Towards a Socially Aware Home Router

Jason T. Gustafson
University of Oregon
jtg@cs.uoregon.edu

Jun Li*
University of Oregon
lijun@cs.uoregon.edu

Haixin Duan
Tsinghua University
duanhx@tsinghua.edu.cn

ABSTRACT

Effective security on home wireless networks remains an elusive goal. The most prevalent method uses a single pre-shared key to enforce access control, but the requirement for convenience often results in poorly chosen keys which rarely change over time. Furthermore, since there is no way to maintain control of the key once it is distributed, there is no way to know who is actually on the network. Methods already exist which provide better security (e.g. EAP-TLS), but few users have the knowledge or experience to deploy them. We propose a new paradigm which brings access control to the average user's level. Our idea is to leverage online social networks to identify relationships between the owner of a home wireless network and its potential users. Rather than being responsible for the distribution and control of a single all-powerful key, the wireless owner simply declares the set of users and relationships which they trust to access their network. From the perspective of the wireless user, authentication is as simple as logging into the online social networking service like normal.

Keywords

home router, social network, access control, home network

1. INTRODUCTION

The quest for better security on home wireless networks has been marred by flawed protocols and poor usability. While the increasingly prevalent use of WPA2 with a pre-shared key (PSK) does much to address these issues, it exacerbates the fundamental tension between usability and security. On one hand, keys should be sufficiently complex to resist dictionary attacks; on the other, they must be simple enough to be easily distributed to the devices which use them. WPS was designed to solve this problem, but its deployment has been hampered by its own set of vulnerabilities.

Furthermore, maintaining strict control of the key is fundamentally incompatible with the desire to share the network with others. Once the key is distributed, control of the network is effectively lost until it is changed. Accounting is impossible when all users share the same authentication token. Enterprise networks typically use the IEEE 802.1x standard to provide stronger authentication and accounting, but the requirements for configuration and management are impractical for users of home networks.

Our objective in this paper is to present a new paradigm for home wireless access control which simultaneously addresses the limitations of pre-shared keys and provides improved usability. Our idea is inspired by recent research into relationship-based access control (ReBAC) for online social networks [4, 6]. Rather than vesting all security in a single all-powerful key, the wireless router owner simply declares the members of their social networks who they trust to use their network. In order to identify these people and relationships, we leverage existing online social networking services. Since people have already integrated these services into their daily work-flows, managing the router becomes much easier. And from the perspective of a wireless user, accessing a network is as simple as logging into the social networking site (if a session is maintained in the user's browser, even this step is unnecessary).

However, this paradigm must encompass several crucial security components:

- *Anonymity:* The identity of the access point owner should be protected from unauthorized users; likewise, the identity of the user should be protected from unknown access points.
- *Authentication:* The user and the owner must authenticate each other before access is granted.
- *Authorization:* A simple language should be used

[*] Corresponding author

for the owner to clearly define the set of trusted users or relationships and the corresponding level of access to be granted.

- *Privacy:* Since the router is effectively a man in the middle, the user must have a secure end-to-end connection to authenticate with the social networking service. Additionally, information about the user or the owner's personal social network should be considered private and not be leaked in any authorization protocol.

We describe our design of these four components below. Before that we first present related work, and our terminologies and assumptions.

2. RELATED WORK

Home Router Usability: The complications of securing home networks have been studied extensively in the literature [9, 7, 10]. Most of the literature has focused on helping users understand the network technology. We are proposing the converse: to bring network technology to the user's level by offering abstractions from their daily lives.

Home networking appliances (e.g., [1, 11]) provide a convenient way for new devices to associate with the network, yet they have no clear way to identify the users of the devices for accounting purposes. The Cisco Valet [3] product line allows the user to insert a USB device into the computer which is seeking access and the network is configured automatically. This handles many of the usability issues, yet it too does nothing to solve the inherent problems with using pre-shared keys.

Relationship-Based Access Control: The emergence of online social networks in the past ten years has fueled the need for a new paradigm in access control. Gates makes the case for relationship-based access control (ReBAC) in [5]. She argues that access control for Web 2.0 resources ought to be based on a model which users are already accustomed to dealing with in their daily lives. Following up on this work is Carminati, et al., who present an access control framework for online social networking content which includes the ability to control access according to the depth of the relationship (i.e. the number of hops between the principals) [2]. Unlike this work, however, we do not depend on the availability of explicit trust levels between users. Similarly, in [8], a distributed identity management system is proposed in which access control policies are controlled by the distance between principals in the social network and the strength of the relationships along the path.

3. TERMINOLOGIES AND ASSUMPTIONS

We introduce some terminology in our design. We refer to the home router as the *wireless access point* (WAP). The *social networking service* (SNS) contains all of the social network information and is responsible for authenticating the WAP owner and its prospective users. We introduce an authorization server (AS), which contains the WAP owner's access policy and is responsible for making access control decisions. We could have instead depended only on the SNS for authentication and authorization, but using a separate service allows us to leverage multiple social networks.

Our design also incorporates a trust model that keeps trust requirements to a minimum:

- The WAP owner and users do not trust each other *a priori.*
- The WAP owner and users both trust the SNS for the purpose of authenticating each other.
- The WAP owner trusts the AS to access her social information and to enforce access decisions according to her policy.
- Wireless users do not necessarily trust the AS.

We additionally assume that both the owner and users have access to the public keys of both the SNS and the AS, and can therefore confirm the validity of signed messages and negotiate secure channels.

4. ANONYMITY

The threat of rogue access points and malicious users forces us to take precautions to protect users and owners respectively. To that end, the authentication should be careful not to reveal information about the principals involved (including their identities) until respective policies have been consulted. We therefore propose the following authentication sequence:

1. Using a secure tunnel (e.g. SSL), the user authenticates with the SNS and her identity is passed to the AS.
2. The WAP owner's policy is consulted. If the user is not authorized, then a 'reject' message is sent to the user. Otherwise, the identity of the WAP owner is sent to the user.
3. The user decides based on the identity of the WAP owner whether or not to join the network. If she declines, then a 'reject' message is sent to the user and the WAP never learns her identity. If she accepts, then her identity is passed to the WAP.

A rogue access point which is hoping to snoop on user's activities must identify its owner to any potential users. Since users see this identity before joining the network, they can take proper precautions to protect themselves. On the other hand, a malicious user can do nothing unless she has managed to infiltrate the WAP owner's social network. She cannot even learn the identity of the WAP owner unless she has been explicitly given permission to access the network.

5. AUTHENTICATION

To implement the anonymity suggested above, secure tunnels between the user and the AS, and between the user and the SNS are required. The former is needed to protect the user's identity from the access point. The latter is needed to protect the user's SNS authentication credentials.

We propose a method that uses the Extensible Authentication Protocol (EAP), which is a generic authentication framework used with IEEE 802.1x. Protected EAP (PEAP) is an EAP method which provides an end-to-end secure channel for tunneled authentication based on the TLS/SSL protocol. The goal using this method is to allow the AS to mediate the authentication of the user to the SNS. However, since the user should not be obligated to reveal her credentials to the AS, an end-to-end tunnel is still required. Hence there are two levels of secure tunneling required: first, the session between the user and the AS must be secure from eavesdropping by the router; second, the authentication of the user to the SNS must be secure from eavesdropping by the AS.

Figure 1 depicts how this protocol would work in practice. The figure shows the sequence of events allowing Alice to use Bob's WAP. The basic authentication steps are described below.

1. The user sends an access request to the access point using an anonymous user-name.

2. The router forwards the request to the AS, a secure session is established with the user, and the user reveals her true identity to the AS.

3. A secure session is opened between the user and the SNS for authentication.

4. The SNS verifies the password of the user, tears down the secure session, and reports to the AS whether the user is valid.

5. The policy of the WAP owner is then consulted. If the user has not been authenticated, or no access is allowed, a reject message is sent to the user.

6. If the user has been authenticated and access has been granted, the AS passes the identity of the owner to the user and queries whether the user wants to connect.

7. If the user decides to connect, her identity is passed to the access point and access is granted according to the previous policy. If not, a final access reject message is sent.

It is worth noting here that the need for the secondary SSL/TLS tunnel is necessitated by the independent authorization server and its need to mediate the authentication. If this piece was actually implemented by the SNS, then a single tunnel would clearly suffice (though it would not be as flexible since it could only support a single SNS). Since SSL tunnels have considerable overhead, this version could face performance issues, but our preliminary results suggest that performance is still reasonable.

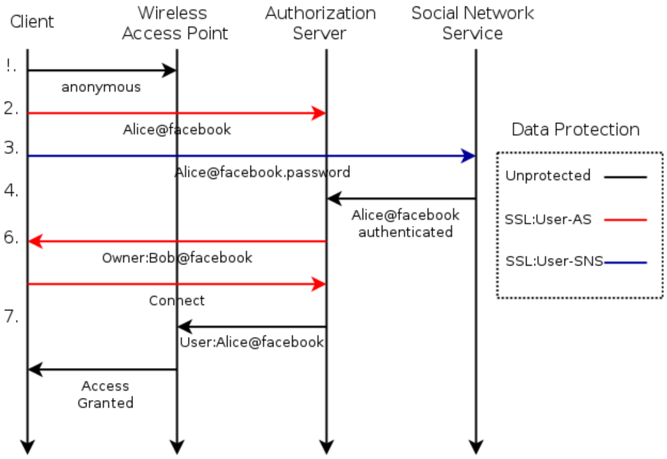

Figure 1: Authentication of Alice to Bob's access point

6. AUTHORIZATION

The goal of the authorization system is to provide a simply way for access point owners to declare the set of users that they trust, the network resources they are allowed to access, and how trust may be extended. One of the key advantages of leveraging a social network for access control is that it allows WAP owners to designate indirect relationships for access to the network. This is convenient, for example, when we wish to give access to all of our spouse's friends; even if we do not know who they are, we can allow our spouse to vouch for them.

Our authorization system can be thought of as a function which sends each potential user to a set of firewall rules. The nature of this function is controlled by a high-level policy which is created by the access point owner. The policy maps network resource permissions onto nodes in the social network through a set of rules. For simplicity in this work, we present a minimal language. The EBNF structure is provided below.

$$
\begin{aligned}
Policy &:= \texttt{policy}\ \ Node\{Rule+\ \ Default\}\\
Rule &:= Action\ \ Resource\ \ \texttt{to}\ \ Selector;\\
Default &:= \texttt{default}\ \ Action;\\
Selector &:= Node \mid Path\\
&\quad \mid Selector\ \ \texttt{or}\ \ Selector\\
&\quad \mid Selector\ \ \texttt{and}\ \ Selector\\
&\quad \mid Selector - Selector\\
Node &:= Label\ \ \texttt{@}\ \ Domain
\end{aligned}
$$

$$\begin{aligned}
\mathit{Path} &:= \texttt{<}\ \mathit{Label}\ (.\mathit{Label}) * \texttt{>}\ \texttt{@}\ \mathit{Domain}\\
\mathit{Resource} &:= \mathit{Network}(:\ \mathit{Port})?\\
\mathit{Label} &:= \mathit{String}\\
\mathit{Domain} &:= \mathit{String}\\
\mathit{Network} &:= \mathit{Num.Num.Num.Num}(/\mathit{Num})?\\
\mathit{Port} &:= \mathit{Num}\ (\texttt{-}\ \mathit{Num})?\\
\mathit{Action} &:= \texttt{allow}\ |\ \texttt{reject}
\end{aligned}$$

Policies are composed of an ordered list of rules along with a default action. When a user is requesting access to the wireless network, each of the rules are tested in order to create a corresponding set of firewall rules. For each rule, if the user is a member of the set selector, then a new firewall rule is added, making sure to preserve their relative order. At the end of the process, if the set of accessible resources is not empty, the user is granted access and the firewall rules are given to the WAP for enforcement.

As an example, suppose that this is Bob's policy:

```
policy bob@facebook {
 allow 192.168.1.0/24 to <family>@facebook.com
 reject 192.168.1.0/24 to <all>@facebook.com
 allow 128.223.0.0/16 to <friends>@facebook.com
 default reject
}
```

Clearly, this language is not intended to be used directly by the WAP owner. Instead, it is just the underlying implementation we propose.

7. PRIVACY

Finally, we mention a couple relevant issues concerning the privacy of both the WAP owner and its potential users. First and foremost, information about respective social networks should not be assumed public knowledge. We believe the anonymity provided to WAP owners and users reasonable privacy, yet there could be concern that the action of allowing or denying access could in itself leak information about the WAP owner's social network. We therefore emphasize that the authorization should not depend on the nature of the connections in the user's own social network since these can be manipulated at will.

We also address the topic of fully anonymous access. Since the user of the wireless network ultimately has control over whether to join a network or not, it ought to be possible for the WAP owner to run an anonymous access point. In this case, the user is notified that the owner is anonymous and given the choice to proceed at her own risk. The user may also desire anonymous access to a WAP, but in this case, it should be up to the WAP owner whether this should be allowed or not.

8. CONCLUSION

In this work, we have presented the design of a "socially aware" home router which offers the promise of better usability and better security by leveraging online social networks to identity the relationship between the router owner and potential users. We discussed in detail the primary security concerns with respect to anonymity, authentication, authorization, and privacy. We also presented several strategies for solving them. Future work will explore the actual usability of this system through an extensive user study.

9. REFERENCES

[1] D. Balfanz, G. Durfee, R.E. Grinter, D.K. Smetters, and P. Stewart. Network-in-a-box: How to set up a secure wireless network in under a minute. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, pages 15–15, 2004.

[2] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security*, 13(1):1–38, 2009.

[3] Cisco Systems, Inc. Cisco Valet, January 2012. http://home.cisco.com/en-us/wireless/valet.

[4] P.W.L. Fong. Relationship-based access control: protection model and policy language. In *Proceedings of the first ACM conference on data and application security and privacy*, pages 191–202. ACM, 2011.

[5] C. Gates. Access control requirements for Web 2.0 security and privacy. *IEEE Web*, 2(0), 2007.

[6] F. Giunchiglia, R. Zhang, and B. Crispo. Relbac: Relation based access control. In *Semantics, Knowledge and Grid*, pages 3–11, 2008.

[7] R.E. Grinter, W.K. Edwards, M.W. Newman, and N. Ducheneaut. The work to make a home network work. In *ECSCW*, pages 469–488, 2005.

[8] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H.C. Choi. D-foaf: Distributed identity management with access rights delegation. *The Semantic Web—ASWC*, pages 140–154, 2006.

[9] E. Shehan and W.K. Edwards. Home networking and HCI: what hath god wrought? In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 547–556. ACM, 2007.

[10] P. Tolmie, A. Crabtree, T. Rodden, C. Greenhalgh, and S. Benford. Making the home network at home: Digital housekeeping. *ECSCW*, pages 331–350, 2007.

[11] J. Yang and W. Edwards. Icebox: Toward easy-to-use home networking. *Human-Computer Interaction—INTERACT*, pages 197–210, 2007.