. The status bar at the bottom right shows 'UTF-16le'.

row_id	tification_row	ssid	phy_id	bssid	bss_type_id	rssi	nel_center_frec	rates_string	i
1	1	MOVISTAR_18D9	2	F8:8E:85:D9:...	1	-92	2437000	1; 2; 5.5; 11; ...	SSID: MOV
2	2	ONO9297	1	00:01:38:F2:...	1	-106	2412000	1; 2; 5.5; 11; ...	SSID: ONO
3	3	ONO0702	1	00:01:38:F2:...	1	-104	2412000	1; 2; 5.5; 11; ...	SSID: ONO
4	4	JAZZTEL_C561	1	64:68:0C:81:...	1	-107	2462000	1; 2; 5.5; 11; ...	SSID: JAZZ
5	5	MOVISTAR_455C	2	8C:0C:A3:37:...	1	-112	2462000	1; 2; 5.5; 11; ...	SSID: MOV
6	6	wifi_10	1	72:68:0C:81:...	1	-108	2462000	1; 2; 5.5; 11; ...	SSID: wifi_1
7	7	WLAN_7432	2	00:1A:2B:A:...	1	-109	2442000	1; 2; 5.5; 11; ...	SSID: WLA
8	8	WLAN_C7A1	2	00:1A:2B:A:...	1	-106	2442000	1; 2; 5.5; 11; ...	SSID: WLA
9	9	hPozuelo	1	00:1D:45:9E:...	1	-93	2472000	1; 2; 5.5; 6; 9...	SSID: hPoz
10	10	SAIENBRUS	2	18:17:25:33:...	1	-101	2472000	1; 2; 5.5; 11; ...	SSID: SAIE

# Rule Matching and Analysis

Analysis Engine

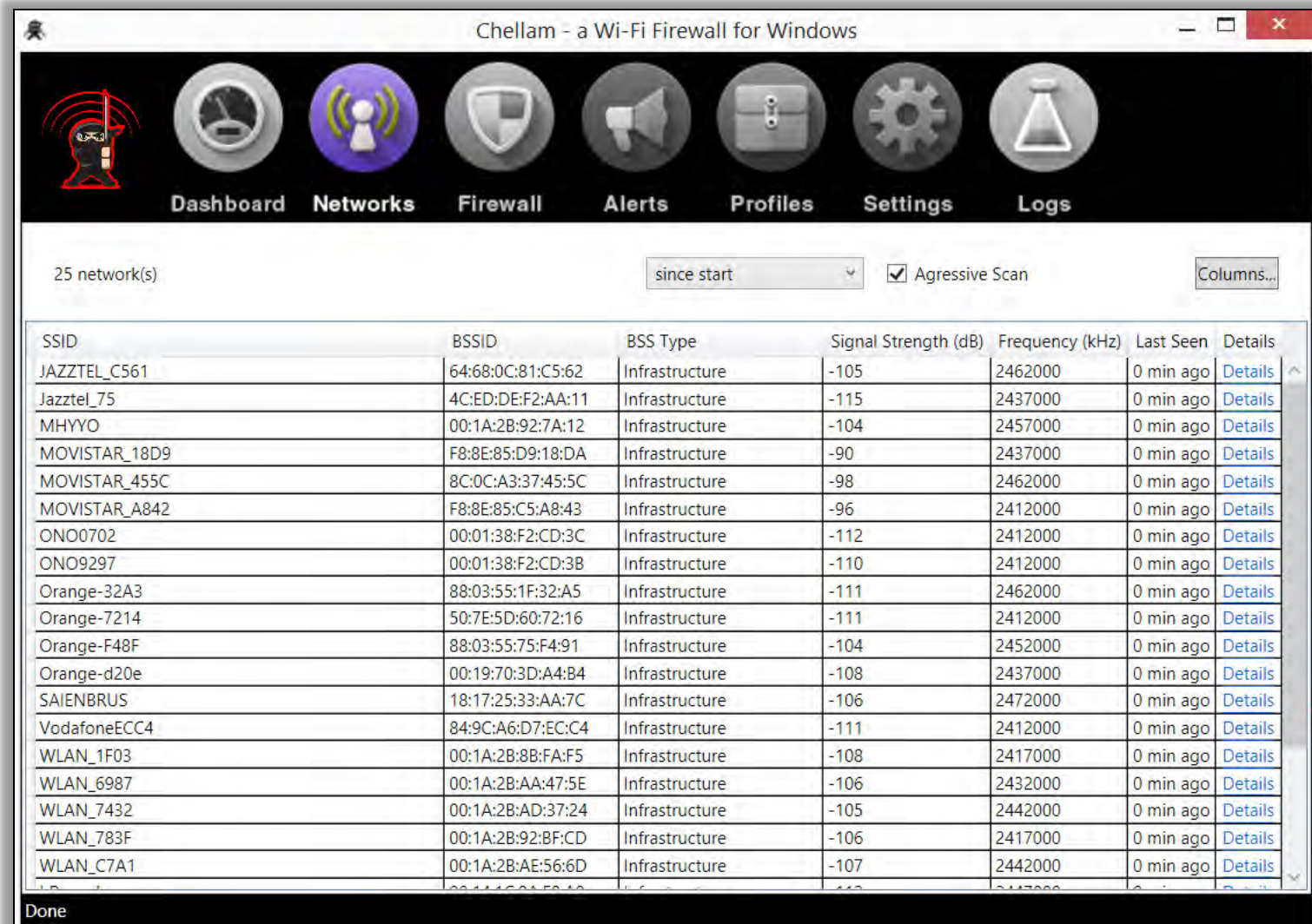
Rule Matching Engine

Data Storage

- 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



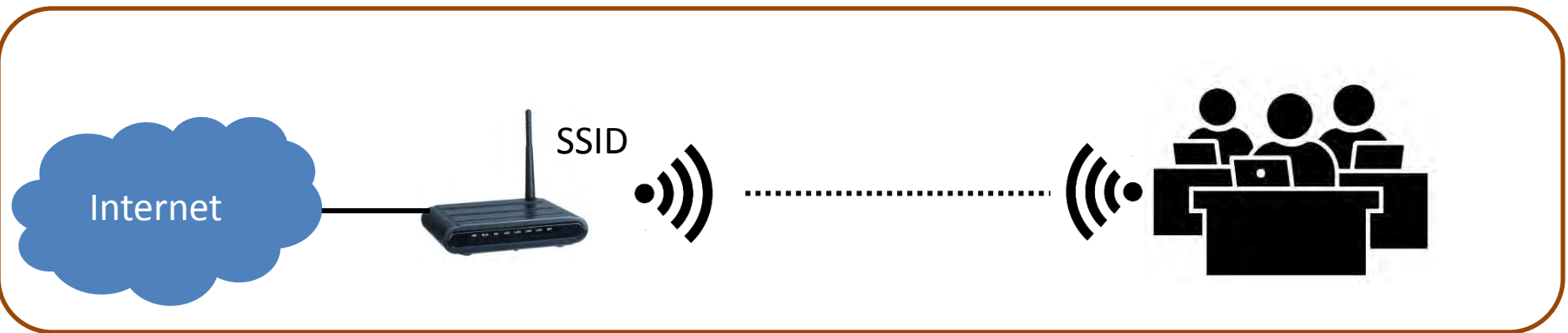
# Demo – Monitoring and Event Detection



The screenshot displays the Chellam - a Wi-Fi Firewall for Windows application interface. The window title is "Chellam - a Wi-Fi Firewall for Windows". The interface features a navigation bar with icons for Dashboard, Networks, Firewall, Alerts, Profiles, Settings, and Logs. Below the navigation bar, there is a status bar showing "25 network(s)", a dropdown menu set to "since start", a checked "Agressive Scan" checkbox, and a "Columns..." button. The main area contains a table of detected networks with the following columns: SSID, BSSID, BSS Type, Signal Strength (dB), Frequency (kHz), Last Seen, and Details. The table lists 25 networks, all of which are Infrastructure type and were last seen 0 min ago. The SSIDs include JAZZTEL\_C561, Jazztel\_75, MHYYO, MOVISTAR\_18D9, MOVISTAR\_455C, MOVISTAR\_A842, ONO0702, ONO9297, Orange-32A3, Orange-7214, Orange-F48F, Orange-d20e, SAIENBRUS, VodafoneECC4, WLAN\_1F03, WLAN\_6987, WLAN\_7432, WLAN\_783F, and WLAN\_C7A1. The signal strengths range from -90 dB to -115 dB, and frequencies range from 2412000 kHz to 2462000 kHz. A "Done" status is visible at the bottom left of the application window.

SSID	BSSID	BSS Type	Signal Strength (dB)	Frequency (kHz)	Last Seen	Details
JAZZTEL_C561	64:68:0C:81:C5:62	Infrastructure	-105	2462000	0 min ago	<a href="#">Details</a>
Jazztel_75	4C:ED:DE:F2:AA:11	Infrastructure	-115	2437000	0 min ago	<a href="#">Details</a>
MHYYO	00:1A:2B:92:7A:12	Infrastructure	-104	2457000	0 min ago	<a href="#">Details</a>
MOVISTAR_18D9	F8:8E:85:D9:18:DA	Infrastructure	-90	2437000	0 min ago	<a href="#">Details</a>
MOVISTAR_455C	8C:0C:A3:37:45:5C	Infrastructure	-98	2462000	0 min ago	<a href="#">Details</a>
MOVISTAR_A842	F8:8E:85:C5:A8:43	Infrastructure	-96	2412000	0 min ago	<a href="#">Details</a>
ONO0702	00:01:38:F2:CD:3C	Infrastructure	-112	2412000	0 min ago	<a href="#">Details</a>
ONO9297	00:01:38:F2:CD:3B	Infrastructure	-110	2412000	0 min ago	<a href="#">Details</a>
Orange-32A3	88:03:55:1F:32:A5	Infrastructure	-111	2462000	0 min ago	<a href="#">Details</a>
Orange-7214	50:7E:5D:60:72:16	Infrastructure	-111	2412000	0 min ago	<a href="#">Details</a>
Orange-F48F	88:03:55:75:F4:91	Infrastructure	-104	2452000	0 min ago	<a href="#">Details</a>
Orange-d20e	00:19:70:3D:A4:B4	Infrastructure	-108	2437000	0 min ago	<a href="#">Details</a>
SAIENBRUS	18:17:25:33:AA:7C	Infrastructure	-106	2472000	0 min ago	<a href="#">Details</a>
VodafoneECC4	84:9C:A6:D7:EC:C4	Infrastructure	-111	2412000	0 min ago	<a href="#">Details</a>
WLAN_1F03	00:1A:2B:8B:FA:F5	Infrastructure	-108	2417000	0 min ago	<a href="#">Details</a>
WLAN_6987	00:1A:2B:AA:47:5E	Infrastructure	-106	2432000	0 min ago	<a href="#">Details</a>
WLAN_7432	00:1A:2B:AD:37:24	Infrastructure	-105	2442000	0 min ago	<a href="#">Details</a>
WLAN_783F	00:1A:2B:92:BF:CD	Infrastructure	-106	2417000	0 min ago	<a href="#">Details</a>
WLAN_C7A1	00:1A:2B:AE:56:6D	Infrastructure	-107	2442000	0 min ago	<a href="#">Details</a>

# 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)

**802.11  
(pre connect)**

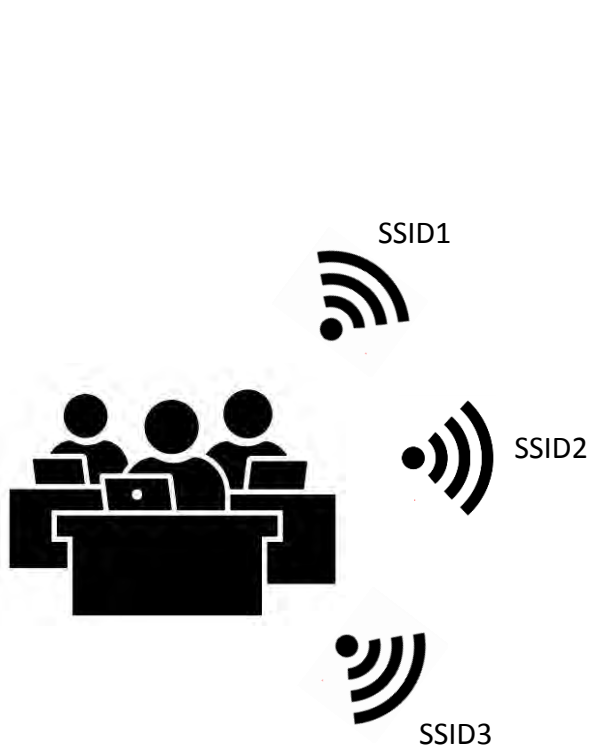
- Neighboring Access Points
- AP details as above

- IP, Gateway
- DNS, ARP cache

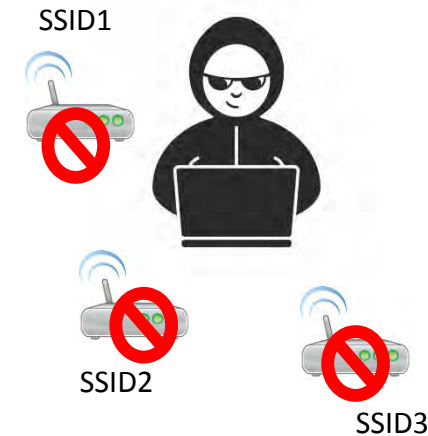
**IP & Above  
(post connect)**

- Subnet scan
- OS and service scan

# 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)

The screenshot shows the Chellam - a Wi-Fi Firewall for Windows interface. The top navigation bar includes icons for Dashboard, Networks, Firewall, Alerts, Profiles, Settings, and Logs. The main area displays a list of 33 networks. The 'Airbase-AP' network is highlighted in red, indicating it is the detected attack tool. An alert box is overlaid on the right side of the interface, providing details about the detected network.

33 network(s) since start  Aggressive Scan Columns...

SSID	BSSID	BSS Type	Signal Strength (dB)	Frequency (kHz)	Last Seen	Details
<b>Airbase-AP</b>	<b>E8:DE:27:20:60:11</b>	<b>Infrastructure</b>	<b>-58</b>	<b>2412000</b>	<b>0 min ago</b>	<a href="#">Details</a>
JAZZTEL_C561	64:68:0C:81:C5:62	Infrastructure	-106	2462000	0 min ago	<a href="#">Details</a>
Jazztel_75	4C:ED:DE:F2:AA:11	Infrastructure	-110	2437000	0 min ago	<a href="#">Details</a>
MHYYO	00:1A:2B:92:7A:12	Infrastructure	-105	2457000	0 min ago	<a href="#">Details</a>
MOVISTAR_18D9	F8:8E:85:D9:18:DA	Infrastructure	-92	2437000	0 min ago	<a href="#">Details</a>
MOVISTAR_455C	8C:0C:A3:37:45:5C	Infrastructure	-102	2462000	0 min ago	<a href="#">Details</a>
MOVISTAR_5E33	F8:8E:85:40:5E:34	Infrastructure	-116	2412000	0 min ago	<a href="#">Details</a>
MOVISTAR_A842	F8:8E:85:C5:A8:43	Infrastructure	-94	2412000	0 min ago	<a href="#">Details</a>
ONO0702	00:01:38:F2:CD:3C	Infrastructure	-108	2412000	0 min ago	<a href="#">Details</a>
ONO9297	00:01:38:F2:CD:3B	Infrastructure	-110	2412000	0 min ago	<a href="#">Details</a>
Orange-32A3	88:03:55:1F:32:A5	Infrastructure	-109			
Orange-7214	50:7E:5D:60:72:16	Infrastructure	-111			
Orange-F48F	88:03:55:75:F4:91	Infrastructure	-99			
Orange-d20e	00:19:70:3D:A4:B4	Infrastructure	-109			
Qlik	08:86:3B:D8:FB:22	Infrastructure	-111			
SAIENBRUS	18:17:25:33:AA:7C	Infrastructure	-104			
VodafoneECC4	84:9C:A6:D7:EC:C4	Infrastructure	-109			
WLAN_0B6F	00:1A:2B:A8:F9:D5	Infrastructure	-112			
WLAN_1F03	00:1A:2B:8B:FA:F5	Infrastructure	-106			
WLAN_2007	00:1A:2B:11:47:55	Infrastructure	-107			

**Attack Tool Detected!**

**Network:** Airbase-AP

**Message**

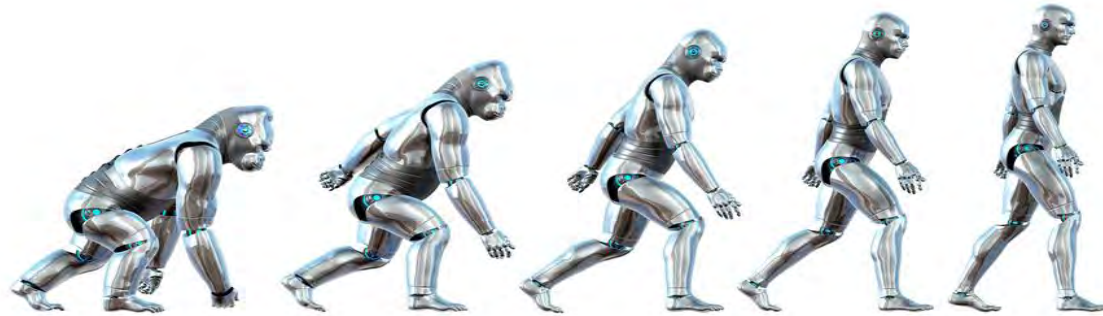
This network seems to have been created by an Attack Tool which creates Fake Access Points! Do not connect to this network.

Dismiss Alert

# 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?

