Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 1, No. 8 October, 1999

ESA Part II: The Four Candidates

On 31 August 1999, four ESA (Enhanced Subscriber Authentication) proposals, each claiming to meet the security requirements described in our September 1999 issue, were presented to the AHAG (TIA *ad hoc* Authentication Group) at a meeting in Toronto, Canada. Two of these proposals are based on symmetric (classical, one-key or private-key) cryptography and two are based upon asymmetric (public-key, two-key) cryptography.

The four proposals were:

1. LESA - Long-term Enhanced Subscriber Authentication
2. 3GPP AKA - Authentication and Key Agreement
3. EPAC - Enhanced Public-key Authentication from Certicom -
4. CESA - CipherIT Enhanced Subscriber Authentication

LESA - Lucent's Proposal

LESA is an authentication framework proposed by Lucent Technologies that relies exclusively on symmetric cryptography. LESA builds upon the existing CAVE-based framework. It meets the security requirements while minimizing changes to the existing technology used in TIA/EIA-41. The LESA key hierarchy is based largely on the existing CAVE-based hierarchy with the A-key as the root secret key that is symmetrically shared by the mobile and the network.

Other salient points about LESA, according to Lucent, are that:

- it is provably secure,
- it provides for a natural evolution (not revolution) from the existing scheme and
- overall, it can be operated quickly.

One important thing to note is that in the LESA proposal, the security of the AC (Authentication Center) is extremely critical. That is, carriers must make sure that the AC cannot be penetrated and the A-key and SSD secrets stolen. Compromise of these secrets could be catastrophic.

3GPP AKA - Time for a Single Global Security Standard?

3GPP AKA is an authentication framework proposed by the 3GPP (third-generation partnership program) SA3 and the ETSI SMG10 security groups. The ESA proposal is also based on symmetric cryptography. It addresses the vulnerabilities in the existing GSM-based framework, and builds a more secure system. The 3GPP AKA key hierarchy is based on that of the existing GSM where the root secret key is symmetrically shared. This key, known as K_i, is stored on the SIM ("smart card") and installed in the wireless network.

Other salient points about 3GPP AKA, according to Vodafone, are that if it is adopted by TIA/EIA-41 it will significantly ease future intersystem roaming. Additionally, it guarantees key freshness through intrinsic key generation capabilities.

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

Analysis of ESA Proposals.

Next Issue Due…

November 16, 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.

EPAC - Certicom's Solution

EPAC is the authentication framework proposed by Certicom. The EPAC proposal is a hybrid crypto-system, based both on public-key cryptography (symmetric) and classical cryptography. As is typical for hybrid implementations (e.g. PGP), it capitalizes on the best characteristics or benefits of both cryptographic systems:

- public key methodologies are used for authentication and key management, but…
- the keys generated during the authentication may then be used for subsequent encryption of voice and data via symmetric cryptographic techniques.

In EPAC, some of the parameters in TIA/EIA-41 messages would have to change but it is still largely the same messaging structure. Like the LESA proposal, EPAC claims that it too is provably secure.

Other salient points about the system developed by the Certicom team are that EPAC uses the relatively new elliptic curve cryptosystem (ECC) technology as the public-key technology employed during mutual authentication and key exchange. Additionally, EPAC, although a public key technology, it is not certificate based. Therefore, it eliminates the complexity of certificates for secret public keys, but at a cost: the public keys must remain secure. The ECC techniques used with EPAC have been standardized by ANSI and adopted by NIST, WAP and IETF for use in numerous implications. Moreover, the cryptographic community has been studying and testing the ECC for many years and its strengths and weaknesses are well known. The Certicom proposal reduces SS7 traffic between home and serving systems and reduces processing overhead at service requests.

CESA - Innovation from Israel

CESA, the authentication framework proposed by the CipherIT, is another hybrid crypto-system based on both public and private key cryptography. The CESA system, like the Certicom proposal exploits the benefits of both symmetric key and asymmetric key cryptography. The public key cryptography, like that used in the Certicom proposal, is ECC. Again, ECC cryptography has gained increased interest because of its performance improvements over other public-key techniques. The CESA proposal accomplishes mutual authentication through the use of the public-key techniques. CipherIT reiterates that the network authenticates itself to the mobile station by proving that it knows something about itself, rather than about the mobile. Conversely, the mobile authenticates itself to the network by proving that it knows something about itself, rather than about the network.

Late Update!

Certicom has formally withdrawn their EPAC proposal from consideration as an ESA candidate stating that "we find hesitation on part of the cellular community to introduce any significant changes for basic cellular authentication as they transition from 2G to 3G".

Other salient points about this system are that it utilizes a self-certification protocol on top of the ECC cryptographic techniques to minimize system overhead and to conserve bandwidth. CipherIT asserts that it provides a higher degree of information integrity than the other proposals because no 'SSD-like' secrets are sent over the SS7 network. Also, according to CipherIT, the CESA proposal has no single point of failure (e.g. compromise of the AC).

One of the features that CipherIT touts regarding its ESA proposal is its support for electronic transactions over the Internet: for e-commerce. The CESA proposal forms an infrastructure for implementing the DSA (Digital Signature Algorithm), which will allow for the computation of digital signatures and the addition of non-repudiation which is critical to e-commerce.

Moving on…Diving Deeper…

In this two-part article, we have provided the fundamental motivation for the development of ESA, identified the security requirements for the framework, and provided an introduction to the proposals. In our next multi-part article in *Wireless Security Perspectives* we will probe deeper into the authentication proposals with our *ESA in the Examining Room* section. We will separate the wheat-from-the-chaff and validate the claims of the various parties by providing a detailed comparison of the technical proposals. Last, we will explore a few of the following questions that the industry must consider as it contemplates a new authentication framework:

- Is all this ESA stuff really needed now?
- Do these proposals meet all the carriers' fraud control needs?
- Although comparing radically different proposals is a bit like comparing apples and oranges, how do they really stack up against each other?
- If the TIA/EIA-41 industry begins now, when will the industry expect to see the ESA in North America?
- What will all this cost? Where is the business case? What if we do nothing about CAVE and the existing protocol vulnerabilities?
- Do these proposals really hit the mark? Do they address the really critical issues like cryptographic key management?
- What are new security issues that will be encountered beyond ESA?
- Is the industry being aggressive enough? Can it learn anything from the IETF and other Internet standards organizations?
- What about EDI (Electronic Data Interchange) and other investments that have been made based on the current authentication framework?
- How does the SIM ("Smart Card", currently used in GSM systems) fit in to all this?
- How does this address, impact, or involve inter-system message security for the signaling links used in wireless networks to carry TIA/EIA-41 and other traffic?
- How will backward compatibility be addressed? Will fraud get worse during the transition period, before it gets better?

- Are the security services offered by the ESA proposals equal? Does it matter?
- Who are the real benefactors of ESA?
- How does ESP (Enhanced Subscriber Privacy) fit in?
- What about the intellectual property associated with this? What does this mean for the purchasers of equipment? Can we get the real skinny?

To Probe Further

For general information related to the ESA proposals, contact the following individuals:

- Chris Carroll (GTE)
  Chair TR-45 AHAG
  +1-781-466-2936

  cc06@gte.com;

- Frank Quick (Qualcomm)
  Vice-Chair TR-45 AHAG
  +1-858-658-3608

  fquick@qualcomm.com;

You may also contact the following individuals for details regarding individual ESA proposals:

- LESA

  Simon Mizikovsky (Lucent)
  Wireless Secure Communications Group
  Lucent Technologies
  +1-201-386-6348

  smizikovsky@lucent.com

- Tim Wright
  Vodafone

  timothy.wright@vf.vodafone.co.uk

- Prakash Panjwani
  Certicom
  +1-630-871-1418

  ppanjwani@certicom.com

- Herbert Zlotogorski
  CipherIT
  +972-2-672-7261

  herbz@cipherIT.com

Further Reading

Berson, Thomas A. "Authentication Analysis: Algorithms and Protocols." Anagram Laboratories report to CTIA, March 1995.

Patel, Savar. "Weaknesses of North American Wireless Authentication Protocol." IEEE Personal Communications, June 1997, p40-p44.

FIPS 180-1, "Secure hash standard," Federal Information Processing Standards Publication 180-1, US Department of Commerce/ NIST, National Technical Information Service, Springfield, VA, April 17, 1995 (supersedes FIPS PUB 180).

Network Concerns

It is only natural that the cryptographic aspects of a new authentication system get the most attention. After all, if the underlying cryptography is deficient, the entire system cannot be secure. But beyond strong cryptographic components, network-based authentication has to be embedded in a strong inter-system protocol (e.g. the TIA/EIA-41 standard), yet be efficient enough to be cost-effective and transparent to users.

To address some of these concerns, TR-45.2 has written a letter to the AHAG requesting a description of:

- The types of information to be exchanged between the home system and the serving system,
- How this information is updated,
- The sizes of the information elements,
- The estimated times required to compute each information element.

To evaluate the impact on network protocols, TR-45.2 has requested that the information flow for various important scenarios be illustrated, so that the new procedures can be compared with the old for bandwidth requirements, frequency of use, complexity and other characteristics. These include:

- Initial registration (i.e. mobile unknown to the serving system),
- Implicit registration due to an origination (e.g. in situations where a mobile can originate a call without registering first),
- Implicit registration due to a page response,
- Secondary key updates
  (e.g. equivalent to the current SSD update procedure),
- Over-the-air service provisioning for authentication and other security-related parameters for a mobile.

TR-45.2 is also interested in functional characteristics of the proposed new systems, including:

- How a system can support both the new algorithms and the existing TR-45 CAVE-based system, and
- How the ESA proposal can be scaled to different key sizes to ensure US export approval (e.g. systems based on large keys may not be exportable). Recent changes in US export requirements may remove the necessity for this requirement.

Acronyms

Some of the less commonly encountered acronyms used in this article are listed below, for more common acronyms consult:

www.cnp-wireless.com/glossary.html

3GPP	-	Third Generation Partnership Program
AKA	-	Authentication and Key Agreement
A-key	-	Root Authentication Key used by CAVE
CAVE	-	Cellular Authentication and Voice Encryption
EDI	-	Electronic Data Interchange
ESA	-	Enhanced Subscriber Authentication
HMAC	-	Hashed-MAC
IETF	-	Internet Engineering Task Force
MD5	-	Message Digest 5
SHA	-	Secure Hash Algorithm
MAC	-	Message Authentication Code
WAP	-	Wireless Application Protocol