SEH WHITEPAPER

# Secure Printing in Wireless LANs

## Important Security Features for Attaching Network Printers to Wireless Networks

*In wireless networks data are transfered via radio in the air. As a consequence efficient security measures are especially important to protect these data. Print documents often contain confidential and sensitive data. This is why network printers should be equipped for a safe connection to wireless LAN. WLAN print servers should naturally support the latest WLAN encryption standards as well as safe methods of authentication (IEEE 802.1X). Depending on the security demands of a network it is possible to implement further security measures such as print data encryption via TLS/SSL. This whitepaper provides an overview of the most important protective measures for network printing in a WLAN and explains how they function.*

**JÖRG HECKE**
*Product Manager*

**MARGARETE KEULEN**
*Marketing Communications Manager*

*Version 1.0*
*November 2008*

# TABLE OF CONTENTS

## 1. SECURITY RISKS IN A WLAN

A few years ago the major questions about wireless printing concerned the development and establishment of standards – WLAN, Bluetooth , and IrDA. Since then WLAN (Wireless Local Area Network) has become the standard for wireless networks. Today the issues around wireless printing focus on WLAN security. This concerns the attachment of network printers as well.

Static keys, open networks, and an exclusively device-based identification of wireless clients harbor a great number of security risks for a WLAN. This is true for handheld PCs and notebooks as well as for WLAN print servers connecting printers, digital copiers, and multifunctional peripherals (MFP). The security risks of a wireless network printing solution fall into two categories:

- **Passive Attacks:** Eavesdropping and analysing data traffic between Access Point (AP) and WLAN print server and exploring the communicating agents
- **Active Attacks:** Unauthorized access to the network or to the WLAN print server and / or the attached output device

Passive attacks aim at gaining important information about data traffic and communicating agents. Attackers later use this information to access network and clients without authorization. Active attacks are conducted with different intentions, such as preventing services and communication, delaying communication, accessing business information, manipulating messages etc. When operating a wireless network printing solution the following types of active and passive attacks should be considered:

- **Sniffing:** Eavesdropping on the traffic between AP and mobile clients and analyzing it is called sniffing. As most of the information transmitted by an AP is in clear text it is easy to sniff. The aim of sniffing is to gain information about the security set-ups of a WLAN. This is used by any kind of device to assume the identity of an authorized device and unwarrantedly access the network (spoofing).
- **Spoofing:** Spoofing denotes that an unauthorized device assumes the identity of an authorized WLAN device which has been found with the help of sniffing. (e. g. spying on. the MAC address). Disguised with this identity the unauthorized device accesses the WLAN under cover.
- **Session Highjacking:** During Session Highjacking an unauthorized user takes over an established WLAN connection between an AP and an authorized WLAN client. Towards this client, the user fakes a disruption of the radio connection and takes on its identity. For the AP the connection remains unaffected.
- **Denial of Service:** Having accessed a WLAN without authorization, a user ties all network traffic by mass traffic generation, causing network congestion.
- **Man-in-the-Middle:** During a Man-in-the-Middle attack an unauthorized user inserts himself into an established connection between AP and authori-

zed WLAN client. He pretends to both sides to be the other's communication partner, diverts all traffic to himself, and eavesdrops on it.

All attacks described above are not specific to print servers but present general security risks for the operation of a WLAN.

## 2. GENERAL SECURITY MEASURES IN A WLAN

The standard security functions of WLAN specifications can impede such attacks. However, the best possible protection is achieved only by wireless network infrastructures which support and activate all relevant security measures across all APs and wireless devices, including print servers. The basic WLAN security measures include the support of WLAN encryption standards (WEP, WPA/WPA2), SSID deactivation, MAC address filter etc. Authentication of mobile users and devices via efficient authentication methods according to the IEEE standard 802.1X is another important security measure. For further protection of data users can utilize additional TLS/SSL encryption.

Depending on the existing security demands these mechanisms can be combined. Security measures in a WLAN ensure that only authorized users can access the network and connect via the correct APs (authentication). Moreover, the integrity of transmitted data is protected by sending unaltered data only to the receiver and reject manipulated data. In order to provide for the confidentiality of a WLAN eavesdropping by unauthorized users must be prevented.

# 3. WLAN ENCRYPTION METHODS

Special encryption technologies for WLAN are core constituents of a WLAN security set-up, providing for eavesdropping-security and confidentiality.

## 3.1. WEP (WIRED EQUIVALENT PRIVACY)

The original standard for WLAN encryption, Wired Equivalent Privacy (WEP, IEEE 802.11) was defined in 1999 and should provide for the same level of confidentiality that exists in cabled networks. WEP utilizes static keys, the RC4 encryption algorithm, 40- respectively 104-bit encryption, and a 24-bit initialization vector (IV). The grave deficiencies of WEP have been detected early: The IV is too short, allowing repetitions (IV collisions) too soon. This enables hackers to decrypt a data package and to extract the WEP key as well as the data. RC4 has been hacked already. Although WEP is implemented into all WLAN devices (802.11a, 802.11b, 802.11g) as a standard this method can no longer be recommended for corporate WLAN networks.

## 3.2. WPA AND WPA 2: SECURITY FUNCTIONS

In order to quickly close the security gaps left by WEP WPA (Wi-Fi Protected Access) was developed as an interim solution, anticipating the new and very extensive security standard 802.11i. The complete IEEE standard 802.11i has been realized with WPA2. Currently WPA and WPA2 are held to be the most secure WLAN standards and have not yet been broken.
Like WEP, WAP uses the RC4 algorithm, while WPA2 utilizes the highly secure encryption algorithm Advanced Encryption Standard (AES) , version AES-CCMP.

The most significant security function of WPA is the utilization of dynamic keys. These are based on the Temporal Key Integrity Protocol (TKIP). The additional security features include a longer IV, a per-packet key mixing function, a re-keying mechanism, and a message integrity check (MIC). The security functions of WPA and WPA2 are mainly composed of four standards

- Temporal Key Integrity Protocol (TKIP)
- Message Integrity Check (MIC)
- IEEE 802.1X-Authentication
- Extensible Authentication Protocol (EAP)

TKIP closes the security gaps of WEP encryption and enables extended data encryption. During this process each data package is encrypted with its own key (per packet key). This key is generated from the sender's MAC address, a sequential number, and the temporal key. Both the temporal key and the key for MIC are derived from the keys negotiated during the authentication process. The IV is used to count sequences. It is initialized to 0 every time new keys are composed. This prevents the insertion of older packages ("Reply-Attack"). The per packet keys keep the connections within a WLAN separate and prevent weak keys.

MIC prevents unauthorized parties from intercepting, manipulating, and re-sending data packages. WPA and WPA2 utilize the MIC "Michael". Other than well-known MICs like HMAC-SHA1 or DES-CBC-MAC "Michael" is extremely powerful and provides for

20 bit high security. Sender and receiver must pass through an integrity check and compare the identities. This integrity check includes the header of the data packages. One counter in MIC is used to determine faulty packages which are then rejected. The likelihood that a forged package is not detected is around one in $2^{-19}$.[1] If during a defined interval a specified number of faulty or forged package arrive, the AP will assume an attack on the respective connection and disconnect it. Hereafter the WLAN client has to register anew.

IEEE 802.1X authentication methods based on the EAP protocol family allow for the identification of clients in wireless networks. 802.1X is a port-based method to control network access in both cabled and wireless networks.

Both WPA and WPA2 offer Personal Mode for SOHO (Small Office, Home Office) and Enterprise Mode for large networks to accomodate the requirements of different user groups. For authentication in Personal Mode users use pre-shared keys (PSK) which are utilized for generating the respective session keys. The security provided by PSK depends heavily on the quality of the password, which is a single point of failure. If an attacker gets the PSK it will be easy for him to gain access to the network and the data. If the password is only 20 characters (of 63 possible characters) and not complex in composition it is prone to a brute force attack. The Enterprise Mode of WPA and WPA2 utilizes authentication via EAP (Extensible Authentication Protocol) which in most cases relies on an authentication method according to IEEE 802.1X via RADIUS (Remote Authentication Dial In Service) Server.

### 3.3. COMPATIBILITY OF WLAN ENCRYPTION TECHNOLOGIES

As the implementation of WLAN encryption technologies usually also affects the hardware platform, technical reasons prevent the operation of WLAN clients with WEP, WPA, and WPA2 together in the same network or to use software updates to bring them to the same level. In case of WLAN clients with WEP users will have to check whether a software-upgrade to WPA or WPA2 is possible at all.
Users will only benefit from all security advantages of WPA if all WLAN devices in the network will be upgraded. For the full security compass of WPA and WPA2 users might have to invest in new devices. When switching to WPA/WPA2, users should follow the recommendations of the Wi-Fi consortium. It is also a good idea to check whether WLAN clients with WPA and WPA2 are compatible with each other.

[1] *Nancy Cam-Winget et al.: „Security Flaws in 802.11 Data Link Protocols", Communications of the ACM, May 2003/Vol. 46, pp. 35-39, http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf.*

| WLAN Encryption Standard | Encryption Algorithm | Authentication |
|---|---|---|
| WEP | RC4 | static keys |
| WPA (Personal Mode) | RC4 | Password (8-63 ASCII characters)<br>PSK (64 hexa-decimal characters) |
| WPA (Enterprise Mode | RC4 | EAP according to 802.1X |
| WPA2 (Personal Mode) | AES-CCMP | Password (8-63 ASCII characters) |
| WPA2 (Enterprise Mode) | AES-CCMP | PSK (64 hexa-decimal characters) |

## 4. 802.1X AUTHENTICATION IN A WLAN

The IEEE standard 802.1X makes it possible to control the access to a network. A new network participant (client) will only be granted access after a successful user- or device-based authentication. Most authentication methods are based on the Extensible Authentication Protocol (EAP), which is definded in . RFC 3748. This protocol supports about 40 authentication methods for both WLAN and LAN. In all of these the client authenticates itself via a RADIUS server. Three parties are involved in this process: First, there is the supplicant, i.e. the device about to access the WLAN. The second is the authenticator which transports communication between supplicant and authentication during the authentication process, ensuring that no other party can communicate with the supplicant as long as authentication is still in progress. In most cases the AP functions as authenticator. When the authentication is successful the authenticator will allow the supplicant to join the WLAN.

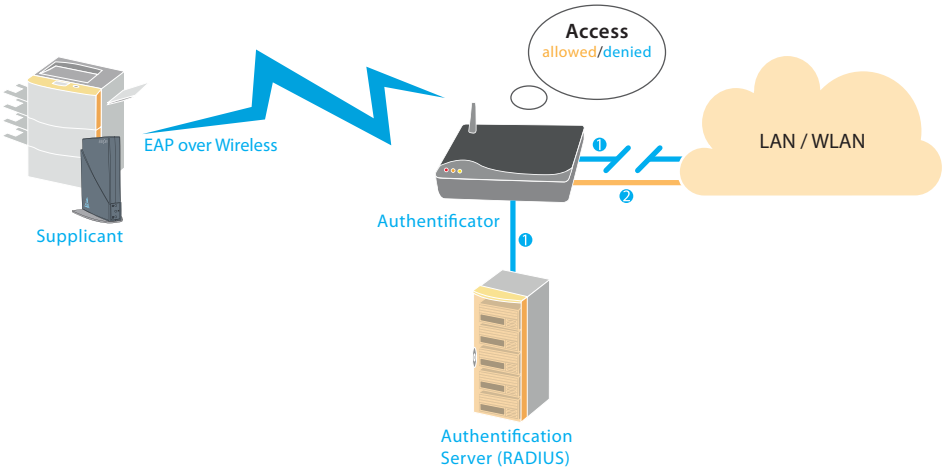


**Image 1: 802.1X authentication of a WLAN- client**

The third party involved is the authentication server (RADIUS) which stores all information about users, required certificates etc. Its task is to verify the supplicant's identity. The RADIUS server is either a dedicated server or another dedicated network device, a software component for servers (e.g. IAS by Microsoft) or a component integrated into the AP. In some cases the RADIUS server can check whether data relevant to authenticating a WLAN client match those listed in a directory service (LDAP-Server, Directory Server etc.).

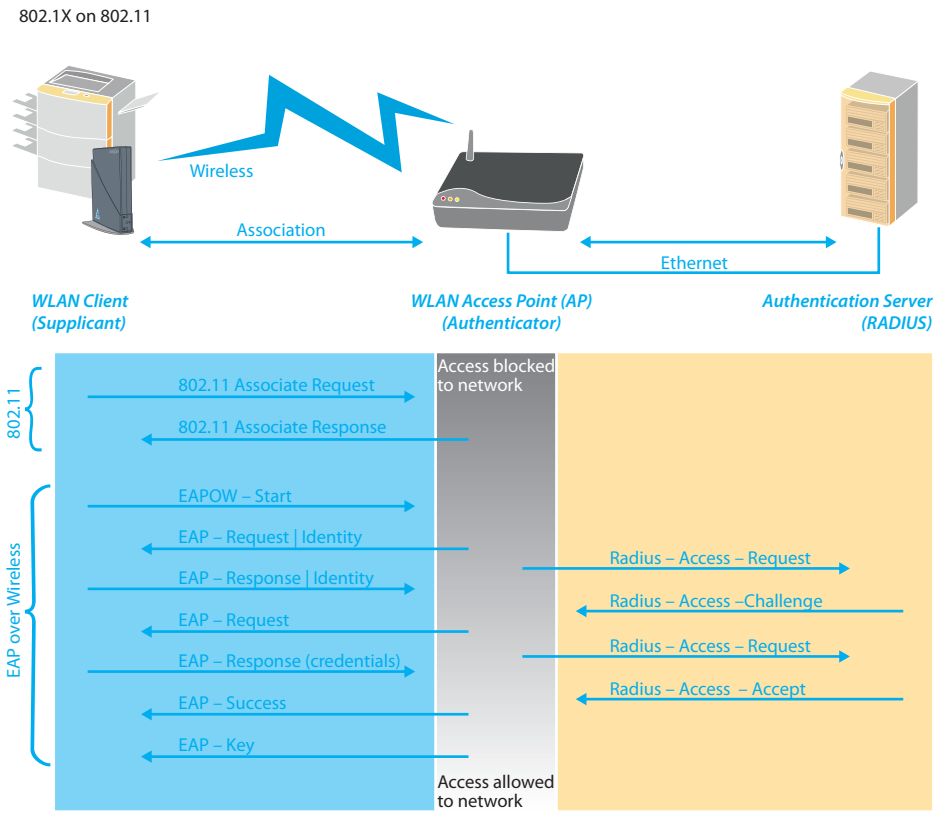


**Image 2: Progression of the 802.1X authentication of a WLAN client**

The following authentication methods are relevant to network printing:

### 4.1. LEAP

Lightweight Extensible Authentication Protocol (LEAP), a proprietary development by Cisco, was the first widely used protocol for authentication in WLAN. The method is no longer considered safe because it is vulnerable to attacks, e.g. brute force attacks. Therefore a high password quality is essential. Windows operating systems do not generically support LEAP.

### 4.2. EAP-MD5

This password-based method defined in RFC 3748 uses the hash function (Message-Digest Algorithm 5) to protect communication. It is also prone to brute force attacks. EAP-MD5 utilizes static keys so there is no mutual authentication between client and server. As a consequence, this method is not considered to be very safe.

### 4.3. EAP-TLS

The Extensible Authentication Protocol over Transport Layer Security (EAP-TLS), defined in RFC 2716, handles communication by providing a secure TLS connection. EAP-TLS is an open IETF (Internet Engineering Task Force) standard. This method requires a public key infrastructure (PKI), i.e. digital certificates have to be issued, distributed, and verified both to the server and to the clients. This is very complex and time-consuming, especially so in larger WLAN installations. The security provided by this me-

thod is very high. Currently EAP-TLS is the most widely used authentication method for WLANs, it has become the de-facto standard.

### 4.4. EAP-TTLS

Funk Software and Certicom developed the Extensible Authentication Protocol over Tunnelled Transport Layer Security (EAP-TTLS) on the basis of EAP-TLS. This method does not require a PKI because only the server authenticates itself to the client. The connection between supplicant and RADIUS server is encrypted with a "Master Secret". This method utilizes a fast symmetric algorithm which builds a tunnel for safe communication. The transmission of authentication data is protected by this tunnel. Contrary to EAP-TLS the supplicant does not have a certificate of its own and is not involved in building a TLS session. It is possible to use not only EAP protocols but any other password protocols (e.g. Password Authentication Protocol/PAP; Challenge Handshake Authentication Protocol/CHAP) within the tunnel. EAP-TTLS is less complex but also less secure than EAP-TLS, because only the RADIUS server uses a certificate. The supplicant, however, has no means to verify the identity of its communication partner. An attacker could collect the data necessary for a "Man-in-the-Middle" attack, decipher it and use it for unauthorized authentication.

Due to the lack of support by Microsoft, EAP-TTLS is not yet very widely used. Microsoft favors the competing PEAP method which it helped to develop.

### 4.5. PEAP

Protected Extensible Authentication Protocol (PEAP) functions similar to EAP-TTLS, i.e. without PKI. This method was developed by Microsoft, Cisco, and RSA and also offers high security. The difference to EAP-TTLS is that only EAP protocols can be used in the tunnel.

### 4.6. EAP-FAST

Developing the Extensible Authentication Protocol - Flexible Authentication via Secure Tunnelling (EAP-FAST), defined in RFC 4851, Cisco aims at closing the security gaps of LEAP. Instead of certificates, this method uses a so-called PAC (Protected Access Credential), which is dynamically administrated by the RADIUS server. EAP-FAST is considered to be relatively secure. It is a good solution if neither a high password quality can be guaranteed, nor a certificate management is deployed.

| Authentication method | Server Authentication | Supplicant Authentication | Possible Attacks | Dynamic Keys | Security |
|---|---|---|---|---|---|
| **LEAP (Cisco)** | Password Hash | Password Hash | Brute Force | yes | medium, strong |
| **EAP-MD5** | none | Password Hash | Man-in-the-Middle, Brute Force, Session Highjacking | no | strong |
| **EAP-TLS** | Public Key Certficate | Public Key-Zertifikat | none | yes | very strong |
| **EAP-TTLS** | Public Key Certficate | EAP-Verfahren, PAP, CHAP | Man-in-the-Middle | yes | strong |
| **PEAP** | Public Key Certficate | EAP-Verfahren | Man-in-the-Middle | yes | strong |
| **EAP-FAST** | Public Key Certficate | EAP-Verfahren | Man-in-the-Middle | yes | medium, strong |

## 5. FURTHER PROTECTION: PRINT DATA ENCRYPTION

When it comes to the protection of print data those who do not want to rely on WLAN encryption and secure authentication alone can use TLS/SSL encryption on top. The printer protocols PCL (Printer Control Language) and Postscript are page description languages. In addition to control and functional characters, they transport the print data almost as clear text. The Internet Printing Protocol, version 1.1 (IPPv1.1) is the only printing protocol which allows print data encryption independent of make and model as a standard (RFCs 2910, 2911, 3196, and 3510). As IPP v.1.1 is based on HTTP 1.1 this protocol can use all extensions of HTTP as well, which includes SSL/TLS encryption. However, Windows operating systems do not support the current version of IPP v1.1. Windows 2000, XP Professional, and Windows Server 2003 can install the Webserver IIS as Windows component in the software category of the system control. This can be configured as print server, enabling printing via IPP as well as SSL encrypted print data transmission via the Internet. Attached network printers are managed via a web interface. However, this is a rather complicated procedure.

In addition to that, only few proprietary solutions for encrypted print data transmission are available for Windows environment. The SEH Print Monitor, developed by SEH for print job encryption in Windows operating systems, is a tool which is easy to handle. Utilizing the SEH Print Monitor, Windows clients choose between Socket Printing (Port 9100) or HTTP Printing (Port 80). In case of HTTP Printing users decide between sending print data without encryption (Port 80) or using encryption (Port 443).

Another example in the print management solution .print by ThinPrint. This allows to encrypt print data which are sent from the terminal server to the client. Via RDP and ICA encryption is already provided for by the session protocols. ThinPrint SSL encryption of print data is not only available for servers and clients in Windows environments but also for heterogeneous environments (Linux, Unix, AS/400, IBM-Mainframes).

## 6. SUMMARY

WLAN continues to be popular as it offers independence from cabling, enabling many fields of application, e.g. fast and cost-effective extensions of cabled networks, networked operations in buildings where structural integrity is essential, mobile networks in meeting or training rooms, and temporary networks at special events. The reputation of WLAN as not being sufficiently secure is disproved. Printing in wireless networks is also secure when the network connection via print server supports all relevant procedures and encryption standards. High-end WLAN print servers must at least support the WPA and WPA2 standards both for Personal and Enterprise modes and master the above described authentication methods.

## 7. SEH WLAN PRINT SERVERS: SECURITY FEATURES

WLAN print servers by SEH are network solutions of excellent quality for business environments. They are equipped with all important security features as well as with the latest standards relevant to secure network printing in wireless networks 802.11b/g).

- **WLAN Encryption Standards**:
  - WEP
  - WPA Personal Mode
  - WPA Enterprise Mode
  - WPA2 Personal Mode
  - WPA2 Enterprise Mode
- **Authentication Methods According to IEEE 802.1X:**
  - LEAP
  - EAP-MD5
  - EAP-TLS
  - EAP-TTLS
  - PEAP
  - EAP-FAST
- **Print Data Encryption:**
  - TLS/SSL
  - ThinPrint SSL

The security package includes even more security features which are integrated into all SEH print servers of the PS series, e.g.

- IP Sender ("user list)
- Access Control
- Password Protection
- Certificate Management (selfsigned certificate, certificate request, root certificate, PKCS#12 certificate)

Currently SEH carries the following WLAN print servers in its portfolio:

| Models | Interfaces |
|---|---|
| **PS54a-G** | 1 x parallel, 1 x USB 2.0 High Speed (extendable to four) |
| **PS56** | 1 x EIO (for HP) |
| **PS159** | 1 x KUIO (for Kyocera Mita) |

## 8. LITERATURE


- Edney, Jon, et al.: Real 802.11 Security – Wi-Fi Protected Access and 802.11i; Addison-Wesley Professional: 2005.
- Gilster, Ron, et al.: Wireless LANs End to End; Wiley: 2002.
- Held, Gilbert: Securing Wireless LANs – A Practical Guide for Network Managers, LAN Administrators and the Home Office User; Wiley: 2003.
- Cam-Winget, Nancy et al.: „Security Flaws in 802.11 Data Link Protocols", Communications of the ACM, May 2003/Vol. 46, pp. 35-39, http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf.


## 9. INTERNET


Wi-Fi Consortium: http://wi-fi.org