# Accessing an existing virtual electronic patient record with a secure wireless architecture

Ana Ferreira, Luís Barreto, Pedro Brandão, Ricardo Correia, Susana Sargento, Luís Antunes

## Abstract

Virtual electronic patient records (VEPR) enable the integration and sharing of healthcare information within large and heterogeneous organizations by aggregating known data elements about patients from different Information Systems in real-time. However, healthcare professionals need to access a terminal every time they treat a patient. This may not be trivial as computers are not available around every corner of big healthcare institutions. The use of wireless technology can improve and fasten healthcare treatment because it can bring information and decision to the point of care allowing also for healthcare professionals' mobility. However, as healthcare information is of a very sensitive nature, it has to comply with important security requirements. The wireless technology makes it more difficult for these requirements to be achieved as it is harder to control disruptions and attempts to access information can be more common and less simple to detect.

The main objective of this work is to model, develop and evaluate (e.g. in terms of efficiency, complexity, impact and against network attacks) a proposal for a secure wireless architecture in order to access a VEPR. This VEPR is being used within a university hospital by more than 1000 doctors, on a daily basis. Its users would greatly benefit if this service would be extended to a wider part of the hospital and not only to their workstation, achieving this way faster and greater mobility in the treatment of their patients.

**Keywords -** Electronic patient records, healthcare professionals' mobility, access at point of decision, wireless standards, information security.

# Introduction

Virtual Electronic Patient Records (VEPR) enable the integration and sharing of healthcare information within heterogeneous organizations (Blobel, 2004). Hospitals are an example of such healthcare institutions with great turnover in terms of healthcare professionals. However, there are usually some constraints in terms of physical location as well as technology in order to access it. Healthcare professionals need to access a terminal in order to get information about the patients they are treating. This may not be easy to attain within a big and complex healthcare institution where computers are not available around every corner.

The use of wireless technology tries to take this integration further. It allows access to patient data and processing of clinical records closer to the point of care. The ubiquitous access to information can minimize physical as well as time constraints for healthcare, enhancing users' mobility within the institution. There have been some experiences with the use of wireless technology in the healthcare environment. These have shown that healthcare professionals were usually satisfied with the use of portable devices to access patient information. They save time and are bound to improve patient care (McAlearney, Schweikhart, & Medow, 2004). The most common devices include mobile wireless patients' health monitoring systems. These equipments add more security concerns (Ramon Marti & Jaime Delgado, 2003) but are out of the purpose of this research.

Among other problems, the lack of security processes is one of the main reasons for the difficult integration of VEPRs into medical processes, within large environments such as hospitals (Benson, 2002). The lack of security increases users' reluctance for VEPRs' acceptance. Both patient and healthcare organization trust can be seriously damaged if no proper security is provided (Denley & S. W. Smith, 1999)

Furthermore, wireless technology adds a higher level of security issues. Disruptions and attempts to access information can be more common and easier to try, and less simple to detect and control; so security needs to be studied and analysed thoroughly before wireless networks are implemented in a larger scale within a hospital (Dixie B. Baker, 2003). Security requirements need to be considered and applied from the beginning to the end of a system's development and implementation (Ana Ferreira, Ricardo Correia, & A. Costa-Pereira, 2004; Ana Ferreira et al., 2005; Ana Ferreira et al., 2004).

This chapter proposes a wireless architecture in order to model access to an existing VEPR within a university hospital that can provide an extra security layer to the wired system. The next section describes the VEPR architecture along with the security requirements for the wireless version. The third section presents the wireless architecture that uses the latest wireless standards and security protocols and takes into account the security services that were implemented within the wired version of the system. Section four describes an evaluation of the proposed solutions against network attacks and its efficiency in terms of complexity and impact on the network. The last section discusses the results and shows some of the challenges where to focus future research.

# The Virtual Electronic Patient Record

With the objective to face one of the major problems within large and complex health organizations - data retrieval and integration - a VEPR was built within a University Hospital with over 1350 beds, by the Biostatistics and Medical Informatics Department, at the Faculty of Medicine in Porto. This system provides a cost-effective solution for most clinical information needs (Ricardo Cruz-Correia et al., 2005).
Currently, more than 1000 doctors use the system on a daily basis. Other healthcare professionals (namely nurses) are expected to start using it soon.

## Architecture

This VEPR allows the collection, integration and availability of clinical reports providing an up-to-date overview of a patient medical history at all points of care. The system uses a traditional three layered approach composed by presentation, business and data layers.
The presentation layer is composed by a web application (VIZ) and a package of graphical user interface components to be used by third party applications. The web-interface was designed to include graphical components and layouts to summarise past patient data (patient chronological bars), and folders that reproduce the traditional types of patient record organisations (source, chronological and problems views).
The application layer is composed by an integration engine (Multi-Agent system for Integration of Data – MAID), and a set of web-services that allow access to the data layer. The data layer includes all repositories, namely the CRep that comprises the VEPR database and clinical documents file system, the central patient system (SONHO) and the hospital statistics system (IEG) (Figure 1).
MAID collects clinical reports from various hospital Departmental Information Systems (DIS), and stores them on the central repository (CRep) consisting of a database holding references to these clinical reports and a file system where reports are stored. After searching the database, VEPR users can access the integrated data of a particular patient through the web-based interface (VIZ). When selecting a specific report, its content is downloaded from the central repository file system to the browser. MAID (the agents' server) communicates with the DIS using XML. MAID connects to the database server through JDBC[1] and operates the files using NFS protocol[2]. The application in the Web Server (VIZ) communicates with the CRep database server using OCI/PHP (Oracle Call Interface with PHP: Hypertext Preprocessor Language) functions and operates the files using NFS protocol. The Web browser client accesses the Web Server using HTTPS protocol. The Web services connect to the CRep database server, SONHO server and IEG server using JDBC, and use SOAP messages to deliver information to the GUI Components.
The VEPR has been working for 4 years, regularly scanning eleven DIS and collecting a mean of 3000 new reports each day (currently holds about 3 million documents). A viewing module for the VEPR was made available in October 2004. Integrated DISs have evolved to send different documents to the VEPR without the need of any type of adaptation.

[1] Java version of the Open DataBase Connectivity (ODBC) designed by Microsoft to provide a common API for accessing databases.
[2] Network File System is an IETF protocol to allow client systems to access remote storage as if it were locally available.

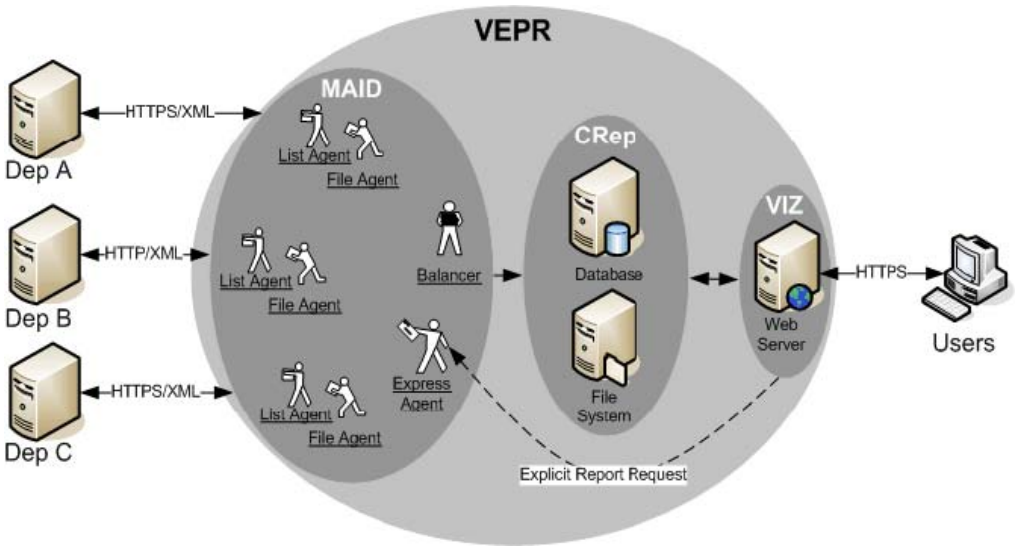


Figure 1. VEPR generic architecture.

## Integration and communication

The integration of hospital data in VEPR is accomplished with the use of different agents assigned to different tasks. Some collect reports' references and others the actual reports from the DISs. When a user requests a report whose file is not in CRep, there is an explicit report request made directly to MAID, by the VIZ module. This request activates the express agent from the agent platform in order to get the report requested by the user, from the right department (Figure 2).

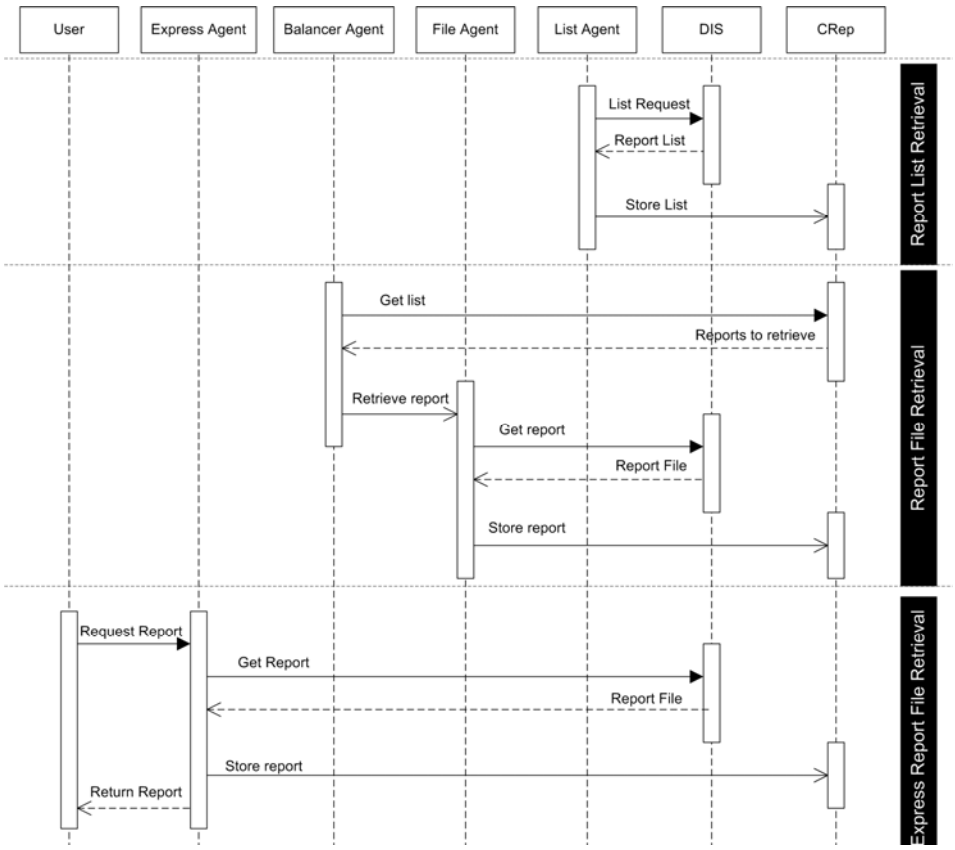


Figure 2. UML sequence diagram of the VEPR

Several integration models had to be used to achieve the necessary integration level. The selection of appropriate integration model was often conditioned by the maturity of the IS being integrated, and by the resources available at that time. It should be noted that the development of communication interfaces was simpler for the eight applications that had Web interfaces because they were already using standard communication protocols such as HTTP. Web-services and shared graphical components were very useful in delivering an integrated view to other ISs.

The process of integration of heterogeneous clinical information systems has shown the existence of organisational or technical problems and, indirectly, contributed to its solution. While some reports cannot be associated with identified hospital patients (e.g. outpatients who are not administratively considered as Hospital patients), some patients had multiple, rather than unique, identification numbers, making their correct identification difficult. A similar problem was found with staff identification numbers, which were reused after staff members left the hospital.

## Statistics

VIZ was made available for testing in October 2004 but only started to be known and routinely used since December 2004. The number of sessions and report views has been growing steadily since. The number of sessions increased 147% in 2006, and 70% in 2007. The number of distinct users using the VEPR has also grown in the same period, representing an annual growth of 29% users in the 4$^{th}$ quarter of 2006 and 41% in the 4$^{th}$ quarter of 2007. Currently, 4$^{th}$ quarter of 2007, 1.24 reports are viewed per session, 0.4 reports are viewed per patient encounter and 82.4 reports are

viewed per user. Also the use of the VEPR is more widespread by the hospital computers (975 computers in 4th quarter of 2007).
The number of report views per user per patient encounter has stabilized around 3.8 views per user per 10 000 encounters since the first quarter of 2006.
The number of direct access to the VEPR from the computer desktop hyperlink has been diminishing since the first quarter of 2006, whilst the number of accesses that originate in the Hospital Patient Record (SAM) as been growing. The number of report views from other referrals is small when compared with direct access and hospital patient record. The number of views per session for direct access is 1.81, for the DISs is 1.20, for the Hospital Patient Record is 1.18 and for the Emergency Department IS is 1.05.
The introduction of wireless technology will allow the access to this VEPR system to a wider number of people and locations. The healthcare professionals will be able to access patient information whenever they need without having to return to their workstation. This allows overcoming most physical and logical obstacles that the hospital offers, therefore increasing VEPR availability.

## Security and monitoring

VEPR present many security challenges namely the need to provide protection to patient's sensitive information. The implementation of security mechanisms was thought from the beginning of the project's development and implementation, allowing for its better integration and acceptability (Ana Ferreira et al., 2004). This subject was tackled according to the three main security characteristics: integrity, confidentiality and availability. One of the main security issues relies in the information collected in the stored patient reports. Digital signatures are security mechanisms that provide the integrity of a report by enabling the detection of unauthorized modifications. If the digital signature does not match the report contents then this report is marked as not valid (Ana Ferreira et al., 2004). Confidentiality relates mainly to the access to sensitive information by authorized individuals. It is obtained by controlling access to information and by protecting it while in transit along network communications. Access control policies were defined by the hospital administration after a proposal from a specifically assigned committee defining roles and levels of access to VIZ. These policies were implemented using Role-Based Access Control (RBAC) (Ferraiolo, Sandhu, Gavrila, Kuhn, & Chandramouli, 2001), an access control model used for large organizations (Ana Ferreira et al., 2005). In order to provide for an efficient way for user identification and authentication, development of access control tools was based on ENV 12251 European pre-standard (CEN, 1999). As the network wiring and equipment is spread all over the hospital, it is necessary to protect the network infrastructure from eavesdropping. This was accomplished using TLS authentication protocol (B. Aboba & D. Simon, 1999) which provides encryption of all information whilst in transit. Availability focuses on means to provide for the continuous access to information by authorized users. Equipment and power redundancy, backups and system monitoring were all put in place to guarantee availability of the system at all times. The number of reports daily retrieved from each DIS is compared to what is expected and the number of sessions of different users is monitored. Any deviation from expected values triggers an alert message to the system administrator.
Monitoring sensors have also been developed within the VEPR in order to detect problems in any of the three security characteristics, as well as for instance systems' malfunctions, errors, services that are not working and even improper behaviour. As

an example, to detect users that share their logins and passwords the logs of sessions from October 2004 until December of 2007 were analysed. The suspicious behaviour that was searched for was users working for more than 24 hours (in some cases doctors work for 24 hours consecutively). All user sessions that started less than 10 hours from the last session were considered to be referring to the same working day.
The number of suspicious cases found was 508; the calculated working days ranged from 24 to 63 hours (average = 29 hours). These working days referred to 139 of 1434 logins ($r_{VPR}$=9.7%). The 10 logins that more frequently have suspicious behaviour referred to the following medical specialties: Anaesthesiology (4 logins), Emergency (2 logins), Infectious Diseases (2 login), Cardiothoracic Surgery (1 login), Gastroenterology (1 login).
Although technical solutions exist to provide secure access control, they demand a clear definition of permissions for each group of actors. Healthcare organisations must comply with current legislation, ethical rules and internal processes which are very difficult to be objectively defined into access control rules. The number of shared logins found may probably just represent the tip of the iceberg. However, it is high enough to raise concern.

## Security requirements

All the security services implemented for the wired VEPR mentioned in the previous section are obviously valid for the wireless architecture.
The wireless technology stresses however the need for extra layers of security. In order for a healthcare professional to access the VEPR with a wireless device, there are 3 main security issues to address:

1) Authentication & authorization from the wireless to the wired network;
2) Secure communications of information in transit;
3) Integrity & trust in the information that is requested and visualized by the users.

For (1) there is the need to create an access control infrastructure that will prevent problems of confidentiality such as masquerading and password sniffing. Also, policy rules need to be set so that access from the wireless to the wired network is properly controlled. Still, the process of access control must be transparent to the users and simple to use and manage.
Point (2) requires that information in transit must travel encrypted at all times to avoid eavesdropping. It should always be available in a certified and trusted manner.
For (3) there is the need for the means to guarantee that the information in transit within the wireless network is protected from unauthorized or accidental modifications. Healthcare professionals must trust the information they use to treat patients. The most accurate and correct it is the better and adequate the treatment will be.

# Proposed wireless architecture

As previously mentioned, users of healthcare environments would greatly benefit with the availability of information anywhere through a Wireless Local Area Network (WLAN). Usually, the healthcare institution where the WLAN is going to be deployed has already a LAN in use. Setting a WLAN on top of this one is seldom trivial. Building dimensions, user locations, connectivity and the security requirements previously mentioned account for the stringent issues. The need for a good location map and distribution is essential for tackling the first two issues. The last two will be the focus of this section. Healthcare professionals must trust not only the technology they use (e.g. robust, usable) but also the information they access. They need quick and reliable access to carry out their job, or the system will be circumvented (Lehoux, Sicotte, & Denis, 1999).

Another important concept is the requirement to access the VEPR infrastructure from outside the local network (eg. from the internet) (Yu & Jothiram, 2007). Also the security in pervasive sensor networks for healthcare monitoring (Ng, Sim, & Tan, 2006) is another relevant trend. These subjects are however outside the scope of this discussion.

This section describes some possible solutions to support security in WLANs. These include a general framework to communicate authentication details (EAP) to allow or deny network access and exchange cryptographic material (802.1X). Building on these, WPA and 802.11i (WPA2) are able to control the access to the network and provide encryption of the communications. IPsec addresses authentication and encryption at the network (IP) layer whereas the previous technologies lie on the data link (medium) layer. The next sub-sections describe all these technologies in more detail.

## Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) (B. Aboba, L.Blunk, J. Vollbrecht, J. Carlson, & H. Levkowetz, 2004) is a general authentication protocol defined by the IETF. It was originally developed to be used with a point-to-point protocol. EAP provides an interface to several authentication mechanisms, as Kerberos, public key ciphering or one time passwords.

EAP cannot be used independently as an authentication protocol. It is just a set of rules of how an authentication server and a client can exchange messages and provides a pluggable architecture for different security protocols. EAP uses the data link layer for message exchange, and so does not require IP addresses for communication.

A network with EAP capabilities has three independent identities: the client (also known as supplicant), the authenticator and the authentication server. The client has to deliver the authentication credentials (a certificate or a username and a password). The authenticator is the equipment that implements security at the port level and does also network access control. According to the EAP authentication protocol used, the authenticator re-transmits the necessary messages, between the client and the authentication server, acting as an intermediary and enforcer in the authentication request. The authentication server specifies the authentication protocol to be used and validates the credentials delivered by the client.

EAP enables the support of multiple authentication protocols without the need to configure the authenticator with each specific authentication mechanisms. EAP allows also the authentication server to control which authentication protocols should be

supported. These features increase flexibility to the process and allow greater interaction.

## 802.1X

IEEE 802.1X (IEEE 802.1X, 2004) is a network security specification initially developed for wired networks, with its concepts and utilization extended afterwards to wireless networks. 802.1X defines a network access control based in ports. It was developed to deny or accept requests based on user authentication information (credentials). 802.1X uses EAP for authentication. The access control is performed at the Medium Access Control (MAC) level and is independent from the physical layer. A port in 802.1X is any type of controlled access element (i.e. switch, router, AP). In this context, the association between one client and one AP is called a virtual port and the access to the network is seen as another virtual port. The client associates first if the port is available and uses this connection to authenticate. If the authentication is successful the AP gives access to the network (thus granting access to the network virtual port). 802.1X provides keys for each client and session. This means that keys have to be regularly changed, thus reducing repetition problems.
The 802.1X three main processes are the mutual authentication between the client and the server, the cryptographic keys dynamically generated after authentication and the centralized policy control.
802.1X is not a protocol; it is an authentication and key management process. In a wireless network it defines authentication and the dynamic generation of cryptographic keys. The ciphering is accomplished using any of the wireless security protocols.

## WPA – security and architecture

WPA ("(Wi-Fi Protected Access)") was developed with the aim of decreasing the problems associated to Wired Equivalent Protocol (WEP)[3] (Walker, 2003). WPA is based on the principles of the IEEE802.11i standard (IEEE 802.11i, 2004) with some simplifications to be compatible with the equipments at the time WPA was released. WPA uses a robust cipher algorithm and introduces user authentication, one of the WEP missing characteristics.
WPA is intended to be implemented in a home/office environment and is available in all Access Points (APs) and Network Interface Cards (NICs) currently available[4].
To improve data codification, WPA uses the Temporal Key Integrity Protocol (TKIP) (IEEE 802.11i, 2004) which, when compared to WEP, improves data level ciphering by using temporal and per packet keys. WPA also has a key mixing function for each packet, a Message Integrity Check (MIC), extended initialization vectors (IV) with sequential rules and a key renewal mechanism.
WPA makes use of 802.1X for user authentication, making it possible to use one of the EAP methods. For security matters in these environments, the EAP- Transport Layer Security (TLS) (B. Aboba & D. Simon, 1999) method is used. This method uses digital certificates for each user authentication. A central authentication server is used to manage mutual authentication, which apart from authenticating the user, it eliminates the danger of rogue APs. The authentication server usually employed is the Remote Access Dial-In User Service (RADIUS) (C. Rigney, A. Rubens , W. Simpson

[3] WEP is part of the original 802.11 standard.
[4] Some older products that do not support directly WPA can (most likely) be software upgradable.

, & S. Willens, 1997). The RADIUS server authenticates the WLAN user and determines the session key to be used. RADIUS is only used to communicate between the AP and the authentication server; in the WLAN, EAP is used between the user and the AP (
Figure 3). Notice that other Authentication, Authorization and Accounting (AAA) protocols (Kim & Afifi, 2003) could be used such as Diameter (Ventura, 2002), COPS (Durham, Boyle, Cohen, Rajan, & Sastry, 2000) or TACACS (Finseth, 1993) server. However, RADIUS is used for WPA.

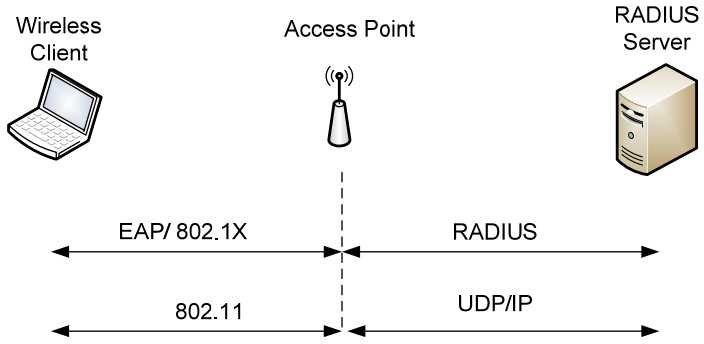


Figure 3. Authentication architecture

A Lightweight Directory Access Protocol (LDAP) (J. Hodges & R. Morgan, 2002) server can also be used for a centralized user authentication. All RADIUS implementations can interact with an LDAP server, making it possible to use a central point of administration of all users, thus creating a strong security policy. Other centralized user authentication implementations that can use LDAP are Active Directory (Microsoft, 2004) and Novell eDirectory (Novell, 2004).
For connectivity between the different networks a layer 2 or 3 switch is used. This type of switch adds a new layer of filter/protection to the system with the use of Virtual LANs (VLANs) and, if needed, allows to route data between the different networks. This solution provides an access level linked to the security standard used by the clients. The proposed architecture uses two security VLANs. These VLANs are configured in such a way that only WPA and 802.11i clients are able to access all network services. The VLANs distinguish, transparently to the user, the security protocol used by the client and trigger all the necessary and specific procedures needed for authentication and authorization.
The implementation of a WPA system requires the development of an 802.1X infrastructure. All the necessary elements for building a WPA network are shown in Figure 4.
It is worth noting that that there is a possibility of using a password based user authentication (for either WPA or 802.11i). However, this approach is not recommended in high security infrastructures (Moskowitz, 2003).

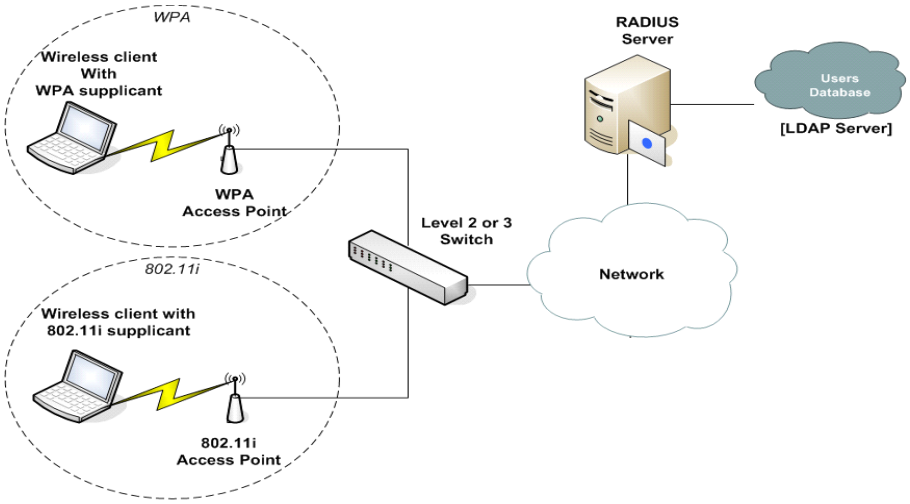


Figure 4. WPA and RSN/IEEE802.11i architecture.

## 802.11i security and architecture

In June 2004, the Institute of Electrical and Electronics Engineers (IEEE) ratified the 802.11i standard, also called Robust Security Network (RSN)[5] (IEEE 802.11i, 2004). This security standard includes the following functionalities: uses the Advanced Encryption Standard (AES) (NIST, 2001) block cipher to encrypt the data packets, 802.1X for user authentication and TKIP for the management of the cipher keys. The standard also recommends a set of new improvements to WEP in 802.11b NICs. Some NICs, due to design limitations, cannot support AES but are able to support TKIP with a small update.

802.11i requires that all clients announce their cipher capabilities in their AP association requests. The AP and the wireless client then establish the appropriate channel for data ciphering. This key agreement is based on their mutual cryptographic capabilities and configured in one of the security policies (eg.: "allowing only associations with AES clients"). Moreover, 802.1X authentication assures key renewal during a session.

AES is currently widely recommended for confidentially. However, AES entails more demanding cryptographic functions. This means that older devices do not have processing capacity to handle AES and keep a normal network performance. To circumvent the problem 802.11i enables the use of TKIP as the cipher protocol. This method is more feasible for less capable devices. Nonetheless, there is already a wide selection of products compliant to 802.11i and WPA2 (including some PDAs)[6].

802.11i actually defines three protocols for data protection: the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) (Whiting, Housley, & Ferguson, 2003), the Wireless Robust Authenticated Protocol (IEEE 802.11i, 2004) and TKIP. CCMP will be the *'de facto'* IEEE802.11i cipher protocol. It is based in AES counter mode. This protocol derives from lessons learned with 802.10 (IEEE 802.10, 1998) and IPsec protocols. It uses strong cipher primitives, which makes it reliable against all (currently) known attacks.

As with WPA, for implementing an 802.11i solution it is necessary to deploy an 802.1X infrastructure.

Figure 4 shows the required elements to support an 802.11i architecture.

[5] The Wi-Fi Alliance certifies products compliant to 802.11i as WPA2.

[6] See http://certifications.wi-fi.org/wbcs_certified_products.php?advanced=1

## IPSec – security and architecture

The two previous solutions are specially designed for wireless networks. However, it is also possible to protect these networks with a network layer protocol originally developed for wired networks, like IP Security (IPSec) (B. Aboba et al., 2004). This protocol, though intended to protect Internet communications and wired networks, has some characteristics that make it suitable to protect wireless communications. While the previously mentioned solutions protect the information at the data link layer, IPsec protects the information at the network layer. This functionality makes it a versatile protocol, which can be used to protect any kind of IP network, and is independent of the application and type of data flow. It comprises a set of protocols for the development of Virtual Private Networks (VPNs).

IPsec VPNs are a very common method for protecting data that traverses public networks (or non-protected networks). IPsec adds security through a set of tunnelling and ciphering mechanisms: it implements network layer authentication and ciphering; keeping end-to-end security within the network architecture. Its main advantage is that it can protect any kind of data packet routed through the network independently of the source application[7]. Its main disadvantage is its complexity.

IPsec has two modes of operation: tunnel and transport. In tunnel mode IPsec protects a completely normal IP packet, thus its payload is an IP packet. This mode is used when the IP packet needs to be sent unchanged to the destination. Transport mode IPsec is integrated with IP and thus transports an UDP/TCP packet from the transport layer.

The IPsec standard includes two security protocols: the Authentication Header (AH) (Kent & Atkinson, 1998a) that provides data integrity and the Encapsulating Security Payload (ESP) (Kent & Atkinson, 1998b) that adds confidentiality. All IPsec parameters are negotiated using the Internet Key Exchange (IKE) (Harkins & Carrel, 1998) protocol. IKE uses digital certificates for end points authentication. ESP makes use of cipher techniques for data confidentiality, and digital signatures for source authentication, while AH only uses digital signatures for source authentication (AH does not cipher data). Thus ESP should be used when confidentially is an issue.

Figure 5 shows an IPsec VPN adapted to a wireless network and the elements required for an IPsec protected wireless network.

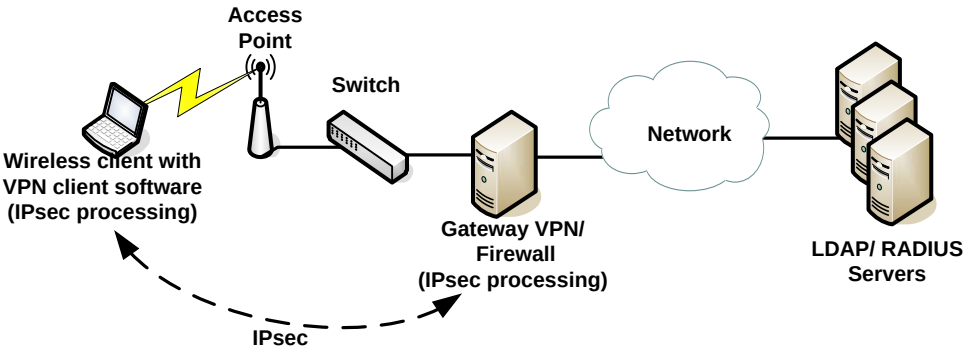


Figure 5. Wireless network IPsec VPN.

[7] Note that WPA and 802.11i also are independent of the source application.

The network has wireless terminals with VPN client software. This software should be able to start protected tunnels between the terminals and the gateway. The firewall assures the right establishment of a tunnel and also guarantees that only specified devices can establish that tunnel. Recent Windows OS have a native VPN client. The wireless terminal connects to the AP that offers, between the wireless and the wired networks, initial filters to the IP protocol. Between the AP and the wired networks there is a layer 2 switch responsible for the connectivity. Recent models of this kind of switch allow Virtual LAN Access Control Lists (VACL), which adds a new filter/protection layer to the system (as discussed previously). As in the previous architectures, LDAP and RADIUS servers are used for centralized user authentication.

## Wireless architecture proposal

This section discusses a secure wireless architecture for accessing the VEPR taking into account the specific characteristics of a health care institution (importance of security) and the characteristics of the available solutions. This architecture uses the WPA-TLS protocol and also considers the use of the new 802.11i standard. All existing equipments can, with a small firmware upgrade, support WPA-TLS and therefore, be reused reducing implementation costs. WPA-TLS should only be considered a transition solution until all devices support 802.11i.

As such, the aim is to support WPA and 802.11i into a single network. The way to accomplish this is by dividing the physical network into separate logical security networks. Most of the last generation APs support WPA and 802.11i protocols, as well as the ability to create separate service set identifiers (SSIDs)[8].

Therefore, in the proposed architecture, each AP is configured with two different SSIDs (SSID=802.11i-VEPR and SSID=WPA-VEPR) and two different security protocols. The APs are enabled with both 802.11i and WPA. This configuration creates a secure logical network, allowing healthcare professionals to have a secure and controlled access to the VEPR. A RADIUS server acts as the policy enforcement point (PEP), configured with different access control policies for each SSID[9]. These policies define the data protection protocol, the key management protocol and the key length used with a specific SSID.

The RADIUS server is coupled with the actual VEPR solution in terms of user management. The previous sections discussed the use of LDAP for the VEPR. For this case, the RADIUS authentication should use the LDAP of the VEPR. This is very important as it will enable the use of the current VEPR access control in the new wireless architecture.

As expected, all terminal/client equipments should support either WPA-TLS or 802.11i.

Figure 6 shows the proposed architecture, where the two logical secure access networks are presented.

[8] SSIDs identify the network that a device is connecting to.

[9] For technical reasons the AP needs to map SSIDs with VLANs. The AP marks all IP packets with the VLAN associated with the corresponding SSID. For interconnecting the AP and the RADIUS server, a layer 2 or 3 switch is used.

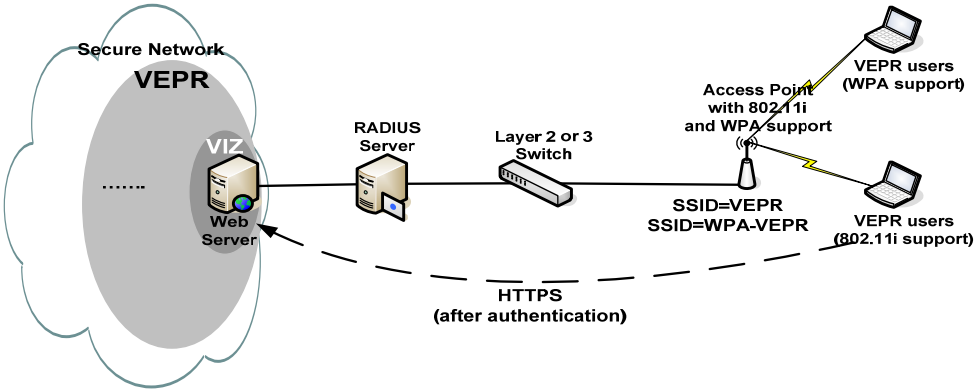


Figure 6. VEPR secure wireless architecture.

# Evaluation and insights

This section presents an evaluation of the security and performance capabilities of WPA EAP-TLS. IPsec. 802.11i is not addressed due to the unavailability of 802.11i compliant devices at the time the experiments where undertaken. The discussion comprises the evaluation of the proposed solutions against network attacks and its efficiency in terms of performance and impact on the network.

## General *testbed*

The *testbed* built to perform the experiments is depicted in **Erro! A origem da referência não foi encontrada.**7. Unless otherwise mentioned, all the experiments hereby described were built upon on open source operating systems and tools. The FreeRADIUS (FreeRADIUS , 2008) implementation was used as the RADIUS server. For the public key infra-structure the OpenSSL (OpenSSL, 2007) suite was used. The IPSec infrastructure was implemented on FreeSwan (FreeS/WAN Project, 2004). The software was installed in computers running the Linux Operating System. In the IPsec tests, open source software was also used to implement Access Points: HostAP (HostAP team, 2007). This software allows building a fully functional AP. In the WPA infrastructure, the wpa_supplicant software (HostAP team, 2007) was employed.

The (Ettercap Team, 2005) tool was used to perform the tests/security attacks.

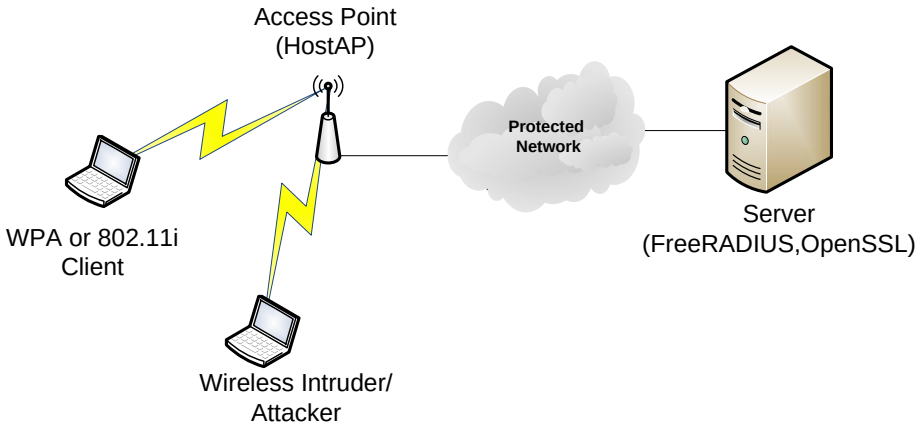


Figure 7. Wireless architecture used for testing procedures.

## Security experiments

The network reaction to network attacks was observed in order to evaluate the security of the proposed solutions. These attacks comprise man-in-the-middle (MITM), impersonation, Denial of Service (DoS) and session hijacking.

In the MITM attack an intruder tries to see (“sniff”) the information exchanged between the active hosts and insert itself in the middle. This allows the intruder to eavesdrop the communications and even alter the data exchanged. A basic approach for this attack, when no security is used, is a technique called arp spoofing (Whalen, 2001).

In the impersonation attack an intruder tries to use the same IP address and the same hostname, as one of the valid clients of the network, to get access to network resources. It differs from the MITM attack in that the attacker’s objective is only to

access the network. So the intention is not to eavesdrop or alter the data exchanged by the valid host.

The session hijacking consists in an intruder trying to obtain full control of a client successful session. It is an extension of the impersonation attack, where the attacker needs to use the session credentials/identifiers from the valid host to steal its current session. It may use a MITM attack to acquire such information.
The Denial of Service (DoS) attack consists of disabling some (or all) of the network services (for example denying authentication) by overwhelming the targeted service. The ultimate objective is to deny network access.

## IPsec results

In the IPsec solution, the DoS attack was only successful before the establishment of the IPsec tunnel; after the establishment of the tunnel the attack did not succeed. For the MITM attack, the *arp spoofing* option was used. We observed that, with the IPsec tunnel established, the MITM attack did not succeed (it was not possible to see or detect any kind of data flow). The impersonation attack also did not produce any result. For this attack an intruder used the same network address and hostname of a recognized client and then tried to establish an IPsec tunnel. As IPsec uses digital certificates for client authentication, the intruder is not authenticated and the tunnel is not established as was expected. Finally, the same negative results were achieved with session hijacking.

## WPA/EAP-TLS results

The same tests were performed to the WPA EAP-TLS implementation. One advantage of the WPA solution is that it is a link layer security protocol. As ettercap is a tool that relies on the network layer, it was not possible to do MITM, impersonation and session hijack attacks. Other tools were also used to try to break the security of WPA such as Cain e Abel (Oxid IT Team, 2005) and Kismet (Kismet Team, 2004). However, none of them was able to achieve a successful result. On the other hand, DoS attacks were performed with a high percentage of success. WPA disconnects the network for 1 minute if it detects an attack against the MIC, this is done as part of a protection against brute force attacks. Although difficult, it is possible with a WPA client to trigger this behaviour with fake network access messages. This issue makes it possible to do a DoS attack against WPA, since it is just necessary to activate a WPA client and ask an AP for network access. The AP verifies the message and, if it detects a fake message, it blocks all network access, and stops all communications, including the access of valid clients. It is important to refer that, with the new 802.11i standard, this vulnerability has not been solved (Wullems, Tham, J. Smith, & Looi, 2004).

## Comments

From the above experiments we can conclude that the IPsec and WPA EAP-TLS solutions are very efficient against MITM, impersonation and session hijacking attacks. Both solutions are not efficient against DoS attacks. It is possible to successfully perform DoS attacks using freely available tools. For systems where availability is essential, it is necessary to complement those solutions with mechanisms that reduce the risk of such attack. It is thus necessary to use tools like Intrusion Detection Systems (IDS) and vulnerability scanners.

## Complexity experiments

The system performance was measured in order to evaluate the complexity introduced in the network elements. For this purpose the sysstat (Systat Team, 2008) and vmstat ("vmstat Man page") tools were used. These tools allow evaluating CPU utilization, memory and interrupts. The results given by those tools are shown in Figure 9 and Figure 10. The WPA experiment impacts on the WPA client and RADIUS server; in the IPsec experiment, the impact is on the VPN components[10] (see Figure 4 and Figure 5 for the architectures). The scale is the percentage of resource utilization except for the processes and interrupts that are absolute values. The pictures only show the RADIUS impact results for the WPA-TLS experiment, as they were negligible in the IPsec experiment. The presented results represent the average values obtained by 35 simulations, with a stochastic confidence interval of 90%.

An UDP flow of 54Mbps was used to represent a fully loaded network. These results show that the IPsec system requires more: CPU utilization, memory, interrupts and processes, therefore, its impact on devices' performance is not negligible. The results of WPA are similar to the ones of the plain system, introducing low impact in the network elements.

From Figure 9 and Figure 10 we can observe that different absolute results are obtained by each tool. This is due to the specific requirements of each tool and its design, i.e. the number of processes, memory usage and number of interrupts is influenced by the specific characteristics of each tool.

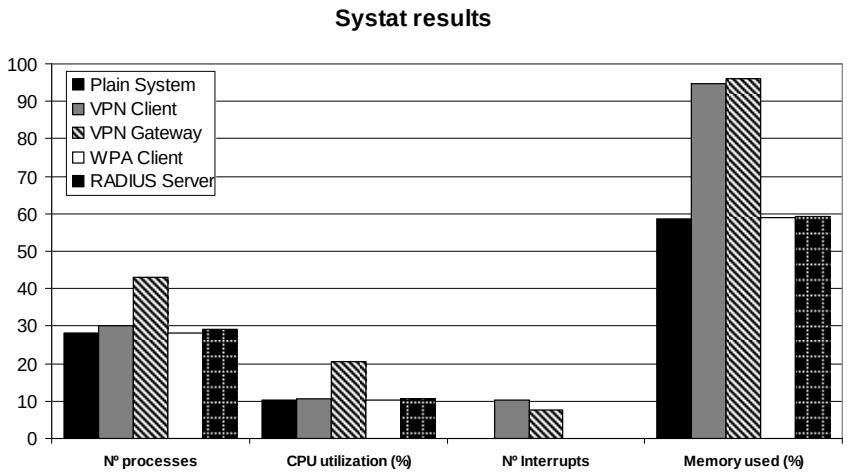


Figure 8. System performance – sysstat results.

[10] It was not technically possible to evaluate the impact on the Access Point.

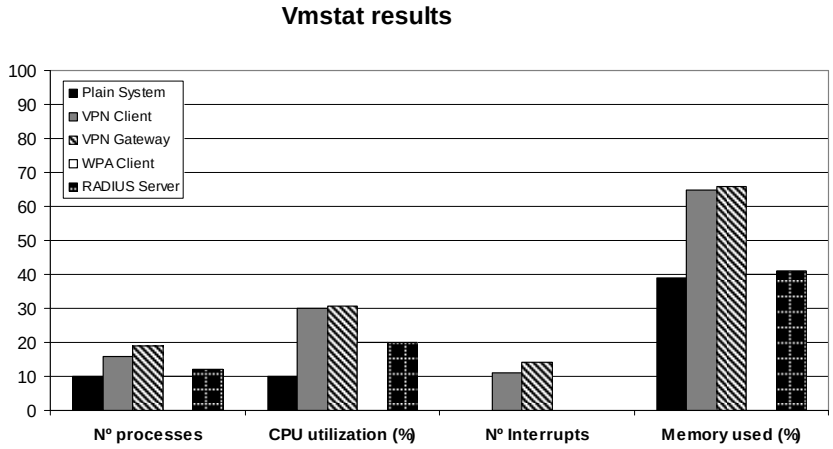


Figure 9. System performance – vmstat results.

Note that the processing of the WPA packets is done in the WPA client and the AP. Thus, the encryption/decryption occurs at these two elements. In the IPsec case the secure tunnel is between the VPN client and the VPN Gateway, thus not impacting the AP (

Figure 5).

## Impact on data flows

To evaluate the impact on data flow when the security mechanisms are in place, we performed experiments using TCP and UDP traffic, and considering a network with and without security implemented.

For traffic generation, IPERF (Iperf Team, 2005) and Crude (Crude team, 2002) tools were used. All traffic was generated after the negotiation of the specific security protocol (IPsec and WPA-TLS).

Figure 10 shows the results of throughput and transferred bytes of a TCP flow with a duration of 120 seconds and a default window size of 85.3 Kbytes, when no security, WPA and IPsec are in place. The presented results represent the average values obtained by 48 simulations, with a stochastic confidence interval of 92%. As can be seen, IPsec is the mechanism that achieves lower throughput; it also adds more overhead, since it conveys less information per bytes transferred (total amount of data transferred for each TCP window) than the WPA solution. The throughput and transferred bytes of WPA is larger than IPsec, but obviously lower than the plain network (without security).

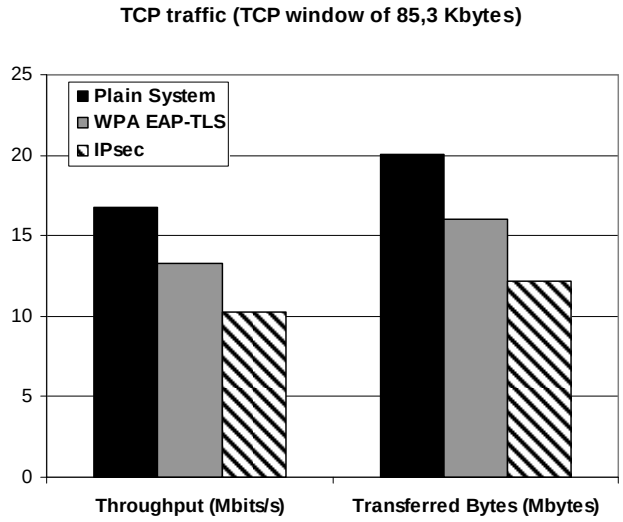


Figure 10. Throughput and bytes transferred

These results are due to the larger complexity introduced by IPsec (ESP with tunnel mode was used, which adds a new header and new authentication field). WPA does not make significant changes to a packet, just ciphers it and adds an IV field. The same experiment was done for different TCP window sizes[11], which also confirmed the fact that IPsec is the solution with less throughput and bytes transferred.

To evaluate the jitter[12] and the number of lost packets, IPERF was used with UDP flows in networks with bandwidths of 10 Mbits/s and 54 Mbits/s. These consisted of 5 flows with duration of 60 seconds, simulating a voice communication. The obtained results represent the average results of 20 simulations with a stochastic confidence interval of 95%. Figure 11 and Figure 12 show the results for a network bandwidth of 10 Mbits/s.

The results demonstrate that, due to its complexity and packet processing, IPsec has worse jitter results. Regarding the number of lost packets, IPsec is the security solution that has better results. This is due to the fact that the process of packet protection happens between the VPN gateway and the client, while in the WPA solution this is done between the AP and the client. As the gateway has more capacity for processing the packets, it can keep its buffer available and the number of lost packets is reduced. The results obtained with 54 Mbits/s and with CRUDE confirm the ones of IPERF with 10 Mbits/s.

[11] The TCP window size controls the number of packets that can be sent without being acknowledged. Increasing its size will mean that a higher number of packets can be sent but if the receiver's buffer can not cope with the amount it will mean that the sender will have to re-send more packets.

[12] Jitter pertains to the variation of packet delay; the delay is composed by sender delay, travelling in the network delay and receiver delay. The variability of this total delay is measured by jitter.

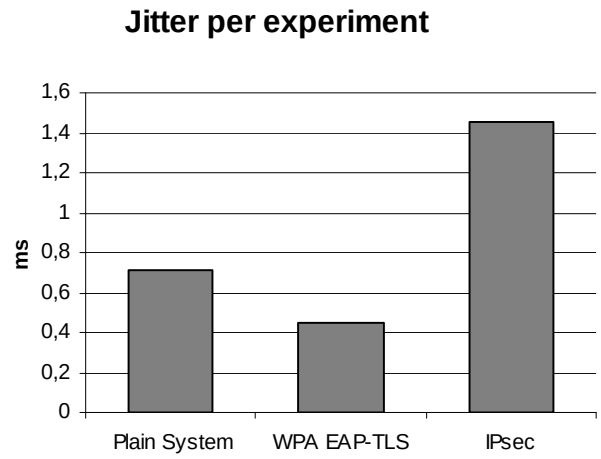


Figure 11. Jitter of UDP flows in a 10 Mbits/s network.

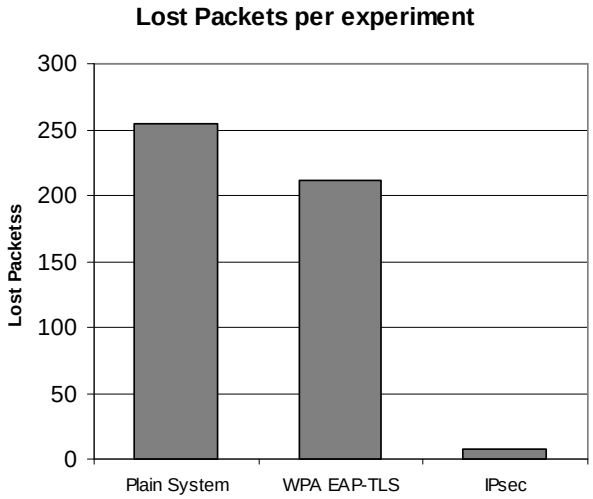


Figure 12. Lost packets of UDP flows in a 10 Mbits/s network.

These data flow results led to the natural conclusion that for TCP communications (e.g. with file transfers), the WPA implementation has more advantages. For UDP communications the IPsec protocol achieves lower loss rates.

## Deployment discussion

The deployment of the infrastructure requires studies regarding the location of access points for the intended coverage, as mentioned in the introduction. The costs associated with the hardware (APs, wireless cards, Ethernet switches and servers) would depend on the required coverage and the number of users enabled with this access. However, notice that current laptops and PDAs have already wireless capabilities supporting 802.11i.

The software associated with the framework is already available with the hardware except for the servers (LDAP, RADIUS). Nevertheless, they are readily available in reliable free open source packages (with support available separately) and also in commercial products.

In terms of user impact, the access to the network could be coupled with the existing credential system, thus easing the needed user interaction. However, as a first approach these two authentication points in the network and in the VEPR should be done separately. The final purpose is to build a single-sign-on system that would provide only one authentication control.

# Conclusions

## Discussion

The wireless architecture discussed above is able to provide wide as well as mobile and flexible access to the VEPR implemented within a healthcare institution. The architecture is modular and flexible in order to adapt itself to the existing features so that it can be incorporated when a LAN is already in place. In particular, the proposed architecture takes into account the fact that the existing devices can be reused with WPA/EAP-TLS; it also integrates the recent 802.11i standard, making it versatile and upgradeable.

To account for the security and performance of the system, several studies and tests were made with the presented technologies. The only exception is the recent 802.11i because no compliant devices were available at the time of testing. Nevertheless, its overall observed performance is believed to be very similar to the WPA solution. The impact of the WPA security is negligible in terms of the performance of the system. The throughput achieved was slightly worse in WPA than in a plain system. However, the difference should not be noticeable to users.

As discussed, the existing VEPR wired solution was designed and implemented with all the security requirements; adding this extra layer of security results in an easier process, as long as it respects the security goals of the VEPR.

With the proposed architecture, secure access to the current system is increased due to the wireless connectivity advantages (e.g. mobility, everywhere access and access to wider range of devices). This access provides secure authentication and authorization, secure communications and also maintains the integrity of the retrieved information, thus preserving the security goals of the VEPR. This is very important and justifies the need for similar studies when implementing wireless solutions.

## Open challenges

As future work, a prototype will be implemented within the real scenario so that the wireless solution can be evaluated. Several issues need to be tested and enhanced. These include performance, access control, availability issues (such as DoS), access point correct distribution and usability.

Further issues are related to the presentation of the VEPR within wireless devices. This needs proper study as its usefulness and success may depend upon it.

## Acknowledgments

This VEPR has already won 2 prizes for its innovation and results from Portuguese Government Institutions. As such, the first author would like to thank all the parties that collaborated in its implementation, specially the Security Commission of Hospital S. João, LIACC and CINTESIS for their interest and support.

## References


Ana Ferreira, Ricardo Correia, & A. Costa-Pereira. (2004). Securing a web based epr: an approach to secure a centralized epr within hospital In , *6th International on Enterprise Information Systems*, 3 (pp. 54-59).

Ana Ferreira, Ricardo Correia, Luís Antunes , Ernesto Palhares, P. Farinha, & A. Costa-Pereira. (2005). How to start modelling access control in a healthcare organization In , *10th International Symposium for Health Information Management Research*.

Ana Ferreira , Ricardo Cruz-Correia , Luís Antunes , Ernesto Palhares, Pedro Marques, P. Costa, et al. (2004). Integrity for electronic patient record reports In , *17th IEEE Symposium on Computer-Based Medical Systems* (pp. 4-9).

B. Aboba, & D. Simon. (1999). *Rfc 2716 ppp eap tls authentication protocol*. IETF. Retrieved from http://tools.ietf.org/html/rfc2716.

B. Aboba, L.Blunk, J. Vollbrecht, J. Carlson, & H. Levkowetz. (2004). *Rfc 3748 extensible authentication protocol (eap)*. IETF. Retrieved February 8, 2008, from http://tools.ietf.org/html/rfc3748.

Benson, T. (2002). Why general practitioners use computers and hospital doctors do not---part 2: scalability, *BMJ*, 325(7372), 1090-1093. doi: 10.1136/bmj.325.7372.1090.

Blobel, B. (2004). Authorisation and access control for electronic health record systems, *International Journal of Medical Informatics*, 73(3), 251-257.

C. Rigney, A. Rubens , W. Simpson , & S. Willens. (1997). *Rfc 2138 remote authentication dial in user service (radius)*. IETF. Retrieved from http://tools.ietf.org/html/rfc2138.

CEN. (1999). *Health informatics - secure user identification for healthcare - management and security of passwords*. CEN.

Crude team. (2002, September 13). (c)rude - rude & crude. Retrieved February 12, 2008, from http://rude.sourceforge.net/.

Denley, I., & Smith, S. W. (1999). Privacy in clinical information systems in secondary care, *BMJ : British Medical Journal*, 318(7194). Retrieved March 10, 2008, from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1115718.

Dixie B. Baker. (2003). Wireless (in) security for health care In , *Advocacy White Paper*. Science Applications International.

Durham, D., Boyle, J., Cohen, R., Rajan, R., & Sastry, A. (2000, January). The cops protocol. Retrieved February 14, 2008, from http://www.rfc-editor.org/rfc/rfc2748.txt.

Ettercap Team. (2005, May 29). Ettercap ng. Retrieved February 12, 2008, from http://ettercap.sourceforge.net/.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed nist standard for role-based access control, *ACM Trans. Inf. Syst. Secur.*, 4(3), 224-274.

Finseth, C. (1993, July). Rfc 1492 - an access control protocol, sometimes called tacacs. Retrieved February 14, 2008, from http://www.faqs.org/rfcs/rfc1492.html.

FreeRADIUS . (2008, January 22). Freeradius server. Retrieved February 12, 2008, from http://www.freeradius.org/.

FreeS/WAN Project. (2004, April 22). Frees/wan. Retrieved February 12, 2008, from http://www.freeswan.org/.

Harkins, D., & Carrel, D. (1998). *Rfc 2409 the internet key exchange (ike)*. IETF. Retrieved from http://tools.ietf.org/html/rfc2409.

HostAP team. (2007, December 2). Host ap linux driver for intersil prism2/2.5/3 wireless lan cards and wpa supplicant. Retrieved February 12, 2008, from http://hostap.epitest.fi/.

IEEE 802.10. (1998). *Ieee standards for local and metropolitan area networks: standard for interoperable lan/man security (sils)*. Retrieved from http://standards.ieee.org/getieee802/download/802.10-1998.pdf.

IEEE 802.11i. (2004). *Part11: wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: medium access control (mac) security enhancements* . Retrieved from http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

IEEE 802.1X. (2004). *Ieee standards for local and metropolitan area networks—port-based network access control*. Retrieved from http://standards.ieee.org/getieee802/download/802.1X-2004.pdf.

Iperf Team. (2005, May 3). Nlanr/dast : iperf - the tcp/udp bandwidth measurement tool. Retrieved February 12, 2008, from http://dast.nlanr.net/Projects/Iperf/.

J. Hodges, & R. Morgan. (2002). *Rfc 3377: lightweight directory access protocol (v3): technical specification*. IETF. Retrieved from http://tools.ietf.org/html/rfc3377.

Kent, S., & Atkinson, R. (1998a). *Rfc 2402 ip authentication header*. IETF. Retrieved from http://tools.ietf.org/html/rfc2402.

Kent, S., & Atkinson, R. (1998b). *Rfc 2406 ip encapsulating security payload (esp)*. IETF. Retrieved from http://tools.ietf.org/html/rfc2406.

Kim, H., & Afifi, H. (2003). *Improving mobile authentication with new aaa protocols*. Retrieved February 15, 2008, from http://citeseer.ist.psu.edu/article/kim03improving.html.

Kismet Team. (2004). Kismet. Retrieved February 18, 2008, from http://www.kismetwireless.net/.

Lehoux, P., Sicotte, C., & Denis, J. (1999). Assessment of a computerized medical record system: disclosing scripts of use, *Evaluation and Program Planning*, 22(4), 439-453. doi: 10.1016/S0149-7189(99)00034-8.

McAlearney, A. S., Schweikhart, S. B., & Medow, M. A. (2004). Doctors' experience with handheld computers in clinical practice: qualitative study, *BMJ*, 328(7449), 1162. doi: 10.1136/bmj.328.7449.1162.

Microsoft. (2004). Windows server 2003 active directory. Retrieved February 15, 2008, from http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx.

Moskowitz, R. (2003, November 4). Weakness in passphrase choice in wpa interface, *Wi-Fi Net News*. Retrieved from http://wifinetnews.com/archives/002452.html.

Ng, Sim, & Tan. (2006). Security issues of wireless sensor networks in healthcare applications, *BT Technology Journal*, 24(2), 138-144. doi: 10.1007/s10550-006-0051-8.

NIST. (2001). *Fips-197: advanced encryption standard*. Natioanl Institute of Standards (NIST).

Novell. (2004). Novell edirectory vs. microsoft active directory. Retrieved February 15, 2008, from http://www.novell.com/collateral/4621396/4621396.pdf.

OpenSSL. (2007, October 19). Openssl: the open source toolkit for ssl/tls. Retrieved February 12, 2008, from http://openssl.org/.

Oxid IT Team. (2005). Cain & abel. Retrieved February 15, 2008, from http://www.oxid.it/cain.html.

Ramon Marti, & Jaime Delgado. (2003). Security in a wireless mobile health care system In . Universitat Pompeu Fabra.

Ricardo Cruz-Correia , P. Vieira-Marques, P. Costa, Ana Ferreira, Ernesto Palhares, F. Araújo, et al. (2005). Integration of hospital data using agent technologies - a case study, *AICommunications special issue of ECAI*, 18(3), 191-200.

Systat Team. (2008, January 6). Sysstat. Retrieved February 12, 2008, from http://pagesperso-orange.fr/sebastien.godard/.

Ventura, H. (2002). *Diameter next generation's aaa protocol*.

Vmstat man page. Retrieved December 17, 2007, from http://linuxcommand.org/man_pages/vmstat8.html.

Walker, J. (2003). *802.11 security séries part ii: the temporal key integrity protocol*. Intel Corporation. Retrieved from http://softwarecommunity.intel.com/articles/eng/1905.htm.

Whalen, S. (2001, April). An introduction to arp spoofing. Retrieved February 15, 2008, from http://www.node99.org/projects/arpspoof/.

Whiting, D., Housley, R., & Ferguson, N. (2003, September). Rfc 3610 - counter with cbc-mac (ccm). Retrieved March 8, 2008, from http://www.faqs.org/rfcs/rfc3610.html.

Wpa . Retrieved February 8, 2008, from http://www.wi-fi.org/knowledge_center/wpa/.

Wullems, C., Tham, K., Smith, J., & Looi, M. (2004). A trivial denial of service attack on ieee 802.11 direct sequence spread spectrum wireless lans, *Wireless Telecommunications Symposium*, 129-136.

Yu, W. D., & Jothiram, V. (2007). Security in wireless mobile technology for healthcare systems In , *e-Health Networking, Application and Services, 2007 9th International Conference on* (pp. 308-311). doi: 10.1109/HEALTH.2007.381659.

# About the Authors

**Ana Ferreira** is an IT specialist at Porto Faculty of Medicine; she is a CISSP and is pursuing a PhD in Computer Science with a joint supervision between the University of Porto and the University of Kent, aiming at improving access control to healthcare information systems. Other main interests include information security for healthcare, wireless networks, usability, users' awareness and education.

**Luís Antunes** obtained a PhD in Computer Science at University of Porto. Currently he is an Auxiliary Professor at the Computer Science Department at University of Porto. Most of his research is on Computational Complexity and Cryptography. He is in the Coordination Committee of the first Health Informatics Master course in Portugal and has a strong collaboration with the Medical School of Porto University. He supervises several Master and PhD students in areas such as Access Control and Information Measures for Cryptography protocols.

**Luís Barreto** received the B.A. degree in Electrotechnical and Telecommunications Engineering from the Oporto University, Portugal, and the Master degree in networking systems and security by the same University. He is a Ph.D. student in Electronical Engineering at the Aveiro University, Portugal. He is currently a Professor, Vice-President of the direction board of Business Science Superior School, Polytechnic University of Viana do Castelo (Escola Superior de Ciências Empresariais- Instituto Politécnico de Viana do Castelo) and Coordinator of the Business Computing Course. He is, also, the manager of different R&D projects, namely: NetStart (http://www.netstart.pt), CSI- Cooperation Servicing Innovation and SeeLe (Seeking Learning Evaluation- http://seele.ipvc.pt). The following subjects are Luís Barreto main interests: Networking Protocols, Wireless Security, Ad-hoc and Wireless Networks, E-learning, Web 2.0, Informal and Formal Learning.

**Pedro Brandão** is an assistant lecturer at the Science Faculty of the University of Porto and a member of the Instituto de Telecomunicações – Porto group NIP. He is currently pursuing a PhD at Cambridge University on body sensor networks. In his past he has worked on network security and ad hoc networks research, subjects that still drive some of his interests. As part of this work he was involved in the identity management system of the European IP Daidalos.

**Ricardo João Cruz Correia** is an assistant lecturer and researcher at the Department of Biostatistics and Medical Informatics at the Faculty of Medicine of the University of Porto. His research interest is the electronic patient records and on the integration of heterogeneous healthcare information systems. He received his MSc in computer science from the University of Porto, and is currently a PhD student at the University of Porto.

**Susana Sargento** graduated in Electronics and Telecommunications Engineering from the University of Aveiro, in 1997 and concluded her PhD in 2003. In September of 2002, she joined the Department of Computer Science in the Sciences Faculty of the University of Porto as an Assistant Professor where she was leading the Network Communications group, and returned to the University of Aveiro in February 2004. Her main research interests are in the areas of next generation networks (infrastructure and

ad-hoc, including broadcast), more specifically in QoS, routing and charging issues. She is currently involved in several projects in the area (IST-Daidalos, Euro FG, C-Mobile, C-Cast, WIP), where she has coordination responsibilities of self-organizing activities and QoS 4G architectures inside the Daidalos project. She has more than 100 papers in the area of communication networks.