A secure wireless architecture to access a virtual electronic patient record

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. The use of wireless technology can improve and fasten healthcare treatment because it brings information to the point of decision allowing also for users' mobility. This has to be done conforming to security requirements as the wireless technology can introduce some specific security problems. The main objective of this work is to model and develop 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 500 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 workplace. They would achieve faster and greater mobility in the treatment of their patients. The wireless architecture includes the latest wireless security standards and protocols, and models security requirements according to users and organizations' needs. It provides an extra security layer to the wired system. In this paper we also present an evaluation of the proposed solutions against network attacks and its efficiency in terms of complexity and impact within the network.**

***Index Terms*—Electronic patient records, wireless networks, information security.**

I. Introduction

Virtual Electronic Patient Records (VEPR) enable the integration and sharing of healthcare information within heterogeneous organizations [1]. Hospitals are an example of such healthcare institutions with great turnover in terms of healthcare professionals.

The use of wireless technology tries to take this integration even further. It allows access to patient data and processing of clinical records closer to the point of decision. 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. The most common is the introduction of mobile wireless health monitoring systems. These can have some security concerns but are out of the purpose of this research [2]. The use of existing technologies, standards and focus in authentication and encryption mechanisms helps the wireless system to become more secure.

Our goal is however different. Our architecture aims to add a wireless network within a hospital in order to access a central repository of patient information. Some experiences already showed 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 [3]. On the other hand, healthcare professionals were concerned about security, trust and reliability of the information they were accessing.

This infrastructure along with the characteristics mentioned above for wireless technology, has great advantages for healthcare treatment but, unfortunately, security is an important factor that is often overlooked because people do not take the time and effort to include it at systems' design [4] . Due to lack of expertise and also the difficulty to change procedures, it is very hard to add or implement security modules to the system afterwards.

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 [5]; the lack of security increases users' reluctance to VEPRs acceptance. Both patient and healthcare organization trust can be seriously damaged if no proper security is provided [6]. Furthermore, wireless technology adds more security issues that need to be properly studied and tackled [7] before they are implemented in a large scale within a hospital. Therefore, when designing a VEPR within a university hospital several concerns in terms of security need to be thought and applied from beginning to end of system's development and implementation [8]-[10].

This paper proposes a wireless architecture in order to model access to an existing VEPR within a university hospital. This architecture will take into account the security services that were implemented within the wired version of the system, and will use the latest wireless standards and security protocols. We also present an evaluation of the proposed solutions against network attacks and its efficiency in terms of complexity and impact in the network.

The paper is organized as follows. The next section describes the VEPR architecture and points out the security

Ana Ferreira is with Center for Informatics at Faculty of Medicine in Porto, Portugal (Phone: +351 22 551 3613; Fax: +351 22 551 3613; email: amlaf@med.up.pt), and CINTESIS – Center for Research in Health Information Systems and Technologies.
Luís Barreto is with Escola Superior de Ciências Empresariais, Instituto Politécnico de Viana do Castelo, Valença, Portugal.
Ricardo Correia is with Biostatistics and Medical Informatics Department, at Faculty of Medicine in Porto, Portugal, and with CINTESIS.
Susana sargento is with Instituto de Telecomunicações - Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, Portugal.
Luís Antunes and Pedro Brandão are with LIACC at Faculty of Science in Porto, Portugal.

requirements for the implementation of a wireless platform in order to access that VEPR. Section III describes the proposal for the wireless architecture and section IV evaluates and presents the results for that proposal. The last section discusses advantages and/or security issues that still need to be analysed.

II. THE VEPR

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 [11].

Currently, more than 500 doctors use the system on a daily basis. Other healthcare professionals are expected to start using it soon.

The VEPR uses agent technologies that enable the successful integration of large amounts of heterogeneous data that can be accessed from any workstation in the hospital intranet. It 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.

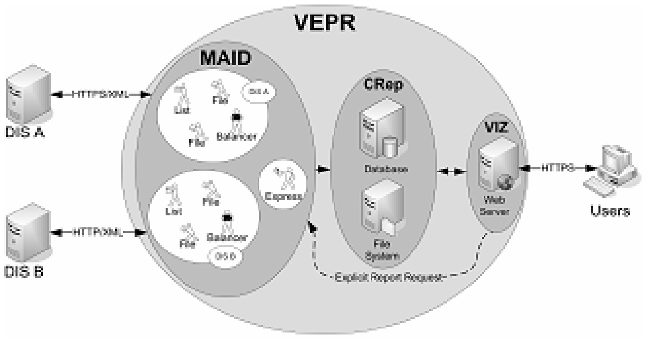

Fig. 1. VEPR generic architecture.

Two major modules were designed (Fig. 1): the *Multi-Agent system for Integration of Data* (MAID) module, which provides for automatic document retrieval and the *visualization* (VIZ) module which shows patient data upon user request.

MAID collects clinical reports from various hospital departments (eg. DIS A and DIS B), and stores them on a *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 a web-based interface. When selecting a specific report, its contents are downloaded from the central repository file system to the browser. When a user requests a report whose reference is not in the database, 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 (Fig. 2).

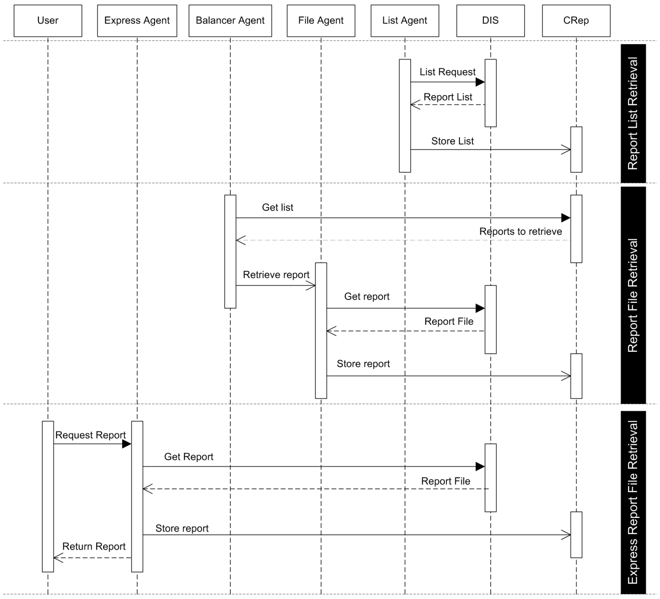

Fig. 2. UML communication sequence of the VEPR

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 the VEPR availability.

A. Security requirements

All the security services implemented for the wired VEPR will be used within the wireless architecture [8]-[10].

The wireless technology stresses however the need for extra layers of security. Information is more prone to disclosure when it leaves the wired system and travels throughout the air.

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 must be the means to guarantee that the information in transit within the wireless network is protected from unauthorized or accidental modifications. Wireless networks are more prone to disruptions and interference.

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.

III. Proposed architecture

As mentioned previously, users of healthcare environments would greatly benefit with the availability of information anywhere through a Wireless Local Area Network (WLAN). However, the university hospital, where the experiment is going to take place, has already a LAN in use; setting a WLAN on top of this one is not trivial, since the hospital is a very big building. The need for a good location map and distribution is essential. As also mentioned, there are security technologies that need to be set in place to secure the wireless '*link*'. 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 they will just bypass the system.

In this section some of the technologies that need to be used for the implementation of this proposal are described. Some possible solutions are addressed to support security in WLANs. More specifically, the studied solutions are based on Wi-Fi Protected Access (WPA) [12], 802.11i standard for security [13] and IP Security [14]. At the end of this section a proposal for a wireless architecture is presented.

A. *WPA*

WPA [12] was developed with the aim of decreasing the problems associated to Wired Equivalent Protocol (WEP) [15]. WPA is based on the principles of the novel standard IEEE802.11i [13] (with some simplifications to be compatible with the current equipments). 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 immediately available. Older Wi-Fi products are WPA upgradeable. This standard can be used in almost all Access Points (APs) and Network Interface Cards (NICs) currently available, with just a software upgrade.

To improve data codification, WPA uses the Temporal Integrity Protocol (TKIP) [13] 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 [16] for user authentication, making it possible to use one of the Extensible Authentication Protocol (EAP) [17] methods. For security matters in these environments, the EAP- Transport Layer Security (TLS) [18] method is used. This method uses digital certificates for each user authentication. To eliminate the danger of rogue APs, a central authentication server is used to manage mutual authentication. The authentication server usually employed is the Remote Access Dial-In User Service (RADIUS) [19] server. 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.

It is also possible to use, for centralized user authentication, a Lightweight Directory Access Protocol (LDAP) [20] server. 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. To simplify the job of the network administrator a DHCP server is used, enabling client's automatic network configuration. 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 VLANs (see sub-section D) and, if needed, allows to route data between the different networks.

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 Fig. 3.

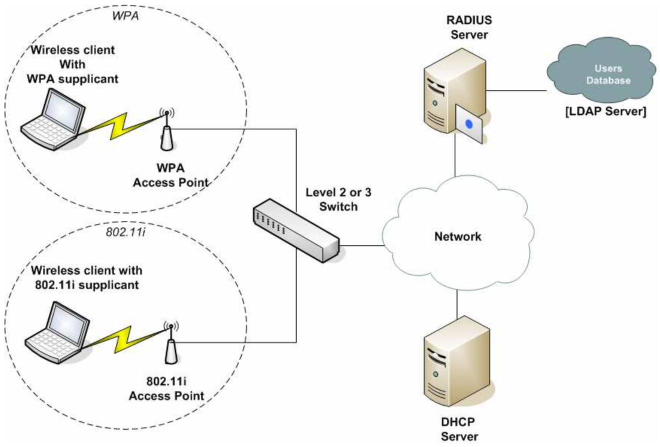

Fig. 3. WPA and RSN/IEEE802.11i architecture.

B. *802.11i*

In June 2004, the Institute of Electrical and Electronics Engineers (IEEE) ratified the 802.11i standard, also called Robust Security Network (RSN)[1]. This security standard includes the following functionalities: it uses the Advanced Encryption Standard (AES) [21] block cipher to encrypt the data packets, 802.1X for user authentication and TKIP for the management of the cipher keys. The group 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 the clients announce their cipher capabilities in their AP association requests. The AP and the wireless client then establish the appropriate key for data

[1] Also known as WPA2

ciphering. This key is based in their mutual capabilities and configured in one of the security policies (eg.: “allowing only associations with AES clients”). Moreover, the 802.1X authentication assures the key renewal during a session.

As there are no known methods for deciphering AES, it is a robust algorithm that assures confidentiality. This characteristic makes possible to use smaller ciphering keys and increases network performance. However, AES has more demanding cryptographic functions. This means that older devices do not have CPU capacity to handle AES and keep a normal network performance. To circumvent the problem the 802.11i also enables the use of TKIP as the cipher protocol. This method is more feasible for less capable devices.

802.11i actually defines three protocols for data protection: the Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP), the Wireless Robust Authenticated Protocol (WRAP) [22] and TKIP. CCMP will be the ‘de facto’ IEEE802.11i cipher protocol; however, it is only considered a long term solution. It is based in AES counter mode. This protocol derives from lessons learned with 802.10 [23] and IPSec protocols. It uses strong cipher primitives, which makes it reliable against all known attacks. However, it is not compatible with available equipment and requires new hardware support.

As with WPA, for implementing an 802.11i solution it is necessary to develop an 802.1X infrastructure. The design of this infrastructure requires that all its elements must be upgraded to support IEEE802.11i.

Fig. 3 shows the required elements to support an 802.11i architecture.

C. *IPSec*

All the solutions previously mentioned 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 IPSec [14]. 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. Its main disadvantage is its complexity.

IPSec has two cipher modes: transport and tunnel. Transport mode only ciphers, without changing the header, the data field of the IP packet. Tunnel mode is more secure, and ciphers the entire packet.

The IPSec standard includes two security protocols: the Authentication Header (AH) [24] that provides data integrity, and the Encapsulating Security Payload (ESP) [25] that adds confidentiality. All IPSec parameters are negotiated using the Internet Key Exchange (IKE) [26] 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, as in our case.

Fig. 4 shows an IPSec VPN adapted to a wireless network and the elements required for an IPSec protected wireless network.

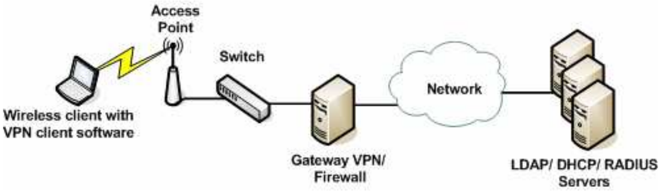
Access Point
Switch
Network
Wireless client with VPN client software
Gateway VPN/ Firewall
LDAP/ DHCP/ RADIUS Servers

Fig. 4. Wireless network IPSec VPN.

Such network has wireless terminals with VPN client software. This software should be able to start ciphered 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 in the previous architectures, LDAP and RADIUS servers are used for centralized user authentication. Again DHCP server is also available for automatic client network configuration.

D. *VEPR Wireless Architecture*

Due to the specific characteristics of a health care institution, and considering how important security is in such an environment (and the complexity of the solutions mentioned before), we propose a secure wireless architecture for accessing the VEPR. This architecture uses the WPA-TLS mechanism and also considers, for the new devices that are compliant, the use of the new 802.11i standard. All existing equipments can, with a small firmware upgrade, support WPA-TLS and therefore, be reused. This can reduce implementation costs. WPA-TLS should only be considered a transition solution until all devices become 802.11i compliant.

Our proposal is the support of WPA and 802.11i in 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).

Therefore, in the proposed architecture, each AP will be configured with two different SSIDs (SSID=802.11i-VEPR and SSID=WPA-VEPR) and two different security protocols. The APs will be enabled (if they support), with both 802.11i and WPA. This configuration will create a secure logical network, allowing doctors to have a secure and controlled access to the VEPR. A RADIUS server will be the policy enforcement point (PEP), which will be configured with different access control policies for each SSID, to enforce them in the network. These policies will set the data cipher protocol, the key management protocol and the key length used with a specific SSID.

It is necessary that all terminal/client equipments support WPA-TLS or 802.11i.

Fig. 5 shows the proposed architecture, where the two logical secure access networks are presented. Although not in the figure, user authentication services for automatic network configuration, such as LDAP and DHCP, can be included.

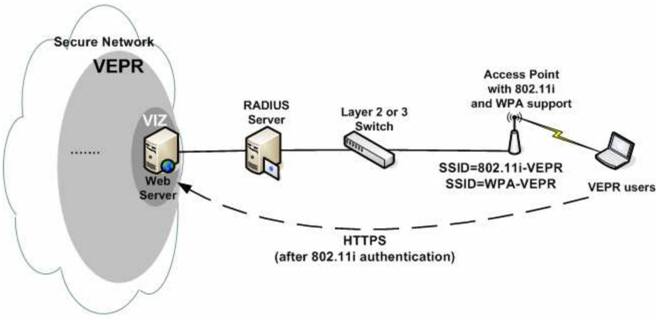

Fig. 5. VEPR secure wireless architecture.

IV. RESULTS

In this section we perform an evaluation of the security and performance capabilities of WPA EAP-TLS and IPSec. 802.11i is not addressed here due to the unavailability of 802.11i compliant devices. These experiments comprise the evaluation of the proposed solutions against network attacks and its efficiency in terms of complexity and impact in the network.

A. Security evaluation

To evaluate the security of the solutions, we implemented some attacks to the network and observed the network reaction to it. These attacks comprise man-in-the-middle (MITM), impersonation, Denial of Service (DoS) and session hijacking. We used the *ettercap* [27] tool to address these tests. For all the security tests it is necessary to use a wireless client as an intruder. For more information on the tests performed to the security solutions, refer to [28]. The following sub-sections present just an overview of the achieved 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, it was used the *arp spoofing* option. 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 had a negative 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. Finally, the same result was achieved with session hijacking.

These 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 break the security of WPA. 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. With the WPA client it is possible to send fake network access messages. WPA defines that, if fake network access messages arrive to an AP, the AP must block all network access. This issue makes it easy to do a DoS attack to WPA, since it is just necessary to activate a WPA client and ask an AP for network access. Immediately, 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.

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 more mechanisms that reduce the risk of such attack. It is thus necessary to use tools like Intrusion Detection Systems (IDS) and vulnerability scanners.

B. Complexity evaluation

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

For traffic generation, IPERF [29] and CRUDE [30] tools were used. All the traffic was generated after the negotiation of the specific security protocol (IPsec and WPA-TLS).

Fig. 6 shows the results of throughput and transferred bytes of a TCP flow with a default window of 85,3 Kbytes, when WPA, IPSec and no security are in place. 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).

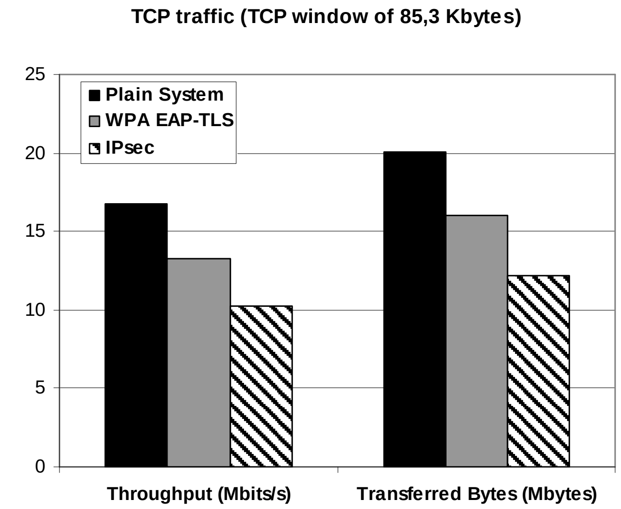

Fig. 6. Throughput and bytes transferred.

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

To evaluate the jitter and the number of lost packets, IPERF was used with UDP flows in networks with bandwidths of 10 Mbits/s and 54 Mbits/s. Fig. 7 and Fig. 8 show the results for a network bandwidth of 10 Mbits/s.

The results show that, due to its complexity and processing of the packets, 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 gateway VPN 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 Mbist/s.

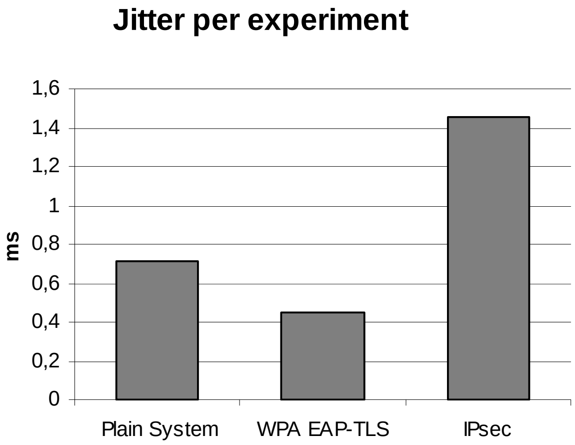

Fig. 7. Jitter of UDP flows in a 10 Mbits/s network.

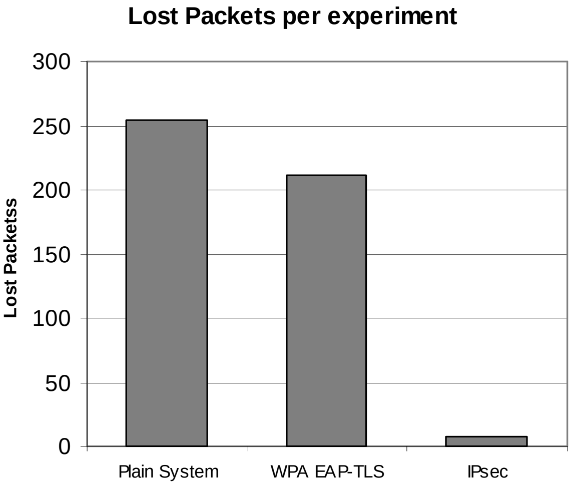

Fig. 8. Lost packets of UDP flows in a 10 Mbits/s network.

With the analysis of all those results we conclude 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.

The system performance was also measured to evaluate the complexity introduced in the network elements. For this purpose we used the *sysstat* [31] and *vmstat* [32] (a linux shell command) tools. These tools allow evaluating CPU utilization, memory and interrupts. The results given by those tools are shown in Fig. 9 and Fig. 10. 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.

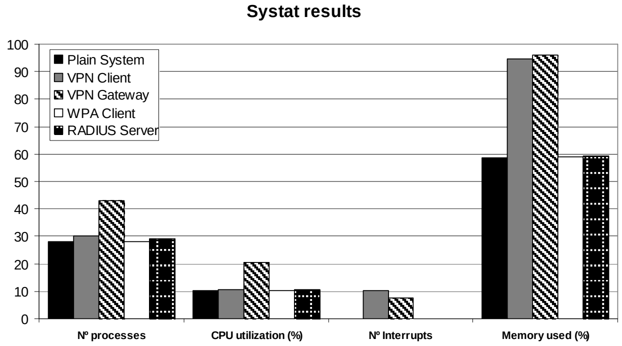

Fig. 9. System performance – *sysstat* results.

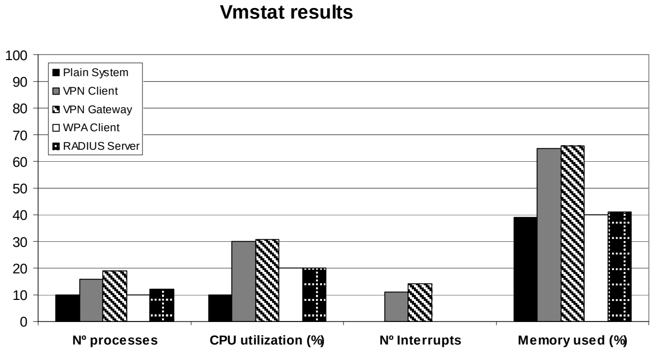

Fig. 10. System performance – *vmstat* results.

Relatively to the 802.11i solution, as the WPA one is based on 802.11i, its overall performance will be very similar to that of the WPA solution.

V. Conclusion

The wireless architecture proposed in this paper is able to provide wider as well as mobile and flexible access to the VEPR implemented within the university hospital. As it has already a LAN in place, the proposed architecture is modular and flexible in order to adapt itself to the existing features. In particular, the proposed architecture takes into account the fact that the existing devices using the WPA-TLS can be reused; it also integrates the recent 802.11i standard, making it versatile and easy to use.

Several studies and tests were made with the presented technologies that allow choosing them according to the environment needs. The only exception is the recent 802.11i because no compliant devices were available. Nevertheless, its overall performance is believed to be very similar to the WPA solution. The use of security standards along with these technologies provides an extra security layer. The fact that the existing wired solution was designed and implemented with all the security requirements makes it easier to add this extra layer as long as it respects the security goals of the VEPR.

With the proposed architecture the wireless technology does not open security flaws to the VEPR and increases user mobility and access to the system. It allows for secure authentication and authorization, secure communications and also maintains the integrity of the retrieved information. This is very important and justifies the need for studies such as this one when implementing wireless solutions.

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 can be related with the presentation of the VEPR within wireless devices. This needs proper study as its usefulness and success may depend upon it.

Acknowledgment

This VEPR has already won 2 prizes for its innovation and results from Portuguese government institutions. As such, Ana Ferreira 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

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

[2] Marti R, Delgado J. Security in a wireless mobile health care system. Universitat Pompeu Fabra – white paper. 2003.

[3] McAlearney A, Schweikhart S, Meadow M. Doctors' experience with handheld computers in clinical practice: qualitative study. BMJ 2004;328;1162-1167.

[4] Godoy C, Carvalho Junior P. A privacidade e o registro informatizado na Faculdade de Medicina de Marília. 2002. Encontro Paulista de Pesquisa em Ética Médica 2002.

[5] Benson T. Why general practitioners use computers and hospital doctors do not-Part2: scalability. BMJ 2002;325:1090-1093, 9 November 2002.

[6] I. Danley, S. Smith. "Privacy in clinical information systems in Secondary care", BMJ – British Medical Journal, 1999, 318:1318-1331.

[7] Baker D. Wireless (In)Security for Health Care. Science Applications International Corporation, 2003.

[8] Ferreira A, Correia R, Costa-Pereira A. Securing a Web based EPR: An approach to secure a centralized EPR within hospital. Proceedings of the 6th International on Enterprise Information Systems. 2004; 3: 54-59.

[9] Ferreira A, Cruz-Correia R, Antunes L, Palhares E, Marques P, Costa P, Costa-Pereira A. Integrity for Electronic Patient Record Reports. Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems. 2004; 4-9.

[10] Ferreira A, , Correia R, Antunes L, Oliveira-Palhares E, Farinha P, Costa-Pereira A. How to start modelling access control in a healthcare organization. iSHIMR 2005.

[11] Cruz-Correia R, , Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F, Costa-Pereira A. Integration of hospital data using agent technologies – a case study. AICommunications special issue of ECAI. 2005; 18(3): 191-200.

[12] Wi-Fi Alliance page http://www.wi-fi.org/OpenSection/protected_access_archive.asp.

[13] IEEE Std. 802.11i (2004), *Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) security Enhancements.*2004. URL: http://standards.ieee.org/getieee802.

[14] R. Thayer, N.D., R. Glenn, *IP Security Document Roadmap, RFC2411.* 1998.

[15] Jesse Walker, *802.11 Security Séries Part II: The Temporal Key Integrity Protocol*. 2002. http://cedar.intel.com/media/pdf/security/80211_part2.pdf.

[16] IEEE Std. 802.1x (2001), *Port-Based Network Access Control*, 2001.

URL: http:// http://standards.ieee.org/getieee802.

[17] B. Aboba, L.B., J. Vollbrecht, J. Carlson, H. Levkowetz, *Extensible Authentication Protocol (EAP), RFC3748*. 2004.

[18] B. Aboba, D.S., *PPP EAP TLS Authentication Protocol, RFC2716*. 1999.

[19] C. Rigney et al., Remote Authentication Dial In User Service (RADIUS), RFC2138. 1997.

[20] J. Hodges, R.M., Lightweight Directory Access Protocol (v3) *Technical Specification*, *RFC3377*. 2002.

[21] (NIST), N.I.o.S.a.T., *FIPS-197: Advanced Encryption Standard*. 2001, National Institute of Standards and Technology (NIST).

[22] WRAP implementation page, http://www.tech-faq.com/wireless-networks/wrap-wireless-robust-authenticated-protocol.shtml. June 2005

[23] IEEE 802.10 Standard pages, http://grouper.ieee.org/groups/802/10.

[24] S. Kent, R.A., *IP Authentication Header, RFC2402*. 1998.

[25] S. Kent, R.A., *IP Encapsulating Security Payload (ESP), RFC2406.* 1998.

[26] D. Harkins, D.C., *The Internet Key Exchange (IKE), RFC2409*. 1998

[27] Ettercap site, http://ettercap.sourceforge.net/. June 2006.

[28] Barreto, L., *Security in Wireless Network Architectures, in Portuguese,* in *Departamento de Ciências de Computadores*. 2005, Universidade do Porto.

[29] IPERF site, http://dast.nlanr.net/Projects/Iperf/. June 2006.

[30] CRUDE site, http://rude.sourceforge.net/. June 2006.

[31] Sysstat site, http://perso.wanadoo.fr/sebastien.godard. June 2006.

[32] Vmstat site, http://linuxcommand.org/man_pages/vmstat8.html. July 2006.