

## Re: Wlan @ bestbuy is cleartext?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-05/0057.html>

---

**From:** Ron DuFresne ([dufresne@winternet.com](mailto:dufresne@winternet.com))

**Date:** 05/02/02

Date: Wed, 1 May 2002 17:02:49 -0500 (CDT)  
From: Ron DuFresne <[dufresne@winternet.com](mailto:dufresne@winternet.com)>  
To: Erik Parker <[eparker@mindsec.com](mailto:eparker@mindsec.com)>

This has been x-posted to the firewalls list as it relates directly to a thread there on a potential WLAN rollout question and VPN solutions considered to 'secure' such open air transmissions. <hoping BB will let this post pass on vul-dev as well>

On Wed, 1 May 2002, Erik Parker wrote:

[SNIP]

>  
> *However, it's best buys decision on what they want to do with their*  
> *customers data.. Even though I'm pretty sure there are legal consequences*  
> *for them as well.. At least with their insurers.*  
>

[SNIP]

I think that the customer data does not totally belong to BestBuy, but also the issuing credit company, as well as the customer. So, there well could be other legal issues involved, and would be if this at all related to HIPPA.

And I know alot of the discussion here so far has been directed at Best Buy and others that have rolledout insecured wireless implmentations, and with some right to be not only shocked at these toys being placed as they are into use by the companies in question. But, if we are going to direct efforts at blame and how to make such toys as semi-secure as we can at present, let's make sure we point fingers at those ultimately responsible for unsafe open default configurations and hiding information deep in CDROMS from the endusers attention about how to attempt to semi-secure these toys, the vendors, Lucent, Cisco, and the others pushing out wireless capabile toys without safe default configurations to begin with. There's alot of talk about how to VPN tunnel and IPSEC tunnel these connections to try and lock down security, but, information leakage is still a serious matter. And none of this should come as new news to anyone. Folks have for quite ometime been doing work on mapping projects

and releasing tools to crack WEP and trying to spread the word in their own fashion that wireless is at present a bad deal<TM>. Now, rather than hint at and push excerpts from, lets just be done with it and push our venture to warn of the problems out to the public now, folks are just not alarmed enough to do the research and fear these toys being deployed in their environments even after the work of many we reference and site in this paper which follows the original post prompting it's release here:

>  
> BB> *This past week I went to bestbuy to purchase a D-link wlan card... egar to*  
> BB> *get my laptop up and running while in the car I put my card in and*  
> BB> *installed the driver. I noticed the traffic light was lit up as if I had a*  
> BB> *connection. Out of curriosity I fired up kismet and sure enough there were*  
> BB> *packets flying through the air right infront of BestBuy. Well I decided to*  
> BB> *run in an try to make a Credit Card purchase real quick to verify that my*  
> BB> *info was not going all over the parking lot in the clear. Well after*  
> BB> *sorting out my logs I noticed what looked to be like SQL queries and table*  
> BB> *headers in my logs ... things such as CUSTOMER\_ROUTEID, BANKNAME,*  
> BB> *REGISTER\_ID and things of that nature... luckily no where in that data did*  
> BB> *I find my own credit card. Non the less I decided to run to the store next*  
> BB> *to BestBuy while I left me PC on grabbing packets. Well yesterday I sorted*  
> BB> *through the data collected and this time I did indeed find a RAW clear text*  
> BB> *credit card number....not mine ... but definately a credit card number.*  
>

Wireless Vendor Woes and Shame  
(c) Ron DuFresne 2002

I heard a fine paper delivered here by Alan Clegg on his efforts to map the local wireless infrastructure in the Raleigh/Durham/RTP area. Art Ehuan, with Cisco Systems gave a backup talk on the threats faced and the tools available to exploit these wireless streams spewing data freely into the airwaves here. Much of these issues have been the topic of treads in this and other security lists as well as covered in the various systems/network security journals. Not having a need at present to consider or deal with the woes of wireless toys, I have watched these discussions and disclosures, and gathered together some of the more enlightening material for the time I have to deal with these new toys in some manner, if it be only to argue against their deployment in areas we work and support.

Even though the weaknesses in WEP are now widely known, and some vendors such as Cisco have developed and are deploying somewhat better proprietary encryption and authorization protocols for 802.11b <LEAP>, it is shocking to note and others have identified the lack of vendor accountability and responsibility in offering these toys with safe default settings and configurations[0]. Not only that, but manuals are sparse on covering safe configurations, and most often the user/implementer has to dig deeply into documentation stashed away on the CDROMS that accompany these products to find anything on encryption and safe setup of these devices. As Alan touched on in his talk, and Steven Connelly pointed out in his

## SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

preview of this article: "most manuals don't explain what/why there are different channels and as a result most admins just use the default ones which in the case of a crowded city is quite detrimental to basic performance (as shown in Shipley's defcon talk where something like 80% of the APs in downtown SF were all on the same channel.)" <Peter Shipley's work can be found in the bottom referenced work for this paper> The emphasis it seems is on plug and pray technology. And the stress on PnP here is not on it working when plugged, as it most often does anyways, but the praying that you are not 'discovered' too quickly and exploited for deploying toys that just are not really safe for the times. As seems always is the case, technology is out pacing our abilities to deal with the ramifications of it's deployment. Neither Lucent nor Cisco are responsible with the tools they are pushing to market as regards safe default setups and configurations. And, we are unaware of any vendor offerings that do any better in an accountable and/or responsible manner. Granted an admin or any other user setting up such equipment and applications should certainly check their configurations and settings. Yet, being that this information is tucked far under the documentation hood, deep enough many without specific insights into the workings of their new toys, and also considering the weaknesses of WEP and even the newer proprietary encryption/authentication methods folks like Cisco are pushing out, the burden rests in the vendor realm to provide safest default setups possible. Shame on these folks!

Alan pointed out the severity of the "problem" in just our local area by mapping out not only many private home wireless deployments, also various corporate ones as well as some local government AP's <wireless access points>, many without even WEP enabled, but found at least one highly visible federal government contractor with a wireless AP deployed, again, \*without\* even WEP enabled![1] This even after the 9/11 attacks and recent supposed focus upon security.

Of course, even with WEP enabled, the way the 802.11b protocol is setup and the fact that it's spewed into the airwaves means that valuable network information is leaked in just the management packets. SSID's, IP address info, and more can be gleaned from only management packets. There is no protection from passive sniffing of these packets due to network segmenting and the concept is pretty much not applicable to wireless Ethernet transmissions. Additionally, neither speaker mentioned there are known weaknesses in the SNMP implementations of many of these devices subjecting them to further exploit wireless networks via less passive intrusion and DDOS attempts.

While most often signals are limited to 300 feet or so, better receiving antennas can put a sniffer or active attacker miles away. Alan showed one off the shelf antenna he purchased that gave him up to a 2.5 mile radius. there are other capabilities that can be even more affective then what Mr. Clegg demonstrated. Steven Hume at Novell <[shume@novell.com](mailto:shume@novell.com)>, recently noted in one of the security mailing lists:

Anyone interested in the Pringles antenna :-

Re: Wlan @ bestbuy is cleartext?

SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

<http://www.oreillynet.com/cs/weblog/view/wlg/448>

Using this they claim they could get 11mbps over 10 miles!

Mr. Hume additionally pointed folks here:

a good article covers many of the points raised plus more:

[http://www.extremetech.com/print\\_article/0,3428,a=13880,00.asp](http://www.extremetech.com/print_article/0,3428,a=13880,00.asp)

This includes additional pointers to wireless mapping efforts in various other US cities. Afterall, wireless mapping has been going on for sometime now. The issues related to wireless roll outs have been known and available for sometime. What the Clegg and Ehan papers disclose is how little attention has been paid by NC IT personnel to these issues, even those tasked with securing their infrastructures. There discussions were meant as a heads up to those maintaining the network infrastructures for their prospective organizations. These people either are not paying attention to the issues and implications of their network roll outs and ventures, due to time or knowledge/training constraints or lack the skills to do so. It also demonstrates a failing in many network security policies for these companies and ineffective network security auditing procedures and practices. Our key admins and corporate security folks are lagging by at least a full year to this information and it's availability! Not that this separates them from those folks tasked with such matters in various other locations about the country that much. Alan's findings are pretty much representative of the findings of others throughout the US in their wireless mapping research, something on the order of what Jason Costomiris reported a few months back;

From: Jason Costomiris <[jcostom@jasons.org](mailto:jcostom@jasons.org)>

Subject: My Saturday with Netstumbler...

Date: Tue, 5 Mar 2002 17:06:30 -0500

...

Highlights of my findings:

- Only 23.53% of APs found were using WEP
- 80.77% of Linksys APs used the default SSID, "linksys"
- 2 out of the 3 Apple AirPort base stations had WEP turned on

Detailed findings follow:

Percentage of Total APs by vendor:

Addtron 3 2.52%

AMI 2 1.68%

Agere (Orinoco/Lucent) 47 39.50%

Apple 3 2.52%

Cisco (Aironet) 20 16.81%

D-Link 4 3.36%

Linksys 26 21.85%

Re: Wlan @ bestbuy is cleartext?

SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

Netgear 2 1.68%  
SMC 2 1.68%  
Other 10 8.40%

---

Total 119

WEP Usage By Vendor:

Clear WEP % Using WEP

Addtron 3 0 0.00%  
AMI 2 0 0.00%  
Agere 37 10 21.28%  
Apple 1 2 66.67%  
Cisco 11 9 45.00%  
D-Link 4 0 0.00%  
Linksys 21 5 19.23%  
Netgear 2 0 0.00%  
SMC 1 1 50.00%  
Other 9 1 10.00%

---

Total 91 28 23.53%

APs With Default SSID By Vendor:

Default SSID Other SSID % With Default

Addtron 2 1 66.67%  
AMI 1 1 50.00%  
Agere 1 46 2.13%  
Apple 0 3 0.00%  
Cisco 1 19 5.00%  
D-Link 2 2 50.00%  
Linksys 21 5 80.77%  
Netgear 0 2 0.00%  
SMC 1 1 50.00%  
Other 0 10 0.00%

---

Total 29 90 24.37%

Tracing and tracking these connections is going to be a very difficult matter for those wishing to seek legal restitution for active intrusions, considering the MAC spoofing as well as the ability of long distance, mobile sniffing and attack vectors. Additionally, considering the issue that these intrusions do not need cross traditional wired boundaries, this limits logging to primarily the network that would be compromised in such attacks. Tracing an attacker would require many of the same illegal tools used to apprehend Mitnick in Raleigh in February of 1995, a task that required months of research and work for the FBI and various law enforcement folks across the US during Mitnick's rampage of intrusions of the period. Tsutomu Shimonura working with authorities, relied upon illegal, at least then, devices to triangulate and trace Mitnick's location to the Hotel within the Raleigh area during the manhunt.

Another perspective on information traversing the airwaves comes from an article in the local papers recently here, The Durham herald Sun, Sunday April 14 2002, titled: Nanny-cams make homes vulnerable, reprinted from the New York Times, by John Schwartz. The article relates the current use of X10 and XCam2 devices being heavily marketed on the web as home security and small business solutions. These wireless devices are sniffable in the same fashion as wireless networking devices are, offering the sniffer full video feedback, they incorporate no encryption what-so-ever. The authors talked to Clifford S. Fishman a law professor at the Catholic University of America and an author himself of a leading work on surveillance law, Wiretapping and Eavesdropping. Professor Fishman mentions there are clear laws on such eavesdropping, most current laws deal with the interceptions of sound, not video, and most are geared towards the telephone systems and their signal processing. While I'm certainly not a lawyer, a quick review of current state law here in North Carolina shows most criminal computer laws are also geared more towards wired technology. This suggests that any attempts to prosecute the interception and or interference of wireless technology might well be precedent setting, and certainly difficult to enforce on those passively sniffing traffic from parking lots or roadways as Mr. Clegg's mapping work in this area and the work of others in various parts of the country. Not to mention that the vast majority of computer related intrusions and "interferences" never make it to the attention of those enforcing the laws in existence.

This last fact is partially related to the high damage costs that must be shown to get the legal authorities to take note and action, and partially dues to how few officers handle already high case-loads in computer criminal activity <see Alan Cleggs web pages on dealing with law enforcement referenced below>. Also, many companies do not wish their security intrusions to be aired publically, which often happens when such incidents are reported to legal enforcement authorities, leading to the oft discussed lack of trust of those institutions to deal with such matters in less then corporately embarrassing manner. Then again, as already stated, even when intrusions cross different physical boundaries they are hard enough to trace via wired systems. Few network/systems crackers really make it before the legal system to be dealt with. It's all quite disheartening as one delves into the issues and ramifications, especially when, as is quite often witnessed, these criminals end up rewarded for their illegal actions with jobs and contracts, often from the very firms and organizations they have violated.

VPN tunnels are often suggested to help overcome some of the ills of wired as well as wireless connectivity. And while I agree, I'm going to add a rant that has become common in alot of talks and papers I have been putting forth recently. VPN's work very well, when both systems incorporate secure policies at both ends of the tunnel. We are talking about the 'weakest link in the security chain' issue here. Far to frequently I have recently been observing users tunneling into their company LANS via VPN tunnels without any anti-viri software on the remote system. Additionally I've seem these same systems not closing routes

outside the tunnel to other external resource. These are home and laptop systems running no personal firewall systems, that are connecting directly to the Internet outside the tunnels domain and the protection of the remote LANS security devices and their corporate security polices.

In such situations my route into the corporate LAN, where I an attacker would be via these exposed and unprotected systems. I gain control of the client side of the VPN and then use it's open tunnel to enter the corporate resources. I'd look exactly like the user with permission to do so, and this would likely not attract much attention because that users system, though under my control, is allowed such access. VPN tunnels on laptops and home systems that do not incorporate secure practices and policies on the client systems are basically open backdoors for exploit.

Mr. Ehuan's discussion concluded with a number of strategies to help lock up wireless communications to a degree, and they were all well and good. Many of those are additionally covered in the referenced links for this paper. I'll leave it to the reader to do their research and identify these practices and procedures for themselves. Yet, it must be restated here that since the management packets still traverse the airwaves in clear text, even if encryption is enabled and VPN tunnels are provided for bridging the corporate firewall, and as there are no real boundaries upon those transmissions like we see with wired subnets, there is still a large amount of information leakage with the 802.11b protocol and these toys on the market. This is probably what prompted the following article on Lawrence Livermore National Laboratory's decisiveness on wireless LANs:

SANS NEWSBITES The SANS Weekly Security News Overview Volume 4, Number 6  
February 6, 2002

—31 January 2002 Lawrence Livermore Bans Wireless LANs  
Lawrence Livermore National Laboratory, a national defense technology research lab in California, has banned the use of wireless local area networks (LANs) due to security concerns. A lab spokesman said that Los Alamos National Laboratory might introduce a wireless network ban as well.

<http://cgi.zdnet.com/slink?169109>

Summary:

The whole 802.11b and WEP implementation was a design disaster. Its present implementations are further hindered and a threat to the majority of organizations due to poor vendor responsibility in putting forth safe, secure default installations, well as safe as they can be within its current state of design. Information leakage is possible even with encryption enabled within the deployment configurations via passive sniffing allowing attackers to freely premap targets for exploit. The legal issues of wireless technology might not be fully up to the present state of technology and we may well have precedent setting fallout in the courts due to the exploit of these new toys. Security professionals and

## SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

network/systems admins in North Carolina and the rest of the US have been slow and ineffective in keeping themselves current on the issues wireless technology presents to their job responsibilities. Wireless technology should well make those tasked with securing their environments feel extremely paranoid and may well not be ready for prime time play in the corporate world in it's present state. Those tasked with determining the risks and security issues for their prospective employers need to get current with the issues prior to deploying these new toys in their environments and need to understand how to best attempt to secure these airwave streams as vendors have left them hanging with their default configurations. Certainly these issue will require a tighter integration of the various security departments within organizations to identify those passively sniffing for attack vectors. Presently war-driving and passive sniffing goes unnoticed by grounds security staff, they need to be educated to help identify potential proximal sniffing efforts within their domain.

[0] Orinoco RG-1000 residential gateway is reported in past advisories to ship with WEP enabled; From: Bill Arbaugh <[waa@CS.UMD.EDU](mailto:waa@CS.UMD.EDU)>  
Subject: RG-1000 802.11 Residential Gateway default WEP key disclosure flaw Date: Mon, 2 Apr 2001;

Unfortunately, the default WEP key is set to the default network name, SSID. The SSID appears in several 802.11 management frames in the clear— even when WEP is enabled. Therefore, an attacker with a sniffer capable of capturing management frames can determine the current WEP key which is the last five digits of the network name, (provided the default has not been changed). Armed with the network name, and the current WEP key the attacker can easily gain access to the users wireless LAN. Additionally, the default network name for the unit studied was the last six nibbles of the MAC address converted into ASCII [1]. As a result even if the key were not the network name, an attacker could determine it by sniffing the MAC address of the unit.

To Lucent/Ornioco's credit, the fact that the default encryption key should be changed is strongly encouraged in the manual. However, the fact that the default key is disclosed in the clear as part of the network name is unfortunate. The default encryption key should be changed to a randomly generated value set at the factory.

### References:

Lucent Technologies Inc., Orinoco Residential Gateway Getting Started, February 2001.

## SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

[1] Alan Clegg's story on this highly visible government contractor <we are leaving them nameless here> is interesting. Alan accounted how after sniffing traffic from their parking lot on his way to work, upon arriving at work launched a very intrusive port scan against their systems. This was noticed and their staff sent out the regular "what are your systems doing scanning ours" series of e-mails. Alan then responded something to the effect how it was good their sensors had picked up his intrusive probes, but asked them if they had noted his efforts earlier from their parking lot that morning. There was as Alan described silence on the issue from that point on from this company. Though if I recall it was a heads up to them as <my notes here are sparse> the next day their AP's were WEP enabled. Prior to releasing this information Alan stated he contacted staff at the company in question, perhaps to avoid surprising embarrassment of his release of this information at the local Infragard meeting here, but they never responded nor did it appear attend the meeting.

Thanks:

To Jose Nazario [jose@crimelabs.net](mailto:jose@crimelabs.net) and Chris Connelly [chris@connelly.net](mailto:chris@connelly.net), both of whom are affiliated with crimelab ([www.crimelabs.net](http://www.crimelabs.net)) for previewing this work and offering suggestions and critiques.

References:

Briefings given by Alan Clegg and Art Ehuan at the recent NC Infragard meeting on April 26th.

<http://alan.clegg.com/802/index.html>

<http://alan.clegg.com/LawEnforcement/>

Various postings cited by specific authors to these mailing lists:  
bugtraq, firewalls, firewalls-wizards, pen-tester, vuln-dev, etc...

Wireless 802.11b Security FAQ By Christopher W. Klaus of Internet Security Systems (ISS) Email: [cklaus@iss.net](mailto:cklaus@iss.net) Version 1.1

"[http://www.extremetech.com/print\\_article/0,3428,a=13880,00.asp](http://www.extremetech.com/print_article/0,3428,a=13880,00.asp)">ExtremeTech  
– Print Article WEP insecurities

"[http://www.iss.net/wireless/WLAN\\_FAQ.php#\[4.2\]](http://www.iss.net/wireless/WLAN_FAQ.php#[4.2]) 802.11  
Security Analysis Tools">Internet Security Systems, Inc. Wireless FAQ

"<http://www.cigital.com/news/wireless/faq.html>">Wireless  
Vulnerability Press Kit: FAQ [Cigital]

<http://www.iss.net/wireless>

<http://www.research.ibm.com/gsal/wsa/>

Re: Wlan @ bestbuy is cleartext?

SecurityFocus Vuln-Dev: Re: Wlan @ bestbuy is cleartext?

<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

<http://www.cisco.com/warp/public/784/packet/jul01/p74-cover.html>

[http://www.wi2600.org/mediawhore/nf0/wireless/ssid\\_defaults/ssid\\_defaults-1.0.5.txt](http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/ssid_defaults-1.0.5.txt)

<http://securingwireless.intranets.com>

<http://www.hackinthebox.org/>

<http://www.cigitalabs.com/resources/papers/download/arppoisson.pdf>

<http://www.dis.org/filez/>

~~~~~  
"Cutting the space budget really restores my faith in humanity. It eliminates dreams, goals, and ideals and lets us get straight to the business of hate, debauchery, and self-annihilation." -- Johnny Hart

\*\*\*testing, only testing, and damn good at it too!\*\*\*

OK, so you're a Ph.D. Just don't touch anything.

- 
- TEXT/PLAIN attachment: [wireless-woes](#)
- 

- *Previous message:* [Michael Cunningham: "Re: Wlan @ bestbuy is cleartext?"](#)
- *In reply to:* (deleted message) [Erik Parker: "Re: Wlan @ bestbuy is cleartext?"](#)
- *Next in thread:* [Jonathan Bloomquist: "Re: Wlan @ bestbuy is cleartext?"](#)
- *Next in thread:* [Ron DuFresne: "Re: Wlan @ bestbuy is cleartext?"](#)
- *Reply:* [Jonathan Bloomquist: "Re: Wlan @ bestbuy is cleartext?"](#)
- *Messages sorted by:* [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)