EduVPN

Secure Access to the Home Realm

Authors

Rogier Spoor
(Rogier.Spoor@SURFnet.nl, +31302305361)

Francois Kooman
(fkooman@tuxed.net)

Author Affiliations

SURFnet
PO Box 19035
3501 DA Utrecht
The Netherlands

Keywords

VPN, respect privacy, secure environment, WiFi

Session format

Regular presentation

Summary

We live in a society that wants to be online whenever possible, and WiFi is popular technology for achieving this. Unlike the ”home” situation which could be described as a trusted network, we also make heavy use of public offerings of WiFi, which we describe as guest networks, and which are in a special position that could make them perform a number of rogue attacks on our connections.

This presentation identifies the dangers of using WiFi on such guest networks, and it analyses methods of running a trusted network over such potentially rogue connections. We describe a system that we call EduVPN that implements such facilities and that is designed with educational institutions as an audience. As the name suggests, we make use of educational infrastructure to achieve this; specifically, we introduce a form of authentication based on SURFconext.

The resulting system offers a range of choices to the roaming user; he might use strongly authenticated eduroam to access the Internet while visiting a befriended institution, and in those and other situations, he might choose to not rely on the security of a guest network, and use EduVPN to obtain secure access to home services that are concealed from general access through eduroam or guest networks.

Abstract

The current offerings to research and educational institutions includes several facilities; there is a facility to gain strongly authenticated access through eduroam; this is often considered to provide considerable ensurance that the network can be trusted. Finally, many places offer public access. The last category is described as a guest network. These guest networks are useful when traveling, and this presentation will highlight the security risks that comes with using them.

Rogue WiFi stations or rogues peers on a shared WiFi station could mount attacks as a result of the following aspects of the WiFi design:

- Unauthenticated traffic, including service announcements
- The use of a broadcast physical layer, which is openly (and even covertly) accessible

- Encryption that is only applied to the air signal
- Offering a range of security mechanisms that includes insecure mechanisms

Devices accessing WiFi rely on protocols that are not sufficiently secure to enable trust in guest networks. One way around this is to focus on making the devices more secure: implement new protocols like DNSSEC, install software updates, enable a firewall, enforce the use of TLS connections for all network traffic, unless there is a very good reason not to do it. However, this is hardly practical; if not for the added complexity of protocols and concerns about their support on guest networks, then because many people continue to use a mobile device after its support has been terminated by the manufacturer, leaving them without security updates.

A more realistic approach for a solution is to decrease the attack surface, and aim for such minimal reliance on the guest network services that the actual usage pattern becomes that of a trusted network. In general, this requires end-to-end authentication and encryption between a device and a network that it can trust, such as a home or office network. The general mechanism through which this can be achieved is a VPN.

This presentation introduces a VPN infrastructure called EduVPN. It is intended to offer facilities reminiscent of eduroam, even when run over a guest network. The infrastructure consists of VPN end points in a trusted network, together with clients that use a form of device authentication derived from SURFconext authentication.

The solution that we introduce with EduVPN consists of the following elements, and integrates with existing SURFnet infrastructure:

- Federated authentication of users through SURFconext for easy deployment;
- A web-based service that enables authenticated users to setup a VPN (through
- a client download and/or a VPN certificate signing service)
- Infrastructure and/or setup instructions for the VPN server

The end user would basically experience the following while setting up EduVPN:

1. Access the VPN service web portal
2. After a redirect, authenticate to SURFconext;
3. Manage VPN configurations, download client, generate a configuration or revoke a configuration

In the presentation we will discuss how we can jointly offer EduVPN based services in the NREN community.

References

EduVPN demo service (public login via Onegini IdP)
https://eduvpn.surfcloud.nl

Author Biographies

Rogier Spoor is manager middleware services at SURFnet. Rogier supports the SURFnet’s security community (SCIRT) and develops new services in area of security and cloud computing (focus on IaaS, personal cloud storage, distributed storage).