Dr. Jon's Wireless Security

Cellular Networking Perspectives

Author: Dr. Jon Hamilton Editor: David Crowe Vol. 1, No. 2 April, 1999

Enhanced Subscriber Authentication (ESA)

ESA is the name for the new cryptographic algorithm and processes that will be chosen to authenticate the Mobile Station (MS) to the AC (Authentication Center) within the TIA/EIA-41 wireless network. Authentication is the process by which a wireless system verifies the identity of the mobile station ("Are you who you say you are?"). By comparison, validation is the process of ensuring that the identity is authorized for service, without regard for whether the identity being presented is true or false.

Entering the CAVE

Before discussing the alternatives and issues involved in the selection of ESA, it is important to understand the current authentication cryptographic algorithm, CAVE, and its processes. CAVE is a private key cryptographic algorithm which uses a 64-bit key, the A-key, as its primary key. CAVE also uses an intermediate (or session) key to generate 18-bit authentication signatures. This key, known as SSD_A or Shared Secret Data, may be shared with the VLR to spread the authentication processing load.

In CAVE, the mobile station uses a cryptographic algorithm to encrypt a random number (Rand), forming the authentication signature (Auth). Auth is transmitted over the air to the base station, and, along with Rand, over the signaling network to the AC. The AC uses the same cryptographic algorithm and the identical Rand to compute its version of the authentication signature (Auth). If the two versions match, then authentication is successful and the identity of the mobile station has been verified.

Why ESA?

One of the major reasons that a new cryptographic authentication algorithm is needed is to improve the security of the authentication process. In today's world of cryptography a 64-bit key is simply not long enough — the key should be at least 90 bits long and preferable 128. Another problem with CAVE is that it is the cryptographic engine for both authentication and privacy (i.e. encryption of voice and user data). This was a serious mistake as export control laws for cryptography are much more severe for privacy algorithms than they are for authentication algorithms. In addition, weaknesses were discovered in the CAVE privacy algorithms that required modifications to achieve an acceptable level of security.

Issues for ESA Selection

The key issues for ESA are:

- Level of security;
- Public key versus private (symmetric) key encryption;
- Complexity of network operations;
- Processing speed;
- Processor requirements;
- SSD retention.

About *Dr. Jon's Wireless Security*

Last Free Issue!

This issue, and the March 1999 issue of *Dr. Jon's Wireless Security* were distributed at no cost to enable you, our subscribers, to make an informed decision. Now is the time to email us at cnpsales@cnp-wireless.com, phone us at 800-633-5514 (+1-403-274-4749) or fax us at +1-403-289-6658 to lock in your copy. Quickly! Before they are all gone.

Price

Dr. Jon's Wireless Security is available at a 50% premium over your current *Cellular Networking Perspectives* subscription price. For example, subscribers to our standard 10-copy license paying $300/year would pay an additional $150/year for *Dr. Jon's Wireless Security*. The stand-alone subscription price is 75% of the cost of *Cellular Networking Perspectives* (e.g. $225 for a basic subscription).

Next Month's Issue

Comparison of public key and private key cryptography for authentication in wireless systems. Discussion of Enhanced Subscriber Privacy (ESP)

Future Topics

Interim CAVE • Global Authentication • UIM • Export Control Laws • Threats to Security Algorithms.

Dr. Jon's Wireless Security is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada. **Contact Information: Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/djws.html. **Subscriptions:** 50% premium on *Cellular Networking Perspectives* subscription, or US$150/yr. in the USA or Canada. US$200/yr. elsewhere. Payment by cheque, bank transfer, American Express, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for $20 in the US and Canada and $25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

External to the TR-45 decision, but still important, are the following issues:

- Suitability for global authentication;
- Capability for mutual authentication;
- Network negotiation of multiple authentication algorithms.

Security Level.

AHAG is relying to a significant degree on public scrutiny to ascertain the strengths and weaknesses of candidates for ESA. Through making the candidate cryptographic algorithms publicly available, AHAG hopes to stimulate cryptographers in the public sector (i.e. non-government) to analyze the ESA candidates for weaknesses.

The four principal components of strength of a cryptographic process for cellular networks are:

1. Strength of the cryptographic algorithm;
2. Key length;
3. Protocol vulnerability;
4. Vulnerability of the network implementation to attacks on the network.

Suppose that we are trying to identify the cryptographic key from intercepted cipher text. If we know of no method of reducing the uncertainty in the key, then the level of security is $2^{(\text{length in bits of the key})}$. For example, CAVE's level of security would be 2^{64}, as the A-key is 64-bits long. If we use this as a measure of cryptographic strength, we are assuming that no attack reduces the key space. This is a critical assumption, which, frankly, should not be left to the designer of the algorithm. Protocol and network vulnerability to a large extent depend on the class of cryptographic process used. All viable ESA candidate algorithms will achieve a certain minimum level of cryptographic security. Once this level of security has been achieved, then the following issues will dominate the selection process. The minimum level of security for an ESA algorithm has not yet been specified — although the "brute force" uncertainty in the key space should be at least 2^{90}.

Public versus Private Key Cryptography

This is a key issue in the selection of ESA, with ramifications in complexity of network operations and interoperability with other standards. As previously pointed out, CAVE is a private key technique in which the cryptographic key must be kept secret in both the MS and the AC, necessitating a critical key provisioning step, that is required for new subscriptions, or whenever the key is compromised. Some private key algorithms are also symmetric, where the same key can be used for encryption and decryption. Public key cryptography uses two keys, one of which is public and the other is private. Public key cryptography offers greater flexibility in provisioning and in the use of session keys for authentication. However, public key cryptography is significantly more complex in terms of network operations, processing speed and processor requirements.

Complexity of Network Operations

The number of operations and their complexity that are required to implement a candidate ESA process are an important practical consideration. At the March 1999 TR-45.2 meeting, the Authentication Focus Group was formed to examine the impact of ESA candidates on network operations. The report of this group will highly influence the choice between reliance on public keys or private keys.

Processing Speed

The amount of time required for a candidate cryptographic ESA to produce an authentication signature should not be a major issue. This is because each of the candidates should process an authentication signature in a short time compared to that required for the transmission and processing of intersystem messages.

Processor Requirements

The amount of memory for calculations, the amount of memory for program code, and the use of 8-bit versus 16-bit arithmetic logic are important considerations, but probably not decisive in the choice of ESA.

SSD Retention

An important issue is whether or not the concept of SSD is retained, or whether ESA is based on a concept like the triplets of GSM. SSD provides a load sharing capability amongst collaborative VLR's that is considered important by carriers. The Authentication Focus

Table 1: Enhanced Subscriber Authentication (ESA) Contenders

Name	Source	Description
DH-EKE	Qualcomm	Authenticates subscriber by downloading UIM via secure password protocol.
LESA	Lucent	Private key cryptographic algorithm based on Bellare-Rogaway.
SHA-1	NIST (submitted by Qualcomm, Motorola)	Secure Hash algorithm, primarily intended as candidate for Interim CAVE.
none	GTE	Public key cryptographic algorithm based on Rabin methodology.
none	Certicom	Public key cryptographic algorithm using elliptic curve Diffie-Hellman key exchange with HMAC.
none	Diversinet	Certificate and permit management methodology.
none	TTA and Korean Universities	Private key cryptographic algorithm.
none	TTA and Korean Universities	Public key cryptographic algorithm.

Group of TR-45.2 will also address this issue. If public key techniques are chosen for ESA, then this issue becomes irrelevant.

ESA Candidates

Table 1 (previous page) contains the current list of ESA candidates being considered by AHAG. This table was included in the March 1999 issue, but the Enhanced Subscriber Privacy algorithms were inadvertently included in the same table. These are shown in Table 2.

Table 2: Enhanced Subscriber Privacy (ESP) Contenders

Name	Source	Description
SCEMA	Lucent	Stream cipher based on CMEA.
SHAZAM	Lucent	Stream cipher with Feistal permutation using SHA-1.
SOBER	Qualcomm	Stream cipher using GF (2^8) LFSR with 17 elements, nonlinear output and clock stuttering.
SOBER 16	Qualcomm	Stream cipher using GF (2^{16}) LFSR with 17 elements, nonlinear output and clock stuttering. Tailored for 16-bit arithmetic and logic processing.
SSC	GTE	Stream cipher using GF (2^8) LFSR with 16 elements and nonlinear output.
TWOFISH	Counterpane Systems and Hi/fn, Inc.	Block cipher (128 bit) which is currently a viable candidate for AES. Cryptographic algorithm is Bruce Schneier's entry in the AES competition sponsored by NIST.

Update on AHAG (TIA TR-45 Standards Committee *Ad Hoc* Authentication Group)

At the March 1999 meeting of AHAG, the final version of SCEMA for ESP (Enhanced Subscriber Privacy) was presented. Preliminary discussions comparing private and public key cryptographic methods were conducted.

AHAG received four new Stage I descriptions requiring security analyses:

- PN-4104. Broadcast and multicast short message service;
- Answer Holding. An enhancement to call waiting.
- Tiered Service. Providing virtual private radio systems with CDMA;
- IS-2000 Annex A. Next generation CDMA security algorithms.

Initial discussions of the security implications of these proposals will be held at the April 1999 meeting of AHAG.

An Israeli cryptographic company, LPK Information Integrity Ltd., presented a proposal for an efficient Diffie-Hellman/ Elliptic Curve cryptographic process. AHAG has advised other TR-45 subcommittees of the schedule for ESA and ESP and requested their consideration of impacts of the new cryptographic algorithms to their areas of responsibility. In particular, TR-45.2 needs to assess the impact of the different classes of cryptographic algorithms being proposed to AHAG on intersystem operations.

Coming Next Month

The May 1999 issue will focus on ESP (Enhanced Subscriber Privacy) and on the key ESA issue of symmetric/private key versus public key cryptography.