CENSUS
IT Security Works

GETTING THE MOST OUT OF EVIL TWIN

wifiphisher

B-SIDES ATHENS 2016

GEORGE CHATZISOFRONIOU (@_sophron) sophron@census-labs.com www.census-labs.com

> WHOAMI

- Security Engineer at CENSUS S.A.
  - Cryptography, Wi-Fi hacking, web security and network security
- Academic research
  - Design of Privacy-enabling / Anonymity-providing protocols
- Lead author of Wifiphisher
  - First introduced at BSidesLondon 2015

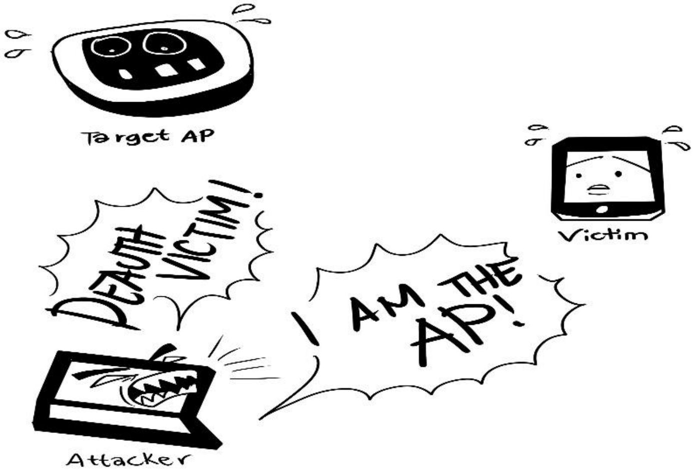
> AGENDA

- Evil Twin Attack
- Wi-Fi DoS Attacks
- Phishing Scenarios
- Wifiphisher

> EVIL TWIN ATTACK

> Evil Twin

- A rogue Wi-Fi AP spoofs a legitimate in order to gather personal or corporate data.
- Common attack vector in Wi-Fi environments

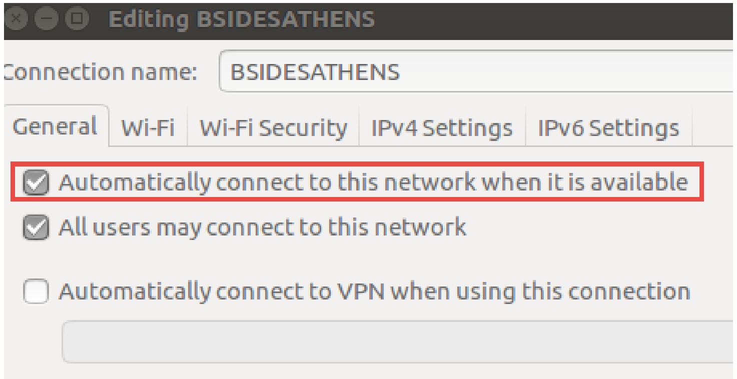


> Getting the Right Equipment

- Essential step for a successful Evil Twin attack
- Wireless card rule: the more power gain, the better
- Ideally, two different attack points:
  - One for spawning the rogue AP
    - May be placed inside the target infrastructure equipped with an omnidirectional antenna, well hidden from prying eyes, low battery consumption
  - One for DoS attacks
    - May be from distant using a directional antenna

> AUTO-CONNECT Flag

- Allows a station to add Wi-Fi networks in its PNL (Preferred Network List) so it can automatically connect to them later
  - Typical usability over security feature
  - Enabled by default in all modern implementations of network managers
- An effective Evil Twin almost always involve the exploitation of this flag



Editing BSIDESATHENS

Connection name: BSIDESATHENS

☑ Automatically connect to this network when it is available

☑ All users may connect to this network

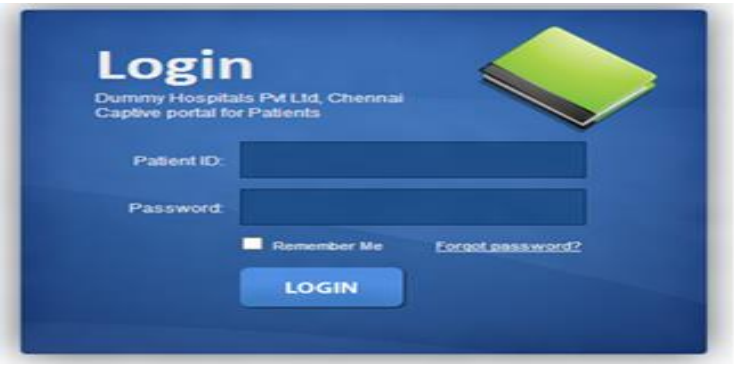
□ Automatically connect to VPN when using this connection

> AP Selection

- Stations will automatically associate with the AP that:
  1) Broadcasted an ESSID that exists in its PNL
  2) From the ones that satisfy (1), the AP offers the best signal
- What is really added in the PNL is an association of ESSID and Encryption Type
  – PNL += (ESSID, Encryption)
  – Encryption = (Open|WEP|WPA|WPA2)
- Attacker needs to replicate both

> Against Open Networks

- Usually employed along with a captive portal mechanism
- Common in airports, hotels, and coffee shops
- Vulnerable to Evil Twin by default
  - Both ESSID and Encryption Type (Open) can easily be replicated
  - Assuming stronger signal, victims will automatically connect to the rogue AP



Login

Dummy Hospitals Pvt Ltd, Chennai
Captive portal for Patients

> Against WPA/WPA2 with Known or Compromised PSK

- Common in conferences or other infrastructures where members are dynamically joining and leaving the network
- Authentication relies on a PSK
  - Secret is held by all parties. Can be compromised at one end without the knowledge of anyone at the other endpoints.
- As in open setups, these are vulnerable to Evil Twin
  - Both ESSID and Encryption can be replicated
  - Assuming stronger signal, victims will automatically connect to the rogue AP

> Against WPA-Enterprise

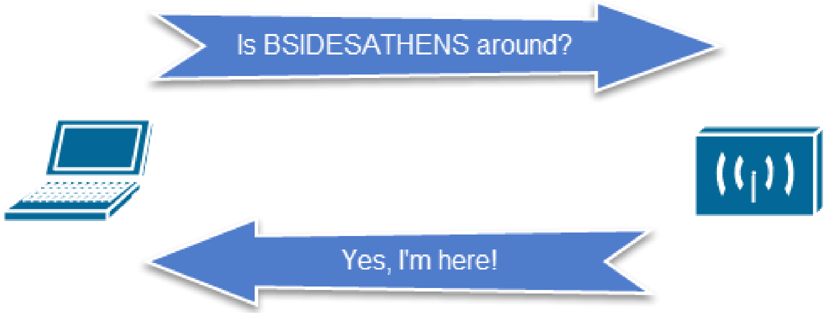
- Widely used in large corporations
- When not authenticating the AP, corporate setups are vulnerable to Evil Twin
  - Yes, PEAP/EAP-TLS is not vulnerable
- Offline brute-force of the captured challenge-response.

> Against WPA/WPA2 with unknown PSK:

- By using a different random shared key the connection with a rogue access point won’t succeed
  - The access point can’t decrypt packets from the client and vice versa
- Downgrade attacks usually need victim interaction

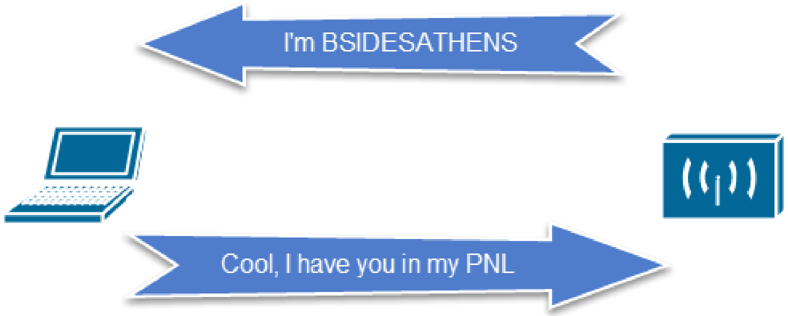
> KARMA

- Featured by Wi-Fi Pineapple
- Listen to probe request frames
  - If the probe request frame is intended for an open network, spawn that network
  - Victims will auto-connect to the rogue network
  - Needs to have already stored open networks in the PNL



> KARMA

- Most network managers have taken countermeasures:
  1) Devices will wait for the correct beacon frame before sending the probe request frame
  2) If they do send probe request frames arbitrarily, the destination address will be the broadcast address (i.e. no ESSID leak)

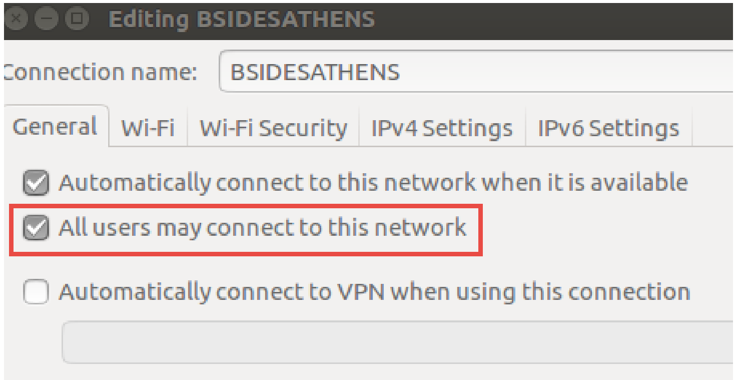


> How about guessing the ESSID?

- Things are easier if we know an open network that the victim has connected to in the past.
  - E.g. victim had visited BSidesLondon conference.
  - We know that BSidesLondon had an open network called “BSidesLondon”.
  - Assuming he has the default settings, “BSidesLondon” ESSID will make him automatically connect to the rogue network.

> “Available to all system users” flag

- PNL becomes global across users
  - Increases the attack surface



Editing BSIDESATHENS

Connection name: BSIDESATHENS

☑ Automatically connect to this network when it is available

☑ All users may connect to this network

□ Automatically connect to VPN when using this connection

> WIFI DOS ATTACKS

> Deauthentication Attack

- Leverage DEAUTH frame (transmitted unencrypted)
  - Sent when all communication is terminated
  - Kick out a client by forging DEAUTH frames
    - 1 from the AP to the client
    - 1 from the client to the AP
    - 1 from the AP to the broadcast address

> Probe Response Flooding

- After de-authenticating a station, keep answering to probe request frames
  - Answer will be equivalent to “Sorry, your PSK is incorrect”
- Victim will stay disconnected
  - Chances are the victim will manually interact with the network manager
  - Useful to downgrade attacks where auto-connections are not possible

> PHISHING SCENARIOS

> Phishing Scenarios

- Typical phishing scenarios may take place
  - E.g. Captive portals or social network pages using OAuth login mechanism
- It’s more interesting to bridge information from beacon frames to templates
  - Beacon frames can be used for information gathering (think automatic template generation).

> Identifying the Vendor

- Beacon frames include the MAC address of the AP
- Display fake messages coming from the router
  - E.g. asking the WPA/WPA2 PSK due to a router firmware upgrade.

> Imitating the Network Manager

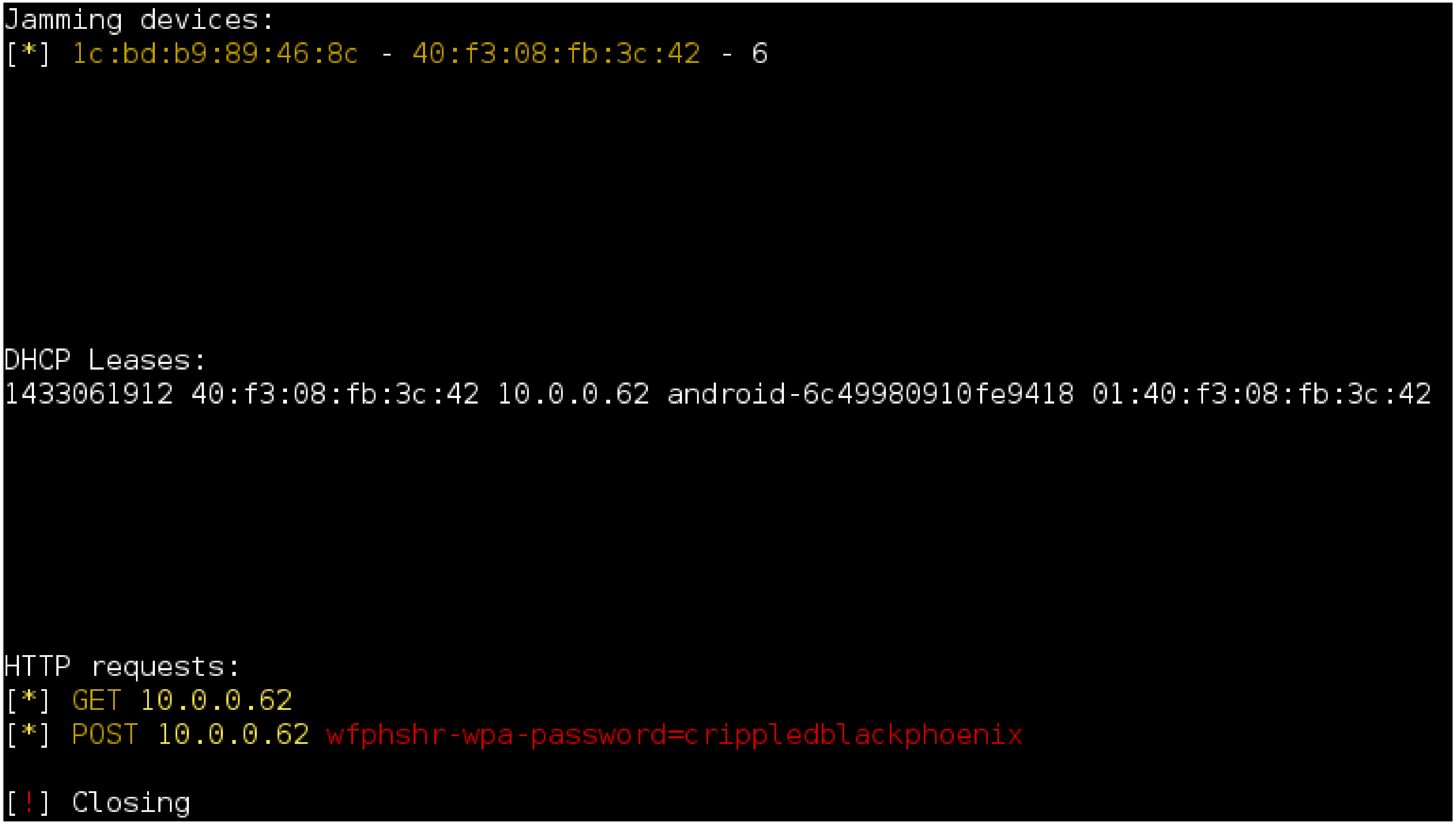
1. Show the “Connection Failed” page.
   - Customize this accordingly based on the User-Agent header
2. Display a network manager asking for the WPA password of the target network
   - Again, User-Agent header may tell us OS details
3. Fill the network manager with around networks

> WIFIPHISHER

> Wifiphisher

- Automates Evil Twin for different cases
  - Creation of rogue AP + Wi-Fi Jamming
- Heavily used by Wi-Fi hacking community
  - ~80 downloads per day
- Current stable release: 1.1
  - Release 1.2 coming soon!

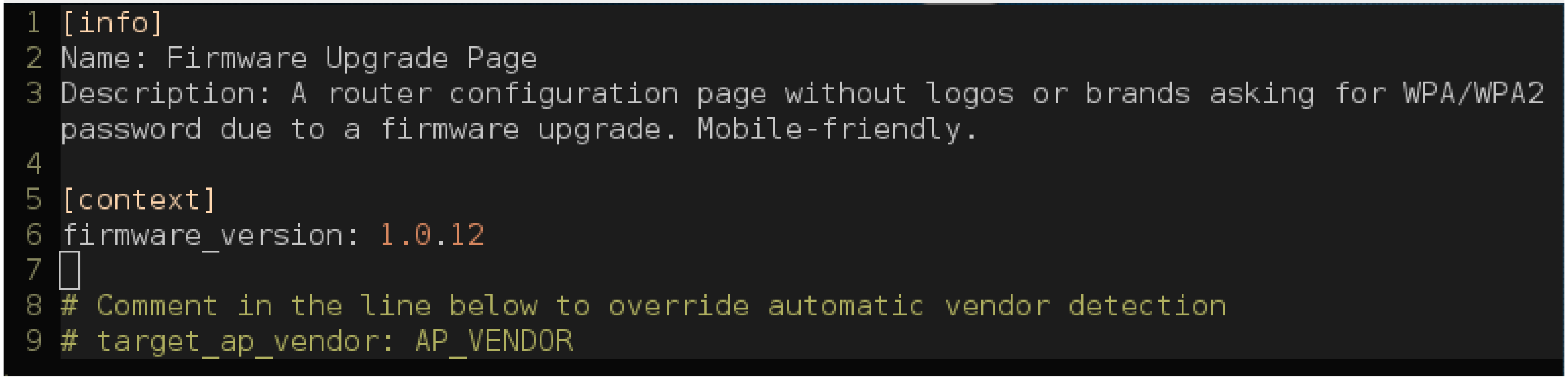
> Wifiphisher



```
Jamming devices:
[*] 1c:bd:b9:89:46:8c - 40:f3:08:fb:3c:42 - 6









DHCP Leases:
1433061912 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42









HTTP requests:
[*] GET 10.0.0.62
[*] POST 10.0.0.62 wfphshr-wpa-password=crippledblackphoenix

[!] Closing
```

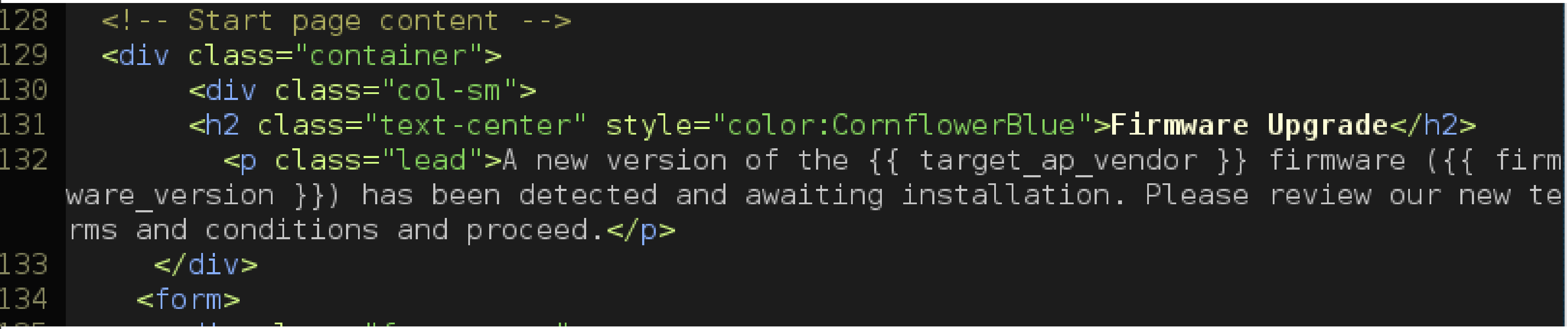
> Template Customization

Phishing page designers provide a config.ini file that may be filled by the user



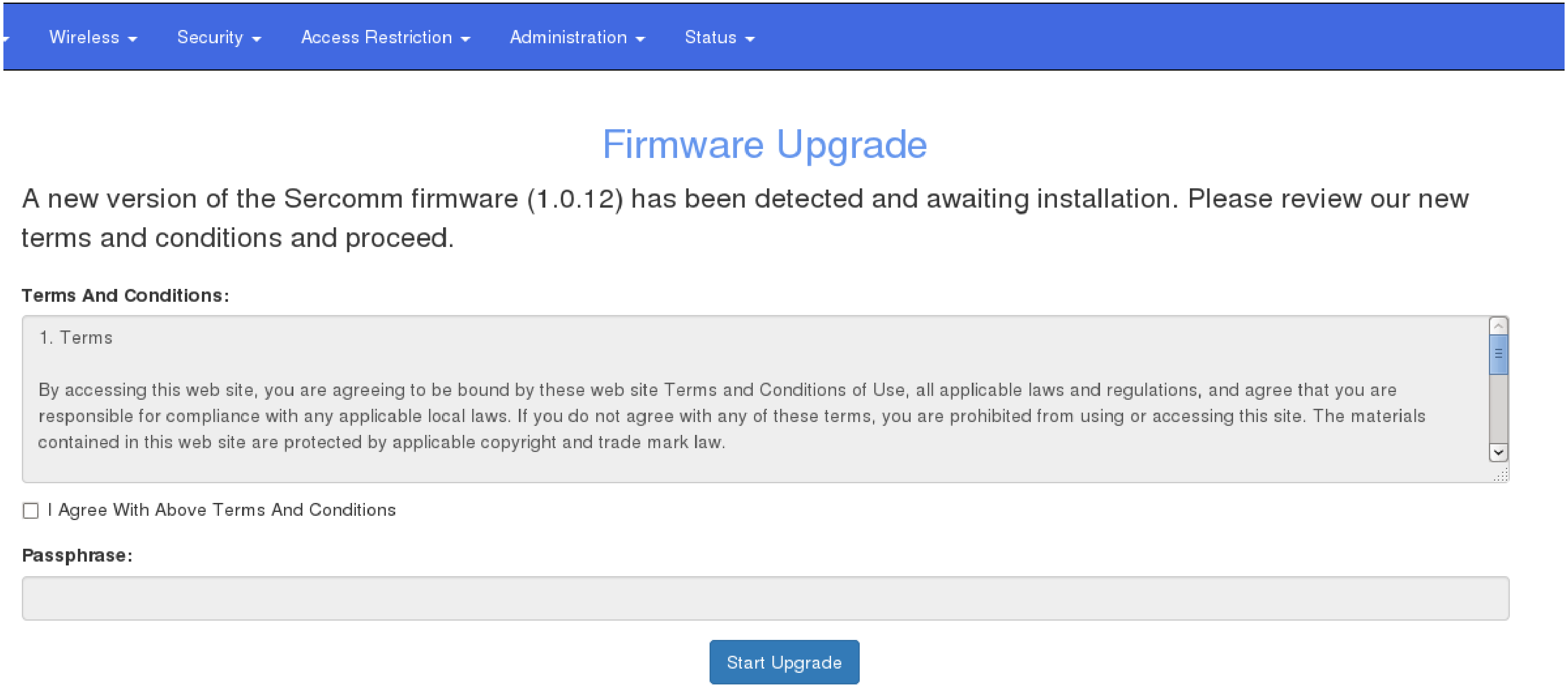
```
[info]
Name: Firmware Upgrade Page
Description: A router configuration page without logos or brands asking for WPA/WPA2 password due to a firmware upgrade. Mobile-friendly.

[context]
firmware_version: 1.0.12

# Comment in the line below to override automatic vendor detection
# target_ap_vendor: AP_VENDOR
```

> Template Customization



```
  <!-- Start page content -->
  <div class="container">
       <div class="col-sm">
       <h2 class="text-center" style="color:CornflowerBlue">Firmware Upgrade</h2>
         <p class="lead">A new version of the {{ target_ap_vendor }} firmware ({{ firmware_version }}) has been detected and awaiting installation. Please review our new terms and conditions and proceed.</p>
     </div>
    <form>
```

> Template Customization



Firmware Upgrade

A new version of the Sercomm firmware (1.0.12) has been detected and awaiting installation. Please review our new terms and conditions and proceed.

Terms And Conditions:

1. Terms

By accessing this web site, you are agreeing to be bound by these web site Terms and Conditions of Use, all applicable laws and regulations, and agree that you are responsible for compliance with any applicable local laws. If you do not agree with any of these terms, you are prohibited from using or accessing this site. The materials contained in this web site are protected by applicable copyright and trade mark law.

□ I Agree With Above Terms And Conditions

Passphrase:

> Wireless cards communication using PyRIC

- Most Python wireless tools rely on Linux command lines tools
  - Newer iw versions may break the parser
- PyRIC is a Python library that allows identification and manipulation of the available network cards by communicating with the kernel
- https://github.com/wraith-wireless/PyRIC

> New templates

- Messages sourcing from browser
  - E.g. Plugin updates
- Imitating the OS
  - Grabbing the PSK
- OAuth login page

> Development team

- Mature open source community
- Contributors: Brian Smith, Leonidas Vrachnis, Dionysis Zindros, Kostis Karantias, Stergios Kolios and many more!
- Hackathons!
- Always looking for new members to join the crew ☺

Thank you!

CENSUS
IT Security Works