

Colligo Security Whitepaper

Version: 1.2

Authors: Mike Blackstock, Nick Sawadsky

Date published: March 7th, 2005

Contents

Introduction.....	2
Approaches to Securing Wireless LAN's.....	3
Wireless Local Area Networks.....	3
WEP.....	3
802.11i and Wi-Fi Protected Access (WPA).....	4
Secure Sockets Layer (SSL).....	4
IPSec.....	5
Colligo's Security Solution.....	6
Core Security Measures.....	6
Authentication.....	6
Encryption.....	7
Securing Windows Folder and Printer Sharing With Colligo.....	7
Access Control.....	7
Encryption.....	7
Protecting Access to the Network.....	8
Summary and Conclusions.....	9

Introduction

Security has always been a challenge when exchanging data over computer networks. Two recent trends, however, are causing security risks to grow rapidly:

- today's business users are exchanging information as never before, using a variety of software tools and services; and
- new technology is permitting these exchanges to occur wirelessly, often over wireless local area networks (wireless LAN's or WLAN's).

Exchanging information in a wireless world represents a significant security risk. Whether data is transferred over an 802.11 wireless LAN in an office, or over an ad hoc wireless LAN between colocated PDA's or laptops, preventing unauthorized access to that data is critical. Flaws in the initial 802.11 security implementation, WEP, have heightened wireless security concerns for many enterprise IT departments. These flaws emphasize the importance of proven encryption and authentication methodologies.

New client-to-client applications like Colligo allow users to remain productive in situations where server-based applications break down. Colligo allows an ad hoc wireless network to be created with a single button click. Users can connect directly to each other without the need for a central server. Collaborative work can then proceed in settings where it is not practical to set up a permanent server, or where access to the Internet is not available.

However, because security systems have traditionally been server-based, client-to-client computing and ad hoc wireless networks present unique security challenges. This whitepaper discusses how important data can be secured over wireless LAN connections, particularly ad hoc wireless networks, and presents Colligo's standards-based solution to ad hoc wireless security.

Approaches to Securing Wireless LAN's

Wireless Local Area Networks

802.11 is a family of specifications for wireless local area networks developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). To access an 802.11 wireless network, a user's device must have an internal or external wireless adapter. These adapters may either communicate to the network through access points (radios which are connected via Ethernet cable to the wired LAN), or to each other, device-to-device. The former method of connectivity is known as "infrastructure" or Extended Service Set (ESS) mode, while the latter is known as "ad hoc" or Independent Basic Service Set (IBSS) mode. These modes are illustrated in Figure 1.

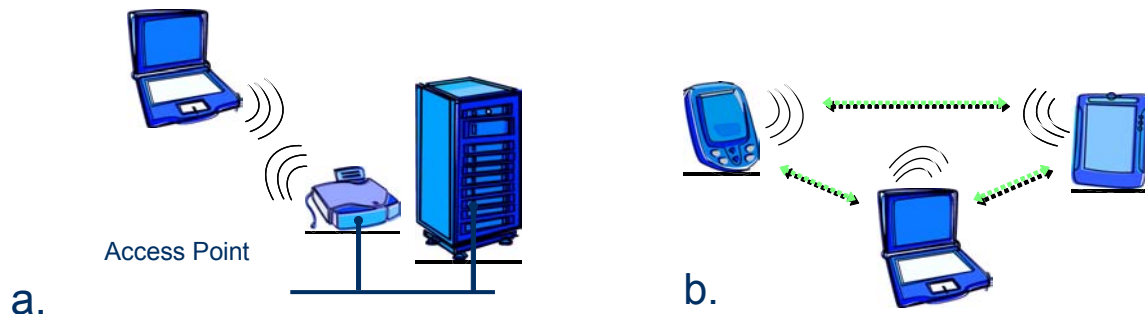


Figure 1. (a) Infrastructure (ESS) and (b) ad hoc (IBSS) modes of wireless LAN's

Colligo's Instant Network function allows users to put their wireless cards in to ad hoc mode with a single button click, so that they can connect to other users around them without the need for an access point.

One challenge for security in ad hoc mode is that there is no central authority to manage device and/or user authentication. Many security measures are limited to infrastructure mode, while those that are available in ad hoc mode may have clear drawbacks, such as relying on a preshared key.

WEP

Within the 802.11 protocol specification, the Wired Equivalent Privacy (WEP) algorithm was intended to protect wireless communications from malicious access, whether the user was connecting to a wireless access point or directly to another user's 802.11 card (ad hoc mode). As its name implies, WEP was intended to provide similar security to a wired (but unencrypted) LAN. WEP security relies on a key that is shared between a device (e.g. a laptop with a wireless card) and one or more access points. The key is used to encrypt packets before they are transmitted.

In terms of the Open Systems Interconnection (OSI) model, WEP operates at layers 1 and 2, the physical and data link layers.

Since the release of the specification, many weaknesses have been exposed in the WEP standard. By passively listening on the network, an attacker can eventually acquire enough information to recover the WEP key. Although it may take days on a low-traffic

ad hoc network or home network to breach security, on a high traffic network it can take only hours.

Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful in deflecting would-be eavesdroppers, especially on low-traffic temporary ad hoc networks. Colligo's Instant Network function supports the use of WEP as an easy way to lock down a wireless ad hoc network.

802.11i and Wi-Fi Protected Access (WPA)

The IEEE 802.11 Working Group instituted Task Group "i" to design a strong replacement for the flawed WEP standard. The 802.11i standard, which was ratified in June 2004, includes enhanced encryption and authentication components, and a negotiation framework called Robust Security Network (RSN).

RSN provides for dynamic negotiation of authentication and encryption algorithms between access points and mobile devices. The two authentication schemes specified in the standard are 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is Advanced Encryption Standard (AES). Since RSN supports dynamic negotiation of authentication and encryption algorithms, it can evolve over time, adding algorithms to address new threats and continuing to provide the security necessary for WLAN's.

WPA is a wireless security standard backed by an industry consortium called the Wi-Fi Alliance. WPA was intended to speed adoption of the new security mechanisms that were still being finalized by the 802.11i task group. WPA2, the latest version of WPA, is based on a subset of the final 802.11i standard.

Like 802.11i, WPA2 offers 802.1X and EAP authentication. It also offers WPA-PSK (pre-shared key), a special mode of WPA for home or small network users without an enterprise authentication server. For encryption, WPA2 offers AES, as well as a backwards-compatible encryption scheme called Temporal Key Integrity Protocol (TKIP).

While 802.11i does specify support for ad hoc networks (IBSS), WPA2 explicitly states that such support is not required. As a result, the landscape for wireless ad hoc security remains in a state of flux. Some card vendors offer support for a version of WPA in ad hoc mode, while others do not.

In addition, we note that authentication will always be a challenge in ad hoc wireless networks, since authentication servers are not accessible. Any implementation of 802.11i or WPA2 in ad hoc mode is likely to rely on pre-shared keys, with their inherent weaknesses. Because of this state of affairs, Colligo has implemented additional security measures of its own, using SSL and IPsec, to ensure secure data exchange over wireless ad hoc networks.

Secure Sockets Layer (SSL)

Secure Sockets Layer (also known as Transport Layer Security, or TLS) is the industry-standard method for protecting web communications. It provides data encryption, server

authentication, message integrity and optional client authentication over a TCP/IP connection. SSL is built in to every major web browser and server.

When communicating with a web server running SSL, the browser requests a certificate, assuring users that they are communicating with the organization they intend to. Using this certificate, an encrypted communications link can be set up for each transaction. In Colligo's implementation, each user has her own certificate, which is used in the same manner. The SSL protocol is used to authenticate other users, and ensure that all communications are encrypted.

IPSec

IPSec (Internet Protocol Security) is a standard for security at the network layer of communication. IPSec can be used to encrypt all of the IP traffic traveling in and out of a machine, whereas SSL is typically used only to encrypt the traffic of a specific application.

IPSec offers two modes of operation: "Tunnel Mode," in which both the address header information and the data "payload" are encrypted, and "Transport Mode," where only the data payload is encrypted. IPSec is especially useful for implementing virtual private networks (VPN's).

While IPSec is integrated into Windows 2000 and XP and may be implemented by the end user (or by their supporting IT group) on those platforms, it is not enabled by default. It is not available in Windows 95, 98 or NT.

Colligo leverages Windows IPSec in preshared key mode, allowing users to take advantage of Windows folder and printer sharing in ad hoc environments securely. In Colligo, the preshared key is generated dynamically between peers, eliminating the usual weaknesses of preshared keys. Colligo's use of IPSec is discussed further below.

Colligo's Security Solution

Colligo's security solution can be broken in to three components:

- (1) the set of core security measures Colligo implements to authenticate users and protect data transmitted within Colligo;
- (2) the security measures Colligo implements to provide authentication and encryption for Windows folder and printer sharing; and
- (3) how port-based access to computers in the Colligo Instant Network can be protected.

Core Security Measures

Colligo's engineering team concluded that the best way to address the current challenges of wireless ad hoc security was to implement a robust, application-level authentication and encryption model. Colligo uses SSL for authentication and to encrypt all data transferred within the application. Colligo's SSL support is based on the popular and field-proven OpenSSL libraries.

Authentication

In order to ensure that only accredited individuals are able to join collaborative Colligo sessions, Colligo's software requires that connected individuals possess a public-private key pair and a self-signed X.509 certificate.

The keys are generated the first time the user runs Colligo, and are unique to the user. The certificate contains the user's public key, as well as the user's name and device ID. The user must enter his or her full name, while the device name is initialized to a default value retrieved from the operating system, and may also be modified by the user. Once this step is completed, it does not have to be repeated, unless the user decides to create a new key pair and certificate, or the certificate expires. The expiry time is configurable, with a default of 12 months.

When establishing a secure connection with a partner for the first time, the user's certificate is transmitted and displayed to the destination partner. While it is important to compare certificates to ensure no "man-in-the-middle" is present, these comparisons can be difficult since certificate hashes are typically 128 or 160 bits. Encoding 128 bits into hexadecimal, for example, means that 32 digits must be compared by the user. To make certificate comparisons easy without sacrificing security, Colligo has developed a unique method of securely encoding a user's certificate using only three keywords.

Thus, when authenticating each other, users must compare only six keywords (three for each certificate) to verify each other's identity. These keywords are usually compared verbally, either through direct communication or over the phone.

Once a user has verified a partner's certificate, it is imported into a local cache of trusted certificates. Subsequent connections with that partner are established transparently, until the partner's certificate expires or is manually removed from the cache.

Encryption

All Colligo communications are protected with Secure Socket Layer (SSL) encryption. Each time a connection to another user is established, a new session key is created for encrypting communications between the two users. The initial exchange of the session key is protected using 1024-bit RSA encryption. Subsequently, Colligo employs the Triple DES (Data Encryption Standard) method of encryption, wherein three 56-bit keys are applied in succession to each 64-bit block of data resulting in an effective key length of 168 bits. Securing data transmission in this fashion results in negligible impact to system performance and throughput.

Securing Windows Folder and Printer Sharing With Colligo

In certain cases, Colligo is used to launch other applications for use over the ad hoc network. Two prominent examples are Windows folder and printer sharing. With such applications, the actual communications occur outside of Colligo. As a result, Colligo's secure SSL link cannot be used to secure the data transferred. To ensure the security of data exchanged through Windows folder and printer sharing, Colligo uses IPSec to encrypt traffic in selected port ranges between the two computers.

In the ad hoc environment, standard Windows domain authentication is no longer possible, as the domain server may not be reachable. In some cases, companies that rely on Windows folder sharing have been forced to compromise access control, allowing users to share login credentials in order to use shared folders in the field. Colligo allows Windows folder sharing to occur securely, leveraging the SSL link to provide strong access control on Windows folder shares.

Access Control

To provide secure access to Windows folder shares in the field, Colligo leverages the secure SSL link and the authentication already performed between two Colligo users. The first time a user shares a folder through Colligo Workgroup Edition 4.0, a "virtual user" named "ApprovedColligoUsers" is created on the local machine. This user is assigned an extremely strong, random 32-byte password which is refreshed each time Colligo runs. When a partner attempts to access a folder share, Colligo first checks the Colligo access control list (ACL). Provided the partner is listed in the ACL, Colligo then transmits the credentials of the "virtual user" across the SSL link to the partner. On the partner's side, Colligo uses these credentials to open the folder.

This approach ensures that even in the absence of domain server, access to folders shared through Colligo is strictly controlled.

Encryption

To ensure data transferred through Windows folder and printer sharing is encrypted, Colligo relies on IPSec security.

It is possible to implement a simple VPN between users on a wireless ad hoc network by creating an IPSec security policy using the administrative tools in the Windows control panel. In one approach, users share a password or phrase which is then used to generate a shared encryption key.

The drawback to this system is that the shared key must be manually provided to each partner. In a practical sense, this often means that the key is written down or sent via email, resulting in a breach of basic security. Furthermore, the key may be transcribed incorrectly, resulting in connection failures. Since longer keys are more error prone, the keys selected are usually simple, and therefore breakable. Finally, it is difficult for end users to configure IPSec settings without IT help.

Colligo addresses these concerns in its IPSec implementation as follows:

- A random 32-byte preshared key is created automatically when a user attempts to access a shared folder or printer in Colligo 4.0. Users never see this key, so they don't need to remember it, and there is no need to write down the key. This key is generated pair-wise – a different key is used for each pair of users. A single key is used only for the duration of a Colligo session – on shutdown of Colligo, these keys are flushed and not reused.
- The key is transmitted by Colligo using application-level security, that is, over the SSL link between authenticated Colligo users. There is no need to distribute the key using a potentially-insecure means.
- Colligo manages the IPSec security policy and settings automatically, making it transparent to the end user.

Colligo's use of IPSec in preshared key mode is not vulnerable to the usual weaknesses of preshared keys. With the use of Colligo, IPSec becomes a safe and easy way to secure ad hoc networks for TCP/IP-based applications.

Protecting Access to the Network

Colligo's use of SSL and IPSec ensures that all data transmitted by Colligo (and by Windows folder and printer sharing) is strongly encrypted. However, neither SSL nor IPSec prevents attackers from gaining access to the network and mounting a port-based attack on the other computers in the ad hoc network. WEP was intended to lock down the network, preventing this kind of attack, but has some well-known flaws, as stated above.

Like WEP, 802.11i provides protection at the physical layer. However, as stated above, support for the ad hoc mode of 802.11i is not yet widely available in the wireless adapters on the market.

At such time as support for 802.11i over ad hoc becomes standardized and widely supported, Colligo will add this capability to its Instant Network function. Until that time, access to the Colligo Instant Network can be protected through WEP. Recognizing the well-known limitations of WEP, Colligo also recommends the use of personal firewall software to provide strong protection against port-based attacks while computers are in the ad hoc network.

Summary and Conclusions

While wireless LAN security has been tackled in multiple standards, these standards still have not fully addressed the challenge of ad hoc wireless security. WEP is known to have security flaws, while WPA cannot yet be applied to ad hoc wireless networks.

Authentication will always be a challenge in ad hoc networks, since authentication servers may not be accessible. In particular, standard Windows network authentication methods cannot be used in an ad hoc environment, as the domain server may not be reachable.

Colligo provides a strong, standards-based solution to the problem of wireless ad hoc security. Through certificates and SSL, it ensures the security of its core communication functions. In addition, it allows Windows folder and printer sharing to be used securely in the field. It provides strong access control for Windows shared folders, even in the absence of the domain server. And it ensures that the data transmitted through Windows folder and printer sharing is IPSec-encrypted.

Port-based attacks on computers in the Colligo Instant Network are prevented through a trusted personal firewall, and, optionally, the addition of a WEP key to the Instant Network.

Although future standards may address network-level security in ad hoc wireless networks, they will not provide an *integrated* security solution (i.e. authentication and encryption) for accomplishing tasks such as Lotus Notes database replication, folder sharing, printer sharing, and file transfer while in the field. Colligo's solution augments current and future wireless standards by providing a single, integrated, easy-to-use interface for common tasks, along with the security those tasks demand.