# SEL-3021 Wireless Interface Security

Allen D. Risley and David Whitehead
*Schweitzer Engineering Laboratories, Inc.*

Original edition released February 2005

# SEL-3021 WIRELESS INTERFACE SECURITY

Allen D. Risley and David Whitehead, P.E.
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

## INTRODUCTION

The SEL-3021 Serial Encrypting Transceiver is a bump in-the-wire encryption device designed to add strong cryptographic security to new serial communications links and to provide an easy and effective security solution for existing serial communications networks. It is designed for use on both multi-drop SCADA networks and point-to-point communications links.

The SEL-3021 incorporates a cryptographically secured wireless local area network (WLAN) to perform diagnostic and maintenance functions without removing the SEL-3021 from service. See Figure 1. The wireless aspect of the device makes connection of the SEL-3021 to a Personal Computer (PC) simple and efficient. The wireless interface has been designed to be immune to malicious reconnaissance (port scans, war-driving, etc.). This paper addresses 802.11b Wired Equivalent Privacy (WEP), the SEL Security Application that cryptographically secures the data in the 802.11b data frames, and how these security features together protect and secure the SEL-3021 wireless port. We will show that the combination of WEP and the SEL Security Application provides a state-of-the-art encryption scheme that is statistically impossible to compromise.

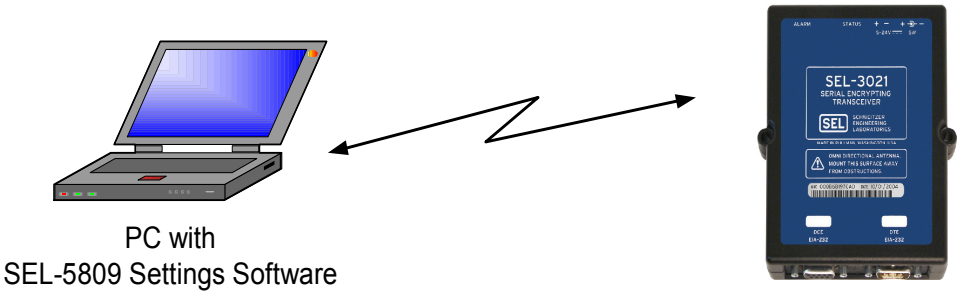


**Figure 1** SEL-3021 and PC With SEL-5809 Settings Software

## SEL-3021 WIRELESS INTERFACE SECURITY OVERVIEW

The SEL-3021 wireless operator interface and SEL-5809 Settings Software implement a two-part encryption system consisting of IEEE 802.11 WEP and the SEL Security Application. WEP is an encryption standard defined by the 802.11 specification and is available on most 802.11-enabled devices. The SEL Security Application consists of National Institute of Standards and Technology (NIST)-approved encryption and authentication algorithms that are cryptographically much stronger than WEP. Together, these two, independent security features provide a secure communications link between the SEL-3021 and the operator PC or Personal Data Assistant (PDA). Strengths of the WEP and SEL Security Application combination are as follows:

- A 104-bit WEP encryption function keeps out all but the most determined attackers. The following pages discuss the relative security of the WEP function.

- The SEL Security Application employs 128-bit AES encryption and 128-bit HMAC SHA-1 authentication. This application provides cryptographic security at greater than 128 bits of cryptographic key strength, using only FIPS 140-2 compliant cryptographic algorithms. The following pages discuss the SEL Security Application.

Figure 2 shows the relationship between WEP and the SEL Security Application.

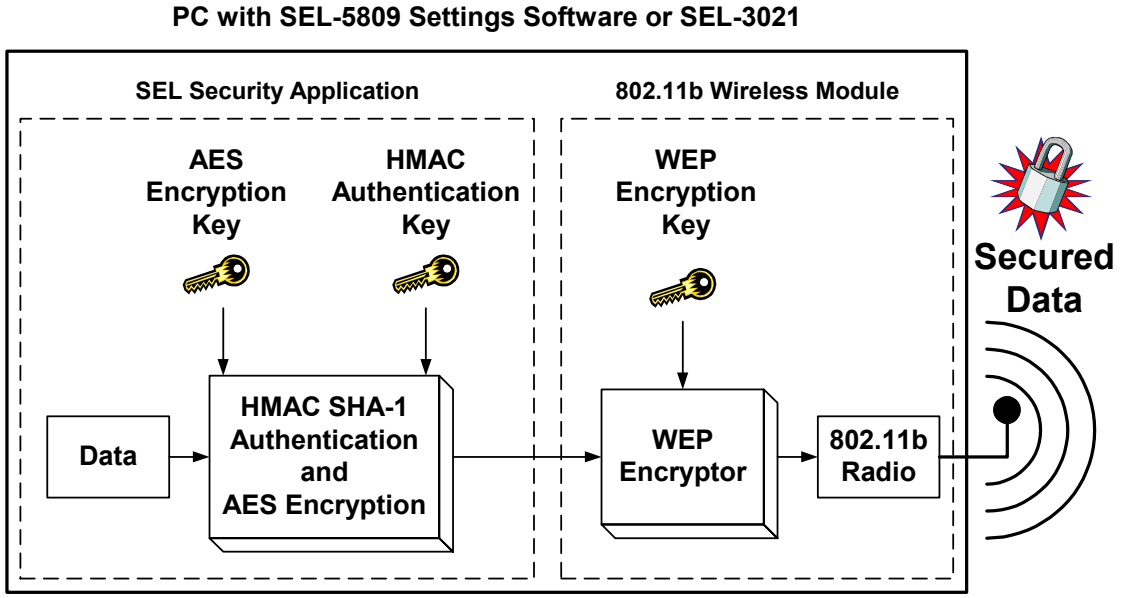


**Figure 2** Two Independent Layers of Cryptographic Security Protect The SEL-3021 Wireless Operator Interface

The decryption process of the SEL-3021 wireless interface consists of multiple cryptographic verifications. When the SEL-3021 wireless module receives a correctly addressed packet, the wireless module WEP decrypts the packet. The wireless module discards any packets that do not decrypt successfully. If the packets do WEP decrypt successfully, the wireless module passes resulting data frames to the SEL Security Application. The data frames must then AES decrypt and HMAC SHA-1 authenticate. If the SEL Security decryption or authentication fails, the SEL Security Application discards these data frames. In summary, before the SEL-3021 considers data to be valid, the data must AES decrypt, HMAC SHA-1 authenticate, and WEP decrypt correctly, or the data are discarded. The process is reversed for the transmission and encryption process.

The SEL-3021/SEL-5809 Settings Software includes the following wireless security features:

- **104-Bit Wired Equivalent Privacy (WEP) Encryption:** The WEP encryption function, provided by the 802.11b wireless LAN module, is always enabled and active on the SEL-3021.
- **128-Bit Advanced Encryption Standard (AES) Encryption:** Because of the relative weakness of the WEP encryption function, the SEL-3021 also incorporates an independent layer of AES encryption.
- **128-Bit HMAC SHA-1 Frame Authentication:** Every frame transmitted on the wireless operator interface is cryptographically authenticated to prevent malicious tampering and to guarantee acceptance of only those frames that authorized users transmit.

- **Message Replay Protection:** The SEL-3021 uses frame sequence numbers with HMAC SHA-1 authentication to ensure that individual frames cannot be retransmitted to cause malicious actions.
- **Session Replay Protection**: The SEL-3021 uses a robust challenge-response session authentication protocol to guarantee that wireless operator sessions cannot be replayed to cause malicious actions.
- **AES and HMAC Session Key Exchange:** The SEL-3021 exchanges unique, randomly generated encryption and authentication keys on each wireless session connection. This limits the amount of data protected by any single key value and strengthens the SEL-3021 against cryptanalytic attacks.
- **Wireless Session Password:** A configurable password is required to open a wireless connection with the SEL-3021. This password is never stored in the configuration software device image, so it cannot be compromised by theft of a configured maintenance PC containing the wireless encryption and authentication keys. In the event of a lost or stolen maintenance PC, this feature gives the system security officer time to change the cryptographic security parameters on the network.
- **Wireless Port Timeouts:** The SEL-3021 will not allow another wireless connection for a short period of time after any failed authentication attempt. This significantly reduces the rate at which a malicious individual can apply a brute force cryptographic key or password guessing attack.
- **Network Reconnaissance Protection:** The SEL-3021 will not reply to any network traffic that fails authentication. Because of this lack of response to unauthenticated network traffic, the SEL-3021 is not susceptible to ping sweeps.
- **Single Active Session:** The SEL-3021 allows only a single active session and rejects attempts to establish a second wireless connection. This feature ensures that only one user can change settings at any given time.
- **No Default Settings:** The SEL-3021 will remain in an initialization mode when any of the critical security parameters are set to the default, zeroized values. During this initialization mode, the SEL-3021 will disable the DTE serial port and the wireless operator interface and force the user to enter the initial encryption keys, authentication keys, and password values via a direct serial connection. This functionality ensures that critical security parameters are never transmitted over the 802.11b radio channel protected by insecure, factory default keys.

## IEEE 802.11 WEP SECURITY

The IEEE 802.11 designers included provisions for data encryption and authentication to provide what they considered strong data security and network access control. The Wired Equivalent Privacy (WEP) procedures outlined in the standard provide both functions. WEP encryption cryptographically scrambles the data contents of the Media Access Control (MAC) packet prior to transmission. The MAC packets can be intercepted, but the data scrambling the encryption process provides will, in theory, make the data payload and network headers (above the MAC network layer) incomprehensible. The encryption and decryption operations are a function of the original message data and a secret encryption key. For symmetric encryption algorithms, such as the RC-4 algorithm that WEP uses, the encryption key and decryption keys are identical. Several factors, including the following, determine the strength or security of the encryption process:

- The secrecy of the key
- The length of the key
- How often the key value changes
- The cryptographic strength of the encryption algorithm

Because the encryption and decryption keys are identical for symmetric encryption algorithms, the theft or deduction of the key value by a malicious individual will remove any protection WEP encryption offers. There are a few common methods for determining a key value. The would-be attacker can simply steal the key value in some manner. If that option is not available, the attacker can attempt to guess the key value. The difficulty of such a guessing, or brute-force attack, grows exponentially with the length of the key. The encryption process can be strengthened against key-guessing attacks through periodic changes to the key value. If someone ever guesses the key value, the attacker can only decrypt the data processed with that key. Changing the key value on a periodic basis can significantly reduce the data a single key processes. Finally, the cryptographic strength of the encryption algorithm determines how difficult it is to compromise portions of the encrypted messages. If the algorithm is cryptographically sound, it is extremely difficult mathematically to compromise the key value or message contents from publicly available knowledge. Publicly available knowledge includes the encrypted message itself, known as ciphertext, and prior knowledge of the contents of the message. This prior knowledge, for example, could include the statistics of English text or knowledge of the location and value of an encrypted header field. The IEEE 802.11 standard specifies that if the incoming packet cannot be decrypted properly, it must be dropped and ignored. All hosts must know the value of the secret encryption key prior to being granted network access. The network designer controls the dissemination of the key value and, therefore, controls who has access to the WEP-protected network.

## WEP Security Flaws Explanation

WEP is based on a two-part encryption algorithm called RC-4. The first stage of the encryption process, known as the Key Scheduling Algorithm (KSA), takes a string of key bits as input and forms an output initialization string. The second stage, known as the Pseudo-Random Generation Algorithm (PRGA), produces a pseudo-random bitstream of arbitrary length. The value of this string of bits depends on the initializing permutation the KSA produces. Note that a given KSA input will always produce the same PRGA output. The designers of the IEEE 802.11 standard wanted the process of decrypting a single packet to be independent of all previous and future packets. Because of this requirement, the output of the PRGA function has to be reset at the beginning of every packet. If this were done without also changing the input to the KSA function, the encryption stream would be identical for every packet and the resulting encryption process would be trivially broken. Because of this, the input to the KSA function is a concatenation of a secret key (104 bits in the case of the SEL-3021 wireless operator interface) with a 24-bit Initialization Vector (IV). By changing the IV on every packet, the WEP encryption process ensures that the probability of any two, randomly chosen packets being encrypted with the same PRGA output (known as an “IV collision”) is sufficiently low.

For each data packet, the concatenation of the key and IV serves as the input to the RC-4 algorithm, which produces a string of pseudo-random encryption bits (with a length equal to the length of the original data packet). To perform the encryption operation, the encryption bit string is added modulo 2 (XOR) to the original contents of the packet. The IV used during the encryption process is then concatenated with the resulting ciphertext to form the final message. A

major contributor to the relative weaknesses of the WEP encryption process is the fact that the IV is appended to the ciphertext and transmitted unencrypted. The following text explains the details of these weaknesses.

In August of 2001, Fluhrer, Mantin, and Shamir published formal proofs of some potential weaknesses in the RC-4 algorithm [1]. In a later paper [2], Stubblefield, Ioannidis, and Rubin demonstrated that the WEP algorithm was designed in such a way as to contain the worst of the weaknesses that Fluhrer, Mantin, and Shamir's paper outlined. Furthermore, Stubblefield, Ioannidis, and Rubin demonstrated that a passive attack could be used to successfully determine a 104-bit secret key in just a few hours on a moderately loaded wireless LAN. Based on these results, Stubblefield, Ioannidis, and Rubin urged network designers to assume that the IEEE 802.11 link layer offers very little security and to employ additional security measures in addition to WEP. The SEL-3021 design incorporates these additional security measures in the form of cryptographically sound 128-bit AES encryption and HMAC SHA-1 authentication (see The SEL Security Application below for further explanation).

The weaknesses Fluhrer, Mantin, and Shamir described are a direct consequence of the RC-4 algorithm. These researchers demonstrated that there are large classes of keys for which a very small portion of the key determines a very large portion of the KSA output. Furthermore, Fluhrer, Mantin, and Shamir showed that the PRGA function is weak in the sense that known patterns in the KSA output are transformed into predictable patterns in the first byte of the PRGA output. In other words, for a large number of keys, the first byte of the PRGA output is highly correlated with a very small number of key bits. This correlation can be used, in certain situations, to guess the value of the secret key. The implementation of the WEP algorithm ensures that these weaknesses can be exploited in an effective manner. Because the WEP algorithm transmits the IV unencrypted with each packet, an attacker has full visibility of three bytes of the KSA input. Furthermore, the first encrypted byte of almost every IEEE 802.11 packet is a known constant. This is a direct consequence of the fact that the first encrypted byte of an IEEE 802.11 packet is the Destination Service Access Point (DSAP) field of the LLC header, which has a value of 0xAA (hexidecimal) for all packets containing TCP/IP protocol data. This known value allows an attacker to recover the first byte of the PRGA output for virtually every packet by simply XORing the first byte of ciphertext with the value 0xAA. Someone could attack WEP by observing the IV values of each encrypted packet transmitted on the network to find weak values that result in the leak of information about the value of a particular secret key byte into the first byte of the PRGA output. An attacker could repeat this process to determine with sufficiently high probability all bytes of the secret key.

The 802.11b wireless LAN protocol provides a very effective wireless networking solution, which has resulted in steadily growing popularity of 802.11b-compliant networking devices, or access points (APs) since the introduction of the standard. This great popularity of such technology has fueled the development of software utilities designed to locate active wireless APs and identify whether WEP encryption is enabled on these devices.

If an attacker finds an AP protected by WEP encryption but interesting enough to warrant further investigation, the attacker can attempt to crack the WEP key. Several tools can passively capture normal wireless traffic on a target network and exploit the security flaws previously discussed to potentially determine the WEP encryption key used to secure the transmitted data. These tools have the potential to guess a WEP key by passively observing as few as four million network packets. Clearly, the time that this process takes is dependent on the average amount of network traffic that the 802.11 wireless network transmits.

## WEP Security Flaws Implications

Because of the previously discussed flaws, the WEP encryption function the 802.11 standard specifies does not provide the advertised 104 bits of cryptographic key strength. It does, however, provide a rather significant barrier to a potential attacker. It is difficult to determine the WEP key from a lightly loaded wireless network. A wireless connection between a maintenance PC and an SEL-3021 will only transmit network packets while the session is open and data are being actively exchanged between the PC and the SEL-3021. Under normal conditions, a potential attacker would have to capture encrypted packets for an extremely long time to analyze the few million packets necessary to determine the WEP key and defeat the WEP encryption function. If an attacker successfully determines the WEP encryption key, the contents of all network packets transmitted between a maintenance PC and an SEL-3021 device would still be protected by the cryptographically strong encryption and authentication the SEL-3021 AES and HMAC SHA-1 functions provide (see The SEL Security Application section below for further explanation). The cryptographic community has scrutinized the AES encryption and HMAC SHA-1 authentication functions carefully, but cryptographers have been unable to find any security flaws similar to those contained in the WEP encryption function.

## SEL-3021 WEP Security Analysis

As described previously, a passive key guessing attack on the WEP encryption function requires an attacker to capture and analyze several million WEP-encrypted TCP/IP network frames. The attack outlined in "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" [2], required 4,000,000 to 6,000,000 captured frames before the WEP encryption key could be determined successfully. A typical wireless session between the SEL-5809 Settings Software and an SEL-3021 device consists of a connection authentication dialog, a configuration upload from the SEL-3021 to the PC, periodic diagnostics data and TCP/IP "keep alive" frames throughout the duration of the active session, and, finally, a single settings download from the PC to the SEL-3021 to program the device with any new settings. The session authentication, configuration upload, and configuration download dialogs generate approximately 150 WEP-encrypted TCP/IP frames. In addition, the diagnostics and "keep alive" functions generate approximately four WEP-encrypted TCP/IP frames per second. If we assume that a single wireless operator interface session is open for 10 minutes, we can conclude that a single typical session will generate approximately 2,550 WEP-encrypted TCP/IP frames. To capture the 4,000,000 WEP-encrypted frames necessary to potentially determine the WEP encryption key, an attacker would have to intercept and analyze all frames exchanged during 1,569 typical wireless operator interface sessions. It is very unlikely that a user would have to change the settings on the SEL-3021 this many times in the lifetime of the SEL-3021 device. We must note, however, that it is possible to take the frames captured from several different SEL-3021 devices and combine these frames into a single analysis if the active WEP key value is identical for all of the devices.

The SEL-3021 also provides extensive real-time diagnostics capability. It is possible that you might want to receive continuous diagnostics information during a series of extended wireless operator interface sessions. As stated before, the SEL-5809 Settings Software and the SEL-3021 device exchange WEP-encrypted frames at approximately four frames per second while the session is open. To capture the 4,000,000 frames necessary to potentially compromise the value of the WEP encryption key, an attacker would have to intercept and analyze all frames transmitted during 11.57 days of active wireless session activity. We do not expect that an operator would ordinarily keep a wireless session active unless the operator is directly evaluating the state of the SEL-3021 device. It would, therefore, be very difficult for someone to capture enough wireless interface traffic to launch a successful key guessing attack against the SEL-3021.

### SEL-3021 WEP Conclusion

As we have shown, WEP in the SEL-3021 provides a significant cryptographic barrier to an attacker. WEP encryption is always enabled (and cannot be disabled) in the SEL-3021 to prevent passage of all traffic that does not properly pass the WEP decryption function (i.e., all traffic that was not encrypted with the correct WEP key) to the SEL-3021 network stack. Also the Shared Key Authentication protocol of the 802.11b standard is enabled in the SEL-3021. This feature requires that both the PC and the SEL-3021 have the same WEP key before the two devices establish a connection. Thus WEP provides an independent security barrier that a potential attacker must compromise before there can be any direct attack on the SEL Security Application. The SEL Security Application uses proven cryptographic security algorithms that will stand up to any direct attack (see the section below).

## THE SEL SECURITY APPLICATION

The SEL Security Application consists of an authentication and encryption scheme that provides very strong data security. Authentication verifies message integrity (i.e., the message has not been altered). Encryption conceals the contents of the message. The combination of the two security techniques provides a state-of-the-art encryption and authentication system with a key strength greater than 128 bits. Proof of the security strength is detailed in the following sections.

### HMAC SHA-1 Authentication Overview

The HMAC SHA-1 function provides protection against frame alteration and ensures (with extremely high probability) that the digital integrity of every frame remains intact. With a 128-bit-long authentication key, the HMAC SHA-1 function also provides strong frame authentication capability for confirmation that an authorized device transmitted the frame.

The National Institute of Standards and Technology (NIST) developed the SHA-1 one-way hash algorithm in 1993. NIST developed the Keyed-Hash Message Authentication Code (HMAC) algorithm in 2002. The SEL-3021 uses the proven SHA-1 one-way hash algorithm to form the NIST-approved HMAC SHA-1 keyed hash function.

The HMAC SHA-1 function takes a variable-length message and an authentication key as input and generates a 160-bit-long, fixed-length hash output value. The hash output is a condensed fingerprint, or signature, of the message input (see Figure 3).

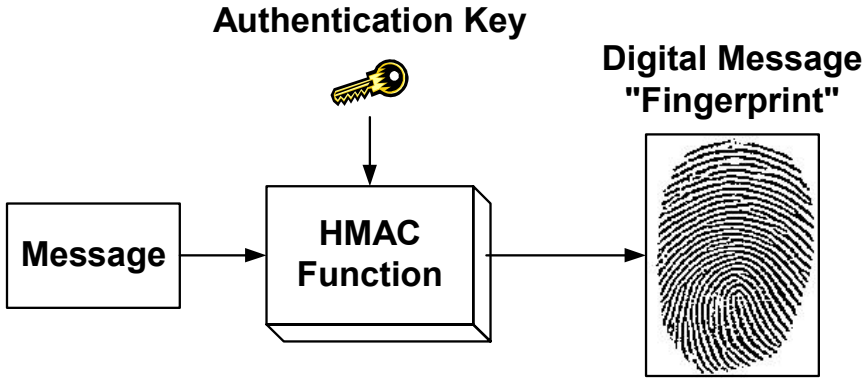


**Figure 3** Operation of the HMAC SHA-1 Keyed Hash Authentication Function

The 128-bit-long secret key gives the HMAC SHA-1 algorithm a strong built-in authentication capability. If an attacker changes the contents of the message, then the hash value appended to the message would not match the value that results from a newly calculated hash value over the new, altered message. Because the HMAC SHA-1 function is keyed (i.e., uses a secret authentication key to form the hash output), an attacker without knowledge of the authentication key value would be unable to recalculate a new, valid hash value over the altered message appended to the new message to hide the fact that the message has been altered.

To produce a cryptographically secure signature of a message, NIST designed the SHA-1 hash function to have the following properties:

- Given the SHA-1 hash function, $H(m)$, and its output, $h$, it is extremely difficult to derive a message, $m$, such that $H(m) = h$.
- Given a message, $m$, it is extremely difficult to find another message, $m'$, that produces the same SHA-1 hash output.

The first condition states that the output of the SHA-1 hash function used in the HMAC authentication function does not give away any clues about the form, or classes, of messages that would likely produce the same hash value. The second condition, known as collision-resistance, states that there is no bias in the mapping of inputs to outputs that would aid an attacker in finding messages that produce identical SHA-1 hash values. Both conditions make it functionally impossible (given all realistic resources) to alter a message in such a way as to produce the same hash value. The HMAC specification provides a cryptographically secure way to combine the secret authentication key and the protected message into the SHA-1 hash function input to produce a key-dependent message fingerprint.

## AES Overview

The AES encryption function uses a 128-bit-long secret key and scrambles the contents of each frame prior to transmission to provide cryptographically strong data confidentiality.

Encryption is the process of transforming a digital message from its original form into a form that an unauthorized individual cannot interpret. The output of the encryption process is a function of the message and an encryption key (see Figure 4).

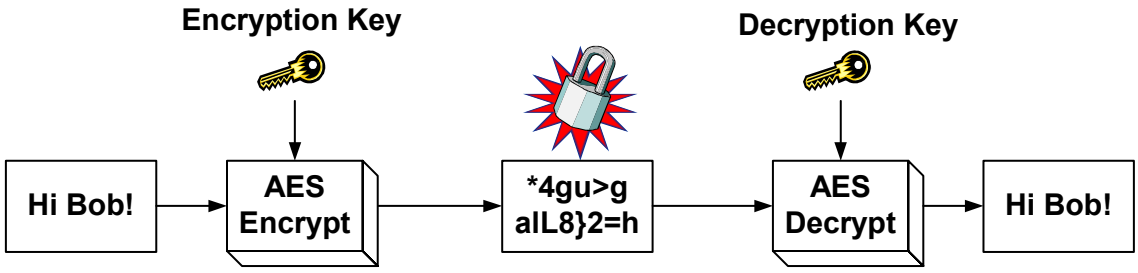


**Figure 4** Operation of the AES Encryption Function

This encryption process must be completely reversible by an authorized individual with access to the secret decryption key. Authority to read a message is only granted by sharing knowledge of the secret decryption key. Ideally, only individuals with knowledge of the decryption key can reverse the encryption operation and interpret the protected message. There are two main classes of encryption functions. Symmetric key encryption relies on the same secret key value, K, to perform both the encryption and decryption transformations. Asymmetric key encryption, on the

other hand, uses a different key for encryption and decryption. For example, asymmetric encryption might use K1 for encryption and K2 for decryption. The AES encryption algorithm the SEL-3021 uses is a symmetric block cipher, with an encryption/decryption key size of 128 bits.

The Advanced Encryption Standard (AES) is the latest encryption standard adopted by the National Institute of Standards and Technology (NIST). In 1997, NIST challenged the cryptographic community to develop the next generation encryption algorithm to replace the aging DES and 3DES encryption standards. In 2000, NIST chose the Rijndael encryption algorithm as the AES encryption standard. During the evaluation of candidates for the AES standard, some of the best cryptanalysts in the world analyzed and approved Rijndael. Since NIST adopted the standard in 2001, AES has proven to be very effective against known attacks.

## Combined HMAC SHA-1 and AES Encryption Security

Every frame transmitted over the SEL-3021 wireless operator interface is authenticated with an HMAC SHA-1 keyed hash digest and encrypted with the AES encryption algorithm (both algorithms are described in detail in the HMAC SHA-1 Authentication and AES Overview sections above). As shown in Figure 5, the SEL-3021 first forms the HMAC SHA-1 hash output from the original frame data payload and the 128-bit authentication key. This keyed message fingerprint is then appended to the end of the frame data payload, and the resulting composite message is encrypted by the AES encryption function through use of a separate, 128-bit encryption key (the authentication key and encryption key are completely independent).

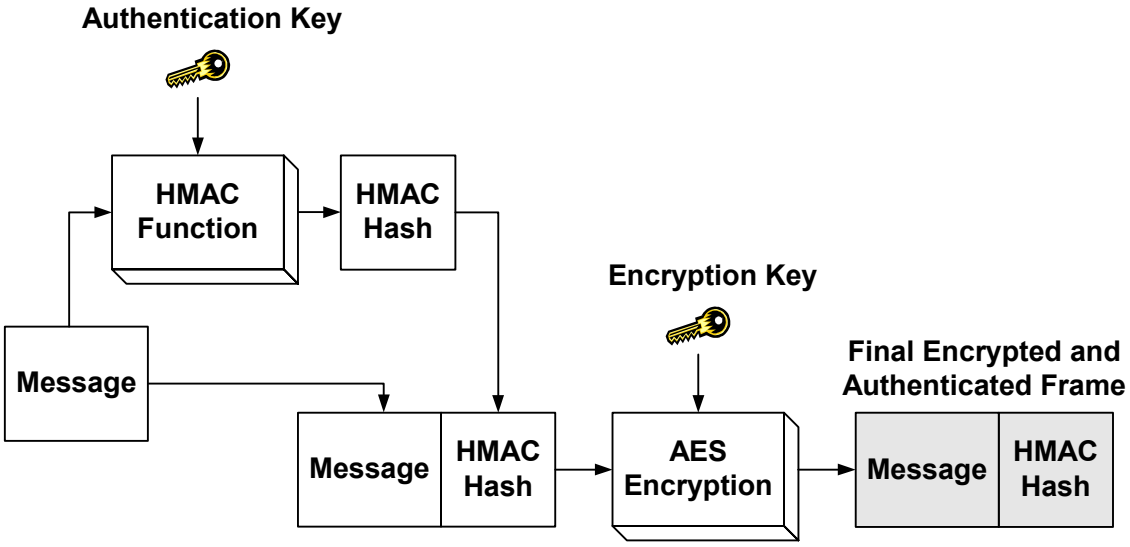


**Figure 5** SEL-3021 Security Application Overview

Upon receipt of any frame on the wireless operator interface, the SEL-3021 uses the programmed 128-bit secret encryption/decryption key to AES decrypt the entire frame. The SEL-3021 then uses the programmed 128-bit authentication key to calculate the HMAC SHA-1 keyed hash value over the payload (message) portion of the received frame. If the calculated HMAC SHA-1 hash output does not match the received message fingerprint, the SEL-3021 rejects and ignores the message.

This arrangement protects the original frame data payload from malicious alteration, authenticates the origin of the frame as a device with knowledge of both the encryption and authentication keys, and protects the contents of the frame data payload from theft.

## SEL Security Application Analysis

Cryptographic experts have analyzed the AES and HMAC SHA-1 cryptographic functions. This analysis process began before NIST accepted each of the functions as standards, and it will continue as long as these standards remain in use. To date, the AES encryption and HMAC SHA-1 authentication algorithms have withstood all public scrutiny in the sense that they provide the advertised level of security. In other words, an AES encryption function with a 128-bit key will, by all analysis to date, provide data confidentiality at a cryptographic strength of 128 bits (the discussion in the following text addresses this concept). Cryptographically sound hash functions, such as SHA-1, are expected to provide message integrity functionality at a strength equal to half the size of the hash output. Because SHA-1 has a hash output length of 160 bits, it should produce message integrity functionality at a cryptographic strength of 80 bits. To date, SHA-1 has maintained the expected cryptographic strength. Finally, the HMAC function has also withstood all cryptographic analysis, in the sense that it has proven to be an effective and secure method of mixing a secret authentication key into the SHA-1 hash output. We will analyze the implications of these statements in the following text.

As stated previously, the AES encryption function has, thus far, provided data confidentiality at a cryptographic strength equal to the size of the encryption key. To successfully guess a 128-bit key, such as the key the SEL-3021 uses, an attacker would have to try an average of $2^{127} = 1.7 \bullet 10^{38}$ keys before finding the correct value (assuming that all key values are equally likely). This is a staggering number of potential key values! If an attacker could test one million potential keys per second, it would take more than $5.39 \bullet 10^{24}$ years, on average, to guess the correct key value (note that the universe is estimated to be only $10^{13}$ years old)! In reality, the time that it would take to launch an effective key guessing attack against the SEL-3021 would be even longer, because the wireless interface on the SEL-3021 times out briefly when an authentication failure occurs. Because of the wireless interface timeout, the maximum rate of a key guessing attack against the SEL-3021 is much less than one million keys per second.

Because the SEL Security Application AES encrypts the HMAC-keyed authentication digest in every frame, both the AES encryption key and the HMAC SHA-1 authentication key must be compromised simultaneously to send data to the SEL-3021. For such a situation, an attacker would have to guess two independent 128-bit key values, which is the same as guessing a single, 256-bit key. To guess a key of this size, an attacker would, on average, have to make $2^{255} = 5.79 \bullet 10^{76}$ key guessing attempts. If an attacker could test one million potential keys per second, it would take more than $1.83 \bullet 10^{63}$ years, on average, to guess both the authentication key and the encryption key values. The analysis just described suggests that it is statistically impossible to launch a key guessing attack against the SEL-3021 device that would result in compromise of the system.

Even if someone were to steal a maintenance PC with the wireless interface encryption and authentication keys programmed and saved on the PC hard drive, an attacker would have to crack the SEL-3021 connection password to use the stolen computer to successfully authenticate with the SEL-3021. To launch a password guessing attack, an attacker would have to repeatedly send an initial session request frame and enter the password guess into the SEL-5809 Settings Software dialog box.

If the entered password value is incorrect, the SEL-3021 terminates the session authentication dialog after receiving Frame 3 of the authentication dialog (see Figure 6 and the discussion in the section SEL-3021/SEL-5809 Wireless Interface Session Authentication Dialog). If the authentication dialog fails at any point, the SEL-3021 performs a timeout of the wireless operator

interface and refuses any session connection requests for five seconds. This limits the rate of a password guessing attack to one guess per five seconds.

The SEL-3021 accepts password entries between 6 and 80 characters in length. These passwords can contain all 96 printable ASCII characters (including the Space character). If we assume that the security officer has programmed strong passwords into the SEL-3021, an attacker would not be able to use a typical password guessing attack dictionary to limit the number of required password guesses. In this case, all possible password values would be equally likely and the attacker would have to launch a brute-force password guessing attack by sending all possible password values to the SEL-3021, one at a time. Table 1 shows the number of potential password values (i.e., the maximum number of guesses that an attacker will have to make) and the average number of years required to launch a successful brute-force password guessing attack on the SEL-3021 as a function of the length of your programmed password value. The value representing the average number of years required to successfully guess the SEL-3021 connection password was derived under the assumption that all potential password values are equally probable (i.e., you do not program a password value that is likely to be in an attack dictionary). Such strong passwords do not form a word, slang term, or other meaningful value. A strong password also contains a mixture of alphanumeric characters (numbers and upper and lowercase letters) and non-alphanumeric characters (punctuation characters, backslash, space, etc.).

**Table 1** Number of Years Required to Guess an SEL-3021 Password

| Password Length | Number of Possible Password Values | Average Number of Years Required to Guess the Password (Assuming Strong Password Choice) |
|---|---|---|
| 6 | $7.91 \cdot 10^{11}$ | $6.27 \cdot 10^{4}$ |
| 7 | $7.59 \cdot 10^{13}$ | $6.02 \cdot 10^{6}$ |
| 8 | $7.29 \cdot 10^{15}$ | $5.78 \cdot 10^{8}$ |
| … | … | … |
| 80 | $3.86 \cdot 10^{158}$ | $3.06 \cdot 10^{151}$ |

Even with a strong, six-character password, an attacker could expect to spend more than 60,000 years trying to launch a successful brute-force password-guessing attack on the SEL-3021. Such a brute-force password-guessing attack is statistically impossible because of the potential strength of the SEL-3021 connection passwords (very long password length with the password consisting of a very large number of possible characters), and the password-guessing rate limit that the five-second wireless port timeout imposes on all connection authentication failures.

## CONNECTION AUTHENTICATION AND SESSION REPLAY PROTECTION

### SEL-3021 Wireless Port Status Prior to Security Parameter Initialization

The SEL-3021 uses two access levels for monitoring and configuration. Each access level has the following security parameters: 128-bit encryption key, 128-bit authentication key, and a password containing as many as 80 characters. Also included in the security parameters are the 104-bit WEP keys. From the factory, cryptographic security parameters are zeroized. At power up, the SEL-3021 determines if the cryptographic security parameters are set to trivial (zero) values. If these parameters are set to trivial values, the 802.11b wireless port is disabled. If the SEL-3021 is initialized with zeroized values, or if any of these initial security parameters are left at a zeroized

value, the device will not leave the initialization mode, and the wireless port will remain disabled. Following entry of non-zeroized security parameters, the SEL-3021 enables the wireless module and enables both WEP and the SEL Security Application. This ensures that data are never transmitted via the 802.11b interface with default/trivial encryption keys.

## SEL-3021 Security Parameters and Passwords

The SEL-5809 Settings Software is necessary to initiate a wireless session. The SEL-5809 Settings Software must be programmed with identical encryption and authentication security parameters as the SEL-3021 to which it will be connected. Furthermore, you must enter into the SEL-5809, when prompted, the same password stored in the SEL-3021. Note that neither a PC nor a PDA stores this password; the user must enter this password from memory. Because the PC does not store password values, no one can use just a PC or PDA to connect successfully with the SEL-3021 without direct knowledge of the correct password value. This remains true even if someone attempts a connection through use of a stolen PC with the correct wireless authentication and encryption keys programmed into the device image.

## SEL-3021/SEL-5809 Wireless Interface Session Authentication Dialog

To begin a wireless operator interface session, the PC or PDA must authenticate with the SEL-3021 to prove that it has been programmed with the exact values of the expected authentication key and encryption key, and that you entered the correct password. Figure 6 provides an overview of the session authentication dialog between a maintenance PC with the SEL-5809 Settings Software installed and an SEL-3021 device. Each frame of this five-frame dialog is protected by the encryption and authentication methods described previously. Because of these protection methods, the data in each frame are secured by strong AES encryption and the SEL-5809 Settings Software, and the SEL-3021 can verify that an authorized device (i.e., a device with direct knowledge of the encryption key and authentication key values) sent every frame.

The connection dialog begins with a connection request frame (Frame 1 in Figure 6) that is encrypted and authenticated with encryption and authentication keys programmed into the SEL-5809 Settings Software device image. Upon receiving the connection request, the SEL-3021 decrypts and authenticates the frame. If the authentication fails, indicating that the session request came from other than an authorized user (i.e., a PC programmed with the appropriate AES encryption and HMAC SHA-1 authentication keys), the SEL-3021 ignores the session request and remains silent. Note that the initial connection frame must be directed at the correct User Datagram Protocol (UDP) port on the wireless TCP/IP interface of the SEL-3021 transceiver. Because the UDP protocol does not require a connection handshake, as does TCP protocol, the SEL-3021 only transmits a TCP/IP frame in response to a fully authenticated connection request frame. This feature ensures that the SEL-3021 is immune to traditional port mapping and network reconnaissance techniques such as ping sweeps, TCP SYN scans, or TCP FIN scans.

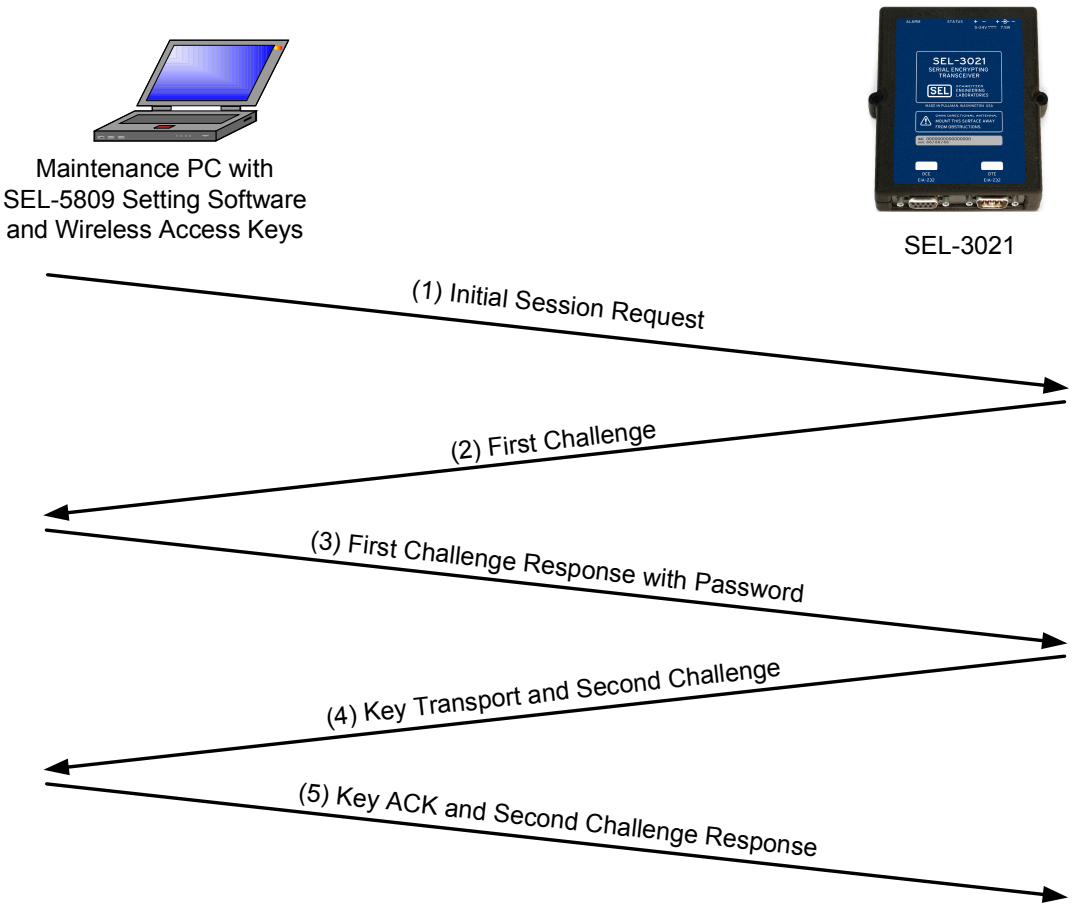


**Figure 6** Wireless Interface Session Authentication Dialog

If the initial connection request frame passes the authentication process, the SEL-3021 generates a large, random challenge value and transmits it to the PC (Frame 2 in Figure 6). Upon receipt of the First Challenge frame, the PC must insert the received challenge value into a new encrypted and authenticated frame and transmit it to the SEL-3021 (Frame 3 in Figure 6). In addition, this First Challenge frame contains the password information you entered in the SEL-5809 Settings Software session connection dialog box. When the SEL-3021 receives this frame, it decrypts and authenticates it. If the authentication fails, again indicating that the session request came from an unauthorized user, the SEL-3021 terminates the session and resets the session connection dialog. If the frame passes authentication, the SEL-3021 compares the transmitted password information with the password value stored in the SEL-3021 settings. It is important to note that if the transmitted password information indicates that the user entered the wrong password, or if the decrypted challenge value does not match the challenge value transmitted in Frame 2 of the connection dialog, the SEL-3021 again terminates the session and resets the connection dialog.

- The password you entered in the SEL-5809 Settings Software must match the password value stored in the SEL-3021 device, or the session connection will fail. This guarantees that a stolen maintenance PC programmed with the correct encryption and authentication keys cannot be used to connect to the SEL-3021 without the user having direct knowledge of the programmed password value stored in the SEL-3021 (the SEL-5809 Settings Software never stores the password value on the PC hard drive).

- The large, random challenge value that the SEL-3021 formed and transmitted in Frame 2 of the connection dialog is, with very high probability, different for every wireless session. Because of this large, random value, a malicious individual cannot capture a previous session dialog and use the captured packets to reconnect to the SEL-3021 (known as a session replay attack). If someone attempted such an attack, the challenge value transmitted in the First Challenge Response with Password frame (Frame 3 in Figure 6) would not match the challenge value the SEL-3021 issued in the First Challenge frame (Frame 2 in Figure 6), and the SEL-3021 would terminate the connection attempt.

If the connection dialog succeeds up to this point (i.e., passes all authentication mechanisms and session replay protection mechanisms described previously), the SEL-3021 generates another random challenge value, a random session encryption key, and a random session authentication key and transmits these values in Frame 4 of the session connection dialog. The SEL-3021 uses these session keys, protected from interception by SEL Security Application cryptographic mechanisms described in the previous sections, to encrypt and authenticate all configuration frames transmitted between the PC and the SEL-3021 after the five-frame session authentication dialog succeeds.

Upon receiving the Key Transport and Second Challenge frame, the PC must insert the transmitted second challenge value into the final frame of the session connection dialog (Frame 5 in Figure 6) and transmit the frame to the SEL-3021. To complete the session authentication dialog successfully, the decrypted and authenticated challenge value the SEL-3021 received in Frame 5 must match the value the SEL-3021 transmits in Frame 4. This requirement for matching values forms a second, independent layer of protection against session replay attacks.

If the final frame authenticates correctly and the second challenge values match, the SEL-3021 opens a wireless operator interface connection with the PC. All configuration frames transmitted between the two devices after successful completion of the session authentication dialog previously described will be encrypted and authenticated through use of the session encryption and authentication keys exchanged in the dialog.

The SEL-3021 connection authentication provides strong security against a number of potential threats. We summarize the security features of this connection authentication dialog as follows:

- There are two, independent challenge/response exchanges to prevent session replay attacks.
- There is strong protection against threats posed by maintenance PC theft. The user must enter from memory, the correct connection password to successfully authenticate to the SEL-3021 (the connection password is never stored on the maintenance PC).
- Unique session encryption and session authentication key exchanges limit the number of frames protected by the programmed operator and security officer role encryption and authentication keys. This makes the SEL-3021 more resilient to cryptanalytic attacks.

## Frame Replay Protection

Every frame in a given wireless operator interface session contains a sequence number field. The value in this field increments every time a frame is transmitted over the interface. The SEL-3021 will not accept any frame that contains a sequence number value that is less than, or equal to, the sequence number value received in the last frame. It is exceedingly difficult to maliciously alter the sequence number in any given frame to bypass this functionality because the sequence number field is protected by the strong cryptographic authentication mechanisms provided by the

HMAC SHA-1 function. Because of the protection these mechanisms provide, an attacker cannot capture a frame, previously transmitted in a given wireless operator interface session, and resend the frame to the SEL-3021 to cause harmful actions.

## CONCLUSIONS

Two independent layers of cryptographic security protect the SEL-3021 wireless operator interface: the 802.11b wireless interface module WEP encryption function, and the AES encryption and HMAC SHA-1 authentication functions in the SEL Security Application. For an attacker to compromise the SEL-3021 operator interface, both the WEP encryption and the SEL Security Application have to be defeated. As we have seen, the probability of an attacker accomplishing this is statistically impossible.

## REFERENCES


[1] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[2] A. Stubblefield, J. Ioannidis, A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," AT&T Labs Technical Report TD-4ZCPZZ, August 21, 2001.


## BIOGRAPHIES

**Allen D. Risley** is a Senior Research Engineer at Schweitzer Engineering Laboratories in Pullman, WA. Prior to joining SEL, he worked at Advanced Hardware Architectures as a Senior Research Engineer specializing in information theory and forward error correction. He received his Master of Science degree in Electrical Engineering from Washington State University in 1998. He has presented papers at the 1998 Conference on Information Sciences and Systems, the 2001 ISCTA conference, as well as many electric power industry conferences. His work has been published in the *Proceedings of the International Symposium on Information Theory* and the *IEEE Transactions on Communications*.

**David Whitehead, P.E.** is the Chief Engineer, GSD Division, and a Principle Research Engineer for Schweitzer Engineering Laboratories. Prior to joining SEL he worked for General Dynamics, Electric Boat Division as a Combat Systems Engineer. He received his BSEE from Washington State University in 1989 and his MSEE from Rensselaer Polytechnic Institute in 1994. He is a registered Professional Engineer in Washington State and Senior Member of the IEEE. Mr. Whitehead holds six patents with several others pending. He designs and manages the design of advanced hardware, embedded firmware, and PC software.



20050214
TP6196-01