Wireless Security Perspectives

Cellular Networking Perspectives

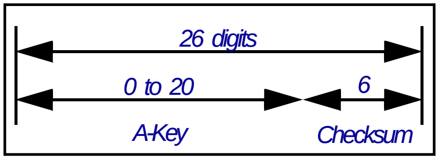
Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 1, No. 7 September, 1999

From Dr. Jon's Wireless Security to Wireless Security Perspectives

As of this issue, Dr. Jon's Wireless Security has been renamed Wireless Security Perspectives. The former name was no longer appropriate because of a change in the lead writer. There will be no loss of quality, as Les Owens has a similar depth and breadth of expertise in wireless security issues.

ESA Part I: What is all this Enhanced Subscriber Authentication stuff anyway?

A-Key Entry



Is the A-Key we've come to know and tolerate going away?

Introduction

On 31 August 1999 the Telecommunications Industry Association (TIA) TR-45 Ad Hoc Authentication Group (AHAG) sponsored a meeting of nearly three dozen engineers, security specialists, standards developers, and cryptographers in downtown Toronto to hear proposals for what many refer to, somewhat imprecisely, as the 'CAVE replacement' (CAVE being the Cellular and Voice Encryption algorithm currently used for analog, TDMA and CDMA authentication). The eclectic group convened for several hours to launch the review and selection of a new Enhanced Subscriber Authentication (ESA) – a much bigger job than just replacement of an algorithm. ESA is a change to the whole authentication framework within the IS-41 system used in North America. That is, the subscriber and network verification system will be modified to better protect wireless operators from potential technical fraud of the future. ESA will, of course, include the replacement of the aging CAVE – the cryptographic algorithm at the heart of TIA's existing 'challenge-response' authentication scheme (see Figure 1). ESA will include the development of mechanisms for key distribution and management as well as for the underlying signaling protocols. In sum, it is not just a simple swap out of CAVE.

The AHAG, TR-45's security arm, is leading the selection and establishment of the ESA. It plans to educate and advise the TR-45 subcommittees on the ESA proposals to allow the seven subcommittees to select the desired approach. The AHAG hopes that they will reach a consensus on the approach to take for ESA. However, if consensus cannot be gained, the TR-45 committee will ultimately have to make the decision. The entire selection process is aimed for completion by the end of December 1999. After selection of the

About *Wireless Security Perspectives*

Price

The stand-alone subscription price for *Wireless Security Perspectives* is 75% of the cost of the corresponding *Cellular Networking Perspectives* subscription (e.g. $225 for a basic subscription).

Current subscribers to *Cellular Networking Perspectives* can extend their subscription to include *Wireless Security Perspectives* for only a 50% premium over their current *Cellular Networking Perspectives* subscription price. For example, subscribers to our standard 10-copy license paying $300 per year for *Cellular Networking Perspectives* would pay only an additional $150 per year for *Wireless Security Perspectives.*

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Month's Major Topic

The four Enhanced Subscriber Authentication (ESA) Candidate Proposals.

Next Issue Due…

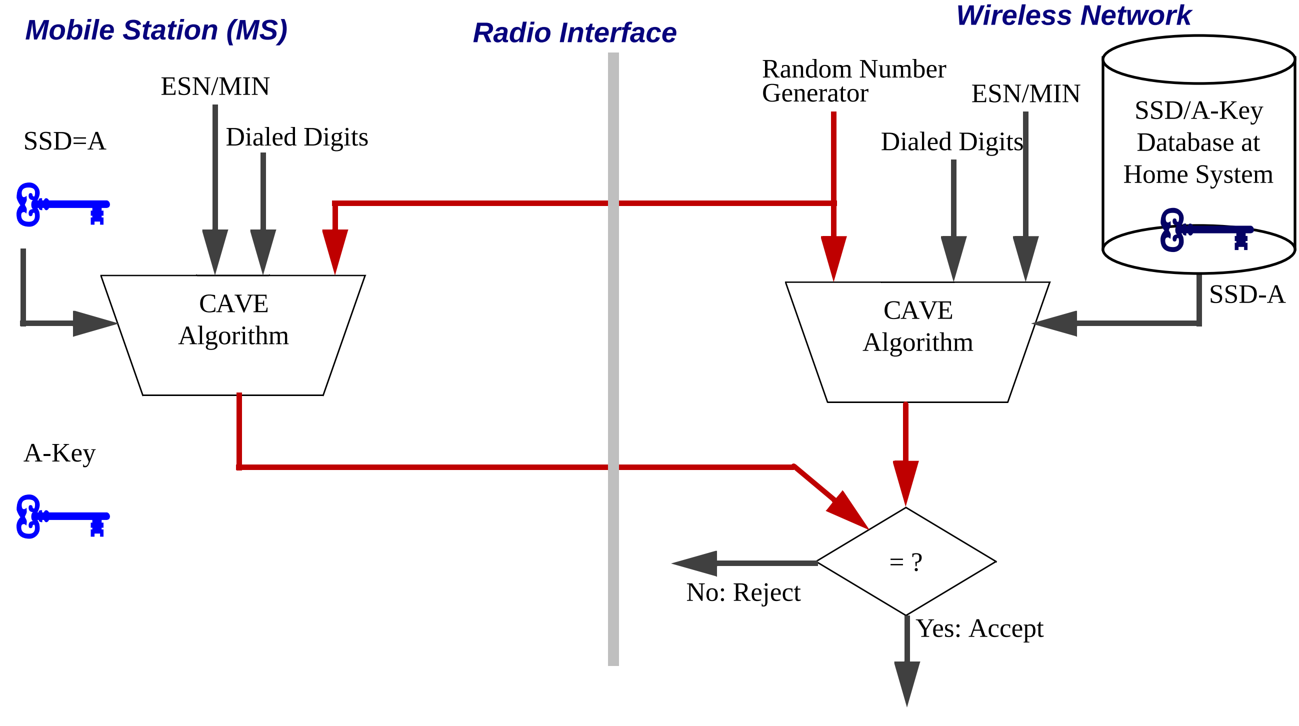
October 15, 1999.

Future Topics

Voice over Packet security • Public Key & Wireless • GSM Security

Wireless Security Perspectives 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/wsp.html.
Subscriptions: $150 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$200 elsewhere. Non-subscribers pay $225/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted 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 US$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.

Figure 1: Simplified View of Current TIA/EIA-41 Authentication



authentication framework, the real work of standardization will begin in early 2000.

In this, the first part of this article, we discuss the fundamental motivation for the development of ESA and identify the security requirements for the new authentication framework. Next month we will provide a brief introduction to the four proposals and present some of the issues for consideration by the wireless operators and the industry in general. Future articles will explore the problems that motivated ESA and their potential solutions in detail.

Motivation for the ESA security initiative

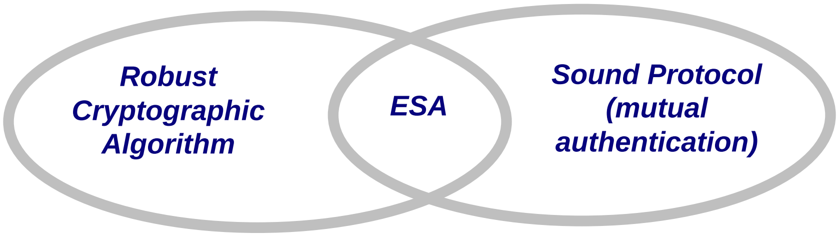
So what's wrong with CAVE? Aren't the current losses due to wireless fraud on the way down? In fact, aren't the endemic losses that the North American carriers experienced in 1995 (over US$1.5 Million per day) now at an all-time low? With the deployment of the CAVE authentication in the networks in the major cities, hasn't cloning fraud shifted (like squeezing a balloon) to subscription fraud as in international GSM (Global System for Mobile Communications) markets? The answer is a resounding, Yes. So one may ask, why is this group 'creating work' for itself? According to members of the AHAG, there are two primary motivations for the development of ESA.

1. It is generally well-known that some weaknesses exist in the cryptographic details of the CAVE algorithm. CAVE was developed and first proposed in the early 1990's. Since that time, numerous cryptographers have been chipping away looking for security flaws. Some weaknesses have been discovered and the AHAG thinks it prudent to move to an algorithm that is considerably more robust – the AHAG has determined that the NIST SHA-1 hash or one-way function will work quite nicely.
2. There is a need to beef up security with a mutual authentication scheme. The current authentication scheme used to validate the mobile user provides only unilateral validation. The AHAG wants to deploy a bilateral scheme that will also provide mechanisms to allow a mobile to authenticate a base station or network. The mutual authentication scheme will allow both:
   i. the network to verify the mobile station to (more specifically, the subscriber) and
   ii. the mobile station to verify the network, to verify that it is communicating with a legitimate carrier and not a rogue, or fake, base station.

In summary, the AHAG intends to ensure that the basic cryptographic algorithm is robust enough to withstand attacks in the long-term and that the underlying protocol design is also sound (see Figure 2).

The AHAG has concluded that even if the CAVE algorithm were replaced, this would not be adequate. Replacing the existing CAVE algorithm with a 'Son-of-CAVE' would be relatively easy as there are numerous strong message digesting algorithms (or hashes) that could be tailored to replace the aging and flawed CAVE (e.g., SHA-1, MD5, AHA, and KT). However, 'fraudsters' would still be able to exploit flaws in the existing protocol design and gain unauthorized access to the wireless network, resulting in fraud and monetary losses for the operators.

Figure 2: Motivation for ESA


Robust Cryptographic Algorithm
ESA
Sound Protocol (mutual authentication)

The AHAG Process and the Security Requirements of ESA

The TR-45 AHAG has evolved considerably since its inception in early 1990's. Today, it is the full-time security consultation group for the entire TR-45 family of subcommittees, which are together responsible for the development of analog, TDMA, CDMA radio interface and supporting network standards. At first, AHAG provided support solely for the TR45.3 TDMA digital cellular subcommittee. This support was provided in a somewhat ad hoc fashion for the development of security services for the TDMA air-interface alone (IS-54). In those early days, with its paucity of security expertise, the AHAG focused largely on the radio interface and did not provide close consideration of the larger system issues such as key management and intersystem performance and operations issues. Now, however, the AHAG has matured and grown into a skilled secure system engineering team that takes a holistic view of the wireless network to ensure adequate security for the wireless operators and their customers. As part of this maturation, this seasoned 'security consulting' team now commands the respect of the other TR-45 groups. The AHAG has now created a formal and open security development process to avoid some of its earlier problems. Their new process uses a methodical secure systems engineering approach to determine the best possible cryptographic algorithms, protocols and techniques for the wireless industry.

Security Development Process

The AHAG security development process comprises the following steps:

1. Develop comprehensive security requirements,
2. Solicit and accept contributions on proposed security designs and models,
3. Conduct an internal review of the proposals,
4. Conduct an external review of the proposals, and
5. Select the security proposal or proposals for standardization.

The AHAG is using this new approach for the establishment of ESA.

ESA Requirements

AHAG has developed the following security requirements for ESA:

1. Employ cryptographic algorithms and protocols that have been standardized and have been openly published and scrutinized,
2. Use an authentication key that is 128-bits in length,
3. Mutual authentication of the mobile station to the network and of the base station to the mobile phone,
4. Authentication without the use of the mobile station hardware serial number (the ESN),
5. Backwards compatibility with the existing CAVE-based authentication scheme,
6. A SIM (Subscriber Identity Module, aka User Identity Module or "Smart Card") interface,
7. Negotiation of air-interface and network cryptographic algorithms,
8. Use SHA-1 for cryptographic hashing, and
9. Use the HMAC-SHA-1 for any message authentication code (MAC) functions.

Additionally, the proposals for the next generation authentication should meet the following critical system requirements:

1. The security of the system should not negatively impact the end-user or the operator,
2. ESA should minimize the addition of network infrastructure. It is important to take into account that operators have invested substantial funds, in the current 2nd generation wireless, that must be leveraged,
3. ESA should provide for the ability to scale, (add customers and cellular systems) without imposing additional costs to the carriers.

To be continued…

We will continue in our October issue with an overview of the four ESA candidate proposals, and will identify some of the many questions that carriers, manufacturers and even consumers may have about the changes that this will bring. In future issues we will address each of these questions.

Huh?

If there are any acronyms or terms that you are unfamiliar with, check our website glossary, you will probably find them defined there:

www.cnp-wireless.com/glossary.html