Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 5 June, 2000

Response to *Global Roaming and Security*

by Frank Quick, QUALCOMM Inc. (fquick@qualcomm.com) and Greg Rose, QUALCOMM Australia (ggr@qualcomm.com)

We are pleased to publish a response to our major article in the May, 2000 issue of Wireless Security Perspectives by two members of the TIA ad hoc Authentication Group (AHAG), including the vice-chair (Frank Quick).

The May, 2000 article entitled *Global Roaming and Security* by Mizikovsky, Berenzweig and Marcovici provides a well-prepared and generally balanced treatment of 3G authentication. There are, however, a few points that bear further discussion.

Network Traffic

In the introductory paragraph, the authors state that there were two common goals of the GSM and TIA/EIA-41 authentication designs. These were to protect against fraud and privacy invasion, and to maintain home system control over security functions.

There is, however, a third important goal: to minimize the SS7 network traffic that is required to support security functions. Without this goal, it would be trivial for the home system to maintain control of security functions simply by having all security functions take place in the home system. The current cost of SS7 traffic makes this simple approach undesirable. The authors defer discussion of this third goal until the later section describing the TIA/EIA-41 approach, thus giving the impression that this goal was present only in the TIA/EIA-41 development. It seems clear, however, that the GSM system was also developed with this goal in mind. GSM approaches this objective by essentially the same method as TIA/EIA-41, which is to transfer authentication key material to the visited system. This allows authentication to take place in the visited system for a controlled period of time, without further SS7 messaging to the home system during that period.

Unlike GSM, the TIA/EIA-41 system makes sharing of the authentication keys optional. This gives the home system the capability to force all authentication functions to take place in the home system by withholding the keys. That the GSM system designers did not provide such a capability suggests that the greater concern in GSM may, in fact, have been to limit network traffic, rather than to provide home system control of authentication.

The authors argue that, in practice, the GSM implementation has not provided a significant reduction in network traffic because many triplets have to be transferred in order to have enough to authenticate all the calls made while roaming in a visited system. This still does not mean that reduced network traffic was not a goal of the GSM design. The intent of the GSM design was that encryption would provide an implicit authentication: if the terminal and visited network can

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…

July 17th, 2000.

Future Topics

Voice over IP security • Public Keys & Wireless • Kerberos • Public Key Infrastructure (PKI) • IP Security • IKE • TDMA Enhanced Privacy & Encryption (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.

successfully invoke encryption, the terminal can be considered authentic. To support this implicit authentication, GSM provides a mechanism for the terminal and serving system to determine that they each have a common ciphering key. If a common key is present, there would be no need to use a new triplet. The existence of this mechanism for key reuse is a very clear indication that GSM was designed with minimization of network traffic in mind.

Of course, as the authors point out, this sort of implicit authentication is not available in systems where encryption is not used. In that case, use of a triplet per call may be necessary. In recognition of this, one of the enhancements that has been provided in AKA is to add a second local key for authentication and integrity checking (IK – Integrity Key), so that authentication can be performed in the visited system without using a new authentication vector, and without requiring encryption. This enhancement should allow 3G systems using AKA to achieve the intended reduction in network traffic in all systems.

Pre-Call Authentication

The authors state that another design goal for TIA/EIA-41 is "providing 'pre-call' authentication of the subscriber on the control channel before giving up a whole dedicated traffic channel for the call." This goal is, indeed, limited to TIA/EIA-41 systems, because it is only in TIA/EIA-41 systems that the resources consumed by allocation of a dedicated channel are considered so significant that the use of dedicated channels needs to be minimized. This is a legacy of the AMPS system, where the limited channel capacity dictated the use of a random-access control channel to perform system access requests. The early TDMA system (TIA/EIA/IS-54) used the same analog control channels as AMPS, and the CDMA system (TIA/EIA/IS-95) incorporated the same random access protocols on its digital control channels.

To support "pre-call" authentication, the systems using the TIA/EIA-41 network provide a "broadcast challenge" procedure. In this procedure, the base station broadcasts a random challenge value, and the mobile stations use the challenge value to calculate an authentication signature. The signature is returned in all reverse control channel messages that request service.

In the GSM system, in contrast, the dedicated channels were designed to support low-rate signaling without excessively consuming system resources. Since the GSM design makes dedicated channels usable for all functions, the reverse control channels were reduced to the very minimum required to obtain a dedicated channel.

The authors state that "AKA in its original form standardized by 3GPP cannot support Broadcast Challenge." But it is hardly a property of AKA itself that broadcast challenge cannot be supported. It would be more correct to say that the specifications developed by 3GPP do not support a broadcast challenge, and the reason is that the 3GPP system does not need a broadcast challenge. Once the AKA authentication keys are transferred to a TIA/EIA-41 serving system, there is no reason that the serving system cannot use the keys to perform a broadcast challenge, and we believe that is precisely what should be planned in the TIA implementation of AKA.

AKA as SSD Update

The authors describe the AKA process as "establishing the Security Association", and state that it can be a "substitute for SSD Update". It is important not to make too much of this analogy, since the intent of AKA is to establish a key that is valid only for the duration of the registration, whereas SSD can be updated much less frequently, or not at all.

Indeed, many service providers update SSD very infrequently, because the update procedures on the air interfaces and the TIA/EIA-41 network are far from robust. Current TIA/EIA-41 procedures for failure handling are seriously flawed, such that certain failures of the air interface or network messaging cause the home system to discard the pending SSD even though the terminal has changed its stored SSD. All subsequent authentications fail until another SSD update is successfully completed. Work is underway in TR-45.2 to fix these flaws, but in the meantime SSD updates are not being done as often as security concerns would require.

In this respect, we believe AKA is a procedure that is superior to SSD, and that its use will eliminate the problems with SSD update without requiring complex network procedures.

Initial Registrations

The authors state that "An extra round-trip of network messaging may be required because the authentication data request cannot be combined with the Location Update Request". It would be more correct to say that the 3GPP network messaging is similar to GSM, where the Location Update is not sent until authenticity is proven. There is no reason why the location update and authentication data request cannot still be combined in TIA/EIA-41 systems.

Looking closely at the cited Lucent contribution (TR-45/000308-31), the following observations can be made:

- The extra round-trip delay applies only to the completion of location updating, not to the provision of service. (Service can be provided as soon as the home system sends the user profile and the user authenticity has been established at the serving system.) Thus, the delay has no effect that is perceptible to the user during "implicit" registrations, where the user has originated a call in a new system without previously registering.
- For initial registration, the extra delay appears to be around 4 seconds out of a total of about 8 seconds for the scenario offered in the contribution. This extra delay will increase in international roaming scenarios, but no estimate has been offered for the increase.
- A significant part of the extra delay is in dedicated channel setup. The contributors assume that AKA must be performed on dedicated channels because control channel messaging is not robust enough. We believe, how-

ever, that simple procedures can make AKA robust on control channels, eliminating some of the extra delay. Such procedures were presented in contribution TR-45/000308-40.

- For "implicit" registrations (i.e. where the registration occurs because of a call origination) the extra delay is much less than stated above, because the setup of a dedicated channel occurs in parallel with the network transactions.
- The extra delay has no important effect on initial registration immediately after power-up, since the user cannot have expected calls to be delivered while the phone was off.
- The extra delay does increase the period, after entering a new serving system, during which location pointers are incorrect. During this period, incoming calls would not be terminated to the mobile. This could have a noticeable effect if the terminal is moved between systems while powered.

QUALCOMM has studied the registration delay issue, and has concluded (contribution TR-45.AHAG/2000.05.09.07) that simple procedures in the home system would permit the use of broadcast challenge for the authentication of initial registrations, thereby eliminating the extra delay. The proposed procedure is as follows:

1. The home system stores IK, and uses it to validate any messages containing broadcast challenge results that are received by the home system. We would expect that only initial registrations, including implicit registrations, would contain such challenges.
2. Whether or not the broadcast challenge passes, the home system always sends a new AV to the visited system. This establishes a new CK and IK in the mobile equipment (ME).
3. If the broadcast challenge fails, the home system will request that the visited system report the success of AKA, and will wait for the success report before updating location pointers. If the broadcast challenge succeeds, the home system will update location pointers immediately. Note that the first communication from 3GPP visited systems will be an authentication vector request. This will not include a broadcast challenge, nor will it request location updating. The location update request will follow successful AKA. Thus, an authentication success report from the 3GPP system is not needed.
4. In the visited system, CK and IK are used to cipher and authenticate all common control channel transactions. CK and IK can be used to derive call session keys at the time of origination or page response.
5. In the mobile station, the ME receives IK from the UIM and uses it to respond to broadcast challenges. The ME deletes IK when the UIM is removed or the ME is powered off. The UIM may optionally store IK for use in broadcast challenges when the ME is next powered on.

Note that the loss of IK in the home system, unlike a failure of SSD update, has no service-affecting consequences. If the home system has the correct IK, it can verify the broadcast challenge and can process the registration immediately. If the home system does not have the correct IK it only has to wait for the authentication report from the visited system before completing registration. Thus, a home system need not implement IK storage at all if it is found that the registration delays are acceptable without broadcast challenge processing. If the home system implements IK storage, we would expect that broadcast challenges would succeed in almost all cases, effectively eliminating any concern about the delay in registration.

Integrity Checking

The authors point out that stream cipher encryption does not provide integrity protection, and note that 3GPP "must rely on a new mechanism" to provide integrity. But this is not specific to 3GPP. We are unaware of any TIA system that will not also use stream ciphers. We would expect all 3G systems to utilize MACs to protect critical messages against spoofing.

The "Rogue Shell" Threat

A security issue that has been raised by the TR-45 AHAG relates to the possibility that a removable UIM could be inserted into a device that would take the local authentication and ciphering keys from the UIM and use them to create clones within the visited system. For example, a reprogrammed ME "shell" holding a legitimate UIM could transmit the keys to the intended clone via Short Message Service or a data service. Some carriers believe this to be a real security concern that should be addressed by both TIA and 3GPP. TR-45 has directed the AHAG and TR-45.2 to investigate this issue as a priority.

The 3GPP approach to this threat would be to use a new AV for each call, or to force use of a new AV after some number of uses of the ciphering and integrity keys, thereby preventing or limiting reuse of the keys. This, however, would increase network traffic significantly, to deliver the increased number of AVs that would be needed. Of course, if the threat never actually materialized, there would be no adverse impact on the 3GPP network traffic.

It appears that any solution to this threat that does not increase network traffic requires keeping some secret information inside the UIM and using that information in some, or all, local authentication procedures. If a necessary secret is kept inside the UIM, no ME without a legitimate UIM can correctly perform these procedures. For example, if the integrity key IK were kept inside the UIM and not passed to the ME, and all procedures using IK were performed inside the UIM, there would be no rogue shell problem. Alternatively, one could create a new integrity key that could be passed to the ME for most message integrity operations, while keeping another key inside the UIM for local authentication.

The authors seem to link this problem to the TIA's "Home System Control to counter the theft of SSD", where SSD is not shared, and all authentications must take place in the home system. This, however, would not mitigate the rogue shell threat; it is the keeping of SSD

inside the UIM that would mitigate the threat. "Home System Control" of this sort appears only to increase network traffic without affecting the threat.

At present, it seems 3GPP does not take the rogue shell threat seriously enough to address it using new authentication procedures, preferring to rely on more frequent use of the existing AKA procedure. TIA/EIA-41, in contrast, can address the threat using existing broadcast and unique challenge procedures, provided that the key material used for these procedures remains inside the UIM.

The debate within both TR-45 and 3GPP over the next few months will likely center on the seriousness of the threat itself. If the threat is to be taken seriously, the groups will then have to determine whether the additional network traffic to mitigate the threat is sufficiently burdensome to warrant the development of new, more network-efficient local authentication procedures.

Is there a "Conundrum"?

The authors describe the discussion of AKA in TR-45 as a "conundrum." According to Webster's New College Dictionary, a conundrum is:

1. A riddle in which a fanciful question is answered by a pun;
2. a. A problem with no solution; or
   b. A complicated problem.

At the most, definition 2b. might apply to the situation in TR-45. However, TR-45, during the meeting held May 31st-June 1st, 2000 in Chicago, Illinois, directed the AHAG and TR-45.2 to proceed to develop AKA. This is a clear indication that TR-45 believes that any problems with AKA can be resolved, hence there is no "conundrum" for TR-45. It would seem that TR-45 has investigated the issues thoroughly and has come to the conclusion that AKA is the best solution for 3G authentication. We look forward to continued cooperative efforts between 3GPP and TIA as we develop AKA for use in all 3G systems.

Acknowledgement

The authors thank Bart Vinck of Siemens AG for his helpful review of this article.

Acronyms

Some of the acronyms used this month are:

AHAG	TIA TR-45 *ad hoc* Authentication Group
AKA	Authentication & Key Agreement
AV	Authentication Vector
CK	Cipher Key (e.g. for voice encryption in AKA)
EIA	Electronics Industry Association
GSM	Global System for Mobility
IK	Integrity Key (used for authentication within AKA)
ME	Mobile Equipment ("phone shell", not including UIM)
MS	Mobile Station ("phone", possibly composed of ME plus UIM).
SSD	Shared Secret Data
TIA	Telecommunications Industry Association
TR-45	TIA standards committee responsible for analog, TDMA and CDMA standards
UIM	User Identification Module ("smart card")
3GPP	3G Partnership Project

For a much more complete glossary, please consult:

www.cnp-wireless.com/glossary.html

Coming…EPE

Enhanced Privacy and Encryption is the TDMA community's 2.5G solution for weaknesses in current voice and data encryption that has been developed by TIA subcommittee TR-45.3 for use in the TIA/EIA-136 standards. We will describe this capability in our July issue.