SNEAP: A Social Network-Enabled EAP Method
No More Open Hotspots

Aldo Cassola,[*] Tao Jin,[*] Harsh Kumar,[*] Guevara Noubir, Kamal Sharma[*]
College of Computer and Information Science, Northeastern University
Email: {acassola, taojin, harsh4a, noubir, kamal577}@ccs.neu.edu

1. Motivation and Goals

As mobile devices evolve, end users have ever increasing demand for ubiquitous network access. WiFi, being now commonplace, has the potential to fulfill this demand. Apart from WiFi hotspots deployed by ISPs, home users start showing interest in sharing bandwidth with others (e.g. Fon [1] bases its business model on users sharing open access points.) However, all existing WiFi sharing approaches are unsecured due to the difficulty of distributing access keys, discouraging potential users. Meanwhile, social networking provides a large scale, well established social graph, which is an attractive candidate for authentication services. Previous work on social networks as authentication mechanisms such as Social WiFi [3] requires users to first register with a third-party server through an open Access Point (AP), which adds an unneeded step to the process, and complicates user management at the third-party.

Our Social Network-Enabled EAP method (SNEAP) integrates the authentication services in social networks with the widely-adopted EAP framework. In addition, the extensibility of EAP and our software-based solution allow easy incremental deployment, and our chosen platform offers broad hardware compatibility.

2. System and Protocol Design

Our system consists of a SNEAP-extended supplicant, AP, Radius server, and a Facebook application. Any AP running our custom OpenWrt [2] firmware can be registered by the owner through our Facebook application to obtain a SNEAP ID, associated with the owner's Facebook profile at the Radius server.

SNEAP authentication consists of two phases shown in Figure 1. In Phase I (steps 1 and 2), the requesting client authenticates the Radius server by setting up a TLS tunnel. After a WPA key exchange, Radius instructs the AP to authorize the client with restricted access, allowing only traffic pertinent to authenticating with the social network. Thus, the client obtains a secure link to the AP early in the process.

Phase II (steps 3 onward) starts with the supplicant opening a browser to authorize our Facebook application to obtain the client's authentication code (AC), which will be used by the Radius server to access his profile. Since Facebook authentication is browser based, our application redirects the AC to a tiny web server integrated into the supplicant, which in turn will forward it to the AP. The AP will send the ⟨AC, SNEAP-ID⟩ pair to the Radius server for friendship verification. Upon success, the Radius server will instruct the AP to instate full access for the client.

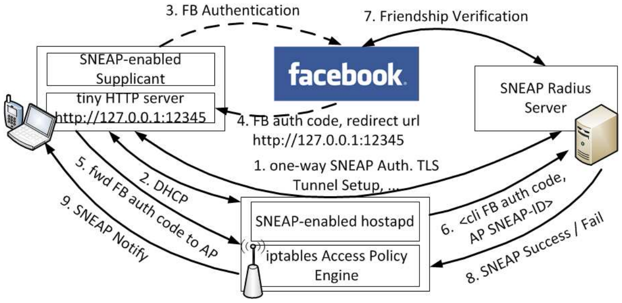
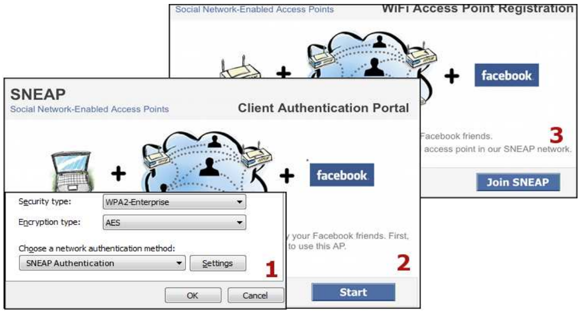

3. FB Authentication
7. Friendship Verification
SNEAP-enabled Supplicant
tiny HTTP server http://127.0.0.1:12345
facebook
SNEAP Radius Server
4. FB auth code, redirect url http://127.0.0.1:12345
1. one-way SNEAP Auth. TLS Tunnel Setup, ...
2. DHCP
5. fwd FB auth code to AP
9. SNEAP Notify
SNEAP-enabled hostapd
iptables Access Policy Engine
6. <cli FB auth code, AP SNEAP-ID>
8. SNEAP Success / Fail

Figure 1: SNEAP Architecture and Flow


Social Network-Enabled Access Points
WiFi Access Point Registration
facebook
Facebook friends.
access point in our SNEAP network.
3
Join SNEAP
SNEAP
Social Network-Enabled Access Points
Client Authentication Portal
facebook
y your Facebook friends. First,
to use this AP.
2
Start
1
OK
Cancel
Settings

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: SNEAP Authentication

Figure 2: 1. supplicant 2. Client Authentication Portal 3. AP Registration Facebook app

The Demonstration

Our demo shows the core functionalities: one-click AP flashing, AP registration, and client authentication.

3. References

[1] *Fon*, http://www.fon.com.
[2] *OpenWrt*, http://www.openwrt.org.
[3] KILBOURN, F., AND ERIKSSON, J. Social WiFi - Leveraging Social Networks for Safe Wi-Fi Sharing. In *MobiCom Demo '10*, ACM.

[*] Students