Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 1, No. 9 December, 1999

Enhanced Security and Authentication…and Then There Was One…

Not long ago there were four candidates for the TIA's next generation Enhanced Security and Authentication (ESA) algorithm (see the October, 1999 issue of *Wireless Security Perspectives*). But then Certicom withdrew their proposal, stating that the TIA was not ready to seriously consider public (asymmetric) key cryptography. CipherIT, a second public key approach, by then had virtually no support. This left two private (symmetric) key approaches – Lucent's LESA and 3GPP's AKA.

At the December 1999 TR-45 meeting it was decided that the winner will (probably be) 3GPP's AKA, with an approach based on current GSM authentication. Some aspects of LESA may be incorporated, particularly the ability to perform local authentication. While LESA is conceptually an advanced version of the existing CAVE-based scheme, AKA concepts are less familiar to audiences that have not used GSM authentication.

3GPP AKA does require some adaptations, and has been given only until March, 2000 to prove itself. At that point, TIA committee TR-45 will review progress and decided whether to continue with 3GPP AKA as their nominee for the ESA throne or to investigate other alternatives.

3GPP Authentication and Key Agreement: Looking under the Hood

The 3GPP authentication and key agreement mechanism (AKA) is an authentication framework proposed by the 3GPP (third-generation partnership program) SA3 and the ETSI SMG10 security groups. The 3GPP ESA proposal, based on classical (or symmetric) cryptography, attempts to address the known weakness of the existing GSM-based framework, including technical additions to combat false base station and key reuse attacks, to which GSM is susceptible. However, the 3GPP proposal was also developed with the goal of achieving maximum compatibility with the current GSM architecture while facilitating a migration to UMTS (Universal Mobile Telecommunication Service). Acceptance by the TIA could allow a single, global method for authenticating wireless phones, simplifying, enhancing and reducing the cost of international roaming.

Price Increase

As of January 1, 2000 the annual subscription price for *Wireless Security Perspectives* will be $200 per year for *Cellular Networking Perspectives* subscribers, and $250 per year for standalone subscriptions.

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees for more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price – only $200 within the US and Canada or $250 elsewhere.

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 Attack on GSM Security.

Next Issue Due…

January 18th, 2000.

Future Topics

Voice over IP security • Public Keys & Wireless • GSM (in-)Security • Kerberos • Public Key Infrastructure * IP Security • IKE

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: $200 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/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.

Goals of 3GPP AKA

The goals of the existing GSM AKA scheme were to authenticate the user and to generate a traffic (e.g. voice) encryption key. The goals of 3GPP AKA extend these with the following:

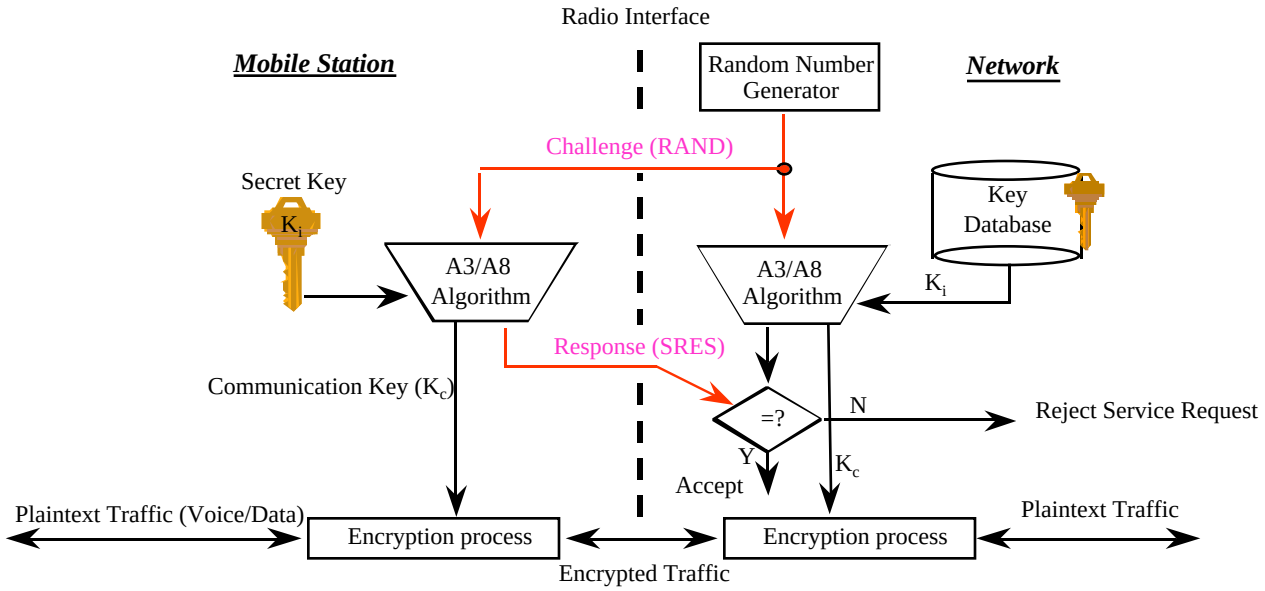
1. To provide full *mutual authentication* by not only authenticating the user but also providing for the authentication of the network to the mobile station. Currently, an interloper using a fake base station could exploit the GSM network.
2. To generate a *shared integrity key* to address GSM's current lack of cryptographic integrity against modification that could result in other false base station attacks.
3. To provide assurance to a user that a "triplet" used in the authentication transaction is not being reused. *Key freshness* addresses the weakness in GSM whereby the cryptographic "triplet" -- the RAND, SRES, and Kc – may be used several times, possibly allowing further theft of service.

Review of GSM AKA

Before presenting the 3GPP proposal in detail, we will review the architecture of current GSM authentication, to allow the reader to compare and contrast the schemes.

The GSM "challenge-response" authentication and encryption scheme is depicted conceptually in Figure 1.

Figure 1: GSM Authentication and Encryption Mechanisms



In the GSM system, a secret key, Ki, assigned when a wireless subscription is started, is programmed into a user SIM card. Ki, which should not be accessible outside the SIM, is only stored in one place (theoretically) in the wireless network – the authentication center (AuC). As shown in the simplified figure, the root secret Ki provides the basis for authentication of the mobile subscriber and for encryption of the information (usually digitized voice) on the radio path.

GSM Challenge-Response

A challenge in the form of a random number is sent from the network to the mobile station, where the A3/A8 authentication algorithm uses the random number and the Kc to compute the signed response (SRES), which is in turn returned to the network. In the network, the SRES from the mobile is compared with an SRES computed with the same inputs. If the two responses are the same, authentication has been accomplished, the mobile station is verified and service is granted. Using another algorithm (a key generator or KG) an encryption key, Kc, is produced both in the mobile and in the network. The Kc is used for encryption of signaling and user voice and data on the radio path.

The GSM approach is very simple. It is also important to note that the home network is in complete control of the cryptographic algorithms that are used. The home AuC chooses the algorithms and performs all cryptographic processing – none is required by the visited system. Also worthy of note, is that the GSM scheme illustrated in Figure 1 does not provide authentication of the network (mutual authentication).

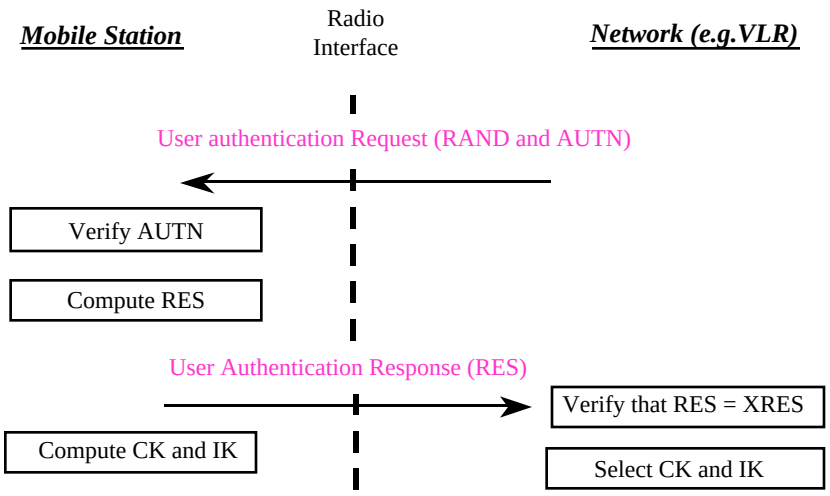
3GPP AKA

The newly proposed 3GPP "challenge-response" procedure is depicted in Figure 2. As in the GSM scheme, a challenge in the form of a random number is sent from the VLR to the mobile station, where an authentication algorithm uses the random number to compute a response – RES. RES is, in turn, transmitted to the network where it is compared with the XRES computed on the network side using the same inputs that were previously supplied by the home AuC. If the two responses are the same, authentication is accomplished and service may be granted.

Mutual Authentication

In the mobile station (specifically, in the SIM or Smart Card), an Authentication Token (AUTN) is also verified, however. This verification allows for the mobile station to validate the legitimacy of the network. By providing this cryptographic validation, the SIM can protect against false base stations, thereby completing the mutual authentication. The mobile can be sure that the 'network' to which it is communicating is not an ESN Reader-like device. As shown in Figure 2 following mutual authentication the SIM computes a cipher key (CK) and an integrity key (IK) that may be used for confidentiality and integrity services. On the network side, of course, the VLR simply selects the appropriate CK and IK from the corresponding chosen authentication vector, as shown in Figure 2.

Figure 2. 3GPP Mutual Authentication and Key Generation Mechanisms



Inside the SIM

The processing performed inside the SIM for the authentication and key agreement is shown in Figure 3. As illustrated, using a 128-bit master secret key, K, the SIM performs several computations: generation of XMAC (expected message authentication code), RES (authentication response), CK (ciphering key), IK (integrity key), and AK (anonymity key) using five algorithms specified by 3GPP. Three of these algorithms are key generation functions and two are authentication functions. The AUTN authentication token comprises three parts: a sequence number bit-wise exclusive ORed with an anonymity key (AK), a mode variable (MODE), and a MAC (message authentication code). The mode is the variable used to distinguish between circuit switched nodes and packet switched core network nodes. The AK is an anonymity key that is used to cover the sequence number and thereby protect the mobile user's location and personal identity information over the radiopath.

The SIM, as part of the authentication processing, verifies that the MAC received in the AUTN token matches the XMAC that is computed. If the two authentication codes are not equal, the SIM returns a reject message to the network and aborts the process. The SIM also verifies that the sequence number is valid. If both of these checks yield positive responses, indicating a legitimate wireless network, the SIM returns the RES value to the network, used subsequently to validate the SIM (mobile user). The mutual authentication as described (without full protocol and cryptanalysis), appears to accomplish the goal of defeating fake base station attacks should they ever be attempted.

Authentication Vectors

Prior to performing air-interface authentication of a mobile station, a visited system must have authentication vectors (quintuplets of security-related data) from the mobile user's home system. The visited system invokes procedures to request authentication vectors from the home AuC which is responsible for the generation of cryptographic keys, random number, sequence numbers and other cryptographic output parameters. This processing is analogous to the triplet requests for the existing GSM system. The visited system sends the request to the home AuC specifying the identity of the user and a mode parameter (MODE) that indicates whether the mobile is packet switched or circuit switched network node. Upon receipt of the authentication vector request, the home AuC sends (by computing in real-time or obtaining precomputed from the HLR database) vectors to the requesting system. The authentication response back to the visited system is an ordered array of authentication vectors AV(1 to N). The authentication vectors comprise the RAND, XRES, CK, IK, and AUTN. This list of parameters is analogous to the smaller GSM triplet (RAND, SRES, and Kc) processing in GSM. The other vectors are computed using the network algorithms that are analogous to the algorithms shown in Figure 3 within the SIM.

This authentication vector request and response process is illustrated in Figure 4.

Figure 3. Authentication and Key Generation Function in User SIM

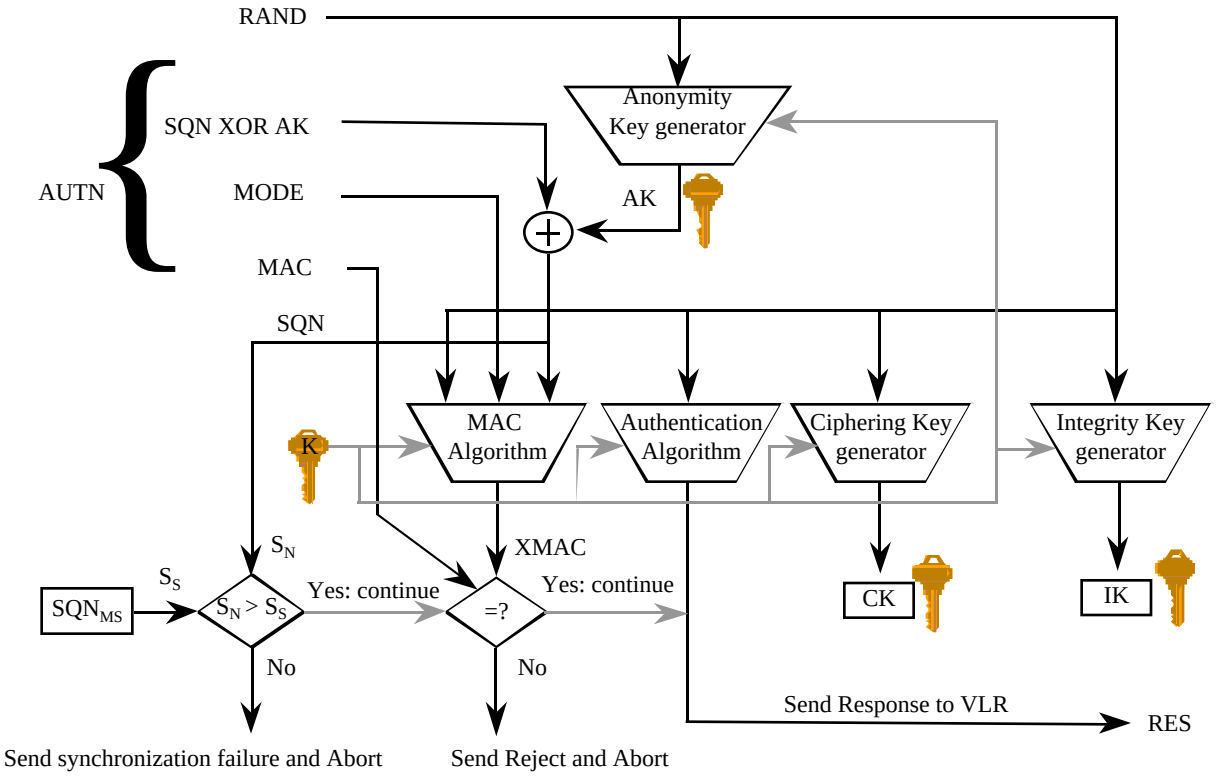
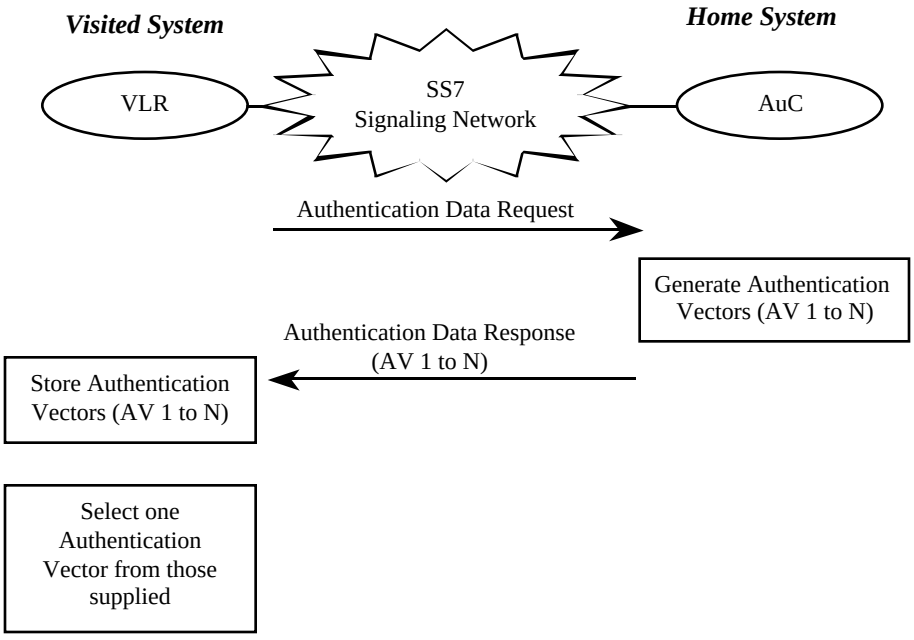


Figure 4. Authentication Vector Establishment between Home and Visited System



Assumptions

As in the GSM system, the 3GPP proposal assumes two things:

1. That the home system trusts the visited system to handle cryptographic keying material and to authenticate mobile subscribers, and
2. That the intersystem signaling links are "secure". The 3GPP proposal does not address the security of signaling message transport between network elements. The links of this network are not cryptographically secure and could be exploited by an insider or determined adversary. The TIA AHAG and member companies still have not addressed this issue. However, until, there is proof that these links have been compromised, the security of SS7 and network elements is likely to continue to remain on the back burner.

Does 3GPP AKA Meet the AHAG Requirements?

We consider whether 3GPP AKA meets each of the security requirements proposed by the TIA AHAG (*ad hoc* Authentication Group):

1. ESA shall employ cryptographic algorithms and protocols that have been standardized and have been openly published and scrutinized.

   3GPP meets the requirement. The 3GPP proposal was developed using experts from ETSI and ARIB. The development process was both open and rigorous.

2. ESA shall use an authentication key that is 128-bits in length.

   3GPP meets the requirement.

3. ESA shall provide a means to provide mutual authentication: authentication of the mobile station to the network and authentication of the base station to the mobile phone;

   3GPP meets the requirement.

4. ESA shall provide authentication without the use of the mobile station hardware serial number (e.g., the ESN or IMEI).

   3GPP meets the requirement. The hardware identity of the mobile is not used in any of the authentication procedures.

5. ESA shall provide backwards compatibility with the existing CAVE-based authentication scheme.

   It is believed that the 3GPP proposal can meet this requirement.

6. ESA shall provide a SIM (Subscriber Identity Module) interface.

   3GPP meets the requirement. As in the GSM system, the SIM is a fundamental component of the 3GPP proposal. It is used as a primary mechanism for seed key distribution and operational cryptographic processing.

7. ESA shall provide the means for the negotiation of air-interface and network cryptographic algorithms.

   3GPP does not meet this requirement specifically. However, the 3GPP mechanism was designed in the spirit of this requirement.

8. ESA shall use SHA-1 for cryptographic hashing.

   3GPP can be configured to meet the requirement. It does not preclude the use of the National Institute of Standards (NIST) developed SHA-1 message digesting algorithm.

9. ESA shall use the HMAC-SHA-1 for any message authentication code (MAC) functions.

   3GPP can be configured to meet the requirement. It does not preclude the use of this approach to MAC computations to prevent certain birthday attacks.

Additionally, 3GPP AKA meets some additional critical system requirements of AHAG for next generation security systems:

1. The security of the system should not negatively impact the end-user or the operator.
2. The ESA candidate 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 Probe Further

In this issue we presented the most salient points about 3GPP AKA. However, we obviously could not cover all aspects of the proposal. For example, sequence number generation mechanisms and re-synchronization methods were not presented. For more information on these topics or for full details of the 3GPP proposal, either contact:

Tim Wright, Vodafone
email: timothy.wright@vf.vodafone.co.uk

Or download the detailed specifications from:

ftp://www.3gpp.org/Specs/October_99/33_series/

Many of the terms and acronyms used in this paper are defined at:

www.cnp-wireless.com/glossary.html

Definitions and Acronyms

Many of the terms used in this issue are listed at:

www.cnp-wireless.com/glossary.html

AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher (encryption) Key
ESA	Enhanced Security and Authentication
IK	Integrity Key
KG	Key Generator function
MAC	Message Authentication Code
RAND	Random Number
SIM	Subscriber Identity Module
SQN	Sequence Number
XRES	Expected Response