

# Implications of 802.11 WEP (in)Security

Peter H. Baumann  
CS 574 – Mondays  
May 5, 2003

Word Count: 3950

# Implications of 802.11 WEP (in)Security

## Introduction

When we have something that's important to us, we want to protect it. If someone else wants it badly enough, they will find a way to get it, or at least try. And so it goes in the world of information as well.

As information gains more and more tangible value, more and more parties will be willing to expend effort to get it. This is further compounded by the fact that data is also more easily accessible (via the Internet), and that the retrieval of that data can now be highly automated. So, we have lots of valuable information, available from one convenient access point, and it can be harvested automatically. All of this translates to risk. This risk is then further magnified by the allure of wireless connectivity. Wireless connectivity means that access to data no longer requires a physical connection. It can literally be grabbed right from thin air. The implications are staggering.

Regardless, the future of data connectivity is wireless. Breaking the bonds of physical wires is too compelling to ignore. According to a recent study performed by NOP World-Technology<sub>[10]</sub>, through the combination of cost savings and increased productivity, an organization can realize an annual ROI of \$4550 per employee through the usage of Wireless LAN (WLAN).

## Implications of 802.11 WEP (in)Security

Cell phones, Wireless LANs, it's here, the revolution has begun. What final form all of this connectivity is going to take; G3, CDMA, 802.11b (Wi-Fi)<sup>1</sup>, 802.11a (Wi-Fi5)<sup>1</sup>, or 802.11g, or some as yet undeclared technology, has yet to be determined. What is clear at this moment, is that for data connectivity, the 802.11 family, with more than 11.6 million units sold in 2002<sub>[4]</sub>, is very well entrenched and is the current king of the hill.

This is an exciting time with an immense array of possibilities. But, before we pop the champagne to celebrate our new found capabilities, it would seem that this silver cloud has a dark lining... for 802.11b (and its siblings 802.11a and 802.11g, for that matter), that dark lining is WEP (Wireless Equivalent Privacy). While there are many technical components surrounding this issue, this paper, while acknowledging those components, will attempt to address some of the more practical, and perhaps, philosophical aspects.

### What is WEP?

WEP is that part of the IEEE 802.11 Standard that addresses security. It was designed to provide a wireless LAN with a level of security comparable to that of a wired LAN, specifically, to provide for data integrity and data confidentiality.

WEP provides for data integrity through the use of an Integrity Check Vector (ICV). This ICV is dependent upon a 32-bit cyclical redundancy check (CRC-32). Data confidentiality is provided through the use of encryption. The encryption is reliant upon the RSA RC4 algorithm. The encryption can use either a 40-bit key or a 128-bit key,

---

<sup>1</sup> Trademark name given by Wireless Ethernet Compatibility Alliance (WECA) in 1999.[1]

## Implications of 802.11 WEP (in)Security

along with a 24-bit Initialization Vector (IV). The function of the IV is to randomize a part of the key in order to expand the key space.

The following steps are taken during the WLAN transmission phase:

1. Plaintext message is processed through the CRC-32 and an ICV is generated.
2. The ICV is appended to the plaintext message.
3. An IV is generated and combined with a symmetric key (shared by the participants on the WLAN), resulting in the key stream that will be used to perform encryption.
4. The entire frame of data (plaintext and ICV) is then encrypted using the generated key stream.
5. The encrypted data frame and the IV are then transmitted over the WLAN (it is important to note that the IV is sent as plaintext).

The receiving partner then performs essentially the same operations, but in reverse:

1. The IV received in the transmission is used in combination with the symmetric key to generate the appropriate key stream.
2. Using this key stream, the data frame is decrypted, yielding the transmitted plaintext message and ICV.
3. The plaintext message is then processed through the CRC-32 and the resulting ICV is compared with the ICV that was sent in the transmission. Matching ICVs indicates that the message integrity was maintained.

WEP was designed to provide the equivalent level of security as you would expect from a wired LAN<sub>[02]</sub>. Not a complete security solution, but a basic foundation. According to the IEEE 802.11 Standard<sub>[7]</sub>,

*IEEE 802.11 provides link-level authentication between IEEE 802.11 STAs. IEEE 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication.*

# Implications of 802.11 WEP (in)Security

*IEEE 802.11 authentication is used simply to bring the wireless link up to the assumed physical standards of a wired link. (This use of authentication is independent of any authentication process that may be used in higher levels of a network protocol stack.)*

It further states,

*IEEE 802.11 specifies an optional privacy algorithm, WEP, that is designed to satisfy the goal of wired LAN “equivalent” privacy. The algorithm is not designed for ultimate security but rather to be “at least as secure as a wire.”*

It turns out, however, that since its release in 1999, WEP has proven to be, in the words of Jim Gemmel, “a security nightmare, pure swiss cheese”<sup>2</sup>.

## How could this happen?

While one can speculate on the motives and short comings of the IEEE Task Group that formulated the 802.11 Standard (and WEP specifically), one thing is certain, they failed, in design, to recognize the significance of a well implemented security mechanism. At a minimum, it would appear that there was a failure to perform adequate crypto-analysis on the recommended security implementation. But, according to one source “*the 802.11 committee was aware of some WEP limitations; however, WEP was the best choice to ensure efficient implementations worldwide.*” [5].

In this excerpt from Section 8.2.2 of the IEEE 802.11 Standard<sub>[7]</sub>, the committee explains some of the required properties of WEP.

*— It is reasonably strong: The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key (k) and frequent changing of the IV.*

*— It may be exportable: Every effort has been made to design the WEP system operation so as to maximize the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the USA.*

---

<sup>2</sup> Jim Gemmel is a senior signals analyst at CACI International, Inc in Arlington, VA. Jim is involved with researching wireless networking technologies for federal government agencies, including the DoD.[3]

## Implications of 802.11 WEP (in)Security

The Standard uses careful language when describing the strength of the algorithm as being “reasonably strong”. But since there have been no claims made against the RC4 algorithm itself, that criteria seems to have been met.

The 802.11 Task Group also refers to the 40 bit encryption export limitations enforced by the US government (since relaxed), over which it had no control. While the 40 bit key limitation may have left WEP vulnerable to a brute force attack, a 128 bit version was also made available by many vendors, alleviating some of that threat. So it would seem that WEP satisfied that criteria as well.

If WEP satisfied the specified requirements, what happened? For one, a flawed assumption, that sending the IV in the clear would not prove beneficial to a would-be-hacker, was accepted.

*The IV is transmitted in the clear since it does not provide an attacker with any information about the secret key, and since its value must be known by the recipient in order to perform the decryption. (Sect. 8.2.3)<sup>[7]</sup>*

Secondly, the Initialization Vector mechanism, used to “randomize” the shared key, was weak. It utilized a relatively short length (24 bits) that resulted in IV reuse fairly quickly. This reuse problem becomes even more pronounced as more people participate in the network. This, as a demonstrated effect of the “Birthday Paradox”, results in IV reuse after only 12,430 frames of data being transmitted (or approx. 11 minutes)<sup>[6]</sup>. Interestingly, the 802.11 committee does address the issue of IV reuse, however, not in sufficient depth with respect to the recommended implementation.

## Implications of 802.11 WEP (in)Security

*When such information is transmitted while encrypting with a particular key and IV, an eavesdropper can readily determine portions of the key sequence generated by that (key, IV) pair. If the same (key, IV) pair is used for successive MPDUs, this effect may substantially reduce the degree of privacy conferred by the WEP algorithm, allowing an eavesdropper to recover a subset of the user data without any knowledge of the secret key. Changing the IV after each MPDU is a simple method of preserving the effectiveness of WEP in this situation.[7]*

The implication of all of this is that an attacker could conceivably collect two encrypted packets with the same IV and start deciphering the plaintext in as little time as 11 minutes. This combination of flaws proved to be the key pieces of the passive and active eavesdropping attacks<sup>[6]</sup>.

WEP's third flaw is the weakness in its integrity checking mechanism. The integrity checking is based on CRC-32, which is a linear function. The implication of this is that a hacker could alter a WEP encrypted message in a predictable manner while appearing to maintain the transmission's integrity. This would allow the hacker to alter messages undetected.

### Who does this Impact?

In a word, everybody. Even if you do not own a wireless network, or work for a company that owns one, data about you could be at risk at a company that does. Worse yet, companies that control your data may have wireless networks that they are not even aware of. Why is that important? Because if an unauthorized wireless access point (rogue access point) has been installed, it's highly likely that the proper security was not established. That, in turn, could lead to unauthorized access to that company's internal network; the very network where your data potentially resides.

## Implications of 802.11 WEP (in)Security

At this point in the discussion it would be practical to characterize the networking audience into 3 broad categories:

1. Large organizations (i.e. government, military, corporate). Networks that:
  - a. Serve internal users.
  - b. Have IT resources/budgets.
  - c. Can control and support client configurations.
  - d. Have a greater need for security.
2. Small organizations (i.e. home, SOHO, small businesses). Networks that:
  - a. Serve internal users.
  - b. Have little or no IT resources/budgets.
  - c. Can control and support client configurations.
  - d. Have a lesser need for security.
3. Public network providers (i.e. hotels, airports, coffeeshops). Networks that:
  - a. Serve external users (tens of 1000's, random).
  - b. Have varying/dispersed IT resources/budgets.
  - c. Cannot control nor support client configurations (economically unfeasible).
  - d. Have minimal need for security.

A relatively new area of risk that has presented itself in the past 3 years is the growing number of public network providers that are appearing in coffeeshops, airports, hotels, etc. According to a report by Analysys<sub>[12]</sub>, the number of these “hot spots” is expected to

## Implications of 802.11 WEP (in)Security

grow from 3,700 in 2002 to 41,000 in 2007. Additionally, there are public network infrastructures that are being deployed by government groups; for example in New York City's Bryan Park neighborhood, and in the Soho district of London<sub>[11]</sub>. Even McDonalds and Borders Book & Music are getting into the wireless access point business<sub>[8]</sub>.

If McDonalds or Starbucks (T-Mobile) has to decide where the market potential lies, do they play to the lowest common denominator and accept the notion of no security; a) because most people don't understand how to set it up, b) because it's based on a shared pass phrase, which makes no sense because everyone has to know it... or do they risk losing business because they "force" their customer to either buy new equipment or upgrade their existing equipment. The easiest answer, of course, is no security. But being the litigious society that we are, T-Mobile then has to protect itself by presenting an array of disclaimers<sub>[9]</sub> warning customers of the lack of security on their network, and that they are not liable for any issues resulting from its use.

### What are the Risks?

From a practical standpoint, there is one issue to deal with; the lack of a basic security foundation for transmissions within a wireless network. This lack of security leads to four fundamental risks:

1. Exposure of the transmissions themselves (i.e. your data).
2. Exposure of the wireless network itself (i.e. access to use the resource).

## Implications of 802.11 WEP (in)Security

3. Exposure of the resources connected to the wireless network (i.e. other PCs **and** the data that reside on them).
4. Exposure of the extended resources attached to the wireless network (i.e. corporate LAN/WAN **and** the data **and** services that reside within).

### What are the Vulnerabilities?

There are an array of vulnerabilities that present themselves as a result of WLAN usage:

1. A not so obvious vulnerability is that most WLAN products come delivered without any security enabled. This is done to make the installation a simple and straight-forward process (read, *saves on technical support costs*). Open the box and plug it in. What this does, however, is leave the uninformed user completely open to the world. Worse yet, the Wireless Access Point is broadcasting its existence!
2. Another not so obvious vulnerability is the fact that these wireless systems, while advertising an effective range of 300ft, can actually broadcast up to 2000 feet<sub>[3]</sub>. What this translates to is that someone with a sensitive enough antenna could actually gain access to your wireless network from a quarter mile away or more.
3. On the more obvious side, there are a number of well documented attacks that can be performed successfully against WLANs. Some of the attacks include<sub>[6]</sub>:
  - Traffic Analysis
  - Passive Eavesdropping
  - Active Eavesdropping with Partially Known Plaintext
  - Active Eavesdropping with Known Plaintext

## Implications of 802.11 WEP (in)Security

- Unauthorized Access
  - Man-in-the-Middle
  - Session Hijacking
  - Replay
4. And, of course, just to keep things interesting, there are a variety of tools available on the Internet that can make WLAN hacking fun and easy for the whole family! OK, perhaps not easy, but certainly more viable. Among the more common ones are; WEBCrack, Airmagnet (actually a network management tool, but useful for a hacker), NetStumbler (also a network management tool), Kismet and AirSnort.
5. And last, but certainly not least, is that this is all still too complicated. So much so that a survey conducted by Information Security<sup>3</sup> magazine found that 74% of 1200 responding IT and security professionals said they were concerned about corporate WLAN security, and that only 24% said they felt ‘very knowledgeable’ about the topic. So, if that is the consensus of IT professionals, where does that leave the rest of us?

### What can We Do?

Should you still use WEP? Absolutely. Any security is better than none. Also, there’s another aspect to this that worth noting, and that is establishing the intent to protect the network and creating a clear boundary. Without WEP, or some other security feature, an attacker can claim that they “stumbled” upon your network unintentionally. With WEP

---

<sup>3</sup> Survey results published in Information Security magazine, January 2002<sub>[13]</sub>

## Implications of 802.11 WEP (in)Security

enabled, however, any attacker would have to intentionally apply effort, regardless of how little, to gain access, thereby discrediting any claim of “unintentional” access. In this respect, WEP serves much the same purpose as a “No Trespassing” sign<sup>[14]</sup>.

For enhanced security, Wi-Fi Alliance has recommend the following ten steps to secure your existing Wi-Fi networks<sup>[15]</sup>:

1. Apply port access-control technology 802.1x to protect WLANs from unauthorized access.
2. Use 128-bit WEP encryption; change the default WEP encryption key that comes with the access point provided by the vendor.
3. Use gateway-protected IPsec VPNs for highly confidential WLAN communications.
4. Change the default vendor-set SSID for access points and for WLAN terminals; use MAC address binding at least for those terminals that don't need to roam across multiple access points.
5. Do not enable access points to broadcast their SSIDs.
6. Change the default access-point administration password.
7. Forbid employees from installing access points themselves. This can be accomplished by periodic scanning of access points through a notebook with a WLAN network card and WLAN scanning software.

## Implications of 802.11 WEP (in)Security

8. Choose WLAN network cards that support password-protection of attribute changes to prevent the settings of the network cards from being illegally or accidentally changed by users.
9. Develop WLAN management policies; internal employees should not be allowed to leak WLAN configuration information to outsiders or to construct an ad hoc network topology with a P2P configuration.
10. Deploy real-time, content-level security measures (such as antivirus firewalls) in conjunction with each WLAN access point to eliminate harmful viruses and worms before they enter or exit the WLAN.

If you're looking for a more in-depth explanation, in *A Survey of 802.11a Wireless Security Threats and Security Mechanisms*<sub>[6]</sub>, Colonel Donald J. Welch, Ph.D. sets out to answer the question of how to overcome the deficiencies in WEP and configure a "secure" wireless network from a military perspective. What he discusses, however, is equally applicable to the large organization category described above. What is researched and discussed in technical detail are WEP's various weaknesses, documented attacks against those weaknesses, a comparison and contrasting of alternative solutions, and finally the study's recommended implementations. For organizations with sufficient resources and the requisite need for security, the study provides viable solutions to address the specific shortfalls of WEP.

## **Implications of 802.11 WEP (in)Security**

For small organizations and public network providers, the solutions recommended in *A Survey of 802.11a Wireless Security Threats and Security Mechanisms* may not be viable from an economic or practical perspective. For the most part, small organizations do not have the expertise and resources to implement the recommended solutions, nor would their security needs warrant that effort and expense.

As for the public network provider, the complexities of managing tens of 1000's of random customers and distributing/requiring certificates, etc. would be prohibitively expensive. This level of management and associated expense would, more than likely, displace their business model, as well as, place additional burdens on their end users. These end users may very likely lose interest, having exceeded their "threshold of pain" vs. the convenience enjoyed.

### **What is the Industry Doing?**

Since the discovery of the WEP problems, several solutions have been offered; many vendor specific solutions, which present interoperability issues, as well as, many "standards" based solutions. In either case, some reconfiguration of the access point and the clients is required.

The two "standards" based solutions are WPA, being developed by the WiFi Alliance, and 802.11i, being developed by the IEEE and slated for release later this year. The good news is that these solutions are compatible with each other. The not so good news is that, according to some sources, they are still susceptible to session high-jacking and man-in-

## Implications of 802.11 WEP (in)Security

the-middle attacks<sub>[6]</sub>. Additionally, these solutions may require digital certificates as part of their implementation. This raises the complexity of deployment and management.

These solutions attempt to solve the security problem, but they all require action to be taken by the network owner and the end user. Additionally, the application of any remedy needs to be coordinated. In other words, you cannot have some clients with WEP and some clients with WPA. All the participants on the same network must use the same protocols. The caveat to this is that if a single device on a WPA network cannot utilize WPA, the entire network will “fall back” to using WEP<sub>[16]</sub>.

For large organizations, this coordinated effort would be an expensive and time consuming endeavor, but is doable. For smaller organizations, it is more easily managed, but the associated costs need to be weighed, but also doable. For the public network provider, however, this is challenging, if not impossible. To coordinate the transition of all the “paying” customers in sync, without any end user technical support (too cost prohibitive), and a myriad of end user products to support (deferred to product manufacturer?), would be monumental. Granted, I don’t understand mass market dynamics and psychology, but it doesn’t sound too feasible to me.

The one advantage that exists with separate, independent networks is that the owner of each network can decide whether, and how to proceed with dealing with these security issues, based on their own needs, resources and level of risk tolerance.

## Implications of 802.11 WEP (in)Security

As with any security decision, one has to ask the question, “do the risks warrant the associated costs for a desired level of security?”. Alternatively, one could also ask, “is the associated risk and/or cost justified by the access gains afforded by the deployment of a WLAN?”. That very question has led several government agencies to abandon the deployment of Wi-Fi LANs<sup>[3]</sup> all together.

### Conclusion

One can certainly ponder the how’s and why’s of the decisions made in the design and development of WEP, but the fact remains, this is where we are. As is usually the case, hindsight is 20/20 and looking back, I’m certain that, the IEEE would have made different decisions regarding WEP and its implementation. You could argue that the 802.11 Task Group did not have the foresight to envision all these specific application troubles. True, after all, if they did, they would all be millionaires. However, the need for valid security is, and was well known, even in 1997.

What is the net result of the design flaw of WEP security? The following come to mind:

1. The manufacture, sale and installation of “insecure” products.
2. End users with a false sense of security (or no security).
3. A myriad of incompatible, “after thought” solutions.
4. Forced upgrades (if you want the new security upgrades and your environment can support the migration effort).

## Implications of 802.11 WEP (in)Security

The current state of basic wireless network security looks somewhat feeble at best. Fortunately, things are going to improve, incrementally, and only if the market adopts the changes. For the large and small organizations that manage “private” wireless networks, the outlook is pretty good in the sense that a move to products with improved security is manageable. For public wireless networks, the fixes will be much more challenging. If their user base has enough interest and motivation, they may accept the costs of whatever change is eventually prescribed by the public network providers. However, one can only hope that they, the public network providers, will also coordinate their efforts when the time comes, as to avoid any further confusion and inconvenience.

In the technology fields, products and technologies are constantly being replaced. The industry has demonstrated that time and time again. The inherent danger in this pattern is that at some point the innovation cycle plateaus. When that happens, we get “stuck” with the limitations defined at that plateau. This is especially dangerous when the plateau occurs at an infrastructure level.

When do we reach a plateau? When critical mass is reached and customers are no longer willing to spend on new capabilities? Or perhaps when it is not economically feasible to supplant an existing infrastructure? In the latter case, only a truly disruptive technology (i.e. cell phones vs. land line telcos) can restart the cycle. And even then, success is dependent upon customer adoption rates.

## Implications of 802.11 WEP (in)Security

Have we plateau'd with 802.11... perhaps not in capacity, but as an infrastructure? Will we be able to "fix" the security flaws in the system in an adaptive manner? Are we going to have to deal with the lack of adequate, base line security? Or are we going to have to go through a disruptive overhaul (i.e. redefine the infrastructure and replace all existing products)? As always, the question comes back to motivation and cost. The market will ultimately decide. In the mean time, we, meaning all users of 802.11, are stuck dealing with a weak security infrastructure... each to fend for ourselves.

# Implications of 802.11 WEP (in)Security

## Bibliography

1. **Michael J. Riezenman**  
*The ABCs of IEEE 802.11*  
IEEE Spectrum Online  
<http://www.spectrum.ieee.org/WEBONLY/resource/sep02/802ABCs.html>
2. *Wire Equivalent Privacy*  
searchSecurity.com Definitions, Mar 2002  
[http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci549087,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html)
3. **Gerry Blackwell**  
*Serious WLAN Security Threats: Part I*  
802.11 Planet.com, Jan 2002  
<http://www.80211-planet.com/columns/article.php/949891>
4. **Robert Hoskins**  
*Attractive Cost of 802.11b Drove Wi-Fi Shipments in 2002*  
Broadcast Wireless Exchange Press Center, 2001  
<http://www.bbwxchange.com/news/2003/feb/instat021003.asp>
5. **Jim Grier**  
*802.11 WEP: Concepts and Vulnerability*  
802.11 Planet.com, June 2002  
<http://www.80211-planet.com/tutorials/article.php/1368661>
6. **Colonel Donald J. Welch, Ph.D., Major Scott D. Lathrop**  
*A Survey of 802.11a Wireless Security Threats and Security Mechanisms*  
United States Military Academy, 2003  
[http://216.239.33.100/search?q=cache:flijAtXxLbkC:www.itoc.usma.edu/Documents/ITOC\\_TR-2003-101\\_\(G6\).pdf+802.11a+security&hl=en&ie=UTF-8](http://216.239.33.100/search?q=cache:flijAtXxLbkC:www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf+802.11a+security&hl=en&ie=UTF-8)
7. *ANSI/IEEE Std 802.11, 1999 Edition*  
IEEE, 1999  
<http://grouper.ieee.org/groups/802/11/index.html>
8. **Carmen Nobel**  
*McDonald's Adds WLAN Access to Its Menu*  
Godlike Productions, March 2003  
<http://www.godlikeproductions.com/news/item.php?keyid=2794>

## Implications of 802.11 WEP (in)Security

9. **High Speed Wireless Internet Access Now Being Served Starbucks Coffee/TMobile brochure.**
10. **Chris Kozup**  
*Welcome to the Wireless Enterprise*  
Packet, Cisco Systems User Magazine, Q2, 2002  
<http://www.cisco.com/warp/public/784/packet/apr02/pdfs/p32-cover.pdf>
11. **Tony Smith**  
*London's Soho to get blanket 802.11 cover for voice, data*  
The Register, April 2003  
<http://www.theregister.co.uk/content/59/30404.html>
12. **Michael Pastore**  
*Big Years Ahead for WLAN Market*  
Markets Wireless, February 2002  
[http://cyberatlas.internet.com/markets/wireless/article/0,1323,10094\\_974711,00.html](http://cyberatlas.internet.com/markets/wireless/article/0,1323,10094_974711,00.html)
13. **Mathew Peretz**  
*WLAN Security Survey Shows Skills Deficit*  
802.11 Planet.com, Jan 2002  
<http://www.80211-planet.com/news/article.php/951211>
14. **Dr. Paul Goransson**  
*802.11... A Standard for the Present and Future*  
Meetinghouse Data Communications  
[http://www.mtghouse.com/MDC\\_8021X\\_White\\_Paper.pdf](http://www.mtghouse.com/MDC_8021X_White_Paper.pdf)
15. **James Liu**  
*How to build a secure WLAN*  
ComputerWorld, February 2003  
[http://www.idg.net/english/crd\\_wlan\\_1145467.html](http://www.idg.net/english/crd_wlan_1145467.html)
16. **Glennf**  
*Weak Defense, But Getting Better*  
WiFi Networking News, July 2001  
<http://wifinetnews.com/archives/001034.html>