Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 3 April, 2000

Enhancing Network Security: TIA/EIA/IS-778

Wireless network security in the TIA/EIA-41 environment is based on the mature CAVE algorithm. While this is expected to be replaced by ESA (Enhanced Subscriber Authentication), this will not be for a considerable time. And, while the voice privacy and data encryption components have significant weaknesses, CAVE-based authentication is still adequately strong.

The strength of a system is dependent upon the strength of its weakest elements. The best locks in the world will not secure doors made out of balsa wood. Although CAVE is still a relatively strong algorithm, it is embedded in a very complex system, and weaknesses and limitations in that system are to be expected.

History

Support for CAVE-based authentication algorithms in TIA/EIA-41 networks was defined in TSB-51, published in May, 1993. It supported authentication for the majority of network operations, including inter-system handoff, and for calls made or received while roaming or at home. By the time carriers were prepared to implement authentication, IS-41 Revision C was nearly ready for publication (February, 1996), which included all the capabilities of TSB-51, along with some enhancements.

Some further refinements are now necessary, and those were published as IS-778 in March, 1999.

IS-778 Capabilities

IS-778 supports a number of new and improved capabilities, of which the first two are the most important:

- Suspicious call originations,
- Profile before authentication,
- COUNT update after handoff,
- More secure inter-system paging,
- Clarified procedures, and other optimizations and correction.

Suspicious Call Originations

The current method of authentication supported by the TIA/EIA-41 family of radio interface standards (Analog, TDMA and CDMA) is based on a primary level of protection using a Global

Your Shot at a Mug!

We have a limited quantity of handsome, useful and styrofoam-saving double-walled stainless steel coffee mugs adorned with the Cellular Networking Perspectives logo. Some subscribers are already enjoying using them. You too can obtain one by purchasing (or upgrading to) a subscription for more than 25 readers, or by purchasing both a *Cellular Networking Perspectives* and *Wireless Security Perspectives* subscription with a license for more than 10 readers. Contact us soon, supplies are limited!

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 for delivery 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

Lucent's Views on Enhanced Subscriber Authentication.

Next Issue Due…

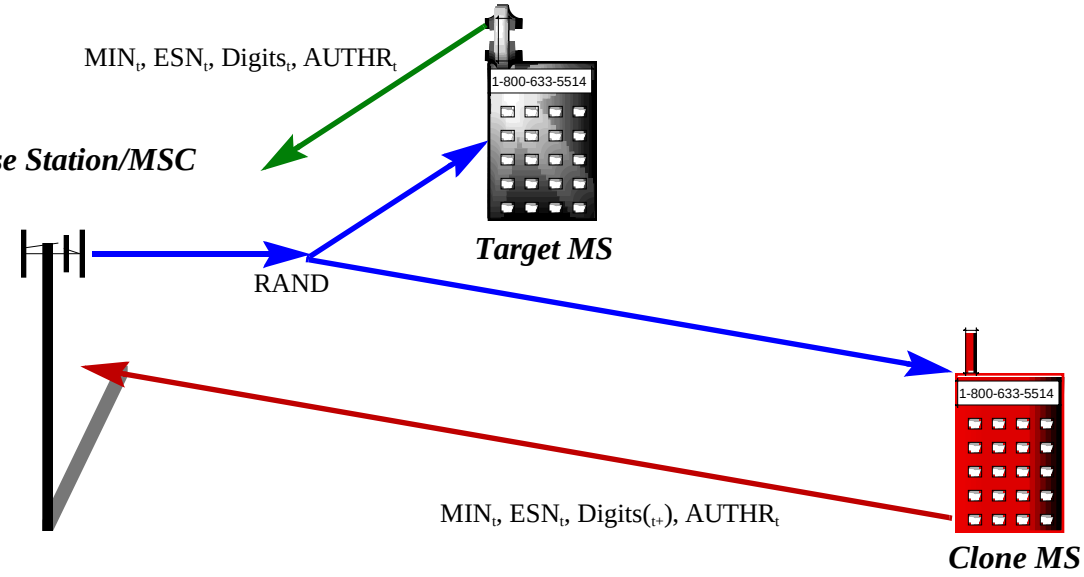
May 17th, 2000.

Future Topics

Voice over IP security • Public Keys & Wireless • Kerberos • Public Key Infrastructure • IP Security • IKE • EPE

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.

Figure 1: Replay Attack on Global Challenge



Challenge, followed by the more secure Unique Challenge, used only if necessary.

Weaknesses of Global Challenge

The calculations used in a Global Challenge and a Unique Challenge are very similar, it is mainly the derivation of the random number used in the challenge that differs. This may make a large difference in the level of security. Because the random number (RAND) used in a global challenge is broadcast to multiple mobiles it may be valid for a significant amount of time (multiple seconds at the very least). By comparison, the random number (RANDU) used in a Unique Challenge is, as the name implies, unique to a single operation, and then, if implemented properly, will probably not be used again for a very long time.

In the simple case of a registration or authentication the global RAND is valid for a lengthy time, the information transmitted by one mobile can be recorded and then replayed by a clone. The relevant information elements transmitted by a target mobile are the MIN (publicly transmitted), ESN (publicly transmitted) and authentication response (AUTHR, publicly transmitted). The secret information that the clone does not know (i.e. Shared Secret Data) is not transmitted, the ability to generate the correct AUTHR is taken to indicate that the clone possesses it.

To combat this problem, mobile originations include the last 6 dialed digits as input to CAVE. Even though these digits are known, it is unlikely that a cloner will want to dial a number that ends with the same last six digits (see Figure 1). However, there are some methods cloners might be able to use to work around this (which we will not divulge here), which can be detected based on a longer than normal dialed digit string, the presence of digits left over after translation or other anomalies.

Unique Challenge to the Rescue

Fortunately, the weaknesses to the global challenge are easily overcome by applying a unique challenge. Because the RANDU used in a unique challenge is used only once, replay attacks are not applicable. So, the attacker may be able to make it onto the porch, but the front door remains secure.

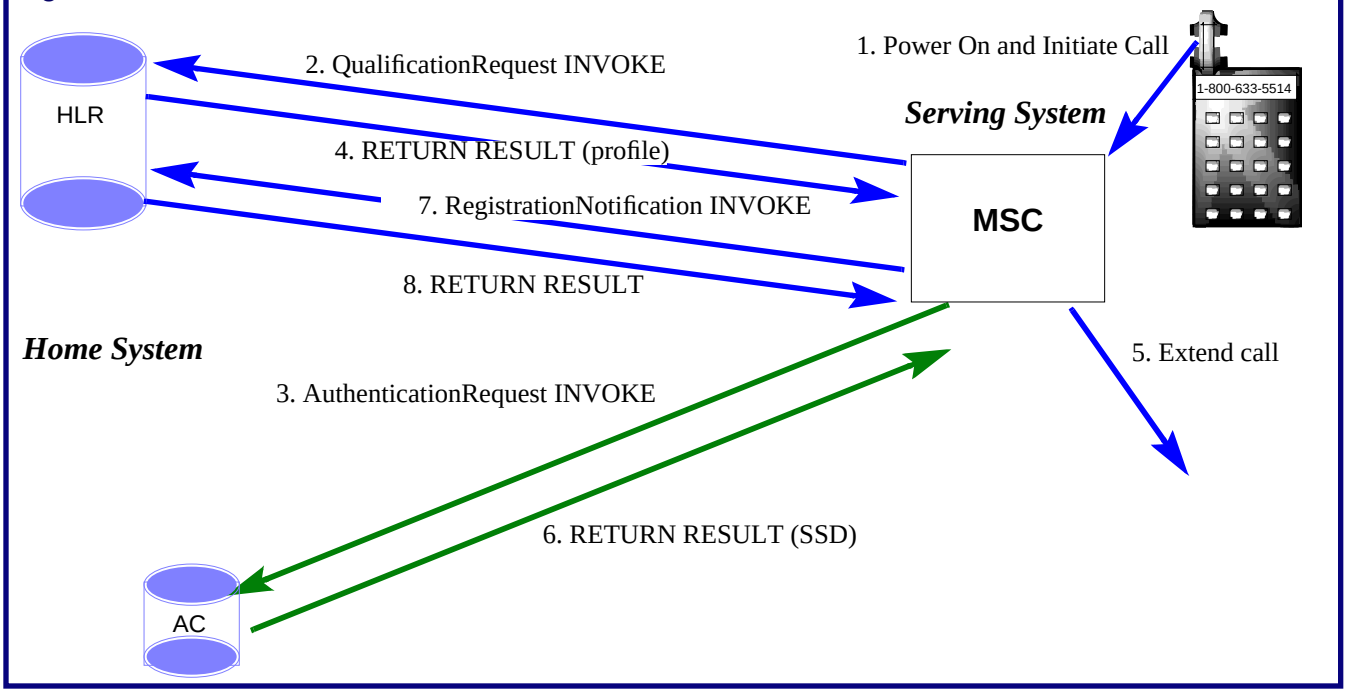
This solution requires no radio interface modifications, because unique challenge is already built in. For systems that allow the sharing of Shared Secret Data, changes are only required in the internal procedures of the MSC or VLR. TIA/EIA-41 changes for intersystem operations are only required for systems that do not share SSD. A new parameter, known as *SuspiciousAccess* is included in the AuthenticationRequest INVOKE from the Serving System to the home system's Authentication Center (AC), which can initiate a unique challenge if it believes it to be necessary.

Profile Before Authentication

Authentication adds complexity to the network, and this sometimes may extend the length of time it takes to process an origination. This is particularly noticeable when a mobile is powered-on and immediately used to make a call.

Authentication, validation and fetching of the profile can normally be accomplished when the mobile first registers, allowing completely local processing of an origination. In the case of an immediate registration, the Serving System must first complete an AuthenticationRequest operation and then, if authentication is successful, initiate a Registration-Notification operation to update the location of the mobile recorded at the HLR, validate the mobile's MIN (or IMSI) and ESN, and to obtain the profile of services for the subscriber. This operation may be dragged out even longer if, as recommended by TIA/EIA-41, the registration in a new system has to wait for the cancellation of the registration in the previous serving system.

Figure 2: Parallel Profile and Authentication



One of the reasons operations are performed in this order is to prevent a clone updating the HLR's location pointer and then failing authentication, thus disabling call delivery until the legitimate mobile registers again. On the other hand, the noticeable delay in call setup can be annoying to customers. Is it possible to both do it right and also do it quick?

QualificationRequest to the Rescue

IS-778 recognizes that the only barrier to initiating a call is obtaining its profile. The call can always be disconnected later if it is determined that the mobile is not authentic. The TIA/EIA-41 RegistrationNotification operation cannot be used prior to authentication because it updates the HLR location pointer, but the similar QualificationRequest operation can be used to obtain profile and to validate the MSID/ESN of the mobile without undesirable side effects. This allows the processing of the mobile origination to begin as soon as the QualificationRequest completes, with the AuthenticationRequest operation being initiated in parallel. Following the completion of authentication, registration can occur to update the HLR pointer as, by this time, the mobile is known to be valid. This process is illustrated in Figure 2.

The downside to this approach is that it actually requires more operations in total, and more complex processing of the parallel operations. The impact on network capacity depends on the percentage of calls that are originated immediately after power-on, which is in turn affected by the cost of incoming calls (or, indeed, the very ability to receive calls) and the battery life of the mobile.

Count Update After Handoff

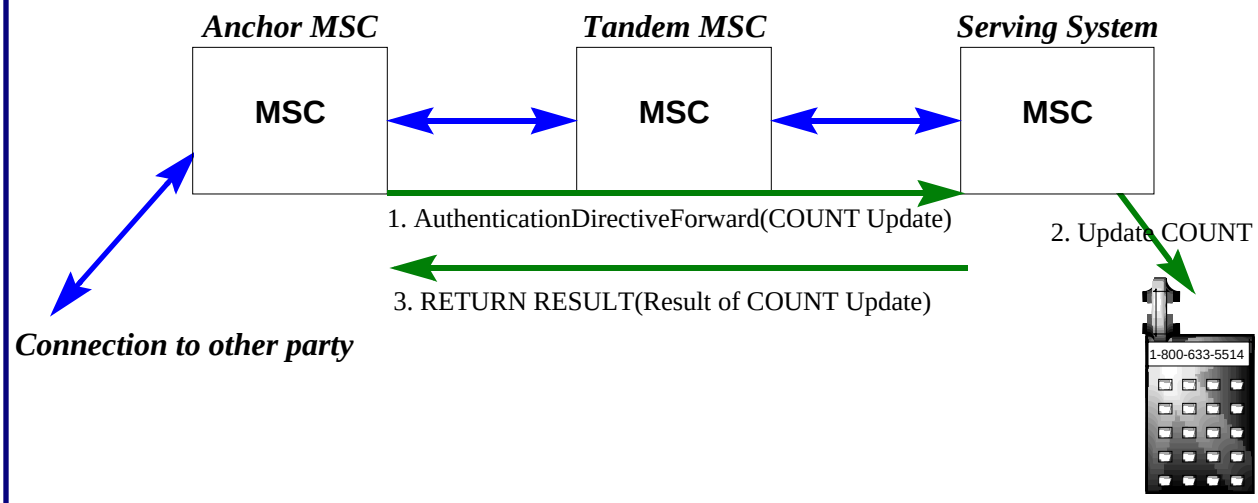
The call history count (COUNT) is used as a complementary mechanism for detecting a clone, one that does not rely on encryption technologies. Both the system and the mobile maintain this number, with the system having the ability to tell the mobile to increment it by one whenever the mobile is on a traffic channel. The phone reports the value every time it authenticates.

Ideally, the values maintained by the system and the mobile should always match. However, the presence of a clone would result in the legitimate phone getting some update commands, and the clone getting others, resulting in a mismatch between the counts, and the detection of cloning.

This technique does have some limitations. Radio interface errors can result in count mismatches, and the technique is relatively easy to defeat if the clone is in the same cellsite as the legitimate mobile (or, is able to monitor the legitimate mobile in some other way). Another limitation has been that once an inter-system handoff has been established, updating COUNT was no longer possible.

IS-778 extends the AuthenticationDirectiveForward operation to allow the Anchor MSC to remotely request that COUNT be updated by the current serving MSC. This command can be passed along the handoff chain, with a response indicating whether it was successful or not (see Figure 3). The response to this message indicates not what the new value of the COUNT is (because the command is always to increment by one), but whether the update attempt was successful. This reduces the chance of the system updating the COUNT when a mobile was not able to due to noise or because it disconnected at about the same time the command was issued.

Figure 3: COUNT Update After Handoff



More Secure Inter-System Paging

There are times when paging has to occur simultaneously in multiple systems, due to a variety of *Border Cell* issues. As with handoff, there are limitations to the authentication operations that can be performed due to the absence of needed parameters from the inter-system paging operations.

One way to avoid failing authentication is for a mobile to merely pretend that it is incapable of performing authentication operations. This loophole was tightened by including authentication capabilities in the subscriber's profile. However, this information is not available to the border system. IS-778 eliminates this loophole completely not by providing the profile to the border system, but by the border system reporting back its authentication capabilities and the terminal type that the mobile reported. These allow the MSC initiating the paging to determine whether a mobile that did not authenticate when paged did so legitimately (e.g. if the border system does not support authentication) or not.

Border cell problems are described in detail in the May, June and July 1996 issues of *Cellular Networking Perspectives.*

Other Improvements

IS-778 includes a major overhaul of the procedures published in TIA/EIA-41 that describe how an MSC, VLR, HLR or AC should handle authentication operations. While the handling of many TIA/EIA-41 operations is self-evident once the purpose of the transaction is understood, the complexity of authentication, and ease of opening security loopholes gives the procedures greater weight.

Conclusions

CAVE-based authentication will be used in wireless networks for several more years, and will only be replaced by ESA gradually. IS-778 represents an important network tune up. As field experience with authentication continues to grow, it is possible that further tune-ups will be required.

Table 1: IS-778 Modifications to TIA/EIA-41 Operations

Operation	Modification	Purpose
AuthenticationDirective	CallHistoryCount (COUNT) note on RETURN RESULT changed	To encourage the inclusion of COUNT.
AuthenticationDirective-Forward	UpdateCount added to INVOKE, CountUpdateReport to RETURN RESULT	To allow COUNT update after handoff.
AuthenticationRequest	New SuspiciousAccess parameter added to INVOKE	To allow the initiation of a unique challenge when SSD is not shared and a 'suspicious' access (e.g. origination) is encountered. The only values supported are *Anomalous Digits* and, for future enhancements, *Unspecified.*
InterSystemPage2	SystemCapabilities and Terminal-Type parameters added	To allow the detection of mobiles that refuse to authenticate during border system paging, even though their profile indicates that they have the capability.
QualificationRequest	LocationAreaID added to INVOKE	To allow validation to be influenced by the location of the mobile.