AirStation One-Touch Secure System (AOSS™)

A Description of WLAN Security Challenges and Potential Solutions

Buffalo Technology (USA), Inc.
October 2004

Summary – The Wireless Security Problem

With the recent proliferation of wireless technology within public and private networks, there is an increasing need for better wireless security methods and standards. To address this need, organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the Wi-Fi Alliance have created new standards like WPA and PSK/AES that offer vast improvements over the inferior WEP standard. However, despite the risks, most end users still do not implement these robust methods of securing their wireless transmissions.

The apparent reason end users fail to commit to the proper use of wireless security is the perceived difficulty in setting-up and maintaining that security. Users can be intimidated by having to enter complex security keys that typically consist of long strings of meaningless characters into multiple devices often from various hardware vendors with differing user interfaces. Essentially, to setup security on even a small wireless network, end users are expected to reference multiple support resources.

The AirStation One-Touch Secure System (AOSS) by Buffalo Technology was developed to address this problem by eliminating the complexity at the end user level and providing a hassle-free way to setup and maintain rigid security features.

The AOSS User Experience

The initial setup of an AOSS secured network is literally completed in two steps. Once the Access Point (AP) is powered up and the wireless client adapter is installed with the AOSS-enabled client management utility, AOSS is ready to begin. First, the user clicks the AOSS button either in the client utility, or in some cases, on the client device itself. Then the user presses the AOSS button on the AP. Alternatively, the AOSS button on the AP can be pressed before the AOSS button in the client utility or on the client device. Within a minute, both devices will indicate AOSS has successfully completed security installation via a displayed message or with the illumination of an AOSS LED on the device.

At this point, the highest available level of encryption supported between the AP and wireless client adapter will be established. For example, if both devices support WPA AES security protocols, then that is the level of security that will be automatically configured. However, if the AP only supported 128-bit and 64-bit WEP, AOSS would select 128-bit WEP as the encryption method. In any scenario, AOSS will select the best encryption method that is mutually supported between all AOSS-enabled wireless devices on the network.

Should an additional wireless client adapter be introduced into the network, the original installation process is simply repeated. Simply initiate AOSS on the client device and then press the AOSS button on the AP, and within a minute, encryption and security will be established.

While the end user experience with AOSS is extremely simple, the processes in the background are quite complex. AOSS was designed to not only to simplify the creation and

management of secure wireless networks, but also to preserve the integrity of wireless encryption by not introducing potential security breaches. When creating and exchanging security encryption keys, AOSS adheres to strict rules for how data is passed between devices on the wireless transmission medium and to prevent the opportunity to steal or hijack the keys during this critical set of data exchanges. At no point is data related to key generation or the keys itself ever transmitted in an unencrypted or decipherable format.

AOSS: Behind the Scenes (Technical Underpinnings)

AOSS is a very simple process, however, behind the scenes the underpinnings are complex. The entire AOSS process is broken down into 5 main steps:

Association Phase (1):
When a user presses the AOSS button on the AOSS AP, the AOSS AP immediately changes its SSID to "ESSID-AOSS". This SSID remains "ESSID-AOSS" for two minutes or until an AOSS client adapter associates with the AOSS AP. At this time the AOSS LED on the front of the AOSS AP will blink (on 0.4 seconds, off 0.2 seconds).

When the user presses the AOSS button on the Client Manager software or on the actual client adapter itself, it instructs the device to associate to any access point with the SSID "ESSID-AOSS". The client device will search for the specific SSID for two minutes or until it associates with an AOSS AP.

Since both the AOSS AP and the AOSS client will attempt association for two minutes, either the AOSS button on AP or the client AOSS button can be pressed first.

Once the AOSS AP and the client adapter recognize each other, they associate using a 64bit WEP key that is statically configured in the Access Point and in the client adapter or Client Manager Software. This WEP key is stored securely in the AOSS AP and client adapter or client manager software. It is not available to the end user.

Key Generation Phase (2):
With a successful authentication in the prior step, the AOSS AP generates a key derived from a timestamp and the AP's MAC Address:
F(x) = (time stamp + MAC Address)

The AOSS AP transfers this key (with positive ACK returned) to the client adapter and applies it to an RC4 algorithm in the AP and client adapter or Client Manager Software. Thus, a unique RC4 encryption tunnel is created for the session. A man-in-the-middle attack would not have all components of the RC4 algorithm, therefore if the 64bit WEP Key was compromised, the RC4 tunnel would not be compromised. All future data transferred during the AOSS process will be protected by this RC4 encrypted tunnel in addition to the 64bit WEP encrypted tunnel that was created during the 'Association Phase'.

The AOSS AP then creates four new encryption keys: AES, TKIP, WEP128, and WEP64 to be used by all wireless clients on the network. These keys are generated from an algorithm

using a random key generator script on the AOSS AP. The keys are organized with randomly generated SSID's into packets:
Packet = [SSID | Encryption Key]

Each encryption key is associated to a different, random SSID.

The AOSS AP publishes the four SSID & Encryption Key packets into the user interface of the AOSS AP (Advanced Settings - > Management -> AOSS). This gives users the ability to extract the SSID and Encryption Key(s) so they may be used on non-AOSS client adapters.

Information Exchange Phase (3):
The client adapter notifies the AOSS AP of its encryption support. The client adapter extracts this support from the device driver. A positive ACK is sent from the AP to the client adapter.

Key Transfer Phase (4):
The AOSS AP sends all four packets (SSID & Encryption Key packets) to the client adapter regardless of what encryption types are supported on the client adapter. Positive ACKS are returned from the client adapter.

The four encryption keys and their respective SSIDs are securely stored on the client adapter or in the Client Manager software. The user cannot extract this information. With the information, the client adapter or Client Manager Software creates four potential profiles for the AOSS AP. These four profiles act as sub-profiles for a main profile, providing the ability to change the SSID and Encryption Key at a moment's notice.

Reboot Stack (5):
The AOSS AP applies the SSID and Encryption Key specific for the client device (discovered in the Information Exchange Phase). For instance, if the client device only supports TKIP, WEP128, and WEP64, it will apply the highest security protocol supported, which in this case is TKIP.

Preferred Encryption Standards (from highest to lowest):

- AES
- TKIP
- WEP128
- WEP64

The AOSS AP then reboots with the newly applied SSID and Encryption Key. After the reboot, the WEP64 and RC4 encryption tunnels are no longer used.

The client adapter reboots or the Client Manager is re-initialized automatically. Upon reboot, the AOSS profile detects which SSID is running and applies the proper Encryption Key. The association is made as a standards based client.

Subsequent AOSS Processes:
After the first AOSS process, all subsequent AOSS processes occur as follows:

- Identical Association Phase.
- RC4 Key Generation Phase is started between AOSS AP and new Client Device. The RC4 tunnel will use different encryption information due to different timestamp.
- Identical Information Phase.
- Four packets (SSID's + Encryption Keys) are transferred to client adapter with ACKS returned.
    - If the client adapter supports the current wireless encryption standard running from the previous AOSS setup, then the stack reboots. The existing AOSS clients will automatically re-associate and reconnect to the AOSS AP after the AOSS AP's reboot process has completed.
    - If the client adapter supports lesser wireless encryption, then the AOSS AP applies the highest wireless encryption standard and SSID supported by the new client adapter and then the stack reboots.
      Existing AOSS clients will identify an SSID change and apply the new SSID and its respective Encryption Key to its AOSS profile. The existing AOSS clients will seamlessly re-associate and reconnect to the AOSS AP.

Wireless Security Challenges Prior to AOSS

To encourage an end user to take action to secure their wireless network, they must first learn what all of the different acronyms associated with wireless security actually mean. This can be intimidating to the average user and often leads to wireless security being disregarded during the setup process.

At the most basic level, wireless security can best be described as a secret phrase exchanged between two or more devices that allows them to not only authenticate one another, but also to encode and decode messages between them. Generation of this secret phrase can occur in several ways. The simplest example is a password or key created by a user, much like when a user creates an email password. However, this can be ineffective and can often lead to distribution of the key to other people. Should the user forget the key, they will need to create a new key, requiring them to repeat the setup process for the entire network, even if adding only one additional device.

Another common method of generating keys includes using a pass phrase, which allows the end user to generate a key by entering a common term. This allows a key to be generated by using the inputted pass phrase against a shared algorithm. While this is an effective way to generate unique keys, the challenge is to remember this key, which typically is not recognizable word. Should a new device need to be added to the wireless network and the machine used to generate that key is not available or does not support the creation of the key; the user will have to repeat the entire setup process.

These two scenarios are not the only challenges facing the end user when trying to establish wireless security on their network. Some wireless devices do not have room for a display or user interface to allow users to manually configure wireless security settings. Future "smart home" devices such as a thermostat or microwave oven could be very tedious to configure onto the local network if they require a 63- character wireless encryption key comprised of a mix of letters and numbers in a seemingly random array.

Vendors' tendency to expect end users to value wireless security beyond the initial hardship of setting up and maintaining wireless security is not logical. The wireless network as a whole can easily become a burden to the end user when wireless encryption is in use and devices are routinely added to the network. Many devices fail to offer the highest level of security- WPA, and very few end users bother to upgrade to more robust security features.

There are solutions available or in development today that attempt to resolve some of the security challenges with which the end user is faced. Typically, these solutions involve using physical media such as a floppy disk, USB memory card or barcode reader. The advantage of this approach is that it does not require the user to understand the information that is being transferred. However, requiring a physical medium is in itself a major disadvantage. The added costs of adding support for the physical media onto wireless devices, such as including a USB port on an AP will ultimately drive up the cost for the end user. Most troublesome about this method of delivering security keys is what options the end user has should they lose their physical media or find themselves where a new device must be added and the physical media for exchanging the correct keys is temporarily unavailable. In both of these situations, the use of wireless security on the network will likely be discarded.

AOSS as the Wireless Security Solution

When considering the future of wireless security maintenance, it is vital to consider wireless-enabled desktops, notebooks, printers and other traditional networked peripherals are not the only devices that will define the wireless environment of the digital home of tomorrow. If this were the case, it might be logical to consider a solution such as a USB media as a viable solution for setting up and maintaining wireless security standards on the network. However, wireless networking is also finding its way into many electronic devices within our homes, including those where the introduction of a USB interface would be a burden on costs and basically undesirable.

The usage of an in band solution such as Bluetooth would be ineffective due to the requirement of devices being within very short range of each other. This could be a burden if the device were for example, the size or a refrigerator or wide screen television. One could also envision using a wired medium such as Ethernet to pass this information. However, like the USB solutions it requires its own interface on devices that might not support or want this type of additional hardware.

While considering all of these challenges and shortcomings, AOSS was designed with a simple push-button mechanism on both the client and AP to trigger the exchange of security information over the wireless medium. Allowing the button to be either a hardware button or a virtual button within a software interface, costs and invasiveness are kept to an extreme minimum, while integration can easily be accomplished on headless devices such as a coffee maker or alarm system motion detector.

The push-button model requires human interaction with their wireless devices. The user can feel a sense of security in the simple act of pushing a button on both sides of the connection. Since only the user knows when the button will be pushed, there is limited vulnerability to attacks and accidents by neighboring devices that should be excluded from the user's wireless network.

Theoretically, the remarkable speed of AOSS configuration could easily allow a user to securely connect over 50 wireless devices within an hour. Once the first AOSS setup is accomplished users can easily add and remove additional devices without ever having to revisit the initial setup process. The nature of AOSS will allow it to evolve just as security methods evolve, without the need to upgrade the client devices until the end user desires. By addressing each of these concerns, challenges and shortcomings of today's wireless security options and solutions, AOSS establishes itself as the security solution of tomorrow.

AOSS is available today from Buffalo Technology.
Visit us at www.buffalotech.com.

Buffalo, Inc. trademark statements. Buffalo is a trademark of Buffalo, Inc. All other trademarks mentioned herein are the property of their respective owners.