

Federated Wireless Net-Auth (FWNA) Academic / Member Visitor Use-Case

Background

The nature of unlicensed RF (Radio Frequency) network technologies requires that secure network access and authentication policies are in place to limit network access to known users. Incidents of network disruption and attacks on users/networks through the use of 802.11 networks are well documented. This has resulted in limited, or no access, for users outside the local domain with legitimate connectivity requirements to perform scholarly or other work/research.

The FWNA is a group of Internet2 member institutions that wish to provide a mechanism for wireless (802.11 a/b/g) network access to visiting / guest members. Visitor / Guest member access would be dependent on credential trust from the home institution. It is envisioned that guests would be granted network access based on local and /or mutual FWNA policies.

Use-Case Assumptions

This use-case defines the term “guest” as a legitimate user at a FWNA member institution. An example of real-world collaboration used as a basis for this use-case is the CIC (Committee on Institutional Cooperation - <http://www.cic.uiuc.edu/>). There is no initial requirement to provide pre-registration information. Users will be identified through their home credentials.

Problem Statement

A CIC traveling scholar’s home institution is within the CIC and the traveling scholar is spending the current semester at another CIC member institution. In addition, both institutions are Internet2, FWNA members.

During the course of the traveling scholar’s research, they need to exchange files/data with fellow researchers working at their home institution and abroad. The exchanged data is required in the laboratory where the scholar is working. The host institution has a public (public wireless is defined with the broadcast SSID and, open to all students, staff and faculty at the host institution) wireless network signal available that the scholar would like to access. The scholar’s office is located two floors from the lab, and moving files back and forth manually is a time consuming and cumbersome process.

Proposed Solution (High-level overview)

The visiting scholar sees the broadcast SSID on their machine. The scholar selects the SSID in their profile manager / location manager. The scholar authenticates to the wireless network using their home user name along with their realm ([j.doe@home-institution.edu](#)) and home password. The local authentication server recognizes this logon as a guest (as defined above) through the use of the @ symbol and redirects the logon information to the home realm identified in the “email address” logon. The home institution’s server authenticates the user. The guest institution accepts the authentication, and the user is allowed to utilize the wireless network.

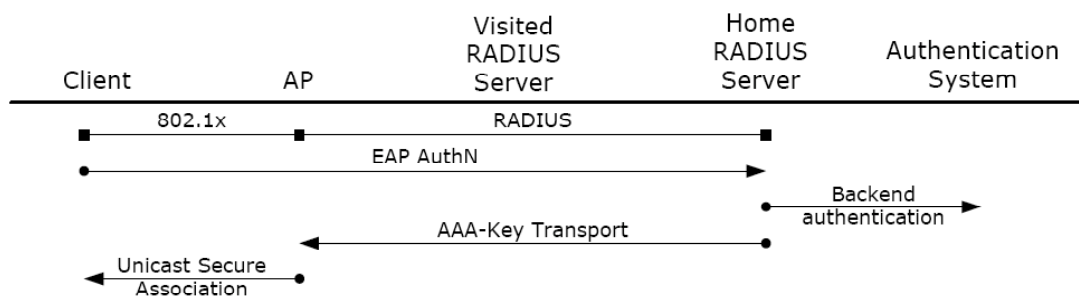
Architecture

Component Overview

The architecture of the proposed system encompasses five (5) main components: Client, Access Point (AP), Visited RADIUS Server, Home RADIUS Server, and Authentication System. In certain cases, these functions / components may be physically collocated. For purposes of this use case, it will be assumed that the components / functions are not physically collocated.

Figure 1 below shows how these components are inter-related and the protocols used to communicate between them. The EAP exchange provides not only authentication, but also keying material for unicast association between the client and the AP for purposes of encryption.

Figure 1 – Wireless Authentication Overview



The client and AP communicate using 802.1x. RADIUS is the protocol of choice between the Home and Visited sites, as it provides support for forwarding requests. Across both of these protocols, the EAP protocol transports the authentication credentials. At the Home RADIUS server, the credentials are extracted from EAP and verified against the Home institution’s Authentication System. A success / reject message is sent back from the Home server, to the Visited Server based upon the success of authentication. Additionally, keying information is communicated to the AP (in the RADIUS message) and the client (in the EAP message) to enable the creation of secure associations between the client and AP for encryption purposes.

EAP Detail

There are a variety of EAP sub-types. There is an overwhelming premise that Home institutions authenticate users through their own choice of EAP type and that Visiting institutions should not unnecessarily limit the EAP types. However, the Visiting institution may deny the use of EAP types that are not “unconditionally compliant,” per the IETF (Internet Engineering Task Force) EAP standards. This enables the Home institution to implement an authentication system that best meets their requirements, be it Kerberos, Active Directory, LDAP, etc.

The selection of EAP types that establish trust and provide confidentiality and integrity protection between the Home site and the client machine is recommended. Some EAP types necessarily require the release of additional user information (such as the entire user name and hashed password) to the Visited RADIUS server. This is consistent with the requirement, but should not be expected by the Visited RADIUS server, which should not expect to have anything more than the user's realm information. Authentication credentials are thus positively protected between the client and Home site and don't rely on the currently weak RADIUS protection mechanisms. This would then suggest the use of EAP-TLS, EAP-TTLS, or EAP-PEAP.

Document History

Date	Rev	Description of Change
April 25, 2005	0.1	Initial Draft encompassing high level use case, removal of specific (web) login method. Added Architecture leveraged from FWNA 0.4