Securing a Medical Wireless LAN System

Thomas J. Owens*, Sapal Tachakra**, Konstantinos A. Banitsas*, Robert S. H. Istepanian*

* e-Med Systems and Health Engineering Group
Department of Electronic & Computer Engineering, Brunel University, Uxbridge, UB8 3PH, UK
www.brunel.ac.uk/departments/ee/Research_P`rogramme/e_med/pages/index.htm
[bany@hol.gr], www.bany.gr [robert.istepanian@brunel.ac.uk], [Thomas.Owens@brunel.ac.uk]

** A&E Department, North West London Hospitals NHS Trust, Central Middlesex Hospital, Acton Lane, London NW10 7NS. [sapal.tachakra@tinyworld.co.uk]

Abstract - **This paper identifies security issues that must be addressed, if a recently proposed Medical Wireless LAN System (MedLAN) is to be accepted. Two classes of security issues are distinguished, technical and managerial.**

I. INTRODUCTION

Recently the concept of MedLAN systems dedicated to application scenarios for Wireless Local Area Networks (WLAN) in hospital A&E departments has been presented [1]. An essential element in the acceptance of the system will be reassuring all stakeholders in the system that data transmitted using the system is secure. This is because the need for specific WLAN applications in the A&E Department include:

- Rescue services to main base A&E Department.
- Point of care clinical protocols or medical information
- Patient transfers

These applications offer the possibility of people being inadvertently associated with their unique health characteristics or health identifiers when the top privacy and security goal for any Healthcare facility is not to allow this.

WLANs are very practical in hospital environments for reasons that include:

- Mobility issues, where staff on the move can access their patients from different access points in complete roaming capabilities.
- The installation and long term running cost of WLAN systems will be cheaper and easier to upgrade.
- Scalability, as the network can be configured to various topologies to suit the changing needs of a hospital.

Consequently, the system has to be designed for operation by doctors and nurses and will be subject to regular upgrading and topology changes so the system must be able to easily accommodate these circumstances without data security being compromised.

II. METHODOLOGY

The IEEE Medical Technology Policy Committee has issued a number of position statements to help members protect their medical information [2]. The MedLAN system will be implemented so that it adheres to the IEEE position statements. The way this will be done is by following the Engineering Principles for IT Security recently drafted by the US National Institute for Standards in Technology in the design, development, and operation of the system [3].

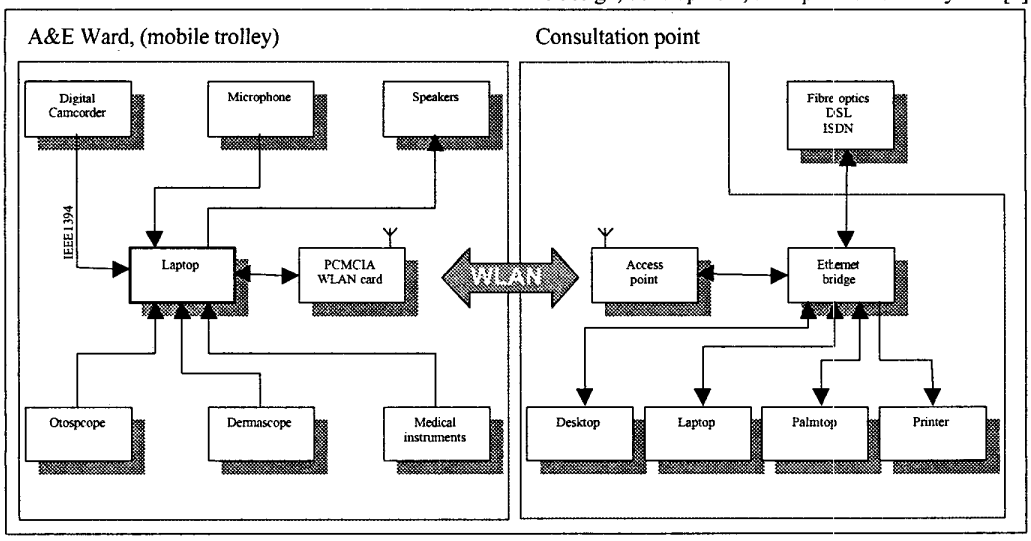

Fig. 1. A simple block diagram of the MedLAN project. It consists of two parts: mobile trolley within the A&E room and the remote consultation site either within or outside the hospital

0-7803-7211-5/01/$17.00 © 2001 IEEE

III. THE MedLAN SYSTEM

The MedLAN system consists of two main parts: The mobile trolley that exists in the Accident and Emergencies ward (A&E) and the consultation point within the hospital. (Fig. 1.)

The mobile trolley consists of a high-end laptop computer equipped with a WLAN PCMCIA card, initially using the IEEE 802,11b protocol, that will permit total mobility within the A&E room and beyond. An access point within the A&E room acts as a transceiver for the network data to be transmitted to and received from the rest of the network.

Work has been ongoing on the way to design a prototype system that will permit the transmission of high quality video and audio between a completely wireless lightweight trolley in A&E and a consultation point within or outside the hospital.

III. TECHNICAL ISSUES OF DATA SECURITY

The Windows 2000 Security Handbook [4] warns: The 802.11 wireless standard is gaining popularity very quickly, as has been shown in California where there are 1m users. This is a radio broadcast although with a very weak signal. Businesses considering the deployment of this type of infrastructure should be very concerned with the potential for abuse. Prior to deploying this you should determine what type of information might be exposed and determine which applications you can easily protect with adequate encryption.

The reason for this warning is that for around $150 a scanner radio can be bought that can pick up cell phone calls [5]. Against eavesdropping attacks against a radio link, encryption has to work perfectly. There is no way to detect eavesdropping, so no response in possible. Digital cell phones can encrypt everything with strong algorithms without perceptibly reducing performance [6]. However, great care has to be taken in selecting encryption algorithms.

In early 1998 it turned out that in a 64-bit key used world wide for protection of access to GSM mobile telephones (D1, D2, E-plus) the last ten bits were set constantly to 0. Consequently, a brute force attack is shortened by a factor of 1000 and will take at most a few days [7]. Worse still, if flaws in the algorithm allow for attacks, this effectively reduces the entropy in the keys. The A5/1 algorithm used in European GSM cell phones, has a 64-bit key, but can be broken in the time it takes to brute force attack a 30-bit key [6]. Although several 128-bit algorithms have been implemented in today's WLANs, work is ongoing to identify the best encryption algorithm for encrypting the wireless links.

Fig. 2. Illustrates the Wired Equivalent Privacy (WEP) introduced by Cisco Systems in their latest Access Points. This can be set and changed both by direct access to the Access Point, or remotely by any computer having established connection to that cell. However, to do that, the client computer must have the WEP key installed (40 or 128 bit) to be able to communicate with the network and go through the authentication procedure (username and password) in order to change the WEP key. Finally, depending on the username, different access levels can be granted to different users and only users with high level clearance can tamper with the WEP keys.

One out of four WEP keys can be used and each of those can be set to either "No", "40 bit" and "128 bit" security. The way to do that is to set a 10 or 26 hexadecimal key that should remain secret and be given only to members of the staff to be included in the group. The administrator can choose one of the following: any computer can be connected to the WLAN regardless of WEP key (open key) or only client computers having the specific key can work within the network (shared key) or both [Fig. 2]

However, as the number of the people that have this key rises, so does the chance of the key being reviled.

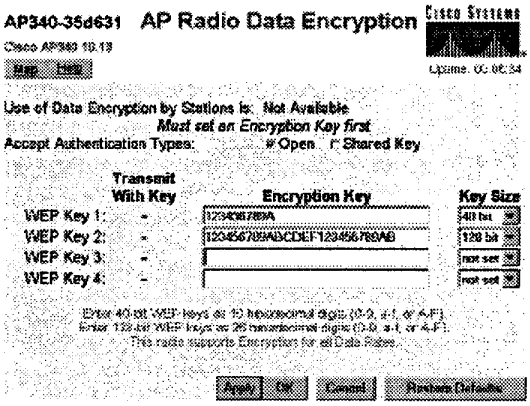

Fig. 2. Configuration screen for the Cisco Access Point. Normal (48-bit) and Wired Equivalent (128-bit) Privacy can be chosen by providing a hexadecimal key that will be shared by any client computer wishing to join the network

By the very nature of the MedLAN system user authentication and authorisation are major issues.

The specification of the Wireless Application Protocol (WAP) was initially released on 30 April 1998. Since then, most cellular vendors have been active in the development of network components and terminals for WAP. Ericsson, among others, have implemented a 128-bit key for WAP communication in its R320 WAP phone.

Windows 2000 does not provide any native support for WAP at this time and it will be interesting to see how authentication and authorisation issues will be handled [4]. However, in this system authentication and authorisation issues can be dealt with through the laptop by fitting a suitable crypto-board. For example, Crypto AG, Zug (Switzerland) offered in 1996 a crypto board for stand-alone or networked desktop PCs and notebooks, that provides user identification and access control, encryption of hard disks, floppy disks, directories, and files at a rate of 38 Mbps. It has its own tamper-proof key carrier and

password storage and works with individually generated psuedo-random keys in a symmetric block cipher algorithm. The key management uses a multi-level key hierarchy. The crypto board is geometrically extremely small but, if used properly, can be expected to withstand a brute force attack using the largest supercomputer for quite some time [7]. However, it should be noted that, in 1994 a senior executive of Crypto AG was arrested by the Iranian government for selling bad cryptographic hardware. When released the executive went public with the news that the company had been modifying their equipment for years at the request of the US intelligence community [6]. Work is ongoing to identify a suitable crypto-board to be fitted to the laptops.

IV. MANAGEMENT ISSUES OF DATA SECURITY [6]

To understand how to secure wireless links it is necessary to understand how the system can be attacked. Assuming that the encryption cannot be broken, the encryption algorithm can be forced to be weak by interfering with the key generation system. It may be possible to make the WLAN cards radiate the unencrypted wireless message or a subliminal channel could be added to make the cards leak the keys onto the wireless link. These attacks could be put into place during product design and development, while the cards are being shipped to the hospital, or during maintenance and system upgrades.

There are a lot of other things that can be done that do not directly involve the secure wireless link. Bugs can be installed inside the computer or the A&E room. The people sending and receiving messages can be bribed and so forth. However, the hospital cannot reasonably expect the secure wireless links to be able to deal with such threats.

A security policy for a system defines the aims and goals. A good policy addresses the threats. The security policy provides a framework for selecting and implementing countermeasures against the threats. All employees have a security policy in mind when they define and implement counter measures. A single written policy forces every employee to follow the same policy. The policy should clearly state who is responsible for what (implementation, enforcement, audit review). A hospital's data security policy would have to be expanded to accommodate the e-Med system if it were introduced.

After a risk has been identified one of three things can be done. The risk can be accepted, the risk can be reduced, or the risk can be insured against. Security does not have to be perfect but the risks have to be manageable. If security is about avoiding threats then it is a cost centre. Managing risk is continuous because a secure computer is one that has been insured and the big insurance companies have been working on insurance for computer security risks. Technical solutions mitigate risk to the point were it is insurable. The need to insure the security of the data handled by the MedLAN system will have to be budgeted for on a yearly basis.

Security processes are a way of mitigating the risks. Counterintelligence is the only way to stay abreast of what is really going on. Insurance will handle the residual risk.

None of this is easy and requires experts. Outsourcing is the only way to do this efficiently. In the near term it is expected that a variety of outsourced security services will become available. Managed security monitoring is required. Someone has to monitor security products in real time and respond to events as they occur. That someone has to be able to maintain the security products in the face of an every changing network and ever-changing services running on the network. Hospitals cannot do this for themselves. The demand for such services generated by the MedLAN system will have to be budgeted for on a yearly basis.

V. THE HUMAN ISSUES

For some time, there has been the problem of confidentiality in telemedicine. [8]. In a public opinion survey it was found that patients were very concerned that details of their illness could be available to relatives or strangers. There was a strong preference for not having the teleconsultations video-recorded as the problems of storage are enormous. One comment was: "how do I know that someone won't scoop an armful of videos and laugh at a whole lot of patients?"

There is also the risk of the teleconsultation being overheard. One of the great advantages of WLAN is the ability of the trolley to be wheeled around a ward area so that an opinion can be obtained from a specialist at another hospital or in another part of the same hospital. There is the obvious risk of the presentation of the case and the clinical details being easily overheard by a patient in an adjacent bed. To reduce that risk, wireless headphones and microphones can be used, to make the conversation between the treating doctor and the consultant as private as possible.

VI. CONCLUSIONS

Recently the concept of MedLAN systems dedicated to application scenarios for Wireless Local Area Networks (WLAN) in hospital A&E departments has been presented. An essential element in the acceptance of the system will be reassuring all stakeholders in the system that data transmitted using the system is secure. In order for the stakeholders to be reassured technical and managerial issues have to be addressed.

Technical issues to be addressed include selection of a suitable encryption algorithm with a 128-bit key for encrypting the wireless links and identification of a suitable crypto-board to be fitted to the system laptop computers (Fig. 2). The crypto-boards will provide for user identification and access control, encryption of hard disks, floppy disks, directories, and files.

In many respects the managerial issues pose bigger challenges than the technical issues. Where the MedLAN system is being introduced members of the E-MED Systems Research Group will have to liase with hospital managers to establish how the hospital's data security policy can be expanded to accommodate the e-Med system and the cost implications of this expansion determined. The cost of insuring the security of the data handled by the MedLAN system will have to be determined. The cost of any managed security monitoring of the system will have to be determined. The ongoing costs identified will have to be budgeted for on a yearly basis.

To ensure that all relevant security issues are adequately addressed the Engineering Principles for IT Security recently drafted by the US National Institute for Standards in Technology are being followed in the design, development, and operation of the system.

REFERENCES

[1] Istepanian, R.S.H., Tachakra, S. and Banitsas, K., "Medical Wireless LAN Systems (MedLAN): State of Art, Challenges and Future", *Proceedings of the 3rd Int. Conference in the Delivery of Care, E-Health; a Future Prospective, E. Carson, F. Harvey and Mike Hughes (Eds.), pp. 43-49, City University, London, 4-6 April 2001.*

[2] Kowalenko, K, 'Protecting your e-Health privacy', *The Institute, No. 4, Vol 25, April 2001*

[3] Engineering Principles for IT Security (A baseline for achieving security) *Draft Recommendations of the National Institute of Standards and Technology, USA, April 2001*

[4] Cox, P. and Sheldon, T., Windows 2000 Security Handbook, *Osborne/McGraw- Hill, 2001.*

[5] Mansfield, R., Hacker attack Shield your computer from internet crime, *Sybex, 2000.*

[6] Schneier, B., Secrets & Lies Digital Security in a Networked World, *John Wiley & Sons, 2000.*

[7] Bauer, F.L., Decrypted Secrets Methods and Maxims of Cryptology, 2nd Edition, *Springer, 2000.*

[8] Tachakra S, Mullett STH, Freij R, Sivakumar A. Confidentiality and ethics in telemedicine. *Journal of Telemedicine & Telecare* 1996; 2(1): 68-71.