Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe

Vol. 2, No. 4 May, 2000

Lucent Technologies on 3G Authentication

The choice of authentication system for 3G systems has proven to be very controversial. In our October, 1999 issue we discussed four candidate proposals. After eliminating two public key encryption systems as being too complex and resource intensive, TIA TR-45's AHAG (ad hoc Authentication Group) was left with a choice between Lucent's LESA which, roughly speaking, is a 3G version of the CAVE authentication system used in analog, TDMA and CDMA systems today, and 3GPP's AKA, which is a 3G enhanced version of the GSM authentication system.

The choice that was made by AHAG was 3GPP AKA. In this article, three employees of Lucent Technologies, Technical Manager Semyon Mizikovsky and Members of Technical Staff Adam Berenzweig and Michael Marcovici, describe their company's perspective on how best to achieve a single, global, 3G authentication standard.

Global Roaming and Security: Let's InterWork Together

Global roaming promises to be an important new feature of third generation wireless systems. In the highly-connected business world, travellers have come to expect global access to information services. But for the most part, mobile phones have remained frustratingly bound to local systems. A business traveller hopping the Atlantic will need a new phone upon landing - a GSM phone for Europe, and an TIA/EIA-41 phone for North America. What part does security play in the barrier between these two systems? How can third generation systems remove these barriers while keeping the important security features that exist today? This article examines these issues and describes some recent developments in the 3G security standards bodies that impact the deployment of secure and efficient global roaming.

To understand the problems involved, we briefly describe the historical reasons for the differences between GSM and TIA/EIA-41 security systems. Then we look at the current Authentication and Key Agreement (AKA) proposal for 3G systems, focusing on how it supports global roaming, and examine its impact on the rest of the system.

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery by emailed PDF file or by first class mail 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 to allow more readers.

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

Back issues are available individually, or in bulk at reduced prices.

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 Issue Due…

June 15th, 2000.

Future Topics

Voice over IP security • Public Keys & Wireless • Kerberos • Public Key Infrastructure • IP Security • IKE • EPE • Wireless Data 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: $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, Diners Club, 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.

Today's Cellular and PCS Authentication Systems

The designers of the current GSM and TIA/EIA-41 security architectures took fundamentally different approaches to accomplish the same goals. Network operators wanted to protect themselves against fraud and protect the privacy of their users. They also wanted to maintain control over security functions, especially when the subscriber roams to other networks. How can the network operator control authentication when the user roams into a visited network? The two systems approach this question in different ways.

GSM Approach

GSM designers chose a simple and elegant authentication system where the home system controls all security keys and distributes pre-calculated authentication information to visited networks. They also designed the User Identity Module (UIM), a secure processing environment inside the mobile that stores security keys and calculates authentication information. Additionally, they chose to use mandatory encryption of dedicated traffic channels (e.g. all voice traffic).

Because authentication calculations are only performed in two places (the UIM and the home Authentication Center – both controlled by the network operator), GSM operators have full control over which authentication algorithm to use and when this algorithm is compromised, can arrange for its replacement in the Authentication Center and all UIM cards. The security keys are kept tightly guarded in these two environments, providing easier security management.

When a subscriber roams into a visited network, the visited location register (VLR) requests authentication information from the home system. The pre-calculated authentication information is known as an authentication triplet because it contains three values – challenge (RAND), response (SRES), and encryption key (Kc). Triplets can be generated offline and stored in a database until needed, so the demand for real-time processing is low at the Authentication Center (the trade-off is the need for lots of storage). Triplets are delivered to a visited system in batches where they are used, one per connection, to authenticate and encrypt communications with the mobile (See Figure 1). For a detailed description of the GSM security system, see the January 2000 issue of this publication, or visit www.gsm.org or www.etsi.org.

TIA/EIA-41 Approach

The designers of TIA/EIA-41 security architectures took a different route to satisfy some additional requirements, in particular TIA/EIA-41 authentication was designed to combat a real fraud problem that was costing the industry a million dollars a day (cloning). The goal was to minimize additional network traffic, while also providing "pre-call" authentication of the subscriber on the control channel before giving up a whole dedicated traffic channel for the call. The idea was to prevent false subscribers (cloners) from wasting bandwidth. In contrast, GSM systems perform authentication on the dedicated traffic channel after call setup.

The resulting solutions were the Shared Secret Data (SSD) to minimize network traffic, and Global Challenge for fast pre-call validation.

The SSD is a secondary key, derived from the root key (A-key), that can be shared with a visited system. This way, authentication can be performed locally between the mobile and the VLR, with no further traffic back across the network. Pre-call validation is made possible by broadcasting a Global Random challenge (RAND) that is updated periodically. The mobile includes a calculated authentication response (AUTHR) with its initial access message so that authentication can be performed before allocating radio resources.

This scheme of sharing a key with the visited system only works if all VLR's in the system have the same authentication algorithm. TR-45 chose CAVE as the standard authentication algorithm for TIA/EIA-41 systems. Also, once keys are shared with visited systems, home service providers give up some control of the authentication process. To give operators back the control they rightly demand, the standard (originally TSB-51, and later IS-41-C and TIA/EIA-41-D) also includes signaling messages that empower the home system to, at any time, revoke or update the SSD or issue a unique challenge to a suspicious mobile. The serving system will report the success or failure of these home-initiated security operations.

2G Authentication Compared

In practice, aspects of both the GSM and TIA/EIA-41 systems have proven problematic. In GSM systems, the transmission of many authentication vectors between home and visited systems can result in a lot of network traffic. To reduce this traffic, serving networks often re-use a single batch of triplets for many calls, severely impacting the security value. The subscriber's home operator, which is financially responsible for the call, has no control mechanism to limit this vulnerability.

Furthermore, network outages can cause a similar problem. In an ironic illustration of this problem, on the first day of a GSM security standards group meeting, an SS7 network outage isolated the host city from the rest of the GSM network. Everyone who arrived before the outage and used their phones allowed a few triplets to be moved over from the home system. People who arrived after the outage couldn't get service, while the early-birds' phones apparently re-used the same triplets for the week.

In TIA/EIA-41 systems, some operators have proven reluctant to share SSD with other network operators. This obviously impacts network efficiency because authentication requests must travel back to the home system in real-time if SSD is not shared. However, SSD sharing is common within the network of an operator, and we are beginning to see SSD sharing between operators as they become comfortable with the concept.

Tomorrow's Systems: AKA

As described in the December 1999 issue, the Authentication and Key Agreement (AKA) proposal has been selected by both TR-45 and 3GPP to be the authentication system for 3G networks…Almost. TR-45 has decided to adopt AKA "*as the basis of its ESA solution provided that it can be modified as required to meet all TR-45 requirements including global roaming*". Specifically, TR-45 drew up a list of requirements for ESA (Enhanced Subscriber Authentication) when it began soliciting proposals for the 3G security system. While AKA satisfies most of these requirements (see the December issue for details), there are a few that it does not. These discrepancies can be traced back to the original differences between the GSM and TIA/EIA-41 security philosophies.

At a recent joint meeting between the security groups TR-45.AHAG and 3GPP SA3, the members discussed a list of TR-45 requirements not currently met by AKA. The recommendations roughly fell into two categories:

- Home system control
- Global challenge

Home System Control

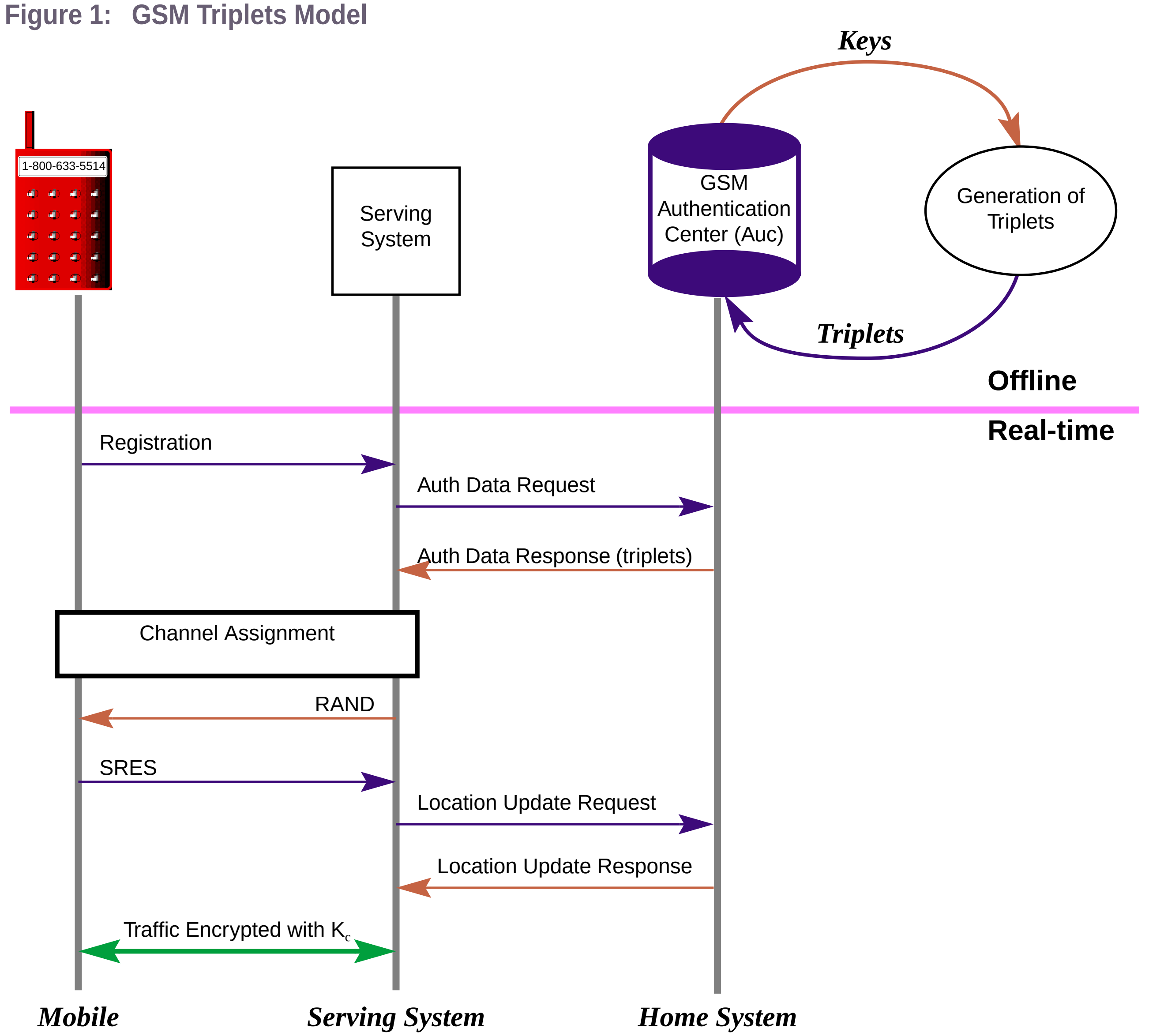
TR-45 requires the Home System to be given the following authentication control capabilities:

1. Ability to revoke the current Security Association (SA) thereby causing an Authentication Vector (AV) update,
2. Ability to control the duration of the Security Association, and
3. Ability to request that the Serving Network (SN) report both success and failure of the AKA procedure.

Note that these are not new features for TIA/EIA-41 networks, they are merely existing system requirements being carried forward to 3G systems. What is very interesting is that 3GPP is now struggling with many issues similar to those that drove the TIA/EIA-41 designers to implement these requirements for home system control.

There are important differences between the AKA proposal and the existing GSM

Figure 1: GSM Triplets Model



security system. For starters, mandatory encryption of all traffic channels is no longer possible due to international political restrictions. In GSM, mandatory encryption provided some form of continued authentication by effectively preventing channel hijacking. Furthermore, stream cipher encryption (which is used in all wireless systems because it does not cause error propagation) does not provide integrity protection. If an attacker knows the location of bits in the stream, she can change bits without knowing their contents. As a result, 3GPP must rely on a new mechanism to prevent channel hijacking and provide data integrity. The solution was to add a second key, called the Integrity Key (IK) to the Authentication Vector; IK will be used for periodic local authentication procedures and to calculate a data integrity Message Authentication Code (MAC) on critical messages.

Due to performance optimization requirements, the Ciphering Key (CK) and the IK are exported from the UIM to the mobile shell, where the encryption and integrity calculations are performed. CK and IK are delivered to the Serving System in the Authentication Vector so that it can locally decrypt and authenticate messages from the mobile. Sound familiar? It is similar to the SSD concept used by TIA/EIA-41 networks. The 3G security specification, 33.102, does not mandate that the AKA procedure be performed at every call setup. In fact, it is assumed that most operators will only perform AKA periodically, and will keep the same CK,IK pair for many calls in order to reduce network traffic and speed call setup time. Sound familiar? These are also benefits of the SSD approach.

However, with these benefits come additional risks. In 33.102, 3GPP acknowledges that "there is the possibility of unlimited and malicious re-use of compromised keys". In fact, at the joint AHAG/SA3 meeting, TR-45 raised concerns about the possibility of a Trojan horse "rogue MS-shell". A public phone or a rental phone could be modified to record the CK,IK pairs from UIMs that are inserted into it, and re-use these keys after the UIM has been removed. Although 3GPP provides a mechanism to limit the "Cipher key and Integrity Key Lifetime" (the UIM keeps a usage counter for each key, and forces an AKA update if the counters reach some limit), this solution does nothing to prevent the rogue mobile scenario.

TIA/EIA-41 systems developed more powerful capabilities for Home System Control to counter the theft of SSD, a risk they understand very well. Now 3GPP faces a very similar problem, and the TR-45 requirements for Home System Control are needed in 3GPP.

At the joint meeting, 3GPP expressed willingness to consider including the requested support in the next revision of the Security Architecture Specification (Release 2000). The changes required by TR-45 are limited to some additional network messages and minor VLR procedural changes.

Broadcast Challenge

TR-45 has decided that Broadcast Challenge is mandatory for all mobiles operating in TIA/EIA-41 networks, and is still debating whether Broadcast Challenge must be supported on initial registration.

AKA in its original form standardized by 3GPP cannot support Broadcast Challenge. Again, the problem can be traced back to a basic difference between GSM and TIA/EIA-41. Because GSM designers wanted to keep the keys and algorithms under control of the home system, it was not necessary to build an Authentication Center that could calculate authentication triplets in real time. Triplets are calculated only using parameters generated by the home system, whereas in TIA/EIA-41, authentication calculations are made in real time at the AC or VLR/MSC, in response to the Global Challenge RAND generated by the serving system. The GSM design was carried forward into 3GPP AKA, and as a result, AKA cannot support Broadcast Challenge.

On the other hand, AKA is very effective in establishing the Security Association, by setting up the keys needed for secure communication between the mobile and the local serving system. Therefore, a potential strategy is to use AKA as a substitute for SSD Update, which will be performed when a mobile registers in a new system. The Security Association would be valid for the duration of registration, where it would be used in a classic Broadcast Challenge scheme.

The impact on the performance of Initial Registration has been examined by the TR45-2 Enhanced Security Focus Group. The ESFG is very sensitive to performance issues caused by authentication, as it just completed IS-778 partly to fix some performance issues involved with authentication at initial registration (see the April 2000 issue of *Wireless Security Perspectives*). Lucent Technologies studied the impact of AKA on system resources (Contribution TR-45/2000.03.08.31). As expected, AKA is less efficient than Global Challenge on Initial Registration. An extra round-trip of network messaging may be required because the authentication data request cannot be combined with the Location Update Request (see Figure 2). With Global Challenge, these two messages can be combined (or run in parallel) because the VLR can send the authentication response to the Global Challenge in the first message. Additionally, there is a potentially significant delay before the mobile can be de-registered from the previous serving network (de-registration cannot occur until the home system receives a Location Update message).

This delay also impacts system capacity. The problem is that AKA must be performed on the traffic channel, unlike Global Challenge which can be performed on the control channel. At peak load, this can amount to a 4% reduction in Erlangs of system capacity. Furthermore, the load on the control channel is not lightened either! The control channel must handle the messages for paging and channel assignment needed to set up the dedicated channel for AKA. This could potentially double the number of Call Termination messages carried on the control channel.

TR-45's Conundrum

This is what TR-45 means when it says that it is still debating whether Broadcast Challenge must be supported at Initial Registration. The 3GPP security scheme based on AKA cannot and does not have to handle it, but leaving it out creates a sizeable impact on authentication speed and system capacity, and significantly increases intersystem network traffic and control channel traffic.

It should be noted that TIA does not expect 3GPP AKA to be modified to support Global Challenge, nor is 3GPP expected to deploy the Global Challenge in UMTS systems. The proposed changes to AKA are TIA/EIA-41 implementation specific (i.e. optional operational procedures). The target is to create a common worldwide method for establishing security association, which will then be used with whatever scheme the local serving system chooses to deploy. So the debate goes on.

Conclusions

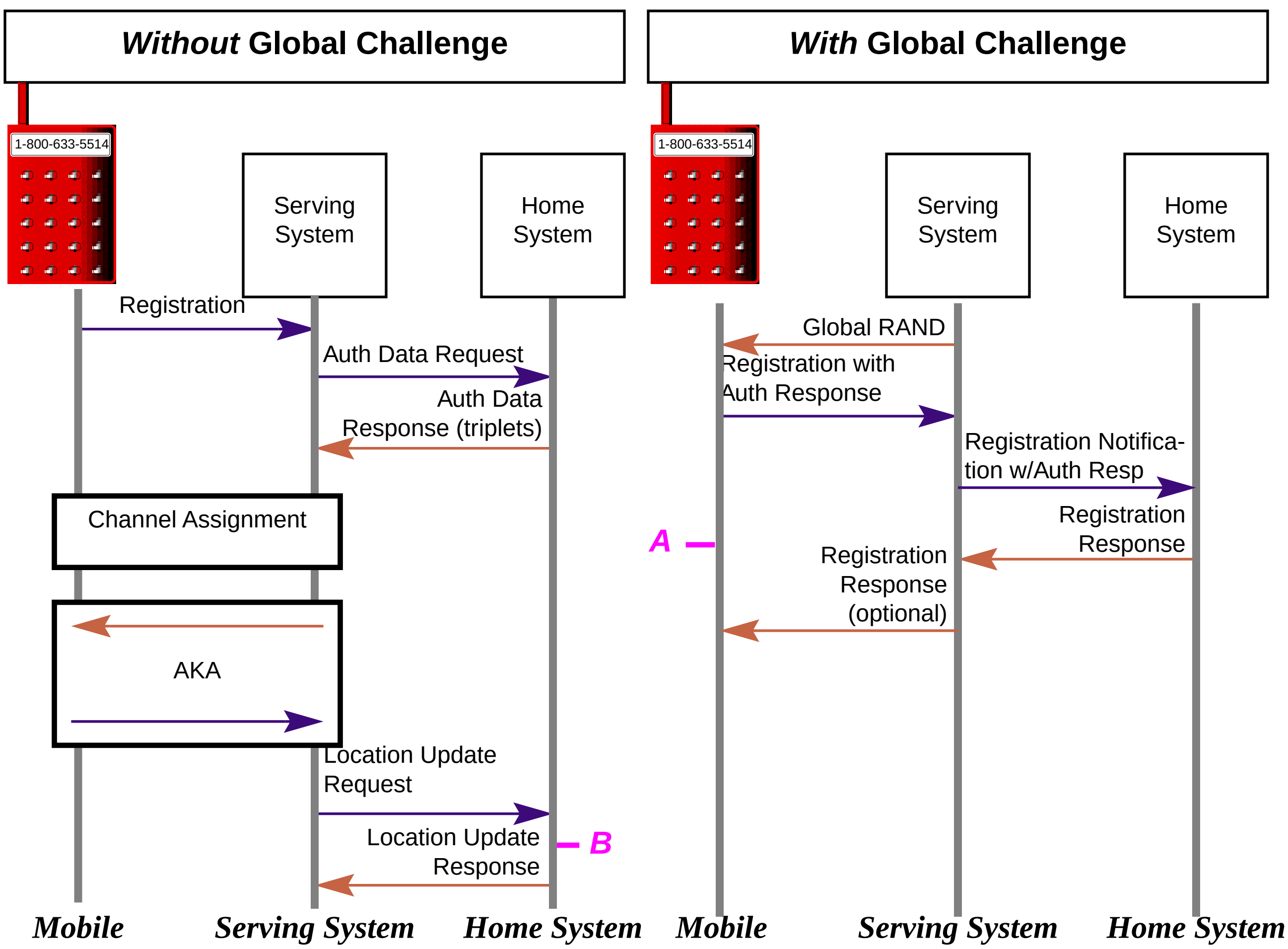
Is AKA better, worse, or just different from what we have in TIA/EIA-41 systems? Can we benefit from commonality with UMTS without losing the efficiency of Broadcast Challenge and SSD? Global roaming is on the horizon. It comes at a price, but hopefully not at the expense of operational efficiency and central control currently available to TIA/EIA-41 network operators. A few issues are still being worked out in the standards bodies, but it seems that the two worlds of 3GPP and TR-45 are cooperatively working towards this important goal.

Postscript

We invite those who have other views on AKA and 3G authentication to respond to this article. Does AKA need modifications to achieve a full set of requirements? Are Home System Control and Broadcast Challenge really major issues?

If you have comments or questions on this article you can forward them to us (crowed@cnp-wireless.com) or to Semyon Mizikovsky (smizikovsky@lucent.com).

Figure 2: Initial Registration *with* or *without* Global Challenge



At time A, the system with Global Challenge has registered the mobile and can send a de-registration to the old serving system. This cannot be done in the system with no Global Challenge until time B.