Global Information Assurance Certification Paper

Case Study: A Path towards a Secure, Multi-role Wireless LAN in a Higher Education Environment

By: Sean Malone

GSEC Certification, Version 1.4c Option 2

December 12, 2004

Case Study: A Path towards a Secure, Multi-role Wireless LAN in a Higher Education Environment

Abstract

This paper is a case study that progresses through four years in the implantation, deployment and development of a secure wireless local area network within a university environment. As institutions of higher learning tend to be trusting and open, the task has proven to be not only a great learning experience but also quite enjoyable.

The reader will progress through three preceding years of WLAN implementation prior to being introduced to the current implementation of the network. Each progression will point out strengths and weaknesses, as well as hurdles that had to be overcome, as the technology of wireless equipment, standards and services continued to grow at a blistering pace. Ultimately, the paper culminates in a solution that seems to be the best derived through years of experience, advancement, and determining just how a WLAN best fit into our particular environment.

Before Snapshot

The before snapshot of this practical is most interesting. Typically, real world information security problems, once identified, are very focused in scope and the duration of their solution depends upon complexity and the expertise of those responsible for implementing the tasks that led to the solution. In this case, however, each of the four stages of the university's wireless LAN were, in fact, deployed to address the current shortcomings and insecurity of WiFi at the time. In essence, the before snapshot of this practical are three tiny case studies in themselves each spanning about a year's time.

University Wireless LAN Number One: Neat New Toy (June 00-June01)
In the summer of 2000, wireless LANs, or WLANs, were rare and limited in scope at most small to mid-sized universities. The corporate sector was still trying to figure out just how wireless would fit into their enterprises and there was no such thing as a home broadband connection with integrated router and access point. A 56K dial-up connection was de facto standard for remote access technology.

During that summer, the university purchased and installed five Cisco Aironet 340 access points in its library with funds obtained through a grant. These devices provided near complete wireless cell coverage throughout the entire structure. However, two problems had to be resolved before the security of the installation could really be scrutinized and addressed.

First, even though the wireless LAN was in place, only a small percentage of our students and faculty had laptops. At the time, people were asking if a sub $1,000

laptop would ever become a reality. Several universities did have laptop initiatives that required such a device but many couldn't really justify why! In a few cases, such initiatives lacked adequate strategic planning, faculty commitment and, in some cases, turned out to be a very expensive marketing experiment![1] Costly laptops weren't for the average student, they were for sales executives in the corporate sector and that sector seemed not quite ready to buy into wireless data networking on a large scale.

Secondly, for the students and faculty that were fortunate enough to have a laptop, due to the slow buy-in of the technology, PCMCIA WiFi cards averaged about $175. Good luck trying to convince a student that only has a hundred dollars a month for food to plop down $175 for a network that they can't physically see! The 56K dialup line from home or the Ethernet connection in the residence hall was good enough for research even if that meant you couldn't physically locate yourself in the place that had the most resources to compliment your work like the library.

It was at that time, about July of 2000, that the university's wireless network was the most secure it would ever be. No users and no traffic. No WEP, WPA, 802.1X, VPN or IPSec, etc. Understandably, we had no information security problems with our WLAN.

The university clearly couldn't hammer down the prices for laptops and we had no plans to subsidize the cost for student purchased laptops. In order to make subsidization economically feasible, we'd need to implement a laptop initiative, which we couldn't justify because, quite frankly, we couldn't see how our students would use laptops in our classes! After all, has anyone ever tried to type out class notes in *Introduction to Latin*? Ever try doing mathematical integrals or deriving the molarity of a substance in Word?

What the university could, and did, do was purchase 10 laptops with wireless cards for checkout in the library. This gave our users a chance to *see* that the network they couldn't see actually worked. We also purchased an additional fifty wireless cards and lent them out to students with laptops so that they might enjoy the benefits of a wireless LAN and still be able to buy groceries.

Finally, we had a wireless network and wireless devices actually using it! It was time to address security.

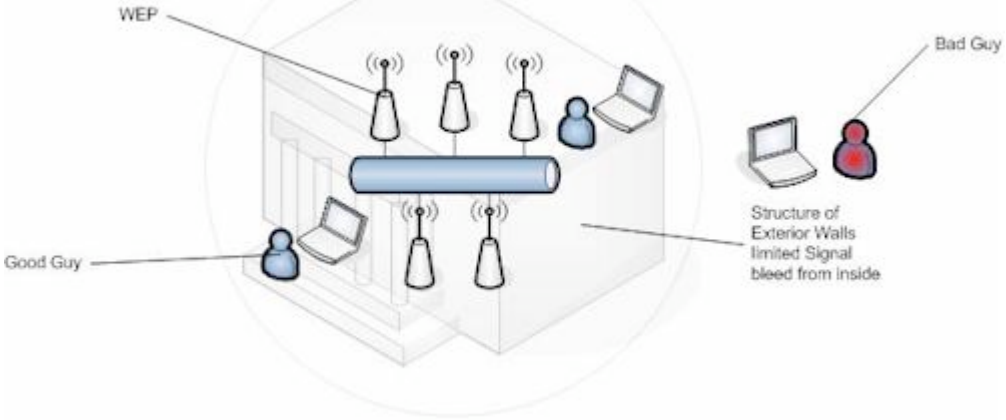
Recall, this was the year 2000. If one had a laptop, with a wireless card in it, the operating systems of the day may not have offered the SSID of available networks around you. Thus, our WiFi network was partially hidden from the bad guys because they didn't know the SSID right? Unfortunately for security, a university is an institution of higher learning in which the students and faculty

[1] TheNode.org. "The Laptop College Vol 1 No 1." LT Report. 1999. 11 Nov. 2004. <http://www.thenode.org/ltreport/laptop/ltreport-vol1-no1.pdf>.

need to easily gain access to networked resources and information. Even if we did disable broadcasting of the wireless network's SSID, arguments existing that that wasn't really a security measure.[2] Further, what's to keep a bad guy from just asking a student for the SSID as if they were just another student? Nothing. As such, the "security" implied by SSID was weak at best. After all, there really is no such thing as security through obscurity.

Additionally, "bad guy" would also need an IP address since static IP'ing was also being used as another hurdle to discourage bad guy. Unfortunately, anyone that would know enough to social engineer an SSID from someone would be smart enough to ask or determine the IP of the target's machine and be able to figure out the IP address scope being used.

If we didn't have things going for us in that universities are traditionally open and trusting environments, what we did have going for us was space and solid architectural construction. Unlike a high-rise or business complex, the university is located on its very own campus, which is not shared with other corporations. So having another business surf and see our waves for free due to proximity wasn't an issue. Secondly, the exterior walls of the library were brick backed by two inches of concrete and steel rebar. The structure might as well have been wrapped in chicken wire fence! Thus, the wireless cells did not penetrate outside the building enough to make it to a parking lot where bad guy was, theoretically, sitting in his van with a wireless laptop. Thus, with little to no signal emission outside the building, we had *a form* of physical security that mitigated unauthorized access through interception.[3]



University WLAN Number One

[2] Symbol. "Why 'Not Broadcasting the SSID' is not a Form of Security." 3 March 2003. <http://www.symbol.com/products/wireless/broadcasting_ssid_.html>.
[3] Pfleeger, Charles, Shari Lawrence Pfleeger. Security in Computing. 3rd ed. Upper Saddle River: Prentice Hall Professional Technical Reference, 2003.

However, the university needed to attempt to implement some form of confidentiality and authentication for its wireless LAN. Availability had been addressed – we handed out laptops, lent cards and configured machines for our users. Data integrity, at *that time* in the WiFi world, was something for the military and financial sector to lose sleep over. However, confidentiality of the various passwords flying through the air was an issue for us. We also needed to try and ensure that even if bad guy got associated with an access point he wouldn't be authorized to go anywhere. Enter Wired Equivalent Privacy, WEP. All the magazines seemed to know that WEP was the answer. Industry pundits would stomp their foot and say any WiFi that lacked WEP would be breached! Even the guy that served mashed potatoes in the cafeteria line seemed to know all about WEP and its importance. So WEP it was! There was only one problem – static keys. If social engineering would work in getting an SSID and IP what's to stop it from getting a static key? Nothing. Of course, that did not result in us not implementing WEP. It just meant that, upon analysis of our environment, we had pinpointed a likely vulnerability.

Thus, the first iteration of the university's wireless network was essentially secured by wrapping "chicken-wire fence" around its library and WEP.

University Wireless LAN Number Two: Toy Gets Burdensome and Dangerous (June 01-June02)

So, a form of physical security around our radio waves and a little WEP (later proven to be ineffective) "secured" the university's wireless LAN. However, a strange phenomenon occurred toward the end of the fall of '00. The library's checking out of its 10 wireless laptops made a great deal of our students much more comfortable with WLAN technology. Likewise, the lending out of university owned wireless cards made that $175 investment in a card for those with laptops a little less intimidating. When one student was stuck in their room doing research using a standard Ethernet connection while their roommate was actually in the library, where traditional resources not to mention other people were located, and doing the same thing…that card was looking more useful in the eyes of our students each day.

Christmas was just around the corner and for whatever the reason, be it truly generous giving or perhaps a feeling that the nation's positive economy would continue forever, a large number of students arrived on campus with new laptops and wireless cards in the spring of 2001.

Since many now had the required equipment, there was a desire from the student body to expand the wireless network to other areas on campus. A hand full of instructors wanted wireless in some of the larger lecture rooms – not for the students, but for their own instructional purposes. Students enjoyed the WLAN in the library but called for cells to be installed in common areas where they tend to meet after class such as foyers, the cafeteria and the university's Cappuccino Bar.

Thus, the expansion was inevitable and our "chicken-wire fence" defense wasn't applicable in all campus structures. Additionally, I was getting tired of manually configuring static IPs and had to face the fact that WEP static keys as a form of authorization with our access points wasn't necessarily going to keep bad guy from the network. Hence, the second wireless network was designed and slowly deployed throughout the spring semester.

Ten Enterasys RoamAbout access points were purchased in addition to the existing five Cisco Aironet APs. The capability of power over Ethernet (PoE) was beginning to prove a necessity in WLAN deployment and Enterasys seemed to have been doing it the longest. That additional functionality allowed the university to fling those ten access points out to places that we could not have otherwise accomplished which significantly increased not only coverage but availability in that all the devices could be powered from central distribution areas and benefit from existing battery backup.

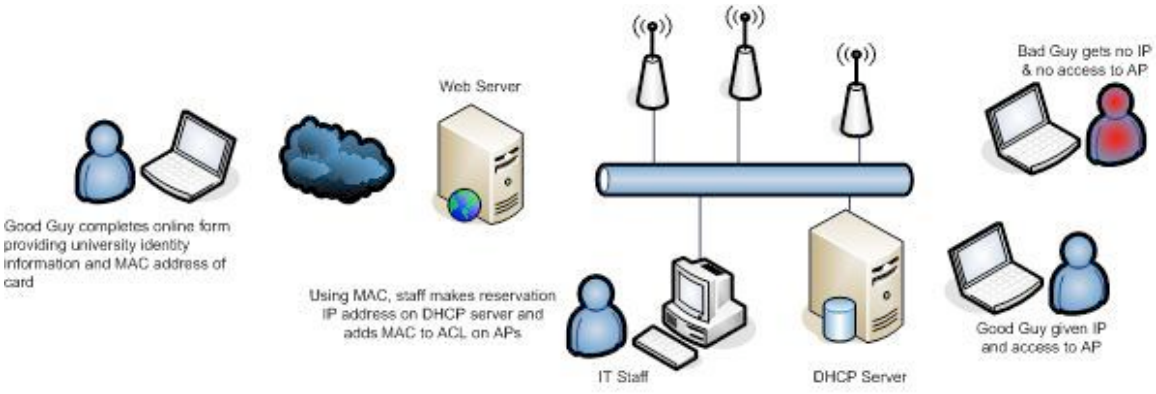
The increasingly time consuming task of manually IP'ing all wireless enabled laptops was beginning to wear on university IT staff – which, for the WLAN, was me, eight fingers and two thumbs. Yet, deploying Dynamic Host Configuration Protocol in its traditional fashion wasn't an option. The access points plugged into the same network as every other host on campus. Although the university IT staff wanted authorized wireless users to obtain an IP we did not want an unauthorized laptop to be able to plug into a standard Ethernet port in one of our classrooms and get an address.

As a solution to the IP addressing dilemma, DHCP was implemented in a unique fashion. A DHCP server was deployed and provided with a portion of address space whose scope was not already statically assigned. Every IP within that scope was then reserved by Media Access Control (MAC) address. So, instead of IT staff manually assigning IP addresses on each wireless laptop, the student or faculty member merely filled out an online request form that included submission of the MAC address of their wireless card.

In retrospect, the process worked well and was simple to implement. If a user wanted access to the wireless network, they merely would provide the MAC address of their wireless card, such as 0001f4ee7545 in an online form. The online form was submitted and received by IT staff. IT staff, respectively, reserved an IP address, such as 192.168.0.4 for the card with that particular MAC address on the DHCP server. From that point forward, the student's laptop would always be assigned address 192.168.0.4 from the DHCP server whenever entering a wireless cell.

Addressing taken care of, it was time to revisit authorization. Since the university already had the MAC address of all the devices needed access to the WLAN, we simply implemented MAC address based access control lists on the access

points. Thus, even if bad guy knew the WEP keys – which by now may as well have been written on the university mall in sidewalk chalk, you couldn't go anywhere or be automatically assigned an address unless the MAC of your card was on the list.



University WLAN number Two

Thus, the manual IP issue had been resolved. The inadequacy of WEP for authorization had been mitigated. For a period of time, all was well. However, by this time the inadequacy of WEP, *as a trustworthy encryption standard*, had been proven.[4] Thus, WEP as an encryption standard began to collapse.

Additionally, wireless networking was really starting to pick up in the business sector. Since many businesses ended up "securing" authorization to their WLAN just as the university had done, easily used open source tools that would allow one to not only "sniff" the air and capture traffic from valid wireless devices- which happened to display that devices MAC address, but also "spoof" that MAC essentially hijacking the identity of a valid wireless device. Something else was clearly needed to lock the WLAN down and that something else was authorization.

University Wireless LAN Number Three: Enter the VPN (June 02-June03)
It was now June 2002 and the university needed to once again reinvent and expand its WLAN. To be fair to the institution and IT staff, none of the changes made or that were to be made were reactive. We simply kept abreast of the technologies that were rapidly developing themselves around WiFi and made modifications that best fit our environment in a proactive manner, within our budget.

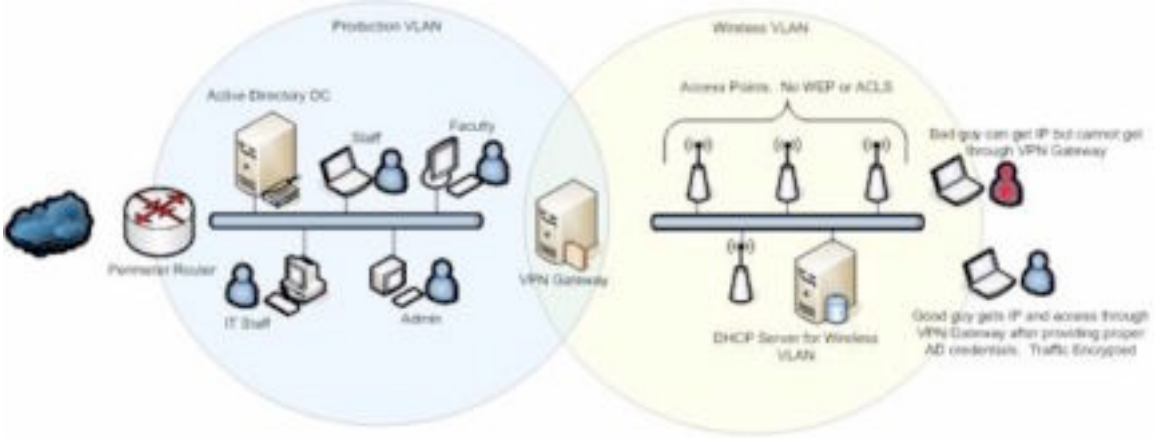
We needed more than authorization. We needed authentication. WEP was out the door and some of the proprietary technologies that popped up to replace it, such as Cisco's LEAP, where more appropriate for the enterprise environment that could enforce standards in terms of which wireless card and access points

[4] Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP Algorithm." <http://www.isaac.cs.berkely.edu/isaac/wep-faq.html>.

were used. Plus, IT Staff were starting to get really tired of adding MAC addresses to the access control list on our ever growing army of access points.

We needed a VPN for our wireless network. Thus, we implemented a VPN using routing and remote access services, Internet Authentication Service and our existing Active Directory database. It was also at this stage that we began placing the university's wireless infrastructure into a separate VLAN.

The access control lists from the access points were cleared and we started validating access to our WLAN through login authorization. The wireless device would obtain an IP from a DHCP server located on the inside interface of the VPN gateway along with the access points. The device would then be required to initiate a VPN connection to the outside, which was actually the production network. If proper login credentials were provided, an IP that was valid on the production network was dynamically (no more static entries) assigned and the device's traffic would then be "wrapped" inside an encrypted tunnel.



University WLAN number Three

In this solution, WEP was not necessary for the limited degree of authorization it provided or encryption. The VPN took care of authentication, IP address assignment and encryption. IT staff no longer had to work with the growing number of MAC addresses in any way and bad guy could sniff air traffic all day and the only data that would be seen in clear-text would be useless DHCP traffic. In fact, bad guy would be assigned an IP that would allow him to ping the inside interface of the VPN gateway, but lacking an account, that was about all he could do.

Hence, all was settled. Everything worked fine…kinda. IT staff was happy to no longer have to work with MACs – that's the address MAC. Unfortunately, Macintosh laptops were once again gaining popularity due to low cost, appealing design and the forthcoming OS X. And, of course, during the phase from MAC OS 9 to OS X, there was no VPN client software developed that could be easily obtained at low cost. Thus, we had a significant percentage of students with

shiny new MAC laptops that couldn't use our network, which resulted in incomplete goals.

Additionally, the new "VPNified" WLAN was a bit slow due to all of the encryption. Students began to ask why encryption was so necessary when they just wanted to browse the web. Other than login passwords, most students didn't care if someone could see their wireless traffic and would gladly trade speed for security. Faculty and staff liked the VPN! They could now access all network-based data knowing that the link was as secured as we could make it at the time.

We made the best of things with our "VPNified" WLAN3 through the end of Spring 2003. The students grudgingly accepted the hit in performance. The Macintosh owning students patently waited for OS X to get itself together and the university speculated that, in the fall of 2003, we would see the largest percentage of wireless laptop usage to date. In light of that fact, the VPN wasn't going to cut it. We needed to drop the enterprise infrastructure WLAN model and implement a model that would serve our customers – the students. A hotspot model it was!

During Snapshot

University Wireless LAN Number Four: Hotspot (June 03-Current)
Wireless LAN Four was the most ambitious reinvention of our wireless network in that it was essentially a complete replacement. University administration appreciated a wireless network that could be utilized by administrative staff and faculty, as well as, students but also understood that the largest user base of the WLAN was the students. It seemed inappropriate that a WiFi infrastructure model that complemented the work of a few should impair the usage of the many.

As such, all access points were pulled and placed into storage so that they might, in due time, be used to build a second infrastructure mode WLAN for the administration. The VPN server's roll was reduced to Internet Authentication Service (Microsoft's implementation of RADIUS) and routing and remote access services were removed.

Clearly, the problem of providing wireless network access to the student body, faculty and staff had been approached in very specific, well-planned steps. Essentially, the problem was approach by three years of research, development, as well as, growth and advancement of wireless networking equipment and technologies.

WLAN One was taken on in WiFi's infancy. Still, once availability had been addressed, security was handled thought the recommended best practice at the time and physical location of the network. WLAN Two continued the recommended encryption standard but also acknowledged it as vulnerability.

Additional security was applied through reserved addressing and access point access control lists. Finally, WLAN Three dropped AP to client encryption all together in favor of client to VPN gateway encryption. VLANing was also implemented for management purposes and to separate the WLAN collision domain from the production network.

It was decided that a hotspot model was necessary so the university began weighing its options. We reviewed several different turnkey product offerings from various venders. We initially attempted to find a solution that would allow us to merely supplement existing equipment with some intelligent device. However, during this time in the development of hotspot equipment, we quickly found that while the user database could be centralized the actual intelligence resided on the access points themselves. Lastly, we also considered outsourcing the entire project to a commercial provider but made the decision to continue hosting the wireless service ourselves for budgetary reasons. Namely, if an outside vender charged our students for wireless access then the university would need to remove or lower fees, which happened to pay for a great deal more than just the wireless network.

Several factors were considered in just what it was we wanted in a hotspot model. Clearly, we wanted to continue authentication with existing directory services. We needed the new network to work well with both PC and Macintosh. We also required power over Ethernet in that we, essentially, would just replace the existing access points with the new, more intelligent devices. Per the request and understanding of the student body, we wanted secured login but otherwise unencrypted traffic for speed. As was common in the hotspot model, this would be achieved through a web-based login page. However, the page had to enforce SSL and a verified certificate in order to mitigate authentication page hijacking, which was becoming common in mainstream hotspot environments.[5]

Lastly, if it could be done away with, IT staff really wanted to no longer maintain a separate VLAN for the wireless network. For our environment, a separate wireless VLAN equated to additional work in trouble-shooting and additional acquisition costs. Anytime a new networking device was to be purchased, we had to ensure that it would support our VLAN trunking and encapsulation requirements, which, for some areas on campus, just wasn't necessary. Yet, under the existing model, we never knew if we'd someday be hanging an access points off new networking equipment.

Ultimately, the decision was made to utilize equipment from Colubris Networks. New CN3000 wireless routers from were installed in the existing AP locations. The CN3000s immediately satisfied all of the requirements that had been deemed necessary for our new hotspot WLAN and then some.

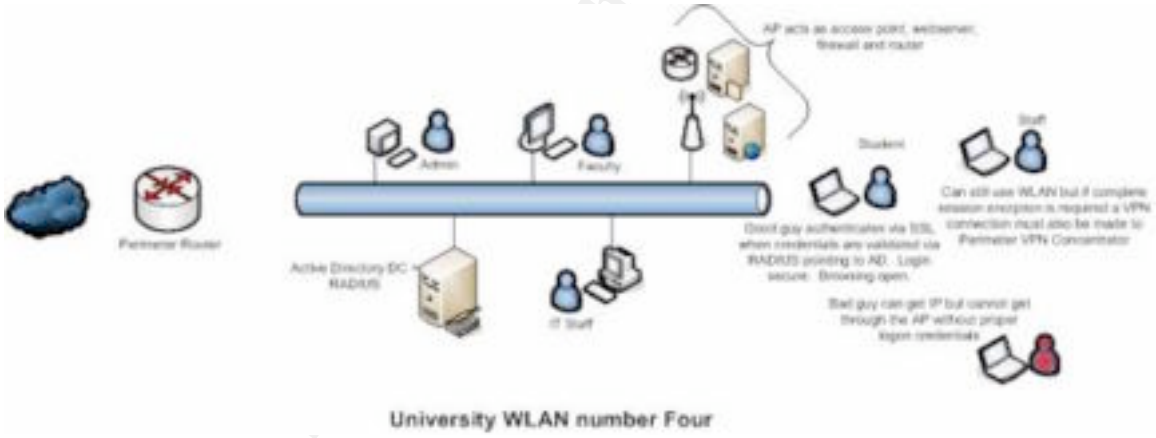
---

[5] Brandt, Andrew. "A latte, a Wi-Fi link and a hacker." Computerworld. 25 Nov. 2003, 6 Dec 2004 < http://www.computerworld.com/securitytopics/security/story/0,10801,87523,00.html>.

Power over Ethernet was an option, which we took full advantage of. The devices themselves acted as firewalled routers. Thus, they came with an internal interface (this was the antenna) and external interface (a NIC) which allowed the university cease management of the previously created wireless VLAN since collision domains were now behind the inside interface of the wireless router. Traffic from the external interface was set to only get through to the perimeter router, and thus, the Internet. The devices had an internal DHCP server to hand out addresses to wireless clients on the internal interface. They also housed their own web server, which hosted an SSL login page. The SSL login page communicated login credentials securely to our existing RADIUS server in order to authenticate users.

The device also implemented captive portal so that no matter how a student's laptop was configured their radio signal was "captured" and their session was pushed to the SSL login page. And, finally, Macintosh with either OS 9 or OS X were no longer a problem.

Taking all of the above into account, the new hotspot model has been a dream. It worked as designed to the delight of university students and simply reduced that amount of support time and operating costs for IT staff.



University WLAN number Four

Such an arrangement satisfies the need for speed while acknowledging the importance of security. In reality, if a user needs security in web-based work, SSL is ubiquitous and if a staff member needs a completely encrypted tunnel, they can connect back into the university network by establishing a VPN connection through the university's perimeter VPN concentrator.

After Snapshot

In the fourth year of this university's wireless network, there is little doubt that the overall security of the network, viewed as a cohesive system, has been significantly enhanced. Beginning in June 2000, the initial problem was simply how one best deploys a WLAN in a university environment such as ours. At

each stage in the network's development, best practices came and went as the technology steamed forward. As with any long-term project compiled with multiple variables and audiences with differing needs, subsequent iterations addressed factors of risk derived from the previous, which resulted in new risks that would require both acknowledgement and mitigation or elimination.

The new vulnerabilities will begin to become evident. The decentralized intelligence of the system places the university at a financial risk in that these devices are more costly than off the shelf access points. Such risks can be addressed in future implementations where the intelligence of perimeter devices can be off-loaded to core, redundant wireless gateway appliances that offer different types of services and varying levels of encryption dependant upon the particular user.[6] At any rate, work such as this could not have proceeded in the fashion it did without the fundamental concepts and practices gained through security training and study. Not only does such knowledge keep one abreast of current trends in technology, it also reminds one that information security is an ongoing practice.

[6] Dornan, Andy. "Wireless LANS: Freedom vs. Security?" Network Magazine. 7 July 2003. 8 Dec. 2004 <http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=10818265>

References

Borisov, Nikita, Ian Goldberg, and David Wagner. “Security of the WEP Algorithm.” <http://www.isaac.cs.berkely.edu/isaac/wep-faq.html>.

Brandt, Andrew. “A latte, a Wi-Fi link and a hacker.” Computerworld. 25 Nov. 2003, 6 Dec 2004 < http://www.computerworld.com/securitytopics/security/story/0,10801,87523,00.html>.

Dornan, Andy. “Wireless LANS: Freedom vs. Security?” Network Magazine. 7 July 2003. 8 Dec. 2004 <http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=10818265>.

Pfleeger, Charles, Shari Lawrence Pfleeger. Security in Computing. 3rd ed. Upper Saddle River: Prentice Hall Professional Technical Reference, 2003.

Symbol. “Why ‘Not Broadcasting the SSID’ is not a Form of Security.” 3 March 2003. <http://www.symbol.com/products/wireless/broadcasting_ssid_.html>.

TheNode.org. “The Laptop College Vol 1 No 1.” LT Report. 1999. 11 Nov. 2004. <http://www.thenode.org/ltreport/laptop/ltreport-vol1-no1.pdf>.