More About
- Bulletins
- Challenges
- Crypto FAQ
- CryptoBytes
- RSA Algorithm
- PKCS
- Advanced Encryption Standard
- Tech Notes
- Staff & Associates
- Standards

WEP Fix using RC4 Fast Packet Keying

Why is WEP Broken?
The weakness in WEP stems back to a key derivation problem in the standard. Because WEP encryption is based on the RC4 stream cipher, it is important each packet have a different WEP key. While the WEP standard had specified using different keys for different data packets, the key derivation function (how to derive a key from a common starting point) was flawed. Simply put, the keys for different data packets were too similar. Hackers could exploit this similarity to extract information about the shared secret after analyzing a modest number of packets. Once the shared secret was discovered, a malicious hacker could decrypt data packets being passed along the exposed network.

Drilling into the problem at a lower level, the vulnerabilities exposed in WEP can be traced back to two main problems: (1) the limitations of the initialization vector (IV) combined with (2) weaknesses in how packet encryption keys are derived from the initialization vector when a secret key is shared between a wireless LAN client and an access point. IV collisions produce identical WEP keys when the same IV is used with the same shared secret key for more than one data frame and this is the weakness attackers exploit.

Is the threat real?
Yes. The report made by Scott Fluhrer, Itsik Mantin and Adi Shamir [FMS01] describing several weaknesses in the key scheduling algorithm of WEP also proposed attacks for exploiting those weaknesses. Based on this report, Stubblefield, Ioannidis and Rubin [SIR01] implemented one of the attacks to demonstrate that WEP is very vulnerable "in practice" and not just "in theory".

Is the WEP threat related to a weakness in the RC4™ algorithm?
No. WEP currently deployed in most WLAN hardware today uses RSA Security's RC4 algorithm for encryption. The attacks against WEP were not a result of a weakness of the algorithm, but instead a weakness in WEP key derivation that produced weak RC4 keys that were very similar for different data packets.
· RC4 is the popular algorithm protecting the millions of users who access secure Web pages and send data via the SSL/TLS protocol. These protocols are secure and RC4 in SSL has never been broken.

- In the SSL protocol, keys are produced for each session and not each data packet, as required in WEP, so there is time to derive unrelated keys with a hash function.
- In WEP, unrelated keys are needed on each packet of data encrypted with RC4 for the highest level of security.
- WEP produces RC4 keys that were too similar and easy to attack. WEP in its current form is flawed because it produces weak RC4 keys.

The new solution proposed by RSA Security and Hifn outlines a way to rapidly produce packet keys for the RC4 algorithm where a unique RC4 key is attached to each data packet.

What is the Fast Packet Keying Solution?

The Fast Packet Keying solution uses a hashing technique that rapidly generates a unique RC4 key for each packet of data sent over the WLAN.
The solution consists of:

- An encryptor and decryptor that share a RC4 128-bit secret key. This key is called the temporal key (TK)
- An encryptor and decryptor that uses the RC4 stream cipher
- An initialization vector (IV) value that is NOT used more than once with each TK

The solution involves a special hash function that is implemented in two phases.

Phase one involves key mixing where the transmitter address (TA) is mixed into the TK to ensure that the various parties encrypting with the TK use different key streams. By mixing the TA and the TK, a different set of keys is used by each party. Traffic sent by a station to the access point will use a different set of keys than traffic sent by the access point to the station. This output is typically cached to improve performance and can be reused to process future packets with the same TK and TA.

Phase two mixes the output of the first phase with the IV and generates a unique per-packet key for each data packet. To avoid any repetition of keys, a different initialization vector is used for each packet encrypted under the TK.

Please click here to see a graphical representation.

For more detail on the temporal key hash technique, see Document Number 550r2 entitled "Temporal Key Hash" submitted by Russ Housley of RSA Security and Doug Whiting of Hifn at www.ieee802.org.

Is this a new technology?
Yes. This is the first time this keying technique has been used to produce RC4 keys on a per-packet basis.

What are the performance issues?
The fast packet keying solution was selected over more traditional hashing techniques because of its ability to generate secure keys rapidly with RC4. This can be attributed to the fact that the output in phase one can be cached. This allows a significant performance improvement over traditional hashing techniques.

Because Phase 1 output can be cached, only the first packet must process Phase 1 and Phase 2. Subsequent packets may generate per packet keys using only the cached output of Phase 1 and mixing this output with the 16 bit IV in Phase 2. This is secure for up to 65,535 packets, after which the next packet must process Phase 1 and Phase 2 again where the output from Phase 1 may be cached and used to generate unique RC4 keys for the next 65,535 packets.

How does this solution affect the Wireless LAN market?
The solution announced by RSA Security and Hifn outlines a fix for the broken WEP encryption standard and will be of interest to vendors of wireless LAN equipment. These vendors will now be able to distribute a software patch to their end customers that will provide the highest level of security and interoperability and replace the broken WEP protocol.

The solution meets the 3 key business factors driving the WLAN marketplace: (1) it's inexpensive, (2) it's easy for WLAN vendors to implement by sending out software upgrades to the field and (3) it provides robust security.

Why weren't other more popular hashing functions like MD5 or SHA-1 used instead?
Unlike in SSL, one-way hash functions, such as SHA-1 and MD5, were too computationally expensive to be used in this environment with a stream cipher.

How do I implement this solution?
Members of the IEEE 802.11 committee have access to the paper proposed by Housley and Whiting that includes a reference design at www.ieee802.org.

RSA Security also offers a commercial implementation backed by warranties, support and maintenance. Please call 877-RSA-4900 for more information.

Has this solution been approved by the IEEE?
The IEEE 802.11 working group has agreed to include this solution as an informative section of the 802.11i document. See Document Number 550r2 entitled "Temporal Key Hash" submitted by Russ Housley of RSA Security and Doug Whiting of Hifn at www.ieee802.org. The 802.11i document specifies security enhancements for wireless LAN. As with other standards documents in development, the 802.11i document is not yet an IEEE standard, and may be subject to further revision.

How will this affect the IEEE 802.11b standard?
IEEE 802.11b is the most popularly deployed WLAN network standard today that uses WEP. Task Group I of the IEEE committee has worked toward outlining the requirements for a WEP fix. The 802.11i standard, currently in preparation, will document this fix.

Do any other security vulnerabilities exist when using Wireless LANs?
This solution solves encryption at the network level and protects data privacy allowing enterprises to run Wireless LANs securely without running a virtual private network overtop of the wireless LAN. However, the WEP fix does not solve authentication problems and organizations deploying wireless LANs should not overlook the importance of strongly authenticating their users coming into mission critical applications over the wireless LAN network. In these situations, passwords are simply not secure enough. Off-the-shelve products like RSA SecurID work well to achieve two-factor authentication in this environment.

For more information on wireless LAN authentication and a new authentication protocol developed by RSA Security, Microsoft and Cisco, see RSA Laboratories' white paper (MS Word, 56K).

United States: 1-877-RSA-4900 or 781 515 5000, Europe, Middle East, Africa: +44 (0)1344 781000,
Asia/Pacific: +65 733 5400, Japan: +81 3 5222 5200