

Trends for Protecting Wireless WANs and LANs

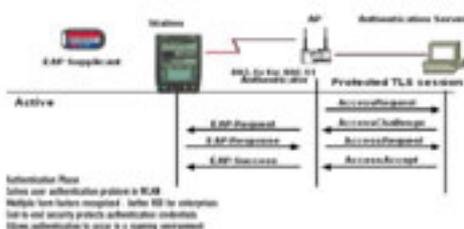
A retrospective look at wireless security issues that made an impact on the wireless market in the last year and unique challenges that will be faced in the year ahead.

By Kim Getgen, RSA Security

By 2003, technology analyst projections estimate that 23 million users in the U.S. alone will use wireless LANs (WLAN), with the Asia-Pacific region and Europe showing tremendous growth as well. Such well-known companies as UPS, FedEx and General Motors already use WLANs to give customers and employees more mobility and access to real-time information. 2001 was certainly the year of experimenting with the idea of a wireless enterprise.

Outside the enterprise, however, even more compelling data began to circulate, claiming that WLANs were positioned to disrupt the adoption of upgrading to next-generation 3G networks for two reasons. First, because 3G can offer only a fraction of the bandwidth available over WLAN today, many argued against waiting for 3G if the bandwidth were already available using WLANs today. Second, analysis in some regions indicated that it would be less expensive to blanket areas in WLAN access points than it would be to roll out 3G to the same region (Nomura, March 2000). By the end of 2001, there was little doubt that WLAN technology offered what the market wanted: cheap and easy wireless bandwidth — today.

But as it looked like WLANs were positioned for serious growth in 2002, security concerns began to resonate within the industry. In February, the International Olympic Committee ruled that 802.11 WLANs would not be used at any of the Olympic Games until at least 2008. This followed an announcement by the Lawrence Livermore National Laboratory that they, too, will be shelving their WLAN in favor of more secure landlines. And there surely have been other similar announcements. With security being pushed higher on many people's agenda this year, WLANs at airports, car rental agencies, banks and businesses are re-evaluating their wireless strategy. This year, many will ask how to secure their WLANs rather than take unnecessary risks.



Trends for Protecting Wireless WANs and LANs

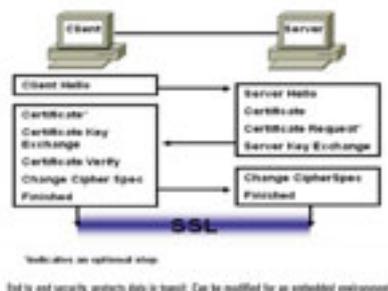
Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

Before the security concerns, WLANs were positioned to be a disruptive technology. After the vulnerabilities, WLANs became disruptive for quite a different reason. The industry realized that these networks were an easy way for attackers to disrupt corporate networks and cause damage inside the enterprise.

WLAN Security: A call to action for 2002

Why are WLANs not secure? The lack of privacy in the network stems back to a broken encryption protocol called WEP — the wired equivalency protocol — which does a good thing: it outlines a way to encrypt data packets traveling over 802.11 networks. Unfortunately, the protocol was inherently flawed because it contained a key derivation problem that crippled any security offered through encryption in the standard.

But, let's have a look in more detail. Because WEP encryption is based on a symmetric stream cipher (RC4), it is important that each packet have a different WEP secret key. And while the WEP standard had specified the need for using different keys for different data packets (a very good idea), the key derivation function that outlined how to derive a key from a common starting point was flawed (not so good). Simply put, the keys for different data packets were too similar, allowing attackers to exploit this similarity and extract information about the shared secret after analyzing only a modest number of packets. Once the shared secret was discovered, a malicious attacker could return and decrypt data packets being passed along the exposed network.



These WEP vulnerabilities can be traced back to two main problems: 1) the limitations of the 24-bit initialization vector (IV) combined with 2) a weakness in how packet encryption keys were derived from the initialization vector. The outcome of these weaknesses created something called IV collisions, which produced identical WEP keys: the same IV used with the same shared secret key on more than one data frame. For simplicity, let's call these "weak" WEP keys because this was the weakness that attackers knew to exploit.

What followed was like a dam bursting. Free tools, such as AirSnort and WEPCrack appeared as scripts on the Internet, allowing anyone to attack WEP. AirSnort authors claimed their code could decipher WEP keys after gathering information from just 2,000 packets with "weak" keys (out of 16 million keys generated, 3,000 were typically weak). Network "sniffers" were then set up to analyze the "weak" keys and discover the shared secret between wireless clients and access points. Once the shared secret was discovered, a malicious attacker could not only have access to the wireless LAN, but go back and decrypt data packets they "sniffed" off the exposed network.

By the end of 2001, RSA Security and Hifn announced a new technology —

Trends for Protecting Wireless WANs and LANs

Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

"fast packet keying" that would fix the key derivation problem in the broken WEP standard: a technology that the IEEE committee has approved. This was the first step in allowing 802.11 vendors to create a software patch that could be applied to update WLAN products already being used by their end-customers. While we have not seen any public statements from vendors on when a patch might be available (this is dependent on concurrent work in other 802.11 committees), we do receive many inquiries from anxious customers who want a way to patch their WLAN. Patches should be made available this year if WLANs are to overcome their perception of being insecure.

The second WLAN security problem was largely ignored last year, but will be just as important for adoption. It is how to securely authenticate users roaming between WLAN access points. While this is aggravating for enterprise users who need to re-authenticate if they move from one end of the building to another, the problem will also affect operators who want to bill customers for WLAN service. These WLAN "hotspots," which are beginning to sprout up for public Internet access, may soon become a source of revenue for operators. Gartner's outlook for the 2002 public WLAN market predicts that U.S. operators are currently "looking at how to make money...[but] they know it is more a matter of when, not if, interest in these technologies will pick up." (January 28, 2002)

Anyone interested in making money from WLAN services or protecting their corporate WLAN should pay attention to the next point. Before you can bill customers for your service, you need to know who they are and when they are using the services you provide. The same goes for enterprises. Before extending the corporate network by deploying a WLAN, you need to have a good strategy for authenticating and authorizing who has access to your network. For this to happen, good authentication standards need to be evaluated and adopted such as:

- Accepting a universal standard that allows any authentication system (PINs, passcodes, digital certificates, tokens or smart cards) to operate with any WLAN access point.

- Ensuring devices (PDAs, mobile phones and laptops) are able to understand authentication methods used.

- Adopting a standard that allows Wireless LANs to authenticate users "behind the scenes" as they roam from access point to access point and without knowing that their digital credentials are being challenged and approved somewhere in cyberspace.

Much work has been done to solve many of these problems. RSA Security, Microsoft and Cisco have already tendered a proposal to the IETF, which outlines how to achieve secure authentication in a roaming WLAN environment called Protected EAP which is based on a universal authentication standard (EAP). The proposal is currently being considered by the 802.1x committee so that next-generation WLAN products will be better able to authenticate their users. Microsoft, one of the first vendors to support the standard, has already shipped this authentication protocol in its Windows XP operating system.

Beyond the WLAN:

Securing the wireless Internet

For many, securing the wireless Internet has meant securing the transport layer in WAP, but even WAP has moved away from their Wireless Transport Layer Standard (WTLS) in favor of more popular Internet standards. The question many will consider

Trends for Protecting Wireless WANs and LANs

Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

this year (probably more as an afterthought) is did WAP dominate too much of the conversation last year but come to the table with a solution a little too late. Indeed, there are already a lot of wireless applications that simply bypassed WAP and instead used SSL to secure communication channels over wireless networks. For example:

•More than 27 million iMode users in Japan have been using secure-socket layer (SSL) connection protocol in their microbrowsers for more than a year now.

•Pocket PC has SSL built into its operating system.

•Palm announced last week that they would offer SSL in their latest operating system so application developers writing code for the Palm would be able to call into Palm's SSL stack to create a secure connection from the client side. Palm estimates that eight times more developers write for their platform than any other platform, which helps increase the dominance of SSL in the wireless world.

•Kyushu Matsushita Electric announced they will use SSL in their portable car navigation system that will allow users to receive email and Internet content wirelessly.

For SSL to work in an embedded client communicating over a wireless network, however, a number of code changes need to take place to maximize the performance and throughput. These are all design issues where trade-offs are necessary to negotiate the best outcome for a particular environment. But these customizations should be left to SSL experts who can minimize code and negotiate these trade-offs, which allow SSL to work well in an embedded environment.

Because these code changes are very complex, commercial security products (like software developer kits) need to be available to support developers as they try to embed mini-versions of SSL into more wireless and embedded environments.

Some lessons we've learned, which are allowing SSL to be successfully used in the examples above, include the following:

Know where to reduce the code size.

SSL was designed for a "fat" client/server environment, but by prudently choosing what to eliminate, SSL code can be minimized, yet still provide a high level of security and interoperability with Web servers running a heavier version of SSL code.

Increase the responsiveness over wireless networks by reducing the size of data blocks sent.

One advantage that WAP's WTLS had over SSL was that it sent small data gram packets (less than 1k) rather than stream data (16k at a time) over the wireless network. This goes back to the original problem WAP was trying to solve, which was how to send data over less reliable, finicky wireless networks. But SSL experts such as Eric Young, RSA Security Technical Director, argue that the SSL protocol can be modified to decrypt smaller blocks of data received by wireless clients. This creates a more responsive application which allows users to watch the data build on their screen. Keep in mind that the server still sends data to the client encrypted in 16k blocks, but now the client can break this 16k record down and decrypt it 1k at a time, creating an environment similar to WTLS.

Encryption is faster than the network and can be optimized for the embedded processor.

Today, the processing power on today's embedded clients combined with the ability to optimize algorithms to specific embedded processors means the encryption being applied to the packets is not the bottleneck. Therefore, any performance

Trends for Protecting Wireless WANs and LANs

Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

degradation the users notice is not encryption, but the slowness of the actual wireless network. For most security experts, this is an obvious point, but many not familiar with the performance speeds assume security is the bottleneck.

Reduce the number of roundtrips made between the client and server during the SSL "handshake."

This can increase throughput, but the challenge is to remain interoperable with all those Web servers without causing a fatal error that would kill the SSL session.

Summing up Wireless Internet Security

For the wireless Internet, interoperability has been the key. By interoperating with the wired world by using Internet standards like SSL, end-to-end security problems are well on the way to being solved. Consequently, we will continue to see SSL being used in new ways.

Kim Getgen is a Product Marketing Manager at RSA Security. The company's RSA BSAFE software developer kits have launched a new product line specifically aimed at supporting developers solve security problems in wireless and embedded environments. For more information on these and other wireless security issues, please contact Kim Getgen at kgetgen@rsasecurity.com.

Source URL (retrieved on 09/01/2014 - 11:16am):

<http://www.wirelessdesignmag.com/product-releases/2002/04/trends-protecting-wireless-wans-and-lans>