Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 4, No. 12 December, 1995

*In This Issue...*



## *A T-Shirt for a Tip!*

We are pleased to offer a unique Cellular Networking Perspectives T-Shirt for any tips that lead to a paid subscription. Just give us contact information for your prospects and you will soon be the proud owner of one of our unbleached, recycled cotton shirts. You can contact us at 1-800-633-5514, by fax at +1-403-289-6658 or email at 71574.3157@compuserve.com. ❒

*Season's Greetings and Best Wishes for a prosperous 1996 from: Cellular Networking Perspectives!*

## IS-41 Revision C Approved for Publication!

Revision C of the TIA IS-41 standard for inter-system operations to support handoff, automatic roaming, validation and authentication has been approved for TIA publication. With some minor layout modifications, the document will also be submitted for ballot as a full ANSI standard. IS-41 Revision C includes the following components:

- All of IS-41 Revision B
- TSB-41 on backward/forward compatibility
- TSB-51 on authentication
- TSB-64 for CDMA terminal support
- TSB-65 on border cell problems
- IS-53 Revision A features (about 25, including many intelligent network style features and short message service)
- NAMPS terminal support ❒

## *COMING SOON...*

☞ An article by Harry Young, one of the wireless industry's most respected consultants, on number portability.

☞ The TIA IS-95 standard for CDMA systems.

*Look for your next issue on: January 5, 1996*

## Randy Snyder on IS-41/ GSM Interoperability

Since the idea of Personal Communications Services (PCS) became a reality with the allocation of new RF spectrum by the FCC, several different wireless technology camps have emerged, primarily due to the enormous business opportunities that beckon. It has always been true that economics drives technological innovation and PCS is no exception. Unfortunately, due to the concentration on the personal voice communications market, the rush to market and the need to compete with a very large existing cellular base, PCS has become more of an evolution of cellular systems rather than the promised revolutionary new system.

US PCS currently boasts seven standardized digital air interface protocols (and one analog), three standardized A interface protocols (between the base station and the MSC) and two standardized network mobile application part (MAP) protocols. While the best solution for PCS would be for the wireless industry to work toward a single standardized solution, this became impossible when standards bodies were asked to standardize already existing technology (making the concept of standards for PCS oxymoronic). Outside the cooperative standards process, competitors can invent value-added features to differentiate their products.

Since there are enormous business and growth opportunities with PCS frequencies, advocates of existing wireless technologies (mostly cellular) have promoted their favored technology as an off-the-shelf solution. Multiple and competing air interface and A interface technologies can co-exist provided that the networking technology

*Cellular Networking Perspectives* (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd.,2636 Toronto Cr. NW, Calgary AB T2N 3W1,Canada. Phone: **1-800-633-5514** or 1-403-289-6609. Fax:403-289-6658. **Subscriptions:** CDN$250 in Canada (incl. GST),US$250 in the USA and US$300 elsewhere. Payment by cheque, money order or American Express Card. Issues are faxed or mailed 1st class. **Copies:** Each subscriber may make up to 10 copies of each issue. Rates are available for more copies. **Discounts:** Educational and small business rates:CDN$150 (incl. GST),US$150 and US$200, by mail only. **Back Issues:** Phone for price list and table of contents.

adopted can simultaneously support the many network access technologies. However, multiple and competing networking technologies introduce a new set of problems. If these networking technologies are fundamentally different, it becomes difficult for a network service provider to achieve the basic service needs for their subscribers: ubiquity and seamlessness.

## MAP Interworking

Without taking sides in the great GSM vs. IS-41 debate, I will give a brief engineer's perspective on the concepts of interworking and interoperability between network MAP protocols. The optimal solution is a single MAP protocol supporting the many network access protocols (e.g. the way IS-41 supports AMPS, IS-54, IS-88, IS-91, IS-95 and IS-136). However, a single MAP protocol is unachievable given the current situation in the industry. Therefore, some form of interworking and interoperability between the two major MAP protocols, IS-41 and GSM, has become a necessity.

Generally, the concepts of interworking and interoperability are not amenable to standardization and must be provided as implementation dependent (i.e. value-added) solutions to enhance existing equipment and services. Examples of this are TCP/IP-to-X.25 and SS7-to-X.25 interworking. But since standards are driven by business needs, there are exceptions. TIA Subcommittee TR46.2 proposes to be one of those exceptions by tackling the job of standardizing GSM MAP to IS-41 MAP interworking and interoperability.

## Interworking and Interoperability

The first part of the problem involves defining "interworking" and "interoperability" (“I&I”):

| | |
|---|---|
| Interoperability | Interoperation with no loss of functional capabilities over the suite of standard functions. |
| Interworking | Any type of successful communications between two dissimilar systems. |

## The Interoperation Set

The second part of the interoperation problem is identifying the set of functions that are to be supported across two dissimilar systems. Since GSM and IS-41 are so different, many functional aspects of intersystem operations have been placed on the back-burner by most of the industry (for standard as well as proprietary solutions). These functions include intersystem handoff and all but the most basic supplementary services specified for both GSM and IS-41. Because GSM and IS-41 are so different and there are so many functions outside the interoperation set being studied for I&I, it is unlikely that any interworking and interoperability solution will ever provide completely seamless service to subscribers. The lack of total seamlessness for every function, though, may not affect the market and business cases for which I&I is being developed.

## Interoperation

The third part of the interoperation problem is to define *protocol conversion*, *database mapping* and *transaction management*.

*Protocol conversion* provides the translation of messages and parameters from one protocol to the other.

*Database mapping* provides the translation and management of information elements that allow each of the application protocols to provide user services (e.g. subscriber identifiers and statuses).

*Transaction management* enables the completion of queries between the two dissimilar networks (e.g. re-originating and maintaining queries and responses into the other network).

## Proposed Solutions

Initial solutions proposed in TIA subcommittee TR46.2 were based on the inelegant concept of interconnections between all analogous network elements supported by GSM and IS-41. An outgrowth of this concept was the "Dual-mode HLR." Both of these solutions are inadequate for such a complex networking problem. A good standard solution should be generic, flexible, scalable and allow many forms of implementation (i.e. the value-added portion of a product). A standard solution for I&I should be implementation independent and provide the three basic functions described above without specifying individual equipment platforms.

The dual-mode HLR solution is inadequate because it does not provide true I&I. What it does support is the implementation of a GSM HLR inside an IS-41 HLR or vice-versa. It should not be necessary to turn an SS7 signaling point into an X.25 packet switch to support I&I between SS7 and X.25 networks. A better solution is to specify protocol conversion, database mapping and transaction management for all of the functions supported between the networks as a single Interworking and Interoperability Function (IIF). The IIF can reside anywhere within or outside of the GSM and IS-41 networks. An example of an implementation of this solution is the RoamFree™ product being developed by Synacom Technology.

### Figure 1: Interoperation with an Interworking and Interoperability Function (IIF)

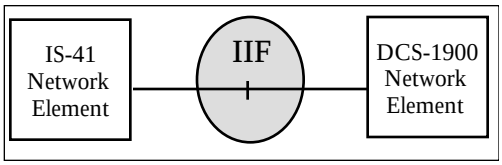



Figure 1 depicts a generic model of an IIF as it relates to GSM and IS-41 network elements. The IIF can also reside within either or both of the network elements shown. Note that it is not necessary to identify the network element type. The IIF should be able to support I&I between any pair of network elements. The physical implementation of such a solution is irrelevant to the communications supported through the IIF.

## Conclusion

Interworking and interoperability between GSM and IS-41 networks will not provide the best of what PCS potentially has to offer. However, in the absence of a single network standard, I&I is a highly desirable short term goal. Since business cases will rely on these functions, imperfect though they may be, it is incumbent on industry engineers to formulate a reasonable solution within the standards organizations. The solution should allow a variety of implementations as well as supporting additional I&I functions as they are required.

## About the Author

Randall A. Snyder is a Principal Engineer with Synacom Technology in San Jose. Randy is well known for his participation in the development of TIA cellular and PCS network standards. Randy can be reached at +1-408-296-0303.

# Fraud and Countermeasures, Part III: How Authentication Works

"Authentication is the answer to cloning fraud" according to Mike Redden, Director of Revenue Security at AT&T Wireless Services, yet the industry has been excruciatingly slow to implement it. We will explain what authentication is, how it works and why it is so powerful. In our next and final part of this series, we will explain why authentication has not yet been widely implemented and counter the fears of authentication by providing a strategy for effective implementation.

## What is Authentication?

Authentication goes beyond accepting an identity transmitted by a mobile and demands that a mobile prove that it is what it says it is, before granting service. TIA authentication for digital and analog cellular and PCS phones is based on encryption, partly because it can be reused to provide voice privacy and other services and partly because it is perceived as the strongest way to authenticate. TIA authentication also includes a "Call History Counter" which is a very simple backup check for the presence of clones.

The fundamental challenge of authentication is how to check a mobile out without requiring it to transmit information that should be kept secret. The TIA authentication method accomplishes this through a (numeric) challenge from the network. The mobile must perform a complex calculation and can only come up with the right (numeric) answer if it has the right secret keys stored inside. The answer that is transmitted back is good for, at most, a small number of calls.

Contrasting validation with authentication, consider the following dialogs. The first illustrates validation, where only a valid identity need be presented:

Villain: My credit card number is 1234-567-890
Victim: Let me check that out…
Victim: Seems okay. Enjoy your new fur coat.
Villain: (chuckle)

But with authentication you ask a surprise question that only the true holder of the identity should know. Now you are Not A Victim Any More (NAVAM):

Villain: My credit card number is 1234-567-890
NAVAM: Let me check that out…
NAVAM: That's okay, now what's your Mother's maiden name?
Villain: er…
NAVAM: Get lost punk!

## The CAVE Algorithm

TIA authentication is implemented with the CAVE (Cellular Authentication and Voice Encryption) algorithm, which incorporates a Motorola private key encryption algorithm with an AT&T idea for maintaining two keys. The algorithm is considered military technology by the USA (governed by ITAR; US International Traffic in Arms Regulations), and consequently an export license from the US Department of State is required to export equipment that contains it outside of the United States and Canada, or even to export the algorithm description to a foreign country or to describe it within the US or Canada to foreign nationals. If you require details of the algorithms, ask for the Technology Transfer Control Plan from the Telecommunications Industry Association at +1-703-907-7700.

The primary characteristic of private key encryption is that the same key is used to encrypt and decrypt information, so this private key must be communicated safely to at least two network elements, in this case the Authentication Centre (AC) and the authenticating mobile (MS). The security limitations of a secret key (which is vulnerable to being stolen by dumpster divers or others) are reduced significantly in TIA authentication through the use of a two level key structure. The primary private key is called the A-Key and should be known only by the AC and the mobile. The A-key is only used to generate a temporary private key, known as Shared Secret Data (SSD). SSD can be communicated around the cellular network (although definitely not over the air interface!) and can be regenerated automatically, if compromised. As a backup, the A-key can also be modified, although not automatically.

## Breaking into the CAVE

One approach to breaking the CAVE algorithm is to throw an enormous amount of computational capacity (i.e. millions of Pentium-years) and sophisticated software at the problem. Alternatively, the SSD can be stolen by breaking into network elements that store or transmit the SSD or by 'borrowing' a phone and tracing through the code until the SSD is used in the CAVE algorithm.

Even if SSD is obtained, it can easily be invalidated by regeneration. Unless the A-key is also known and the random number used to generate SSD can be obtained, most easily by being in the same cell as the victim when the SSD update occurs, the cloner is out of luck. Even if these stiff challenges can be met by the cloner, the A-key can always be changed. Since the A-key is updated in the phone manually, the cloner will be unable to eavesdrop and will be totally shut out.

## Standards

Authentication is currently available in phones conforming to the following standards:

TABLE 1: Authenticating Cellular Standards

| Type | Standard | Published |
|---|---|---|
| Analog/ NAMPS | IS-91 Rev. 0 | 12/94 |
| | IS-91 Rev. A | in press |
| | EIA/TIA-553-A | development |
| CDMA Digital | IS-95 Rev. 0 | 07/93 |
| | IS-95 Rev. A | 05/95 |
| Network | IS-41-B+TSB-51 | 02/93 |
| | IS-41 Rev. C | in press |
| TDMA Digital | IS-54 Rev. B | 01/92 |
| | IS-136 Rev. 0 | 12/94 |

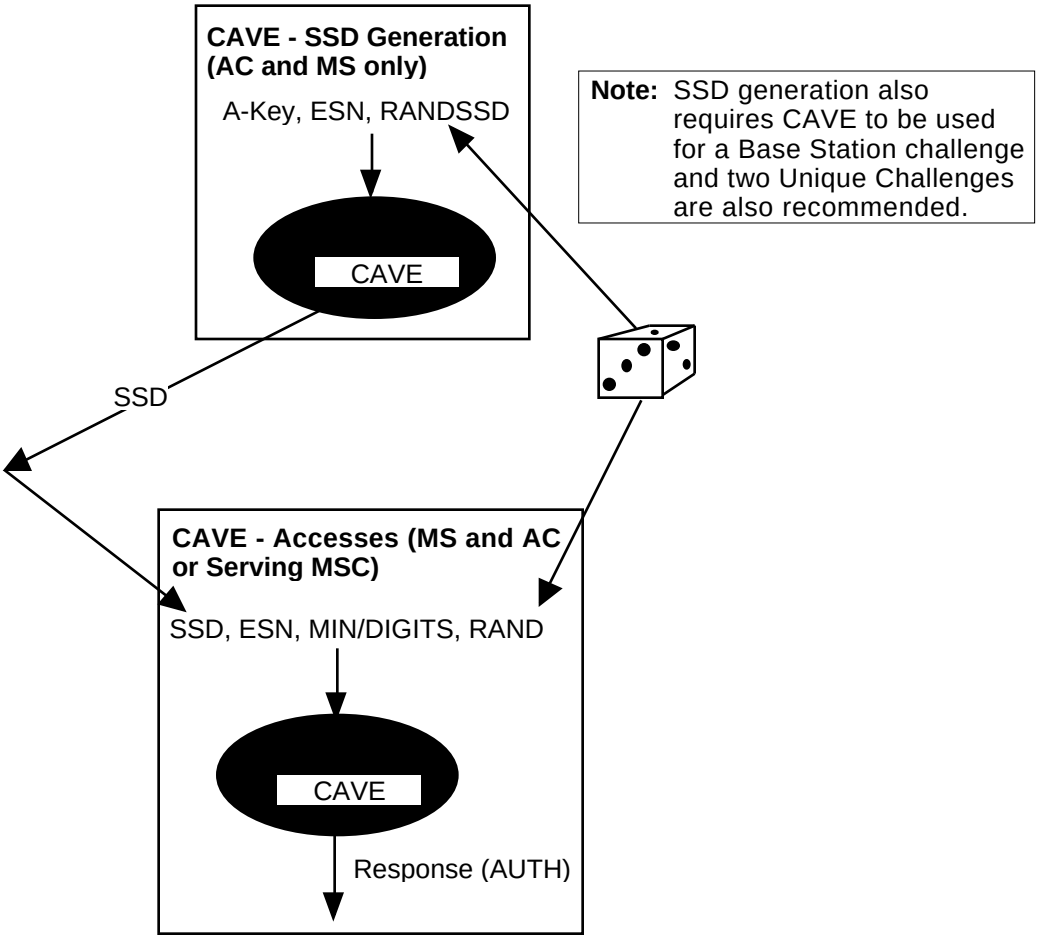
It is just as important to know which standards do not support authentication:

TABLE 2: Non-authenticating Cellular Standards

| Type | Standard | Published |
|---|---|---|
| Analog | EIA/TIA-553 Rev. 0 | 09/89 |
| Analog, in-building | IS-94 | 05/94 |
| NAMPS | IS-88 | 02/93 |
| TDMA Digital | IS-54 Rev. A | obsolete |

All digital cellular phones support authentication, all AMPS-based PCS phones support authentication and any analog phones built to IS-91 or the upcoming EIA/TIA-553 Revision A (as opposed to the old IS-3 or the more recent EIA/TIA-553 Rev. 0) support authentication. However, the majority of the millions of cellular phones that are in use today still do not support

## Figure 2: Use of the CAVE Algorithm in Authentication




authentication, as most conform to the EIA/TIA-553 Rev. 0 standard.

## Authentication Operations

It would be illegal to describe the internal workings of CAVE, and incredibly mind-numbing as well. What is more interesting, at least from the network view that we like to adopt, is to examine the purposes to which CAVE can be applied:

### *1. Global Challenge*

The first hurdle for authenticating cellular phones on any system is the global challenge, named because the same challenge number (known as RAND, and broadcast on the control channel) is used by all mobiles. However, the result of the challenge, known as AUTH, is different for each mobile, due to the inputs to the CAVE algorithm:

RAND — The global challenge random number. This can be changed by the base station at any time, in practice likely to be no more often than every few minutes and no less frequently than every few hours.

MIN/ESN — Makes the results of the algorithm unique for each MS. MIN is not used for originations.

DIGITS — The last 6 dialed digits (padded with zeros) are used to make the result different for originations from the same MS.

SSD — Shared Secret Data. This is the only parameter that is hidden from view.

### *2. Unique Challenge*

The Unique Challenge is much stronger than the Global Challenge because a unique random number (known as RANDU) is used for each operation. This challenge may be performed on a voice channel at the start of a call, or even during a call (e.g. when setting up a 3 way call). Because of the unique challenge number, even for the same mobile, the result (AUTHU) will be different every time:

RAND — The unique challenge random number. There are over 2 billion to choose from, to ensure that the answer from one unique challenge is of no value to cloners.

MIN/ESN — Makes the results of the algorithm unique for each MS.

SSD — Shared Secret Data. This is the only parameter that is hidden from view.

### *3. SSD Key Generation*

In a new mobile, the first use of the CAVE algorithm is for creation of the temporary key, known as Shared Secret Data (SSD). This is the only time that the primary key (A-Key) is used. Consequently, the A-key can be restricted to the Authentication Center (AC) and the Mobile Station (MS), and never transmitted over a network, reducing the likelihood that it can be stolen. The inputs to the algorithm each have a specific purpose:

| | |
|---|---|
| RANDSSD | A random number that makes each SSD created unpredictably different for the same MS. |
| ESN | Makes the results of the algorithm unique for each MS, even if the same A-Key and RANDSSD are used. |
| A-Key | The semi-permanent secret key, the only secret number in the process. |

### *4. Base Station Challenge*

This operation is unique because it is the only use of CAVE by a mobile challenging a base station. It is used during the SSD update process to prevent a false base station from forcing a mobile to change its SSD and consequently lose service. The inputs are:

| | |
|---|---|
| RANDBS | A random number chosen by the MS and transmitted to the base station. |
| MIN/ ESN | Makes the results of the algorithm unique for each MS. |
| SSD | The temporary secret key, the only secret number in the process. |

### *5. Voice Encryption*

The CAVE algorithm is also used to generate a voice encryption mask in two steps. First, the SSD is generated. Then, a portion known as SSD-B is used to generate a unique voice encryption mask whenever a mobile attempts to originate or receive a call.

### *6. Signaling Message Encryption*

Selected parameters in signaling messages sent on a voice or traffic channel can be encrypted, in order to protect the network and also user data. The specific parameters that are encrypted is controlled information.

### *7. COUNT Update*

The call history counter (COUNT) is the only aspect of authentication that does not rely on encryption. Each mobile contains a simple 6 bit counter that can be incremented by the network from 0 to 63, then wrapping back to 0. Unless a clone is always in the same cell as the potential victim, or has access to the cellular network, incrementing the COUNT will cause one mobile to report the new value and one the old. While this technique cannot distinguish between a good mobile and a clone, it does work in the presence of a complete clone (i.e. one that has the A-Key and current SSD).

## Security of CAVE Parameters

It is important to consider the ease with which inputs to CAVE and outputs from CAVE can be obtained, as the algorithm is only as secure as the weakest link:

TABLE 3: Illicit Access to Authentication Parameters

| Parameter | Access | Lifetime | Comments |
|---|---|---|---|
| A-Key | Difficult | Until changed | Obtainable only by access to AC or internal workings of an MS. |
| AUTH | Easy | Minutes or hours | Same on every registration and page response by a mobile for the life of a RAND. Same for originations only if MIN, ESN and DIGITS are the same. Different for every mobile. |
| AUTHU | Medium | Per operation | Different for every unique challenge. |
| DIGITS | Medium | Per call | Used to randomize authentication for originations. |
| ESN | Easy | Permanent | Not supposed to be changeable! |
| MIN | Easy | Until changed | |
| RAND | Easy | Minutes or hours | Broadcast on forward control channel, and used by all mobiles. |
| RANDSSD/ RANDU | Medium | Per operation | Different for every SSD update or unique challenge. |

Since access to the SSD and A-Key is difficult, and they can be easily changed, authentication will put the carriers in the drivers seat for a change. Currently it is much easier for a cloner to change a MIN and ESN than it is for the carrier to reprogram a MIN, replace a phone (to obtain a new ESN) or even to change the PIN (which is the simplest, but still requires customer contact, cooperation and inconvenience). With authentication, a carrier can modify the SSD transparently to the customer (and, just as important, transparently to the cloner).

## Security of Authentication Operations

The ultimate test of authentication is the strength of the authentication operations:

#### *Global Challenge for Registrations*

Authentication for registration is quite weak as a mobile will keep responding with the same value (AUTH) as long as the global RAND remains the same in a cell. Consequently, unless registrations utilize a unique challenge (which is unlikely), it is easy for a clone to have a registration falsely accepted. There is, however, little motivation for cloners to take advantage of this loophole as there is little to be gained from a false registration.

#### *Global Challenge for Page Responses*

Authentication for page responses is also quite weak, as the inputs to CAVE are the same as for registration. However, since the cloner must be in the same cell as the victim in order to obtain the correct AUTH, there is little to be gained except to interfere with paging to the legitimate subscriber's phone. This loophole can be plugged by using a Unique Challenge at the start of each mobile terminating call.

#### *Global Challenge for Originations*

Authentication for originations is stronger than for registrations and page responses. This is accomplished by using the last 6 dialed digits as input into CAVE. Consequently, the authentication response (AUTH) will be different (even for the same MIN, ESN and global RAND) on every call … unless the same digits are dialed. The big weakness is that some

subscribers may commonly dial the same number several times, for example a long distance carrier's 1-800 number. Consequently, the global challenge is not sufficient for originations, but read on…

### *Unique Challenge*

The unique challenge is very secure because the random number used as a CAVE input can be changed for each operation. The only way to pass a unique challenge (apart from guessing, and surmounting odds that are greater than winning the grand prize in a lottery) is to have possession of the SSD. And, even then, the SSD can be modified quite easily, and without customer intervention, leaving the cloner high and dry.

### *SSD Update*

The basic SSD update process is very secure in preventing a cloner from obtaining the new SSD, but not very secure in preventing vandalism. This could occur by a cloner that received an SSD update and just responded affirmatively without actually performing the SSD regeneration. This would result in an apparently successful SSD update, locking both the cloner and the legitimate mobile out of service. Consequently, an SSD update should always be followed by a Unique Challenge, to verify that the target mobile has successfully generated the new SSD. It would also be useful to precede an SSD Update with a Unique Challenge using the current SSD to filter out cloners that have obtained the A-Key but not the current SSD.

The only way for a cloner to successfully generate a new SSD is to have possession of the current A-Key and, if a pre-update Unique Challenge is performed, possession of the current SSD.

For the ultimate in security, carriers can require SSD Updates to be performed during a call to an operator that will verify the subscriber's authenticity by other means (e.g. by asking for address information or their mother's maiden name).

### *Voice Encryption*

The voice encryption included in digital AMPS standards is not considered very secure in comparison to some forms of voice encryption, however it is in order of magnitude harder to crack than having no encryption at all! Its weakness stems from the use of a fixed mask, versus a constantly changing mask in more secure systems. This weakness was intentionally included in order to ensure that export approvals for the algorithm could be obtained.

Perhaps surprisingly, voice encryption assists with authentication. This is because even if authentication challenges can be passed, if the clone mobile cannot generate the voice encryption mask, the stolen service will be unusable.

### *Signaling Message Encryption*

In a similar way that voice encryption assists authentication, so can signaling message encryption. This encryption applies to certain data fields in signaling messages. Again, even if authentication hurdles are passed, the clone mobile may be unable to properly encrypt or decrypt these fields, and consequently will have stolen an unusable service.

### *COUNT Update*

COUNT update is a useful adjunct to CAVE-based authentication. It can be used to detect an authenticating clone. Manual techniques can be used to determine which phone is legitimate, and an SSD update can be used to invalidate the clone.

## Security Summary

If implemented with adequate attention paid to the strengths and weaknesses of TIA authentication (see sidebar), cloning will finally be brought to an end. Authentication is not just a little bit stronger than alternatives, such as the PIN, it is millions of times stronger. Authentication does not distinguish good from bad most of the time, like RF fingerprinting or call pattern analysis, it works virtually every time. Authentication is like a virus that only attacks cloners.

Authentication will not make cellular fraud disappear, but fraud will be reduced to traditional crimes, most likely subscription fraud and phone theft. While both these types of fraud can never be eliminated, the losses can be capped at an acceptable level through traditional business loss management techniques. While cloning fraud is currently causing massive hemorrhaging of revenue, other types of fraud will likely be less damaging.

Acknowledgements

Thanks to Mike Redden of AT & T Wireless Services and Dave Wenk of Hughes Network Systems for reviewing a draft of this article.

## Authentication Gotcha's

When implementing authentication, carriers should keep the following points in mind:

- Secure the Authentication Center, both physically and through encryption of all data.
- Secure your network. Make sure that hackers cannot break into network elements or tap into network facilities.
- Use the Unique Challenge on every call.
- Do not change SSD without justification (i.e. suspected fraud).
- Turn on voice encryption at no charge, or at a low charge.
- Use signaling message encryption.
- Use a different RAND in every cellsite and change it more often than your underwear.
- Ensure that your system checks for authenticating phones that refuse to authenticate.
- Don't give service to new phones without a valid A-Key, at least not for very long.
- Correlate A-Key losses to your points of sale to track down corrupt employees and dealers.
- Give out A-Keys in sealed envelopes with the MIN on the outside (for the installer) and the A-Key printed on the inside (for the subscriber to enter).
- Implement COUNT as a backup check for the presence of complete clones.

## To be continued...

Next month we complete our series on fraud and countermeasures by discussing the implementation of authentication:

- How TIA TSB-51 and IS-41 Rev. C support authentication for roamers.
- Misconceptions about authentication.
- The CTIA Total Fraud Management initiative.
- An authentication implementation strategy. ❒