Análisis y mejora de la red inalámbrica de la UC. Auditoria de seguridad e integración con la iniciativa EduRoam

José Mª Zamanillo Sainz de la Maza[(1)], Borja Santander Ruiz[(1)], Luis Fernando Romero Laguillo[(2)], Alfonso Iglesias Martínez[(3)].
jose.zamanillo@unican.es, borja.santander@alumnos.unican.es, lromero@ciin.es, alfonso.iglesias@gestion.unican.es.
[(1)] Departamento de Ingeniería de Comunicaciones (DICOM). Universidad de Cantabria
ETSII y Telecomunicación, Av. de los Castros s/n, 39005 Santander (Cantabria), Spain.
[(2)] Gobierno de Cantabria, Centro de Innovación en Tecnologías de Integración (CIIN), Edificio Simeón, Pasaje de la Peña 2, 39008 Santander (Cantabria), Spain.
[(3)] Servicio de Informática, Universidad de Cantabria,
Edificio de Filología, Av. de los Castros s/n, 39005 Santander (Cantabria), Spain.

***Abstract*- Wireless technologies are recently introduced in the Spanish universities and these technologies have supposed an improvement of the services offered to the users mainly, in the aspect of mobility within the campus, and the mobility between different institutions. Since, the conventional protection techniques used with Wi-Fi networks [1], like Wireless Equivalent Privacy (WEP) are obsolete, new solutions are needed in order to ensure the adequate network protection. This communication summarizes the ambitious project developed by the University of Cantabria in order to improve the security of the wireless network that exist in our University, and the adjust of those procedures to the paneuropean EduRoam (Education Roaming) initiative. Eduroam, is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming. Being part of eduroam allows users visiting another institution connected to eduroam to log on to the WLAN using the same credentials (username and password) the user would use if he were at his home institution.**

I. INTRODUCCIÓN

Desde el año 2003 la Universidad de Cantabria ofrece a todos sus alumnos, profesores y trabajadores la posibilidad de acceder a la red mediante sus dispositivos inalámbricos, facilitando de esta manera la conexión en cualquier parte del campus de las Llamas. En el inicio de este nuevo servicio se decidió implementar dos redes independientes, una destinada a los alumnos, y otra que sería la utilizada por los grupos del PDI y PAS , independientes, tanto desde el punto de vista de los servicios ofrecidos por cada una de ellas, como por la infraestructura presente tras ellas. La red destinada a PAS y PDI, UNICAN-i, basa su acceso en el sistema de VPN´s que ya existía previamente para que estos usuarios pudieran acceder a los servicios de la universidad desde fuera del campus. Sin embargo, se decidió que el acceso a la red que utilizarían los alumnos, ALUMNOS-i, fuera más sencillo, sin la necesidad de excesivas configuraciones, a través de un portal Web cautivo.

Desde el Servicio de Informática de la Universidad de Cantabria, se decidió estudiar las posibles mejoras en la seguridad de ALUMNOS-i, y las nuevas tecnologías surgidas desde la implantación de la red, sin descartar en ningún momento la implantación de estas nuevas técnicas en UNICAN-i, siempre y cuando ofreciesen a los usuarios una mayor facilidad de uso y protección.

En concordancia con esta idea de dotar de mayor calidad la red Wi-Fi de la Universidad de Cantabria, surgió la idea de estudiar la posible incorporación de nuestra institución a la iniciativa EduRoam, desarrollada en nuestro país por RedIRIS a través del proyecto MovIRIS [2]. Esta iniciativa introducirá un servicio de movilidad a nivel europeo, que permitirá, a todos los usuarios itinerantes, conectarse a la red de la institución visitada, sin la necesidad de pasar por los incómodos trámites que son necesarios en la actualidad. Esta idea se ha visto refrendada por la creciente adhesión de universidades tanto españolas como del resto de Europa a este proyecto, dotándolo de gran prestigio e interés.

Como premisa final, aunque no por ello menos importante, la idea en la que se apoya el trabajo aquí presentado es la de enfocarlo desde el punto de vista del usuario, tratando siempre que éste pueda utilizar la red con la mayor seguridad posible, evitando en lo posible configuraciones excesivamente complicadas, y darle nuevos servicios que mejoren su estancia en la Universidad de Cantabria y faciliten la posibilidad de completar sus estudios en otras instituciones..

II. SEGURIDAD EN LAS REDES INALÁMBRICAS

Desde los inicios de la tecnología inalámbrica, se han generado muchas recomendaciones para dotar las redes WLAN de un nivel de seguridad adecuado. Inicialmente, algunas de estas recomendaciones solo pusieron en evidencia más riesgos, pero posteriormente se han venido diseñando y estableciendo otros mecanismos que realmente permiten mejorar el nivel de seguridad en las redes inalámbricas, como los tratados a continuación. Posteriormente, se mostrarán las soluciones adoptadas para proteger la red inalámbrica de la Universidad de Cantabria.

A. Encriptación

Entre los diferentes sistemas de encriptación para redes inalámbricas destacan los siguientes:

- *WEP (Wired Equivalent Privacy)*: Es el primer sistema de cifrado propuesto por el estándar IEEE [3] 802.11, para proteger la información transmitida en redes inalámbricas. Se trata de un sistema de encriptación que trabaja en la capa de enlace del modelo OSI (nivel 2), y está basado en el algoritmo de cifrado RC4, aunque ligeramente mejorado. Como es mundialmente conocido, el algoritmo WEP ha sido roto y el IEEE ya no recomienda su uso, lo cual es debido a la gran cantidad de puntos débiles que presenta: tamaño del Vector de Inicialización de tan sólo 24 bits, vulnerabilidad del algoritmo CRC32, o la ausencia de un Código de Integridad del Mensaje (MIC).
- *WPA (Wi-Fi Protected Access):* Es un sistema de protección de redes inalámbricas desarrollado por la Wi-Fi Alliance [1] para corregir las carencias del WEP. Al coincidir en el tiempo con el desarrollo del estándar 802.11i, WPA no está cerificado bajo este estándar pero lo implementa en su mayoría. En principio fue desarrollado para ser integrado en una estructura 802.1x/EAP/RADIUS (WPA-Enterprise), aunque también se permitió el uso de claves compartidas (WPA-Personal o WPA-PSK), no tan seguro, pero adecuado para entornos domésticos. WPA sigue utilizando el algoritmo RC4 para cifrar los mensajes, fundamental a la hora de utilizar dispositivos ya existentes, pero se han incorporado mejoras que cubren las carencias del WEP. No obstante, dicha utilización del algoritmo RC4 le confiere una debilidad ya presente en su antecesor, que ha posibilitado su ruptura bajo ciertas condiciones.
- *WPA2 (Wi-Fi Protected Access 2):* Se trata del estándar 802.11i mejorado desarrollado por la Wi-Fi Alliance. La principal mejora de este sistema se fundamenta en el abandono del algoritmo de cifrado RC4, que es sustituido por el nuevo AES (Estándar Avanzado de Encriptación), e igualmente, se sustituye el anterior método de comprobación de la integridad del mensaje (MIC) por el sistema CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol). Al igual que el primer desarrollo de WPA, el WPA2 dispone de una versión 'Personal', que permite la autenticación mediante clave compartida, y una versión 'Enterprise' que requiere una infraestructura 802.1x/EAP/RADIUS.

Es por estas razones que tanto la opción WPA como WPA2 han sido adoptadas como soluciones validas para la encriptación en la red wireless de la Universidad de Cantabria.

B. Autenticación

Entre los diferentes sistemas de autenticación para redes inalámbricas destacan los siguientes:

- *EAP-TLS (Extensible Authentication Protocol-Transport Layer Security):* Protocolo desarrollado por Microsoft con el fin de sustituir el anterior estándar SSL (Secure Socket Layer) por el más novedoso TLS, que ofrece una fuerte autenticación mutua, basada en certificados digitales, tanto en el cliente como en el servidor, además de credenciales de seguridad y claves de encriptación dinámicas. Sin embargo el intercambio de identidades entre el solicitante y el autenticador se realiza sin ningún tipo de protección. Debido a la necesidad de certificados en la parte cliente, y el consiguiente requerimiento de una infraestructura de gestión de certificados (PKI), muchos administradores de red son rehaceos a utilizar este protocolo.
- *EAP-TTLS (Extensible Authentication Protocol-Tunnelled Transport Layer Security): Este sistema d*esarrollado por Funk Software y Certicom, permite a los usuarios autenticarse de una manera más sencilla (usuario/contraseña) y segura debido a que sus credenciales viajan protegidas por un túnel TLS, evitando así su transmisión en plano, como es el caso del EAP-TLS, además, como ventaja añadida, este protocolo solo necesita de certificados de servidor, y por supuesto, se mantiene el uso de claves de encriptación dinámicas. Soporta una gran cantidad de protocolos internos dentro del túnel como MD5, CHAP, PAP, MS-CHAP o MS-CHAPv2. El resultado es un protocolo que proporciona prácticamente el mismo nivel de seguridad que EAP-TLS, más sencillo de gestionar y económico, compatible con las bases de datos y la infraestructura existentes.
- *PEAP (Protected Extensible Authentication Protocol):* Protocolo muy similar al EAP-TTLS en el que el cliente, igualmente, se autentica mediante usuario y contraseña, los cuales se protegen a través de un túnel TLS, y únicamente es necesario un certificado de servidor. Fue propuesto por Microsoft y Cisco para seguir los pasos del EAP-TTLS. Así, Microsoft, lo incorporó a partir de la versión Windows XP SP1 y 2003 Server, haciendo que no fuera necesario un software propietario para configurarlo, y facilitando el uso de bases de datos Microsoft. Existen dos versiones de este protocolo, PEAPv0/EAP-MSCHAPv2, la más extendida y la difundida por Microsoft, y PEAPv1/EAP-GTC, desarrollada por Cisco.

C. Necesidad de un sistema AAA

Los sistemas AAA (Autenticación, Autorización y Auditoría), son imprescindibles en cualquier entorno de red empresarial o institucional, tanto para mejorar la seguridad como para disponer de información fiable sobre el uso, que facilite el cobro de servicios, el aumento de capacidad de la red o el cumplimiento de la legislación en la provisión de servicios de red debido a los exigentes requisitos de gestión, control de uso y auditoria de los mismos.

III. INICIATIVA EDUROAM

Desde el punto de vista administrativo, EduRoam [4] (Education Roaming) ha sido desarrollada por la Asociación Europea de Redes Académicas y de Investigación (TERENA), dentro de su grupo de trabajo Terena-Mobility, con el objetivo de crear una infraestructura de autenticación,

autorización, y movilidad a nivel europeo. En España esta iniciativa fue incluida dentro del proyecto MovIRIS [2], promovido a su vez por la Red Académica y de Investigación Española (RedIRIS), tomando el nombre de ***eduroam.es***. La principal misión de esta iniciativa es la de dotar a los estudiantes e investigadores de nuestro país de un espacio de cooperación a nivel de movilidad entre las organizaciones académicas y de investigación españolas y europeas, con el fin de que se disponga automáticamente de servicios de conectividad, acceso a aplicaciones u otros servicios que se desarrollen en el futuro, cuando se visiten otras organizaciones pertenecientes a la red.

Desde el punto de vista técnico, EduRoam consiste en una infraestructura basada en servidores RADIUS y el protocolo de seguridad IEEE 802.1X. TERENA posee dos servidores RADIUS centrales en sus sedes de Holanda y Dinamarca, los cuales están interconectados con los servidores centrales de los NREN's de cada país, y estos a su vez son la raíz de los RADIUS propios de las instituciones adheridas a la iniciativa. Esta "cadena" de servidores RADIUS es la que permite que un usuario que visita otra institución pueda conectarse a la red inalámbrica usando las mismas credenciales que utiliza en su institución de origen, evitando con ello la sobrecarga de procesos administrativos que serían necesarios para dar estos servicios a los visitantes, si estos dependieran de unas credenciales propias del centro visitado.

Entre los aspectos necesarios para regular el espacio de colaboración entre instituciones a través de EduRoam destacan:

- *Técnico:* El más evidente, trata de regular el uso de tecnologías y estándares adecuados, y hacer que se cumplan los mínimos impuestos.
- *Normativo:* Establece la seguridad necesaria a la hora de autenticar a los usuarios, así como realizar un correcto seguimiento de los recursos utilizados.
- *Gestión:* Se encarga de que los usuarios dispongan de unos servicios mínimos y un soporte adecuado para dichos servicios en todo momento.
- *Informativo:* Los centros asociados se comprometen a facilitar a los usuarios visitantes toda la información necesaria acerca de los servicios de los que disponen, zonas de cobertura, o SSID's, bien sea a través de una página Web, personal de la institución, etc.

En la actualidad existen más de 25 países en toda Europa, además de Australia, Taiwán, Hong Kong y China que participan en EduRoam, mientras que en Estados Unidos han comenzado a desarrollar una iniciativa similar por su cuenta. En estos momentos en España existen unas 50 instituciones asociadas a eduroam.es, habiéndose producido el mayor aumento de participación durante la realización de este proyecto. En la Fig. 1 se muestran los países que forman parte de EduRoam en la actualidad.

IV. Despliegue del proyecto en la UC

Para la implementación de este nuevo servicio se optó por adquirir un servidor, que se encargara de realizar las funciones de servidor RADIUS.

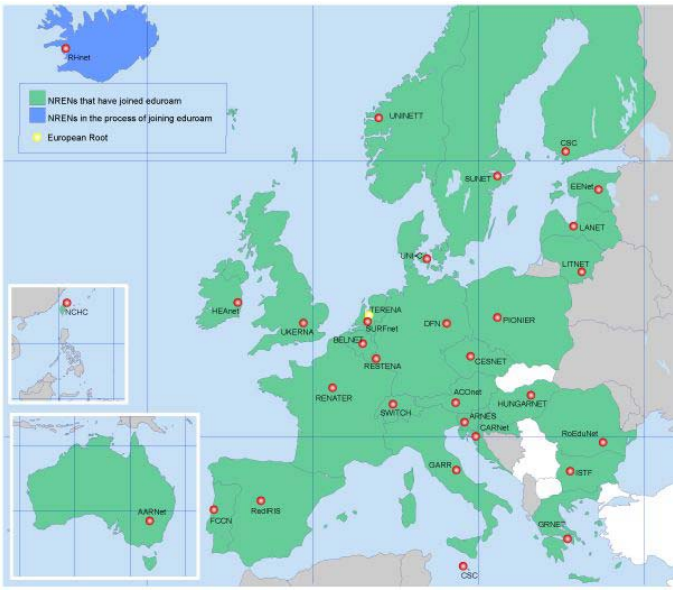

Fig. 1. Países miembros de la iniciativa EduRoam, Islandia ha solicitado su ingreso y se encuentra en fase de adjudicación (Abril-2007, fuente: www.eduroam.org).

Para la configuración de dicho servidor se ha utilizado la plataforma Red Hat Enterprise Linux 4, sistema soportado por Red Hat Inc., que proporciona aplicaciones software y hardware totalmente certificadas, actualizaciones periódicas, y un precio asequible a través de suscripciones. Manteniendo la idea de utilizar software libre, fue el servidor freeRADIUS [5] el escogido, ya que se ajustaba perfectamente a nuestras necesidades, en cuanto a las configuraciones que soporta y por tratarse de un producto de libre distribución, y por tanto gratuito. En lo que respecta a la encriptación de la información transmitida, desde que se comenzaron a asentar las bases teóricas de este trabajo se supo con certeza que los estándares que debían ser utilizados para cifrar la información serían WPA y WPA2. Esta elección era clara debido a que son los protocolos más actuales (sobre todo en el caso del WPA2) y, además, el abanico de posibilidades no es tan amplio como puede ser para la protección de los datos en el proceso de autenticación.

Resaltar que deben ser ambos, WPA y WPA2, los protocolos configurados, ya que, aunque WPA se lleve utilizando ya varios años, existan algunas dudas sobre su total hermeticidad, y el WPA2 haya sido desarrollado como su sustituto natural, existente aún demasiados dispositivos móviles cuyas antenas no reconocen el protocolo WPA2.

En cuanto al método de autenticación, no fue posible cumplir la premisa de ofrecer a todos los grupos de usuarios el mismo método, debido fundamentalmente a la estructura de la red existente. Por una parte, se descarto la utilización del EAP-TLS, debido a la necesidad de certificados de usuario que, por un lado, generaría una gran carga de trabajo por parte de los administradores de red, y por otra estaríamos obligando a los usuarios a instalar un certificado, complicando la utilización del servicio.

Por tanto, se hizo necesario escoger entre el protocolo EAP-TTLS y el PEAP. La elección se realizaría en base a las bases de datos de usuarios utilizadas. Las credenciales de los alumnos se encuentran almacenadas en el etc/passwd y etc/shadow, del servidor RADIUS utilizado para el servicio de correo electrónico.

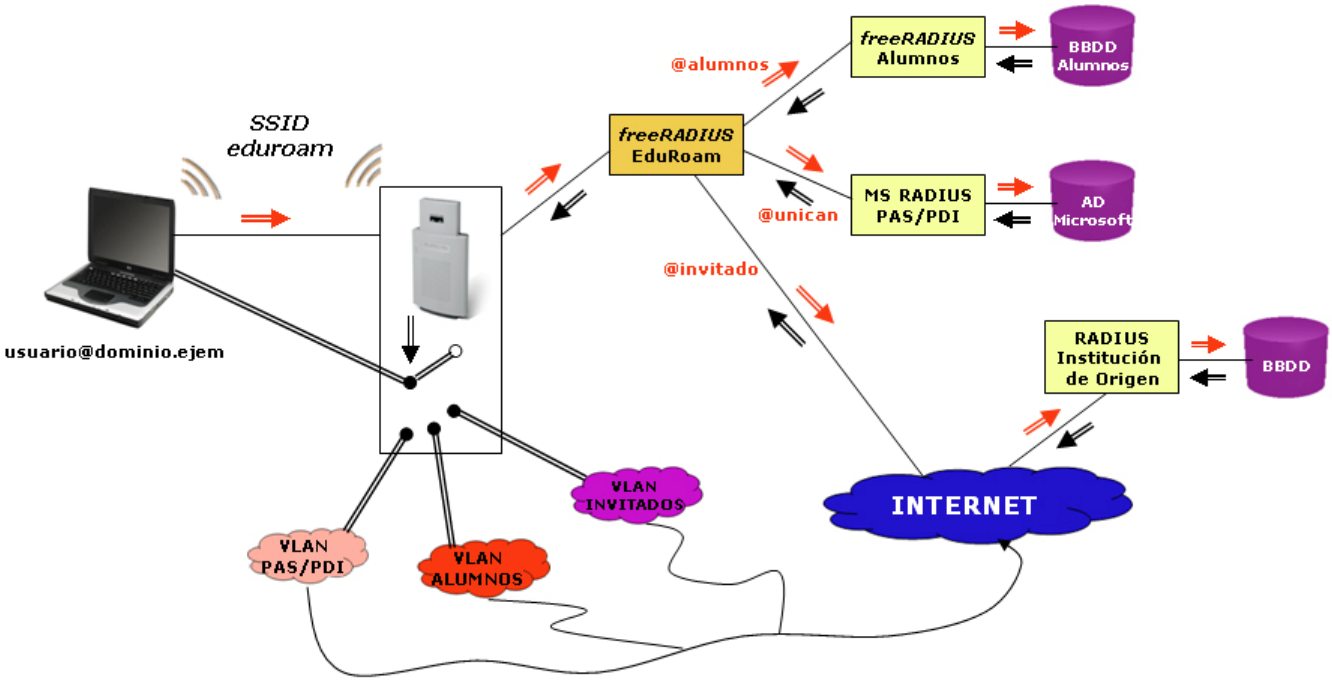

Fig. 2. Esquema general del desarrollo propuesto.

En el caso del PAS/PDI, las credenciales se encuentran en el *Directorio Activo de Microsoft*. Finalmente, se decidió implementar EAP-TTLS en el caso de los alumnos, debido a que el protocolo PEAP utiliza la encriptación MSCHAPv2 para generar el túnel TLS por el que viajan las credenciales, y dicho protocolo necesita que las credenciales no se encuentren encriptadas, cosa que sucede en el etc/shadow. Sin embargo, la configuración relativa al PAS/PDI, se basó en el protocolo PEAP, que se ajusta a la medida al tipo de base de datos existente, puesto que es el protocolo de autenticación desarrollado por Microsoft. Además, en ningún caso sería posible la implantación del EAP-TTLS, debido a que el IAS de Microsoft no soporta dicho protocolo. El método de autorización escogido fue la división de la red en distintas VLAN's, y la utilización del firewall del propio servidor Linux de EduRoam para la creación de políticas. Básicamente consiste en asociar a cada grupo de usuarios una VLAN, otorgando al usuario una IP del rango que le corresponda, y de esta manera enviar todos los paquetes de información a través de dicha VLAN. Mediante el fichero IPTABLES del servidor Linux se establecerán las restricciones o privilegios que tenga el usuario en función de su IP. El fichero IPTABLES permite multitud de configuraciones, denegando todos los servicios y abriendo solo algunos puertos concretos (http, ftp, IMAP,…), o bien, dejando pasar toda la información y negando el acceso a ciertos servicios (como el P2P por ejemplo).

En cuanto a la auditoría de las sesiones de autenticación y el acceso a la red, en base a las políticas del proyecto EduRoam, se han considerado suficientes, la utilización de los ficheros históricos (ficheros de log) generados tanto por el servidor RADIUS, como por los propios puntos de acceso, así como también los datos guardados en el fichero 'messages' del propio Linux. De estos ficheros se obtiene toda la información acerca de la sesión de un usuario: hora de comienzo y fin de la sesión, VLAN utilizada por el usuario, IP otorgada, método de autenticación utilizado, paquetes de información enviados y recibidos, punto de acceso al que se ha conectado, motivo de la desconexión, etc.

V. Conclusiones

Desde el punto de vista económico los resultados de la solución aquí adoptada han sido inmejorables, debido al empeño en utilizar software libre. La faceta más importante ha sido el facilitar al máximo el acceso de cualquier usuario autorizado a la red, y que dicho acceso sea seguro, tratando de conseguir una protección adecuada de los datos transmitidos a través de la red inalámbrica. En este aspecto hay que resaltar un pequeño inconveniente, debido a la imposibilidad de conseguir que todos los grupos de usuarios puedan acceder del mismo modo a la red, y tampoco evitar que ciertos usuarios cuyo software propietario de la tarjeta inalámbrica, no soporte la autenticación EAP-TTLS, deban instalar una aplicación SecureW2 adicional. Hay que destacar que este pequeño inconveniente viene condicionado por otro de los objetivos iniciales del presente trabajo: la adaptabilidad a la estructura previamente existente. En este aspecto, los resultados han sido óptimos, y se ha conseguido utilizar de forma prácticamente transparente dispositivos y servicios ya existentes, lo que ha producido unos mejores resultados económicos. Además. mediante el presente trabajo se ha logrado, incluir a la Universidad de Cantabria en la iniciativa EduRoam, permitiendo, a los usuarios de nuestra institución, que visiten otras universidades, y a los visitantes de nuestra universidad, obtener un acceso a la red inalámbrica más cómodo y sencillo.

Agradecimientos

Los autores agradecen la colaboración del personal del servicio de informática de la Universidad de Cantabria, así como el soporte económico del Gobierno de Cantabria a través de la consejería de Industria.

Referencias

[1] Wi-Fi Alliance - www.wi-fi.org
[2] Iniciativa MovIRIS - www.rediris.es/moviris
[3] Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) - www.ieee.org
[4] Proyecto EduRoam – www.eduroam.org
[5] FreeRADIUS – www.freeradius.org.