Secure Wireless Access to a Campus Network

Manuel Pérez, Miguel Sánchez and Román García
Computer Engineering Department
Polytechnic University of Valencia, Spain
Email: {mperez,misan,roman}@disca.upv.es

Carlos Turró
Computer Center
Polytechnic University of Valencia, Spain
Email: cturro@cc.upv.es

***Abstract*— This paper presents a twofold view of campus-wide wireless networks: Users and network managers. Providing an easy network experience to the user while keeping the wireless network secure and manageable is a key issue. This paper presents the description of the vendor-independent approach to a secure wireless local area network being implemented on this university campus. User configuration is kept simple and preliminary usage patterns are shown.**

I. Introduction

The Polytechnic University of Valencia is a quite young university, it was founded thirty-one years ago. It offers education in several Engineering areas, Computer Science, Architecture and Fine Arts. Current computer count is approximately sixteen thousands units, mostly PCs. Campus network user population is composed of 34.500 students, 2.030 faculty and 1.000 staff members.

The campus network backbone is currently a mixture of Gigabit Ethernet and ATM from the different campus buildings towards the Computer Center, where most of the central equipment is located. Inside each building we have a combination of Ethernet and Fast Ethernet, either switched or shared-media.

This paper main focus is about how to implement a secure campus-wide wireless network (WLAN from now on) to be easy to configure to the user, mostly students.

As the WLAN hardware has become available, different units within the campus started using it. At first, each unit effort was uncoordinated, but now it seems clear that this technology is here to stay and a campus-wide wireless infrastructure is going to be deployed at a consistent rate during the next years. Whether 802.11b or faster technologies (i.e. like 802.11a or HiperLAN2) are going to be the mainstream supporting technology, security and privacy considerations are quite the same: Wireless networks are broadcasting network data to the air so anyone can eavesdrop easily.

Valuable experiences that took place on other campuses, like the ones at Tennessee University or Carnegie Mellon University detailed in [1] and [2], can provide an important insight about the complexities of these networks. Some of the proposed policies there can be taken in consideration here too.

Given the wide availability of wireless networking devices, it is must to enable a campus-wide policy to avoid a negligent use of access points. This may happen when users not aware of potential security threats are setting up unprotected access points (APs) anywhere in the campus network. This APs maybe used to get unauthorized access to the campus network from even miles away of the campus. Such uncontrolled access may happen even to protected areas of the campus network where policies are based on the source address of the request. To prevent such a thing to happen it is better to create up-front a specific and independent backbone for wireless devices where the proper security policy will be enforced.

The rest of the paper is structured as follows: Section 2 presents users point of view and Section 3 presents network managers concerns. Section 4 shows the security issues that affects both users and managers. Section 5 proposes a wireless access network architecture to address those issues of the Sections 2, 3 and 4. Section 6 presents some of the measured usage patterns with this architecture. Finally, section 7 ends the paper drawing some conclusions.

II. What users want

Most users want to get ubiquitous access to the network. Now, more than ever, laptops capability spans computer use to almost any place. But users need to keep network connectivity for some of the tasks. WLAN coverage along the campus is an element of freedom that enable them to use network service from almost anywhere in the campus.

Users need to configure their laptops to get wireless network access. If the procedure is difficult, complex or if it requires additional software it may render wireless access useless. It is, therefore, very important to have simple, easy and straightforward configuration procedure.

A second, but important users desire is to keep a level of trust not lower than the one they have when using a wired access. Users are aware that wireless networks can be insecure and they want a system that they can trust.

On the other hand, several special user profiles have been identified:

- Disabled persons: Using their adapted laptop they may have some extra help anywhere in the campus.
- Security staff: They may have remote access to different information services and video streams in the campus network while on the go.
- Visitors: They may log on the campus network using their own laptop as soon as they arrive to the campus cafeteria.

For all these users, new services will be available that will expand their current possibilities. At any rate, easy access and network security is required too.

III. What network administrators want

Network administrators are worried about several topics. Security seems to be the main concern, but as soon as they think it twice, network deployment and management are two key issues too.

The problem about security is that it has captured a lot of interest during the last year due to the different vulnerabilities that have been shown in the technical literature. The idea that any wireless technology is a network troublemaker is not true but, it is almost certain if the wireless gear is kept in manufacturer's default configuration. That is why a lot of reports show many wide open Access Points (AP) on most of the cities where a test is conducted. The report in [3] shows examples of open or rogue APs on Manhattan, Jersey City, areas of New England and Silicon Valley. Figure 1 shows some of the gathered data on that study: More than 50% of the APs are deployed without any security precaution, like enabling encryption.

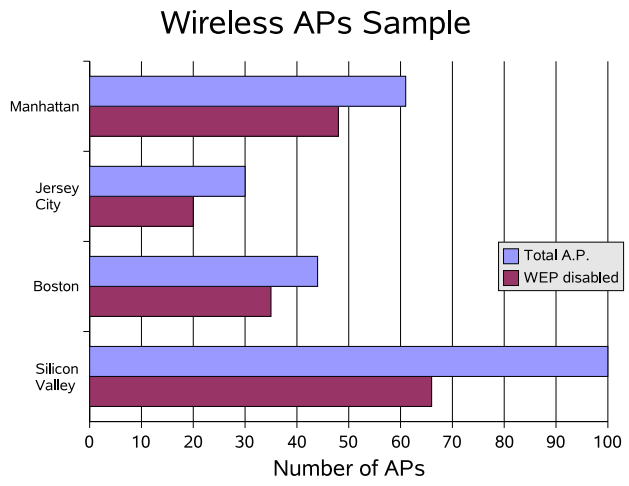

Fig. 1. Wireless networks open wide.

Any nearby user can log on the wireless network if no precaution is taken. This is a risky business and some networks will, eventually, run in trouble.

While some vendors have modified their standards-based products to secure them, vendor-independence and standards-based devices is a rule we want to keep on our approach. Some brands, like Cisco, have a broad offering of products that provide a secure wireless networking environment, solving all the known security vulnerabilities.

Most users will buy their own wireless for their laptops. An open wireless network will allow users to buy the network hardware of their choice. However, if we decided to go only with a one brand-name solution, users will be forced to buy only from them. Over the years we have tried to keep user options open by using industry standards on the network. Same rule will be used for the wireless network.

Finally, but not to be underestimated, help desk workload should be kept low by designing a user setup procedure as easy as 1-2-3. If not, the expected population of hundreds of first-time users will overload a shared help desk. So keeping users configuration easy is also a goal of the network administrators.

IV. Addressing wireless network security

In this section we present a review of the security mechanisms included on most WLAN devices and other alternative technologies used to secure WLANs. We focus on WEP (and WEP2) and 802.1x as security related technologies for WLANs. Virtual LAN (VLAN) and Virtual Private Network (VPN) are presented as standard network technologies that can be applied effectively to obtain a secure WLAN.

Wired Equivalent Privacy

The 802.11b standard defines Wired Equivalent Privacy (WEP). It is a stream cypher so that wireless data packets have a reasonable level of protection against potential eavesdroppers. WEP uses the RC4 encryption algorithm, a known stream cipher algorithm that expands the (short) key into a pseudo-random key stream. The transmitter uses the exclusive-OR function with the plaintext and the key stream to perform the encryption. The receiver repeats the same operation to get the plaintext back. This can be done at full network speed but, since WEP was created, several research groups have shown different vulnerabilities in it [4], [5].

There are several programs available that exploit some of these known vulnerabilities to the point that automatic secret-key guessing is possible with just one day of eavesdropped encrypted traffic [6], [7]. This renders the use of WEP almost useless in its current version unless secret-key is changed quite often. The use of session keys would help here, but this is a proprietary solution that may tie the network to one manufacturer.

WEP can use 40-bit or 128-bit keys; but this does not make any big difference when it comes to exploit WEP vulnerabilities. The IEEE 802.11 working group developed a new mechanism, named WEP2, to address the causes of the known problems of WEP. Unfortunately, WEP2 is not as strong as it was expected to be and, again, there are some weaknesses that can be exploited, see [8]. Besides, WEP2 is only available from certain vendors and only for the newest equipment, which also prevents its widespread use if you want to keep older APs and NICs.

802.1x

For a wired network user to get network access a physical setup is needed (i.e. cable wiring). A misbehaved network card can be tracked down and its switch port can be disconnected remotely using network management tools. Wireless users are not connected to any physical socket, they are at an unknown location and network access can be obtained almost spontaneously. User authentication to connect to the wireless network is called *Port Based Network Access Control*, also known as 802.1x. It defines the changes necessary to the operation of a MAC Bridge in order to provide port-based network access control capability. Access points, that act as bridges between the wired and wireless networks, can use this protocol to authenticate network users. 802.1x allows the use of a centralized authentication server (i.e. RADIUS) so user management is done at a single server. 802.1x authentication for WLANs makes the APs to grant network access to the user only after user credentials have been approved by the authentication server. Otherwise, the user will not have access to the wireless network.

However, 802.1x has been shown to be vulnerable to several attacks (i.e. a man-in-the-middle attack and a session hijacking attack), see [9] for a detailed information. Besides, 802.1x does not provide a privacy mechanism (encryption) that, as it has been discussed in Section 2 and Section 3, should be a must on any wireless link. 802.1x is only supported on the newest APs and requires a new NIC driver, which makes its use a bit more difficult.

It has been shown that WEP provides a privacy level that may be not good enough. WEP also requires the distribution of a secret key to the user, which in fact adds up another complexity in the user configuration. On the other hand, port based access control (802.1x) has been shown to be breakable and it does not provide an additional privacy mechanism. Therefore the use of these two technologies does not solve the security requirements mentioned above. So, we complete these technologies with other network security resources, namely VLANs and VPN.

VLAN

On the wired campus network, the evolution is replacing shared access by switched access. Some campus buildings have almost all the users are connected to intelligent switches. One of the advantages is that switches can be asked about a port's MAC address list, to track down network problems (i.e. wrong computer IP). Another advantage of the use of switches is the ability to create Virtual LANs (VLAN). VLANs are detached LANs that share a common network

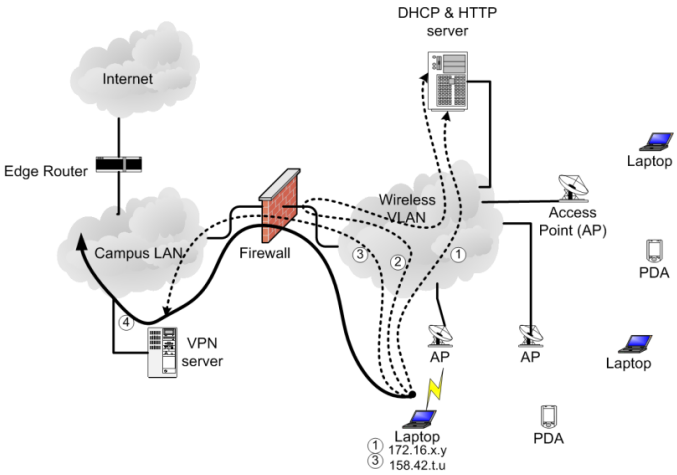

Fig. 2. Wireless network integration diagram.

infrastructure. By confining the wireless access to a separated VLAN no wireless user can send traffic to or receive data from the campus network.

Virtual Private Networks *(VPN)*

Virtual Private Networks are an alternative when looking for other solutions to get a secure communication over untrusted networks. VPNs have been used successfully to provide trusted access to the corporate LANs from the (untrusted) Internet. VPN servers are available from several vendors and also as software-only services for a variety of operating systems.

A user establishes a secure VPN tunnel to the VPN server after successful user authorization and then, all the traffic sent through the tunnel is encrypted. If the user is on a WLAN, all the data sent through the wireless link will be encrypted. So the VPN is actually solving the two required criteria: user access only after successful authentication and communications privacy by the use of strong encryption.

Over time, VPN vulnerabilities may be discovered (it happens from time to time) and then, a software update patches the hole until the next time. In some cases only the VPN server needs to be updated, which results in a negligible downtime and no impact on user's configuration.

V. Proposed wireless access network architecture

Access to the wireless campus network will be based on the following guidelines:

1) User access should be granted after the user credentials are verified. (No one should be a able to send data to the wired backbone unless logged as a valid user).
2) Wireless network data should be encrypted so that privacy is kept.
3) Installation and connection procedures should be kept as easy as possible.

Then, using both VLAN, VPN and WLAN technology we design the complete system as shown in Figure 2. It shows the complete set of interactions between the wireless users and the campus network.

Wireless nodes register on the strongest signal AP, this event can be logged and monitored from the network management console. It may be interesting to check that normal users get eventually validated. Users that are only being associated to an AP but not trying to log on the VPN should be carefully examined because this is an unexpected behavior.

TABLE I
Usage-data highlights

Sample period	3 months
Number of users	62
Total sessions	535
Mean session time	1,2 hours
Sent data	20 GB
Received data	1,5 GB

Users get configuration data from a local *Dynamic Host Configuration Protocol* (DHCP) server located on the private VLAN where all the APs are connected to. If needed, they can also obtain configuration information and software from a local web server. Communication with the outside world is possible after successful user authentication to the VPN server.

Network management computers have access to the wireless VLAN to be able to exchange management information with network devices. This information exchange may be either configuration changes or event logging. One of the management computers is actually a member of the wireless VLAN. This makes possible the management information to flow freely within the wireless VLAN unencrypted. Management information is only sent through the wired (and switched) part of the wireless VLAN, so management data eavesdropping is not possible for a wireless user.

Wireless user setup

Once a laptop is powered on, it will go through the boot or resume sequence and it will try to obtain an IP address and other configuration parameters from a DHCP server. This interaction is shown with the number 1 on the Figure 2.

DHCP server is assigning IP addresses dynamically from a pool of private addresses as described on [10]. Once a computer gets an address, DNS server address and gateway address; it can send and receive packets to and from any other computer on the wireless VLAN. If this is the first time a user is using the laptop on the WLAN, the next step will happen as soon as the user opens a web browser window. The HTTP request will be blocked at the firewall and redirected to the Wireless VLAN web server. This interaction is shown as number 2 in the Figure 2. The user then gets a web page with the required help to properly setup the computer to use the VPN server to be able to reach the campus network and the Internet. All the traffic sent until now is not encrypted. Once VPN client software is installed, the user may create a secure tunnel through the VPN server in a similar way it creates a dial-up connection, this is shown as the number 3 on the diagram. After the VPN connection is established, the laptop gets a virtual network device with an IP address from the the campus network IP address range.

The laptop routing table is updated so that all network traffic to the Internet or to the campus network is routed through this new virtual device (VPN tunnel). The WLAN is confined to an isolated VLAN, there is a router/firewall that only allows *Generic Routing Encapsulation Protocol* (GRE) to cross from the wireless network VLAN to the campus LAN. This firewall only allows traffic addressed to the campus VPN server, so no user may configure an off-campus VPN server to be used. All user traffic, after establishing a successful VPN link, is shown as number 4 on the above diagram. It is worth noting that all this traffic is encrypted using one of the tunneling protocols available (i.e. IPSec, PPTP, L2TP).

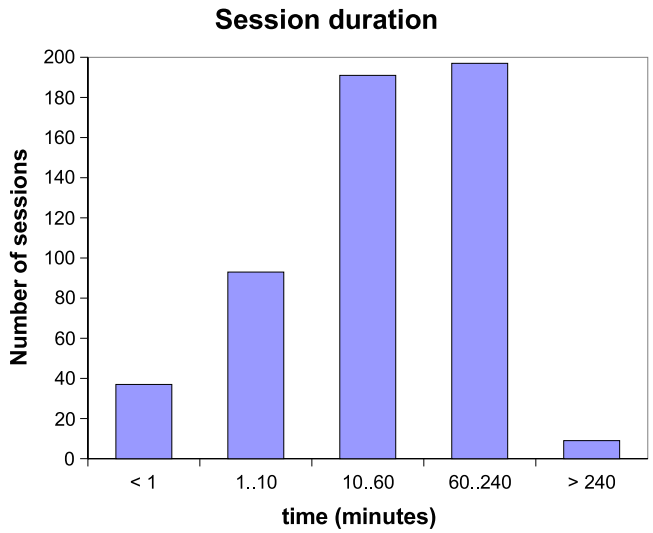

Fig. 3. Sampled network-use data.

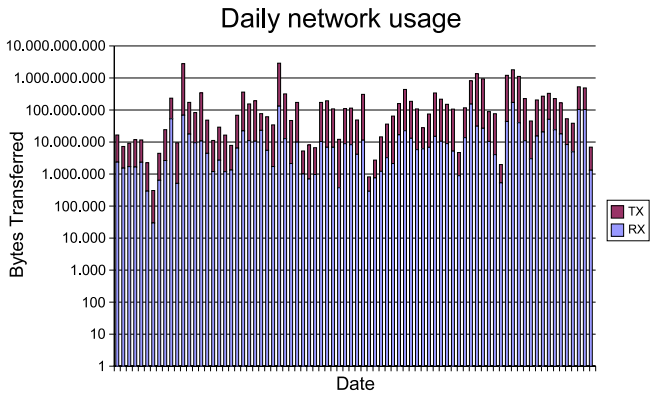

Fig. 4. Sent and received data over the sampled period.

Regular wireless users, once they have their computers properly setup, only need to start the VLAN connection once the boot-up sequence is over. This operation may even be configured to happen at the end of the boot sequence. Preliminary results are showing us that most of the users can successfully configure their laptops unattended with the help they find on the wireless VLAN web-site. However, some Linux users had some trouble when a kernel function was removed from 2.4.18 kernel version because the available software was using the missing function. This was fixed with an updated Linux driver.

VI. Measurements

Most of our available date is only for a few weeks of network use. Table I shows some details of the gathered data. Wireless network is being deployed to provide outdoors coverage on most of the campus and partial in-building coverage.

Figure 3 shows the distribution of the session length. It is interesting to note almost all of the users are connected to the network less than four hours. This data seems to match what a modern laptop can last with only one battery. On the other hand not all the users are using the wireless link for such a long period, a large user group is using the wireless connection to perform a short task like sending e-mail, surfing the net to get some data or having a short online chat of just a few minutes.

The number of sessions a user has held over the sample period is shown in Figure 4. As it happens with most of the network users, the wireless users are clearly asymmetric in their bandwidth usage. Thus users receive almost ten times more data than what they transmit. Because the sampled period started in late May, 2002, students and faculty were finish the semester and then the summer holidays followed. A significant rise on the network use is expected after next semester start on late September. That is why the user population of the sample is so low and the network use does not show a clear trend of increasing use.

Results on Figure 5 show that, for the time being, the users are using the wireless network for work mostly. There is a marginal use over the weekend.

Users are just beginning to connect to the wireless network. First impressions are positive but more coverage is requested. Figure 6

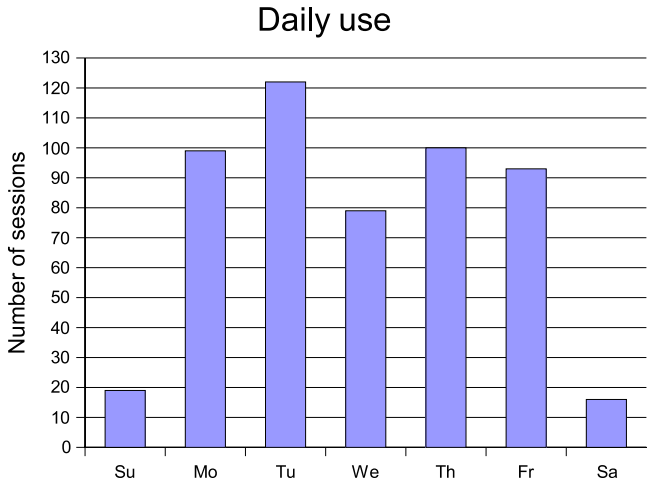

Fig. 5. Day of week wireless network use.

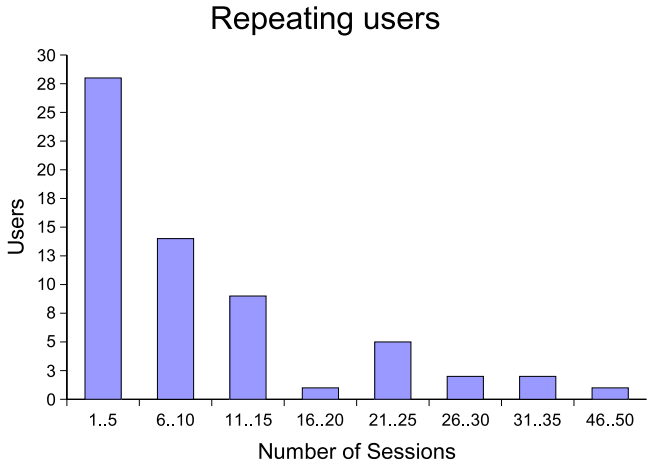

Fig. 6. Number of sessions per user.

shows how many sessions a user has had over the measurement period. Only a few users connect almost every day and, at the moment, the usage pattern is that most users connect only once or twice a week. All of the users on the logged sample use a desktop computer, the laptops are not their main system.

Wireless setup seemed to the users no more complex than wired one when we asked the help desk staff. It is true that the software side is slightly more complex. It seems that is compensated due to the lack of physical connection issues, cables to plug-in or switches to be configured.

VII. Conclusions

This paper reviews the issues of a campus-wide wireless network taking in consideration network managers and users point of view. Security and privacy problems of most widely used standards are discussed, and so are the different known vulnerabilities on some of the proposed security mechanisms.

While some vendors have addressed all the concerns expressed, a vendor-independent security architecture is proposed, explained and implemented. Easy user configuration has been present along the design process and the final system fulfills a simple and friendly user configuration.

We have omitted some considerations of scale that might favor other kind of solution for smaller networks. Our focus on this work is towards campus-wide networks only.

Experimental results are also presented. Our results show that most of the users are using the wireless link only for a short period. They perform tasks like sending e-mail, surfing the net or having a short online chat of just a few minutes. Users are not transferring software or other heavy network loads.

Acknowledgments

Authors wish to thank J.M. Pasamar, who is with the University Computer Center, for his valuable support on this work.

References

[1] Tennessee University Wireless Network, “http://wireless.utk.edu/-overview.html,” 2001.

[2] Carnegie Mellon University: Wireless Andrew, “http://www.cmu.edu/-computing/wireless/,” 1994, 2000.

[3] C. Ellison, “Exploiting and protecting 802.11b wireless networks. pc magazine,” October 2001.

[4] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4. Eighth Annual Workshop on Selected Areas in Cryptography.” August 2001. [Online]. Available: citeseer.nj.nec.com-/fluhrer01weaknesses.html

[5] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: The insecurity of 802.11.” in *MOBICOM*, MOBICOM 2001. [Online]. Available: citeseer.nj.nec.com/article/borisov01intercepting.html

[6] P. D. Anton Rager, “WEPCrack tool, http://sourceforge.net/-projects/wepcrack,” 2001. [Online]. Available: http://sourceforge.net/-projects/wepcrack

[7] The Shmoo Group, “AirSnort Homepage, http://airsnort.shmoo.com/ ,” 2001. [Online]. Available: http://airsnort.shmoo.com/

[8] W. A. Arbaugh, “An inductive chosen plaintext attack against wep/wep2,” in *802.11 group meeting in Orlando, May*, 2001.

[9] A. Mishra and W. A. Arbaugh, “An initial security analysis of the IEEE 802.1x standard,” 2002.

[10] D. K. G. J. d. G. E. L. Y. Rekhter, B. Moskowitz, “Address Allocation for Private Internets,” February 1996.