Dr. Jon's Wireless Security

Cellular Networking Perspectives

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

Introducing Dr. Jon's Wireless Security

This new report will be published monthly as an optional enhancement to your existing *Cellular Networking Perspectives* subscription. It will inform you about authentication, voice and data privacy, and network security issues for wireless systems. Its focus is on security algorithms being developed by the TIA AHAG (Telecommunication Industry Association's Ad Hoc Authentication Group) for TIA/EIA-41 based networks, however we will also keep you up to date on GSM and international issues, as well as more general security issues.

Introduction to AHAG

Despite rumors, AHAG is not a code word for a predatory mother in law, but rather the TR-45 Ad Hoc Authentication Group, which is responsible for authentication, voice and data privacy, and network security issues for TIA/EIA-41 wireless networks. This covers analog cellular, D-AMPS cellular/PCS and cdmaOne/cdma2000 cellular/PCS. Highlights of each AHAG meeting are presented in a manner not requiring intimate knowledge of cryptography. Our intent is to make the understanding of authentication and cryptographic issues slightly less painful than root canal surgery before the invention of anesthesia. Nevertheless the mathematics of cryptography will be discussed when necessary for a high level understanding of security issues.

Interim Security Enhancements

An interim alternative to CAVE (Cellular & Voice Encryption algorithm) is under consideration by AHAG. Conceivably it would be used in place of CAVE during the period before the ESA and ESP algorithms discussed below are accepted and implemented.

Why go to this trouble? Only if the current CAVE is "broken" before the introduction of ESA and ESP into the TIA/EIA-41 network. Will it happen? Probably not, as CAVE is not currently "broken" in the sense that street vendors can sell cloned authenticating wireless phones. However, AHAG is taking due precaution to prepare for the eventuality that CAVE becomes publicly broken.

Enhanced Security Algorithms

The major goal of AHAG in 1999 is to develop cryptographic algorithms and processes for Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP). AHAG will select one ESA algorithm for both TDMA and CDMA formats, whereas several algorithms may be recommended for ESP with the selection to be performed by the air interface subcommittees of TR-45. Selections and recommendations are scheduled for January 2000. Table 1 presents the contenders with a short description of their key attributes. In subsequent issues of this report, details of the principal contenders will be presented along with side by side comparisons.

About *Dr. Jon's Wireless Security*

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.*

Next Month's Issue

Extended report on enhanced subscriber authentication (ESA) — issues, comparisons and possible changes to the TIA/EIA-41 network.

More Detailed Reports

If you required more detailed reports on all AHAG contributions and security matters (including mathematical descriptions and analyses of cryptographic algorithms), you might consider subscribing to our "In Depth Report" which is also available monthly. Subscribers will receive Special Reports on key issues involving wireless telecommunications.

Upcoming Special Reports

Enhanced Subscriber Authentication (ESA) • Enhanced Subscriber Privacy (ESP) • Interim CAVE • Global Authentication • UIM • Export Control Laws.

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.

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	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.
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.

Network Enhancements

TR-45.2 has approved Authentication Enhancements to TIA/EIA-41-D (project PN-4081) for TIA publication as IS-778. It is also scheduled for inclusion in TIA/EIA-41E. It provides the following enhancements:

- COUNT update after handoff,
- Obtaining subscriber profile before authentication on initial system access,
- Handling of suspicious call origination,
- Identifying the Serving MSC when reporting the outcome of a requested authentication operation,
- Handling of authentication capable mobile stations when the home system is not authentication capable, and
- Several clarifications (editorial corrections) of authentication procedures.

An attempt to resolve the problem of multiple overlapping Unique Challenge transactions was removed at the last minute.

Global Roaming

Global roaming requires global authentication in this age of authenticatable wireless phones. The key issue is to allow a subscriber to move seamlessly between countries that use different authentication algorithms and procedures. How do we make TIA/EIA-41 and GSM authentication work together without introducing unacceptable complexity and still follow the cryptographic laws of each nation? This question, plus the allied issue of functional requirements for the UIM (Universal Identity Module) are hot issues for international standards organizations in 1999. TTC, the Japanese equivalent of TIA, is pushing for an early 1999 resolution, especially for UIM. TTC favors a removable UIM concept.

Look for TIA's new 3GPP2 to take the lead in the development of standards for this issue.

Replacing DES

The United States Government, through NIST, is sponsoring a competition for the replacement of 25 year old DES (Data Encryption Standard). The new standard, known as Advanced Encryption Standard (AES), is on a schedule similar to ESA and ESP, with selection scheduled for early in 2000. About 15 candidates still remain viable for the second round of analysis. Considerable public scrutiny of each algorithm is underway — which produces more confidence in the security of the algorithms that survive unbroken. The AES algorithm will be available royalty free to all users.

Dr. Jon's Security Recommendation #1

Replace your existing database security cryptographic algorithms by AES as soon as practical, after it is published.