Providing Security for Wireless Community Networks

Milena Radenkovic
Murray Goulden
Derek McAuley
Richard Mortier
University of Nottingham, UK
first.last@nottingham.ac.uk

Heidi Howard
Jon Crowcroft
University of Cambridge, UK
first.last@cl.cam.ac.uk

Christian Greiffenhagen
Loughborough University, UK
c.greiffenhagen@lboro.ac.uk

ABSTRACT

This paper describes a new Internet access paradigm based on Lowest Cost Denominator Networking - the Public Access WiFi Service (PAWS) - that utilises the unused capacity of home broadband connections and provides users who are unable to afford paying for the service with Less-than-Best-Effort access to these resources. We identify the security and architectural challenges faced by the project and propose our solution that enables free internet connectivity to public services for the local community, in a secure and scalable manner.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection; C.2.1 [**Network Architecture and Design**]: Wireless communication; C.2.3 [**Network Operations**]: Public networks

Keywords

Less Than Best Effort Networks, Security, Community Networks

1. INTRODUCTION

The Public Access WiFi Service (PAWS)[7] aims to enable digital inclusion of under-privileged members of society through ensuring secure access for all to everyday online services. These are currently enjoyed by the majority but are typically not accessible to those who come from poorer backgrounds 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.

Related initiatives in the past have assumed that all users of the Wireless Community Networks are either sharers (share their bandwidth with other users) or pay to become users. Companies such as FON [4] have been very successful in attracting a large community of users, with 8 million FON hotspots currently available. This demonstrates that broadband customers are willing to volunteer to share their high-speed broadband Internet connection for free with fellow citizens. Since we are considering those do not currently have access to these services, we are likely to have many vulnerable internet users. We argue that it is essential to provide easy-to-use service with better-than-average security to them.

LCDNet'13, September 30, 2013, Miami, Florida, USA.
ACM 978-1-4503-2365-9/13/09.
http://dx.doi.org/10.1145/2502880.2502890.

2. REQUIREMENTS

Inspired by Lowest Cost Denominator Networking [6], PAWS provides free internet services to users over a wireless network that they neither own nor can control. The majority of PAWS users will come from digitally-excluded background and so we need to provide better-than-average security for them. We are therefore faced with some interesting security and infrastructure challenges that our solution must address:

- **Confidentiality:** Users need to be able to access the internet securely without worrying about the possibility that the sharers or other users on the network may eavesdrop on their traffic. PAWS users must be protected from either other PAWS users connected to the same hotspot or from any other wireless users within reach. As all PAWS user traffic is routed through equipment located inside sharers' homes, to which sharers have full access, the PAWS user traffic needs to be reliably protected from interception or eavesdropping.
- **Ease-of-Use:** Without any special training, users need to reliably use a secure connection and sharers need to be able to set up the PAWS hotspot.
- **Priority:** Sharers' internet use must not be noticeably affected by sharing their connection with the PAWS network.
- **Authentication, Authorisation & Accounting:** The PAWS project need to be able to control which users are allowed to access what services, how much of the resources to use and to be able provide detailed record of services accessed and resource usage.
- **Scalability:** The PAWS network must be scalable across deployment areas.

3. PROPOSAL

Our proposal is designed to achieve secure end to end network access over unsecured network infrastructure. We realise this by enabling users to connect to a dedicated PAWS WiFi router on the sharer's network and on top of this connection establish a secure VPN tunnel from the user's device

to the PAWS VPN service, using federated identity management. We describe our approach in more detail below.

Hotspot Deployment

PAWS works by using a separate dedicated router connected via Ethernet to the sharer's domestic router so that no further set-up is required.

Alternatively we could connect the PAWS router directly to the sharer's internet connection and then connect the sharer's router to the PAWS router, this would have the advantage that we can accurately measure the sharer's network usage and therefore infer the unused capacity that could be made available to the PAWS network. However, this would not work for many reasons: The PAWS router would have to work as a modem therefore would have to be configured and suitable for all ISPs and connection methods (fiber, ADSL, etc.). Many ISPs will not provide support if the router they provide is not used and thus would create another barrier for volunteers. The original router would have to be reconfigured so as to no longer act as a modem requiring guides available for PAWS sharers.

FON [4] uses a dedicated router ("La Fonera"), which is connected behind the sharer's modem but then the sharer uses the FON box as their AP for their home network. This is not a feasible option for us as it requires the sharer to connect all their devices to the new AP. Existing works [1] [2] implement this purely in client side software; it is not a suitable solution due to the range of devices that we intend to support.

We deploy PAWS Access Points in volunteers' houses, advertising an open WiFi network with "PAWS" SSID. The PAWS Access Points are configured to use only a fraction of the sharers' bandwidth so that sharers' internet use is not noticeably affected. The users' devices connect to the PAWS advertised network.

Confidentially

As outlined in the requirements above PAWS user traffic needs to be reliably protected both while wireless and while being routed through sharers' homes.

While WiFi encryption is typically considered to be the obvious option for securing the wireless traffic between the user device and the PAWS wireless router, it cannot reliably provide the required level of confidentiality. Existing research shows that the majority of available WiFi encryption algorithms such as WEP, WPA, WPA2, are not sufficiently secure. Arguably one of the latest encryption algorithms such as WPA2-Enterprise should be able to offer adequate encryption, however the WiFi networks suffer from a major drawback as they are designed to provide security against outsiders but not among insiders. WPA2 can perform satisfactorily against users who do not have a valid password and cannot associate legitimately to the network SSID, but it does not prevent already associated users from eavesdropping on newly associating users' initial handshakes and intercepting their keys.

In home or enterprise environments this is little cause for concern as it can be assumed that sufficient degree of trust exists among connected users.

In the case of PAWS, no trust can be assumed among users, and ensuring users associated with the same network SSID cannot eavesdrop on each-other's traffic is a major confidentiality requirement.

The second confidentiality requirement is ensuring that sharers cannot eavesdrop on PAWS users traffic. The PAWS WiFi routers are connected to the sharers' routers and all PAWS users traffic can be eavesdropped at this point [5]. The sharers also have physical access to the PAWS WiFi routers and there is nothing that we can practically do to prevent them from taking over these routers. Even if the sharers lack technical expertise to obtain administrator-level privileges to the PAWS WiFi routers, they can easily turn them off and advertise the "PAWS" SSID via their own routers.

Encrypting sensitive traffic at the PAWS users' devices addresses the confidentiality requirements listed above but PAWS users cannot be assumed to be able to do this themselves.

We, therefore, propose to use a VPN tunnel between the PAWS users' end devices and a secure endpoint, so that user traffic is not vulnerable while traversing the unsecured link.

The VPN servers for the PAWS network are located near to each geographical area that the PAWS network is deployed, to minimise latency. Each PAWS VPN server could be funded by the local council or charities.

We have designed the VPN servers to provide the L2TP and PPTP protocol implementations because they offer the best trade-off between security, ease of set-up, and built-in device and OS support. Most computers and mobile devices have built-in support for L2TP and PPTP which is a major benefit for the PAWS targeted user-base. More secure VPN protocols and implementations exist but they require additional installation and complicated configuration.

Authentication, Authorisation, Accounting

As highlighted in the requirement section, we need authentication, authorization and accounting for the users connecting to public services via the PAWS network. We have chosen RADIUS network protocol because it is popular and is well supported by a wide range of operating systems and devices.

We configured the PAWS router firewall to only allow control protocols and traffic to the local PAWS VPN server for two reasons. First the user initiates a VPN session to the local PAWS VPN server and provides their PAWS credentials. The VPN server checks the credentials with the local RADIUS instance that confirms if the user has been authenticated and is authorised to establish a VPN session.

In the case that the PAWS RADIUS server uses external RADIUS servers (e.g. 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 client and starts acting as a router to the Wireless Client. The user can now access the internet. This is shown in Figure 1 (Nottingham).

Our infrastructure is highly scalable and can efficiently manage user mobility, roaming and federated identity management utilising the forwarding of authentication requests by RADIUS to another RADIUS server (Figure 1). Consider a case when a Nottingham PAWS user travels to Manchester and connects to a Manchester sharer's PAWS router and provides their PAWS username (using the RADIUS format "user@Nottingham") and password to the Manchester PAWS VPN server. The Manchester PAWS VPN Server for-

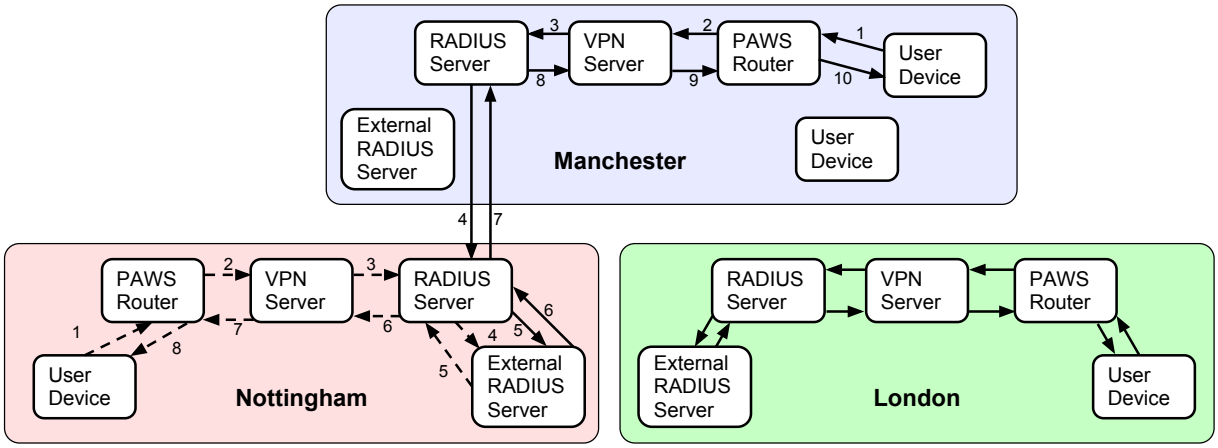

Figure 1: Federated Authentication

wards the username and password to the Manchester PAWS RADIUS server for authentication. The Manchester PAWS RADIUS Server determines, based on the Realm in the username, that it needs to proxy the authentication request to the Nottingham PAWS RADIUS Server. The Nottingham PAWS RADIUS Server responds back to the Manchester PAWS RADIUS server and confirms the username and password are authorised. The Manchester PAWS RADIUS server forwards the confirmation to the Manchester PAWS VPN server. The Manchester PAWS VPN server confirms to the client that the username and password are correct and proceeds with establishing the PAWS VPN connection.

4. DISCUSSION

Current laws controlling the sharing of wireless internet access are hindering the digital economy and the digital social inclusion plans of Governments [3] [9] because they refuse to recognize the novelty of socially transformative technology. For example many ISPs currently specify in their terms and conditions that they shall be entitled to terminate the Service if they discover that customers have permitted (whether knowingly or not) a third party to access the Service using a wireless connection over their communications line.

The law should be clarified to help spread broadband access more widely. At present many theories of law exist that are trying to address the problem of internet sharing regulation but they are still not managing to fuse their understanding of human, technological, and business aspects of internet regulations [3]. They aim to achieve one coherent theory that would offer a flexible, responsive and effective regulatory model for bandwidth sharing in cyberspace. We argue that the impact of the introduction of community networks on the primary traffics needs to be studied further in order to be fully understood. Virtual Public Networks [8] addresses many of the challenges faced by PAWS, whilst also allowing third party stakeholders as ISPs.

5. FUTURE WORK

At present the PAWS project has active deployments in a digitally deprived area in Nottingham. Further deployments to explore other applications will take place with funding from the DE dot.rural [1] Research Hub at Aberdeen University.

6. ACKNOWLEDGMENTS

This work was supported by the EPSRC Grant EP/K012703/1. We would like to thank Arjuna Sathiaseelan and Professor Fairhurst for there comments and feedback.

7. REFERENCES

[1] Whisher wifi sharing community. `www.whisher.com`.

[2] X. Ai, V. Srinivasan, and C. Tham. Wi-sh: A simple, robust credit based wifi community network. In *INFOCOM 2009, IEEE*, pages 1638–1646, 2009.

[3] M. Gilen. Lawyers and cyberspace: Seeing the elephant. In *9:2 SCRIPTed 130*, 2012.

[4] Fon Ltd. Offical FON International Community Website. `corp.fon.com`.

[5] N. Sastry, J. Crowcroft, and K. Sollins. Architecting citywide ubiquitous Wi-Fi access. In *HotNets: Proceedings of the 6th Workshop on Hot Topics in Networks*, 2007.

[6] A. Sathiaseelan and J. Crowcroft. LCD-Net: Lowest Cost Denominator Networking. In *ACM SIGCOMM Computer Communication Review*, April 2013.

[7] A. Sathiaseelan, J. Crowcroft, M. Goulden, C. Greiffenhagen, R. Mortier, G. Fairhurst, and D. McAuley. Public Access WiFi Service (PAWS). In *Digital Economy All Hands Meeting, Aberdeen*, October 2012.

[8] A. Sathiaseelan, C. Rotsos, C.S. Sriram, D. Trossen, P. Papadimitriou, and J. Crowcroft. Virtual Public Networks. In *2nd European Workshop on Software Defined Networking (EWSDN)*, October 2013.

[9] D. M. Sithigh. Law in the last mile: Sharing internet access through wifi. In *6:2 SCRIPTed 355*, 2009.

[1] `http://www.dotrural.ac.uk/`