Providing security for PAWAS

Authors

Universities

1 Introduction to PAWS

This paper is concerned with how to enable secure digital inclusion of underprivileged members of society through ensuring secure access for all to everyday services and benefits that are currently enjoyed by the majority but are typically not accessible to those who come from poorer background and deprived areas. Ensuring that all members of society are able to participate fully in the Digital Economy is a significant step towards improving social equality. We briefly describe PAWS (Public Access WiFi Service), a new Internet access paradigm based on Lowest Cost Denominator Networking (LCD-Net), that makes use of the available unused capacity in home broadband networks and allows Less-than-Best-Effort access to these resources (lower quality service compared to the standard Internet service offered to paid users) to users who are unable to afford paying for the service.

Related initiatives in the past have looked at sharing a user's broadband Internet connection via their wireless connection (for example FON). Although these methods are gaining worldwide acceptance, they are usually viewed as an extension of a user's paid service - PAWS aims to extend this to support free and secure access to users. PAWS takes the approach of community-wide participation, where broadband customers can volunteer to share their high-speed broadband Internet connection for free and in a secure manner with fellow citizens.

2. Security challenges

While PAWS aims to provide free internet services to users, the users access internet over wireless network that they neither own nor can control. We are therefore faced with some interesting security challenges such as:

* Users need to be able to access the internet securely without worrying about the possibility that the sharers’ may eavesdrop on their traffic from their own broadband equipment.
* Users need to reliably secure their own connections without any special training.
* Sharers need to be sure that their own networks and traffic will not be compromised because they are sharing their bandwidth and equipment without having to go through any special training or add new equipment.
* As we assume that large number of users will be vulnerable people coming from deprived areas or having underprivileged background, it is very important to provide better-than average security for them. For example, card fraud, distressing as it is, would cause relatively minor inconvenience to a person of middle-class background but would much more seriously affect PAWS users financial resources and well-being.

We need to ensure that these challenges are resolved before we can provide internet access to PAWS users.

3. Proposal

We propose secure end to end network access over unsecured network infrastructure: more specifically, users connect to sharers’ routers and over them establish a secure tunnel from their end devices to the PAWS VPN service authenticated by RADIUS.

There is a range of other possible solutions but they suffer a range of issues both in terms of limited security and high complexity.

WIFI authentication is not adequate as the user traffic gets forwarded in plaintext after the PAWS router where it can be monitored at the sharer’s router. Additionally existing research shows that WIFI authentication is not sufficiently secure.

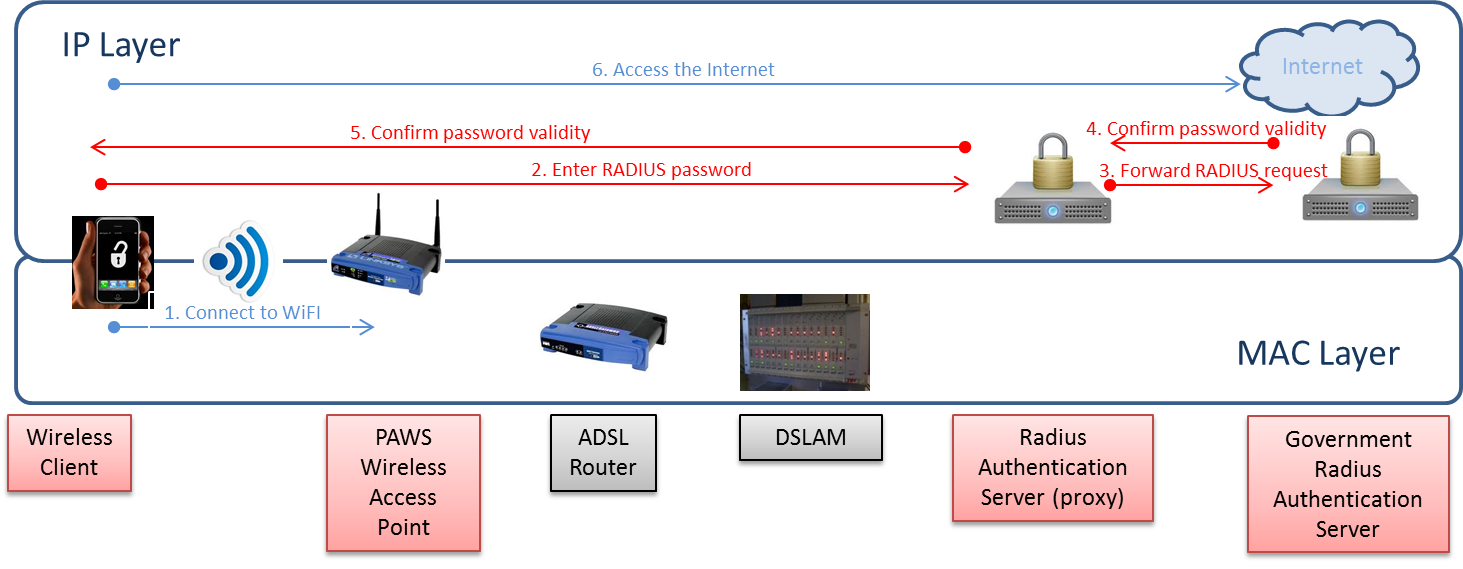
To overcome the shortcomings of WIFI authentication VPN tunnel over WIFI to the wireless access point can be used that provides a better security of the traffic over the wireless connection. This approach, however still suffers from the same vulnerability as the WIFI authentication as the user traffic would still go in plain text through the sharer’s equipment where it can be monitored.

It is also possible to configure VPN tunnel between the PAWS router and the PAWS VPN service that can be used in conjunction with the WIFI authentication or VPN over WIFI.

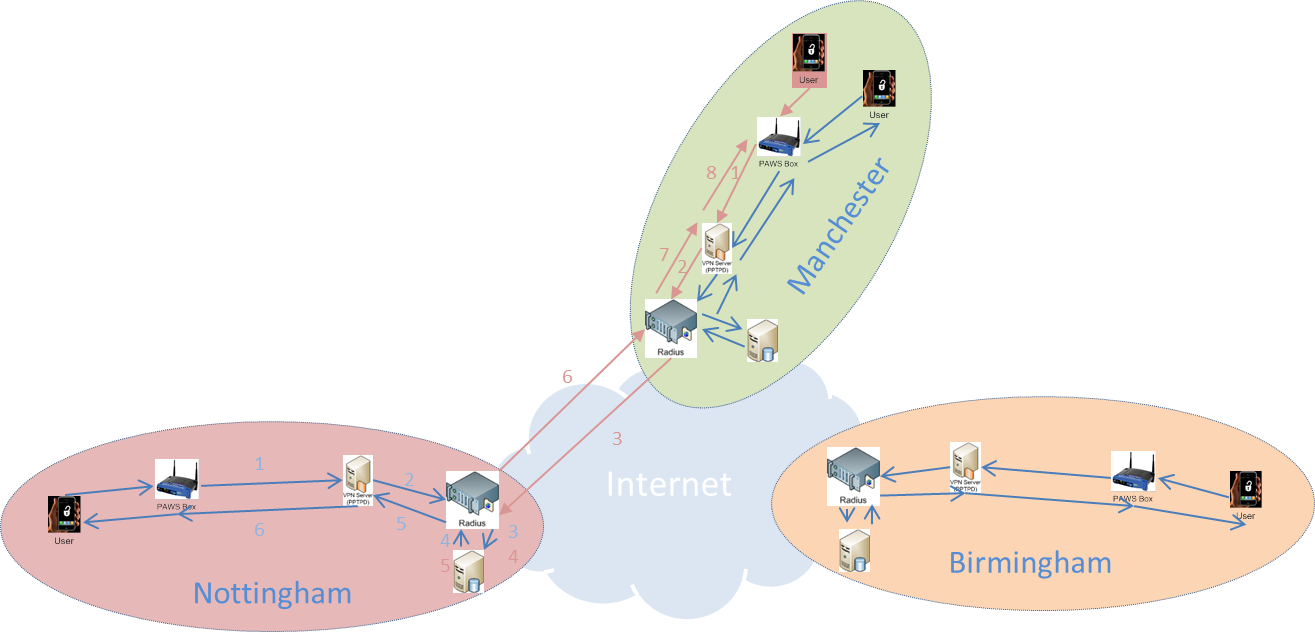
All of these approaches however allow for user traffic to pass through the PAWS router unencrypted. As the PAWS router is based inside the sharer’s home there is a chance that it can be hacked into and the user traffic captured.

To solve all of these issues we propose VPN from the user end device directly to the PAWS VPN service. We describe our approach in more detail below.

We assume that the routers in volunteers’ s houses (PAWS Wireless Access Points) are configured to advertise an unsecured network SSID. A user (wireless client, Mobile phone) connects to the advertised network SSID without a password and then establishes a VPN session to the IP of the RADIUS Authentication Server for which they enter a password. In case that the PAWS authentication server uses external RADIUS servers (Government, Council, Library, Bus Operator) for authentication, the PAWS authentication server proxies the request to the external server. The external RADIUS server confirms the password validity. The RADIUS Authentication Server completes the VPN session, authorises the Wireless Client and starts acting as a router to the Wireless Client. The Wireless Client can now access the internet. This is shown in Figure 1.



Our infrastructure is highly saleable and can efficiently manage user mobility (Figure 2). Consider a case that Nottingham PAWS user connects to a Manchester PAWS box and provides their username (using the format “user@Nottingham”, user@Realm) and password to the VPN server. The VPN Server forwards the username and password to the Radius server for Authentication. The Radius Server determines (based on the Realm in the username) that it needs to proxy/forward the username and password to the Nottingham Radius Server. The Nottingham Radius Server forwards the username and password to its internal database. The database confirms the username and password to the Nottingham Radius server. The Nottingham Radius Server responds back to the Manchester Radius server and confirms the username and password are ok. The Manchester Radius server forwards the confirmation to the Manchester VPN server. The VPN server confirms to the client that the username and password are correct and proceeds with establishing the VPN connections



4. Discussion and Future Work

5. References