

Horizon Newsletter

Wireless Security



Using wireless connections can be convenient but can also easily lead to security breaches. You must make sure you have implemented encryption correctly to help protect against unauthorized access. When wireless technology first appeared, WEP was the standard for encryption. It has since been discovered that WEP is not adequate and all wireless devices should be switched to WPA encryption for better protection.

Wired Equivalent Privacy (WEP)

Originally intended to give you the same or similar level of security as a wired network.

WEP works by using secret keys or codes to encrypt data. The Access Point (AP) and the client must know the codes in order to get a wireless connection. WEP uses either 64 or 128 bit keys. The actual user keys are 40 and 104 bits, with the extra 24 bits used for Initialization Vector (IV).

Data is transmitted using packets, i.e. small chunks of data. The encryption is created by taking the IV and randomizing it for each packet, while keeping the secret code the same. The Access Point and the client decrypt and retrieve the data.

Problems

There is no limit on using the same IV value more than once.

This makes the encryption vulnerable to collision-based attacks.

Because the IV is only 24 bits, there are only ~16.7 million possible variations. Seems like a lot, but it's quite small in the cryptography world.

Master keys are used directly, when they should instead be used to generate other temporary keys.

Users don't change their keys very often on most networks, giving attackers ample time to try various techniques.

Wifi Protected Access (WPA)

It bridges the gap between WEP and the upcoming WPA2 802.11i standard. It is implemented via firmware upgrades in older hardware. WPA uses Temporal Key Integrity Protocol (TKIP), which is designed to allow WEP to be upgraded through corrective measures that address the existing security problems.

WPA Advantages

IV length has increased to 48 bits from 24 bits, which allows WPA to achieve over 500 trillion possible key combinations.

IVs are better protected through the use of the TKIP sequence counter, helping to prevent the re-use of IV keys.

Master keys are never directly used.

Better key management

Impressive message integrity checking

Future WPA2 (802.11i)

WPA2 features upgrades to WPA to make it even more secure.

WPA2 uses Advanced Encryption Standard (AES) to provide stronger encryption.

There are specific solutions for Enterprise and Personal use versions. Enterprise uses IEEE 802.1X and EAP to provide authentication. Personal uses a pre-shared key, or password.

WPA2 creates new session keys for every association.

WPA2 Advantages

The keys used for each client on the network are unique and specific to that client. Every packet sent over the air is encrypted with a unique key and avoids re-use.

If you are using wireless technology we suggest checking with us to ensure you are using the latest encryption technology.

Inside this issue:

- Wireless Security 1
- Spam Control 2
- Digital Signage 3
- Dear Tech Support 4



Printed on the
Xerox 7400

Recycle Info

Getting rid of old equipment is becoming a more difficult task. We strongly recommend recycling your old equipment to help our earth's ecology. Here are some sites that will take old equipment and in some cases pay you for it.

www.Buy.Com

Earth911.org

www.freecycle.org

craigslist.org

Dell, HP, Gateway and Sony all have recycle programs.

Other sources are to check with your schools, churches and charitable organizations.



Free Wireless Internet Access

Free wireless access points, available at the airport or coffee shops, can result in the likelihood of someone examining your packets of data.

Examining packets, i.e sniffing traffic, is an exercise in simplicity. Anyone can download the sniffing software off the Internet, turn it on, configure it to see everything that goes by, and then save it in a file or look at it in real time. It would be possible for anyone within signal strength range to see everything you do on the Internet. Signal strength might be strong enough to carry as far as a city block.

By capturing and reconstructing packet data, user/password pairs, credit card numbers, or other financial data and non-encrypted email can be read. If email is encrypted with something like ROT13, which in most cases email is not encrypted, it can be read anyway.

The bottom line, when using free wireless access points, do not access anything where you provide a login or password unless you are confident you are using an encrypted connection such as SSH or VPN technology.

Sniffing is not restricted to wireless networks. It can also be used for wired networks. Just using a firewall doesn't protect your data after it leaves the machine.

A Virtual Private Network (VPN) is probably the best answer to ensure secure communications. A VPN works by building an encrypted tunnel to your external network and then forwards all your traffic from there, as if it were originating on your trusted network. The path from the VPN to your mail or web server is on a trusted path and not likely to be sniffed.

Spam Control

Spam has continued to grow at an alarming rate and no decrease is expected in the near future. It is estimated that over 95% of all email is spam. Why does it continue to grow? Because people make money doing it, lots of money. It is alleged that organized crime is now behind a good deal of the spam you receive. Who would have guessed?

How can you protect yourself against spam? There is no 100% method, but we have found three applications that can assist in detecting spam.

The first two, *Spamassassin* and *Mailwasher*, are filtering techniques. They have formulas that are applied to each email. For each indication that an email may be spam, points are assigned and accumulated. When enough points are reached, the email is flagged as spam. These applications have been found to reduce spam from 80 to 90%.

Both of these applications require continued training. If you receive an email that you know is spam and was not flagged as spam, you must move it to a special spam folder. The application uses this special folder to improve the detection of spam.

The one downside is that occasionally email that is not spam will get flagged as spam. Because of this you still have to review flagged spam email and move any email that is not spam to a special non-spam folder. This is then used by the application for training on what is not spam.

The third method is a challenge/response method. This method does not allow any email from a given address until 1) they are already on your whitelist of acceptable email addresses or domains. 2) The sender replies one time to a special email they automatically receive from you.

If you want to reduce the amount of spam you are receiving, please call us so we can discuss and determine which is the best solution for your organization.

Phishing

Phishing is a very popular spam technique where the email appears to be from a legitimate source and requests that you validate your account information. If you click on the link supplied in the email you will probably end up on a web page that appears to be real, i.e. Chase Bank, eBay, Paypal, etc.

If you supply your account, login or password information you have just provided it to a crook who will use it to take money from your account.

No real organization will ever send you email requesting you update your account information. To avoid getting exploited by phishing, never click on any email link that is asking for personal information.

Digital Signage

Last year Digital Signage really took off. It is expected to at least double this year, if not more.

What is Digital Signage? It is **the ability to display what you want, where you want, any-time you want.**

By using large screen displays with a player attached to each screen you can control the content that appears on the screen over standard network connections, even over the Internet. The content can be still images, or movies or even sound. You can even display the latest news, sports and financial information.

What is the benefit?

The content can easily be changed and as often as you like. No need for expensive printed material plus the labor cost of changing the printed material.

The display can have more of an impact on the viewer than printed material. More information can be displayed vs. printed material.

Advertisements can periodically display that produce revenue and help offset the cost.

You may think that you don't have a need for digital signage within your own organization. But you may want to consider providing media content to your customers for assistance in marketing your products using digital signage.

We are offering a veritable smorgasbord of software, support, and services to craft the digital signage system that's right for your goals and objectives.

How involved we are, and at what stages, is completely up to you.

Our goal is simple: **To enable you to communicate effectively with your customers and other audiences, maximizing the impact of your marketing, entertainment and educational messages.**

Need more information?

If you want to learn more about Digital Signage, visit our web page: www.ahinc.com/digitalsignage.html. You can also request a CD that provides more information.



Don't turn your computer off!

It was determined several years ago that hotels and hospitals had the lowest failure rate of equipment. This is due to the fact that they operate 24 hours and never turn their equipment off.

The surge of power actually when turning on equipment is stressful to the electronics. In addition the cooling and heating that occurs when turning equipment on and off also produces extra wear and tear.

Log on/off daily

Even though we recommend **not** turning your equipment off, we **do recommend** that you log off at the end of day.

During the day, as you open and close applications, memory may not always be released correctly and some processes still may be running that are not necessary.

Logging off frees up the memory and can clear the unused processes.

Advanced Horizons, Inc

323 Ferndale Avenue
Elmhurst, IL 60126

Phone: 630.941.9332
Fax: 630.941.9338
E-mail:Info@AHinc.com

©2007 by Advanced Horizons, Inc.
All Rights Reserved

On the Web

www.AdvancedHorizons.net

www.EZforYou.com

Dear Tech support:

I upgraded from Girlfriend7.0 to Wife1.0. I soon noticed that the new program began unexpected child processing that took up a lot of space and valuable resources. In addition, Wife1.0 installed itself into all other programs and now monitors all other system activity. Applications such as PokerNight10.3, Football5.0, Hockey7.5 & Male Bonding3.6 no longer run. I can't seem to keep Wife1.0 in the background while attempting to run my favorite applications. I'm thinking about going back to Girlfriend7.0, but the uninstall doesn't work on Wife1.0. Please help!

A Troubled User

Dear Troubled User:

This is a very common problem that men complain about. Many people upgrade from Girlfriend7.0 to Wife1.0, thinking that it is just a Utilities and Entertainment program. Wife1.0 is an OPERATING SYSTEM and is designed to run EVERYTHING! It is also impossible to delete Wife1.0 and to return to Girlfriend7.0. It is impossible to uninstall, or purge the program files from the system once installed. You cannot go back to Girlfriend7.0 because Wife1.0 is designed to not allow this. I recommend that you keep Wife1.0 and work on improving the situation. I suggest installing the background application "Yes Dear" to alleviate software augmentation. The best course of action is to enter the command C:\APOLOGIZE because ultimately you will have to give the APOLOGIZE command before the system will return to normal anyway. Wife1.0 is a great program, but it tends to be very high maintenance. Wife1.0 comes with several support programs, such as Clean&Sweep3.0 , CookIt!1.5 & DoBills4.2 . However, be very careful how you use these programs. Improper use will cause the system to launch the program NagNag9.5. Once this happens, the only way to improve the performance of Wife1.0 is to purchase additional software. I recommend Flowers2.1 and Diamonds5.0!

WARNING! DO NOT, under any circumstances, install SecretaryWithShortSkirt3.3. This application is not supported by Wife1.0 and will cause irreversible damage to the operating system.

Best of luck, Tech Support