SENSE – Secure Enterprise Networks Simple & Easy

Stefan Winter <stefan.winter@restena.lu>, +352 424409 1
RESTENA Fondation, 6 rue Richard Coudenhove-Kalergi, L-1359 Luxembourg

Biography: Stefan Winter graduated in Computer Science at the University of Karlsruhe, Germany, in September 2004, with a specialisation in telematics and foundations of Computer Science. He is working as R&D Engineer for the Luxembourg Research and Education Network RESTENA, where network roaming and identity federations are in the focus of his activities. He led the R&D work for eduroam during the GN2 and GN3 projects. In the GN3plus project, he is member of the eduroam Operational Team in Europe (leading the development of the eduroam CAT software), and a participant in the SENSE OpenCall project. He is one of Europe's representatives in the Global eduroam Governance Committee.

Tomasz Wolniewicz <twoln@umk.pl>, +48-56-611-2750
Nicolaus Copernicus University, pl. Rapackiego 1, Torun, Poland

Biography: Tomasz Wolniewicz has graduated and later received a PhD in mathematics at the University of Warsaw, Poland. Since 2001 he has been Director of the ICT Centre, Nicolaus Copernicus University in Torun. On behalf of the Polish PIONIER network he leads the eduroam activity in Poland and is involved in setting up the Polish Identity Federation. Within the GN3plus project he leads the eduGAIN Operations Team and is one of the main developers of eduroam Configuration Assistant Tool – CAT. He is also the author of the successful virtual library catalogue KaRo (http://karo.umk.pl).

Keywords: EAP usage in IEEE 802.1X, eduroam, Authentication, Usability, Security

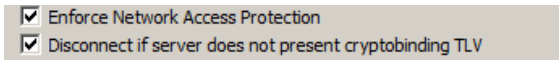
---

SENSE – Secure Enterprise Networks Simple & Easy

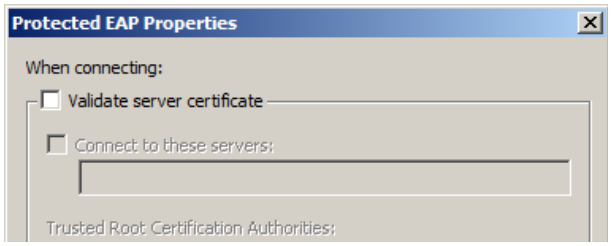
Setting up an enterprise-class WiFi network is a complex task. The steps needed on the server side are complex enough (setting up a RADIUS server with almost 100% uptime!), but the much more time-consuming task is to set up end-users' devices **correctly** and **securely**.

In a BYOD world, where the IT department does not have full control over the user equipment, it's up to the user to 'get it right'. As a consequence, the configuration will very often be

wrong: people can't authenticate because they misunderstood the meaning of some settings and configured something incorrectly



insecure: even if their configuration technically works - i.e. allows them to connect to your network - it probably does not set up the server-side identity checking correctly; and the same configuration would also connect the user to a rogue network and disclose his login credentials to an attacker. That is exactly what enterprise-level WiFi should prevent!



not privacy preserving: users will very likely not go through the extra configuration steps to set up an anonymous outer identity to hide their real username. Even if otherwise configured securely, a rogue access point would still be able to learn the actual username and could brute-force the password from there.

Setup instructions in PDF documents and helpdesk pages certainly help a bit, but will not be followed by everyone; and any shortcut or deviation means trouble - either for the organisation's helpdesk or for its site security. Of course very much depends on default OS settings, which unfortunately tend to assume the least secure and least identity preserving approach.

The SENSE OpenCall project of GN3plus aims to improve usability and technical completeness of end-user devices (specifically, their EAP supplicants) so that enterprise networks (such as eduroam) can be setup and used smoothly and at the same time securely. SENSE started in October 2013; by the time of the TNC2014 conference, significant preliminary results will have been achieved in all aspects mentioned below.

The project attacks the EAP setup and usability problem from four angles simultaneously:

1. **Define a standard for EAP configuration information**

Currently, every supplicant implementation stores its EAP configuration in its own proprietary format. A few supplicants can import EAP configuration items automatically, but again each relying on their own formats and (partly closed) specifications. Web services like eduroam CAT need to be able to produce configurations in all those dialects. SENSE will prepare and submit to the IETF a suggestion for an XML-based “EAP metadata” file format, along with a MIME-Type definition and a “well-known URI” where a device can expect to find the configuration for its network. The ultimate goal is that supplicants across the industry would be able to consume this single EAP configuration format, find the corresponding configuration file and set up devices with the right EAP configuration details automatically. eduroam CAT will be retrofitted with the ability to create this configuration file format.

2. **Make supplicants comparable and judge their relative strengths and weaknesses**

The project will define a set of criteria in the categories security, usability, and error handling, which will form a weighted checklist. The checklist will assign scores to supplicants to determine if they are technically secure and complete, and whether they are user-friendly (i.e. easily comprehensible and visually appealing).

The checklist will then be applied to a number of existing EAP supplicants in the field. Supplicants which score sufficiently high will be awarded the label “Complete and user-friendly EAP supplicant”; the checklist itself along with extensive documentation on why particular items are desirable will be published

permanently for new supplicant implementers to take into consideration.

One supplicant, the K Desktop Environment 's “Plasma NetworkManager” will be modified to achieve as high a score as possible according to the previously defined metrics.

3. **Create a permanent and open test environment for implementers to test their supplicant implementation against**

The project will set up a convenient and openly accessible testing environment for EAP configuration and supplicant testing with a purpose of lowering the difficulty and therefore cost of implementation and testing. EAP Lab will provide an easily configurable RADIUS environment allowing Lab users to remotely connect their access points, test devices and supplicants against a number of configuration scenarios. Each RADIUS configuration will be supplemented with downloadable installers and configuration profiles supplied by a dedicated CAT instance. Two main Lab use cases are anticipated: device and supplicant testing; eduroam CAT module testing.

4. **Implementation of EAP supplicants/front-ends on select devices**

Current eduroam CAT code contains a configurator for Network Manager in Linux systems. SENSE will create a new installer implementation which will be based on its work on the existing CAT Python code. Instead of the current approach, where configuration details are built into the configuration script itself, it will consume configuration supplied in the form of the EAP metadata profile built according to the project's specification (see point 1). The new installer will have to introduce new elements like XML parsing and a much better GUI. It is also expected that more Linux distributions will be covered including some which are not NetworkManager based. Such an installer could be included in Linux distributions by default, which would add the feature of automatic connection setup ubiquitously.

Another class of devices with a dire need for a better EAP configuration are those with the Android operating system. By TNC2014, SENSE will have developed a supplicant front-end to Android devices running versions 4.3 and higher in form of an app which will be able to consume EAP configuration data in the format discussed in point 1 and set up the device correctly without significant user interaction. The workflow will be similar to that of the well-known EAP supplicant on the iOS operating system.