Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-800-633-5514 • Fax 403-289-6658 Vol. 6, No. 4 April, 1997

In This Issue ...

Try our Quiz!

Test your telecom trivia knowledge against the best in the industry. You could win a T-Shirt or our famous IS-41 trading cards! There is a new quiz every month on our web site at:

http://www.cnp-wireless.com/quiz.html

Next issue due: May 1, 1997

Has Digital Cellular Been Cracked?

There has been much fuss recently since it was announced by Bruce Schneier and John Kelsey of Counterpane Systems (http://www.counterpane.com/), along with graduate student David Wagner of the University of California at Berkeley, on March 20th, that the digital cellular signaling data encryption algorithm (CMEA - Cellular Message Encryption Algorithm) had been broken.

This is embarrassing for the TIA, as CMEA was designed to be strong. However, it is important to recognize what parts of digital cellular were broken, and which were not, and where Schneier *et al*'s charges have merit, and where they do not;

- The TIA process is not deliberately secretive.
- CMEA was not deliberately made weak.
- Strong encryption is not needed by most people.
- Voice encryption was not cracked, but is deliberately weak.
- The strength of CAVE authentication is not affected.
- Clones are no closer.

What is CMEA?

The TIA Cellular Message Encryption Algorithm (CMEA) is designed to encrypt user information, such as PINs and credit card numbers. It does not provide digital data call encryption (which is provided by the ORYX algorithm), nor voice encryption, nor authentication (provided by CAVE). According to the TIA, CMEA has not yet even been implemented by any US digital cellular carriers, although some do (did?) have plans. Even if CMEA was used, it would not be used often by the average subscriber, so the Schneier attack requirement for 40 unencrypted messages would be very hard to meet. However, the TIA *ad hoc* group responsible for this standard (AHAG), is aware of more practical methods for cracking CMEA, so CMEA must be considered completely broken.

The TIA Process

The TIA process for developing standards is open to all companies with an interest in the technology being standardized. Consequently, it is not fully open, but any company or organization that can meet the TIA membership requirements can attend meetings. Because the TIA standards-setting arm was set up to allow the cooperative development of telecommunications standards in the face of US anti-trust legislation, it is not possible for the TIA to exclude companies with an interest in the technology, even if they wanted to. Consequently, cryptography companies like Counterpane could have participated in the development of TIA encryption technology.

Participation in the TIA AHAG (ad-hoc Authentication Group) is somewhat restricted - but not due to TIA rules. Because some of the subject matter (encryption) was governed by US ITAR (International Traffic in Arms) rules,

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 (+1-403-274-4749). Fax: +1-403-289-6658. **Subscriptions**: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. Payment by cheque, American Express or Visa. **Delivery:** Email, fax or 1st class mail. **Copies:** Each subscriber may make up to 10 copies of each issue. Rates are available for more copies. **Discounts:** Educational and small business discount: 25% off any order (no fax delivery). **Back Issues:** Available individually for $35, or in bulk at reduced rates. **Email:** cnpsales@cnp-wireless.com **Web:** http://www.cnp-wireless.com/

some discussions had to be limited to US and Canadian citizens. This is due to the requirements of US law, not on a desire of the TIA to be secretive. The output of these restricted deliberations (known as "Appendix A: Common Cryptographic Algorithms") is available from the TIA to any US or Canadian citizen who agrees not to export the technology - again in accordance with US laws. Whether the US laws make sense is not an issue for the TIA to decide autonomously.

Another set of meetings that have been somewhat restrictive are those discussing a standard for conformance to the US CALEA laws for lawfully authorized electronic surveillance ("wireless wiretaps"). Attendance at these meetings was not limited (except by normal TIA membership requirements), but participants had to agree to limit distribution of documents outside the meeting. In the end, the output document (PN-3580) was submitted for ballot as a public standard, in accordance with the requirements of CALEA.

CMEA Not Deliberately Weak

The TIA CMEA algorithm was not deliberately made weak. Only voice encryption must be weak to ensure that US export approval can be obtained. Consequently, the design flaws that allowed successful attacks on CMEA came as a surprise. The TIA AHAG is currently working on a successor to this algorithm.

Similar weaknesses may also plague the ORYX algorithm for encrypting data calls. A new version of this algorithm may also be required.

Strong Encryption Not Needed

Strong encryption is not required by most users of cellular phones. Analog cellular phones have little protection from eavesdropping and few people are adversely affected. Even if uncrackable encryption was possible, it only protects the air interface, from the phone to the cellsite. If your conversation is extremely important and someone wants to hear it really badly, it is still possible for them to corrupt a telecommunications or law enforcement employee to gain access to the unencrypted voice at the MSC, or to obtain the secret keys required for decryption.

People that need strong encryption, will require end-to-end encryption, and cellular phone add-ons for this purpose are currently available (which work only over analog cellular channels). Digital cellular encryption is still effective at discouraging casual scanning.

Voice Encryption Unaffected

Voice encryption is the one part of the TIA encryption algorithms that was deliberately made weak. Through the use of a fixed mask, rather than a rotating mask, voice encryption was weakened to the point that US export approval could be obtained. The US government (NSA) has historically been concerned that strong encryption exported from the US may end up in the hands of people who are, or who may become, enemies of the US. They did not, in this case, mandate an algorithm to be used. With the transfer of export approval to the US Department of Commerce, it is expected that stronger voice encryption algorithms now being developed, will be exportable.

The Schneier attack, which requires access to decoded transmissions, is not applicable to voice encryption, except in a trivial way. Obviously, if a conversation is captured both encrypted and decrypted, the fixed mask can easily be deduced. A practical method of breaking the voice encryption algorithm must work solely on encrypted voice.

Authentication Unaffected

Authentication of mobiles is based on the TIA CAVE (Cellular Authentication and Voice Encryption) algorithm. There are no US government restrictions on the strength of authentication, and the CAVE algorithm was made as strong as possible, when it was initially incorporated into a standard (TIA/EIA IS-54 Revision B for TDMA digital cellular).

The CAVE algorithm provides the basic data for authentication, signaling message encryption, voice encryption and data encryption. Each capability requires additional operations beyond CAVE. It is not CAVE that is weak, it is the use of CAVE by CMEA that was weak.

Clones No Closer

Because the CAVE authentication algorithm is still believed to be secure, cloning of authenticating phones is still not possible. Even if, in the future, the CAVE algorithm is broken, the cost of breaking it will have to be much less than the benefit, or it will not prove attractive to criminals.

Summary

People using digital cellular phones should continue to use the same caution when talking about secret information as they would on any phone. If you have attracted the attention of law enforcement agencies, your call may be tapped. If you have attracted the attention of a crime syndicate, a corrupt employee may be listening in at the switch site. If the other party to your call is using a landline phone, cordless phone or analog cellular phone, they could be much more vulnerable than you. And don't forget lip readers and people with parabolic microphones who happen to be in your vicinity!

WIN: The Wireless Intelligent Network, Part II: The ITU View

The Wireless Intelligent Network standardization effort, introduced in Part I of this series, does not exist in isolation. The work is derived from, or overlaps with, the TIA IS-41 intersystem operations standard (particularly Revision C), international standardization of IN, Bellcore's AIN and has some parallels to the GSM CAMEL strategy. The WIN standardization group (an ad hoc group within TIA standards subcommittee TR-45.2, Working Group II) has incorporated some aspects of current international standardization work, notably the call model and distributed functional

plane network reference model, into WIN.

The inclusion of ITU concepts alongside IS-41 concepts creates a kind of schizophrenia in the developing WIN standard. There are two distinct halves, with the call model on the ITU side and message flow diagrams, transaction and parameter definitions on the IS-41 side. The meeting point between these two disparate worlds is the mapping between two network reference models; one based on the ITU Q.1224 Distributed Functional Plane (DFP) and one from the TR–45/IS-41 network reference model (NRM).

The Call Model

The most significant elements of the ITU call model are DPs (Detection Points) and PICs (Points in Call), which exist within the telephone switch (MSC in the WIN context). A DP starts by deciding whether conditions are right to launch an external message (a "trigger") and either terminates immediately, or emits the message and waits until a response to the message is received. A PIC is a portion of call processing without the possibility of launching external messages.

A call model would be most useful with a standardized service creation environment, one of the ideals of the IN concept. If such a concept was realized, a non-technical person could sit down at a workstation and define a new feature by manipulating icons representing DPs and triggers and PIC's. However, this is outside the scope of the first phase of WIN standardization.

The call model defines internal call processing for an MSC, and therefore is more restrictive and less efficient than today's proprietary models. In order to lessen the restrictions of the call model, considerable flexibility is allowed in the arrangements of DPs and PICs, as there are many legitimately different orderings of call processing. Even so, to fully implement the call model would require massive changes to call processing, with a cost in CPU consumption to pay for the additional flexibility provided. However, since the call model largely defines internal call processing, in the absence of a standardized service creation environment it is impossible to determine whether a switch conforms to the call model. Or, to put it another way, every switch that emits WIN messages under the right conditions can claim conformance to the call model. This is similar to the ISO 7-layer protocol concept that did not result in changes to protocols, but did result in repackaging of protocol documentation to indicate how even the most lightly layered protocol could be mapped onto the pure 7-layer model.

The call model may have greater relevance in the future, especially if its complexity can be pruned down to the essentials, to allow a better balance between flexibility (i.e. where a trigger can be launched) and practicality.

The ITU Network Reference Model (DFP)

The ITU-Q.1224 based network reference model for WIN (known as the DFP: "Distributed Functional Plane" model; see Figure 1) defines functional entities that are different both in name and in concept from the TR-45/IS-41 network entities also defined for, which were introduced in part I of this series

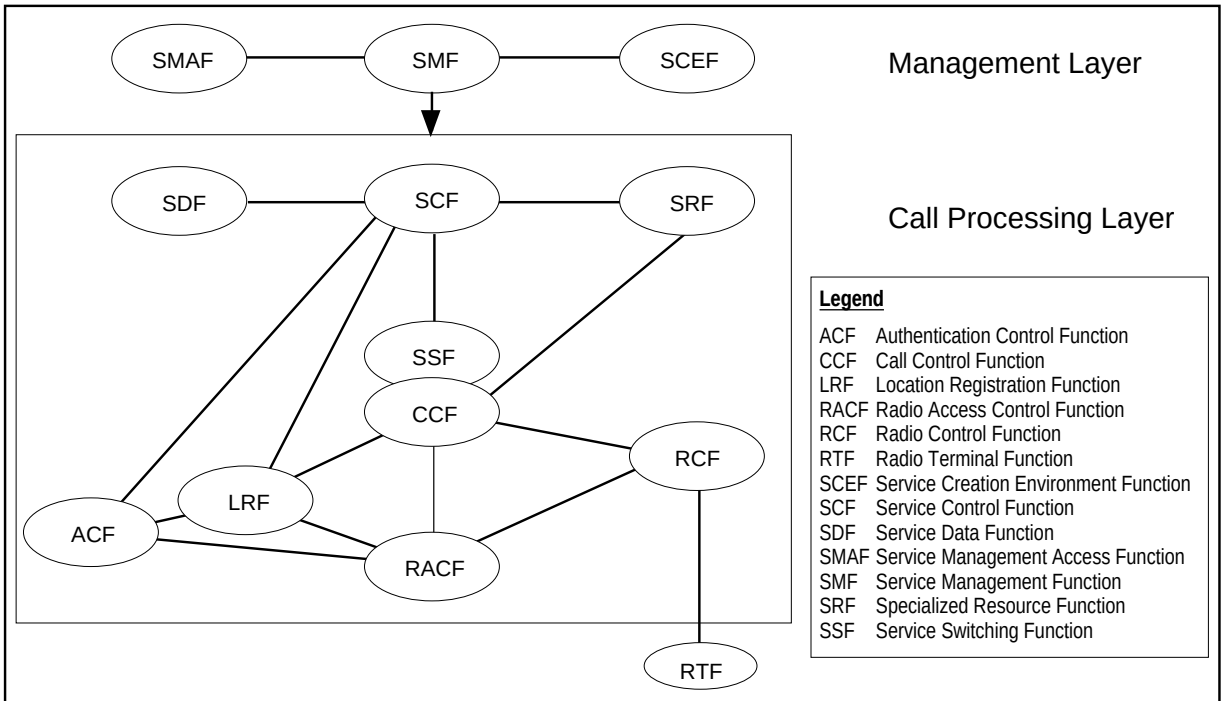

Figure 1: ITU-based Distributed Functional Plane Model (simplified)

(see the March 1997 issue of Cellular Networking Perspectives). The DFP for WIN does not define the lowest level of network elements that can be communicated with, as does the TR-45 model ("NRM"), but clusters of related functionality. In fact, most ITU functional entities could not be implemented as a standalone network nodes, but must be combined. Also, a single functional entity provides all services related to a single capability, even if they are distributed in the general case. The TR-45/IS-41 NRM, by contrast, consists of elements that can be implemented as standalone physical network nodes, for the most part.

To illustrate the difference, consider the case of authentication. In the TR-45 network reference model, authentication is provided by several different network entities - the Authentication Center (AC), the Home Location Register (HLR), the Visitor Location Register (VLR) and the Mobile Switching Center (MSC). In the ITU case, all authentication functions are provided by the Authentication Control Function (ACF). Consequently, while each NRM network entity can be implemented as a standalone physical node in an IS-41 network, the ITU model applies the same name to different functions that (to support roaming) have to be distributed across several physical network nodes. Because of this limitation, the ITU style of network reference model is of little use in defining the interfaces for a network standard.

Descriptions of DFP Functional Entities

ACF Authentication Control Function
Performs all network-based authentication and voice encryption functions.

CCF Call Control Function
Performs all call processing.

LRF Location Registration Function
Performs mobility management (tracking mobiles to facilitate terminating service delivery)

RACF Radio Access Control Function
High level radio access control (similar to a base station controller).

RCF Radio Control Function
Low level radio access control (similar to a cellular base station transceiver).

RTF Radio Terminal Function
A mobile.

SCEF Service Creation Environment Function
Human interface to dynamically create services, at least for prototyping, if not for production use.

SCF Service Control Function
WIN service processing.

SDF Service Data Function
WIN database management.

SMAF Service Management Access Function
Human interface to SMF.

SMF Service Management Function
Service monitoring, provisioning and testing, etc.

SRF Specialized Resource Function
WIN service hardware - voice processing, tone generation and detection, recorded announcements and other capabilities that require a trunk connection.

SSF Service Switching Function
Basic switching functionality.

Mapping of DFP to NRM

A precise mapping of ITU-based DFP elements to TR-45/IS-41 NRM-based elements is not possible, but the approximate mapping shown in Figure 2 is useful. Note how some DFP functional entities (with, paradoxically, different functions) occur in multiple NRM network elements. It is this that dilutes the power of the DFP modelling technique.

To be continued…

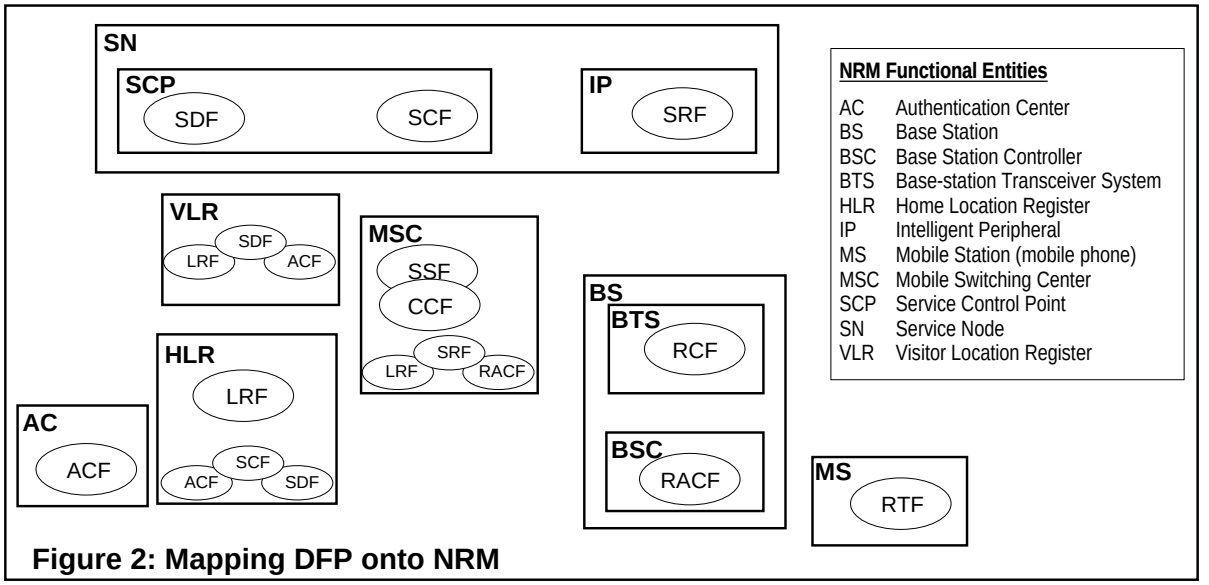

Figure 2: Mapping DFP onto NRM

TIA TR-45.2 Standards Update

Two new standards reflecting US government mandates are in the ballot process - the highly controversial SP-3580 that defines a standard to provide wiretap capabilities to law enforcement agencies and PN-3581 that supports Phase I of the FCC requirements for enhanced wireless 9-1-1.

In Press

Inter-System Link Protocol (ISLP) (PN-3660) • This new inter-MSC rate adaption protocol is required to support the transmission of data from digital phones following an intersystem handoff. Also see PN-3770, below, which is still in the ballot process.

Online Call Record Transfer (IS-124 Rev. A, PN-3293) • Includes a variety of improvements and corrections over Revision 0, such as internationalization (i.e. support of IMSI) and some support for GSM and data calls.

Ballot

IS-41 Rev. C ANSI Ballot (ANSI/TIA/EIA-41, SP-3588) • The "IS-41 Rev. C" ANSI ballot review was completed at the September, 1996 TR-45.2 meeting. The document has been *approved for publication*, but has not yet been submitted to the TIA for publication.

International Applications (TSB–29 Rev. B, PN-3173) • This revision adds lists of known non-NANP MIN usage, a list of applicable SS7 global titles and a recommendation to use ANSI TCAP even if ITU SCCP and MTP SS7 layers are used. It accommodates the IFAST 0-XXX and 1-XXX MIN format for use by countries outside the North American Numbering Plan. *Ballot comments are under review.*

In Development

Subscriber Features (IS-53 Rev. B, PN-3362) • The future of this standard is under debate. It may be reorganized or merged into other standards.

TDMA DCCH (PN-3579) • Definition of network support for the IS-136 Rev. A TDMA digital features "User Group" and "Non-public mode service". Also contains enhancements to support vendor- or carrier-specific terminal capabilities. *Ballot comments are under review.*

Over-The-Air Service Provisioning (PN-3769) • OTASP will provide the ability to program, or re-program, a digital (TDMA or CDMA) mobile over the radio interface. *Ballot comments are under review.*

Data Services (PN-3770) • Transmitting data from CDMA and TDMA digital phones is more complex because voice coders are incompatible with analog modem tones. *Ballot comments are under review.*

Law Enforcement Intercept (PN–3580) • Squeezed between the cost concerns of the industry, the constraints of the US CALEA law and the demands of law enforcement, a new standard for lawfully authorized intercept is emerging. It will apply to both IS-41 and GSM based wireless networks. This standard *is out for ANSI ballot until May 12, 1997.*

Enhanced Wireless Emergency Services (PN–3581) • A standard to use normal PSTN signaling (Feature Group D MF or SS7 ISUP signaling) to support the FCC-mandated Phase I for enhanced wireless 9-1-1 is nearing completion. It will apply to both IS-41 and GSM based wireless networks. Both cell/sector location and mobile identification will be transmitted to the emergency services system using standard PSTN interconnect signaling. This standard *is out for TIA ballot until April 15.*.

CDMA Capabilities (PN-3619) • The definition of advanced features based on IS–95 Rev. A capabilities, such as TMSI, is expected to be approved for ballot in April 1997.

Interconnection (IS-93 Rev. A, PN-3295) • Modifications to this PSTN interconnect standard include enhanced wireless emergency services (from PN-3581), definition of ANI II digits related to wireless calls and various enhancements and corrections from Revision 0. Future modifications may include international roamer identification with a full E.164 number (i.e. including country code) and local number portability.

WIN: Wireless Intelligent Network (PN-3661) • The description of intelligent networking for IS-41 based mobility networks is complete at a high level. The description of IS-41 transaction and parameter modifications is under development. The schedule for *ballot is May-June, 1997.*

TIA/EIA-41 Rev. A (PN-3590) • Work on TIA/EIA-41 Rev. A (originally IS-41 Rev. D, and then TIA/EIA-689 Rev. A) will begin in earnest once the ANSI/TIA/EIA-41 Rev. 0 document and subsequent annexes are published (see above). The exact format and contents of this document is under review.

Call Detail/Billing Records (IS–124-B, PN-3725) • A new project has been initiated to study modifications to IS-124 to fully support data services and intelligent peripherals.

New Projects

Emergency Services, Phase II (PN- 3890) • The second phase of enhanced wireless emergency services must provide enhanced location information to the emergency services system, required to an accuracy of 125 meters (67% of the time) by a recent FCC rule making. This may be accomplished through extensions to the SS7 ISUP protocol or by a separate datalink.

International Mobile Station Identity (IMSI; PN- 3892) • Support for the E.212 IMSI mobile identifier will resolve international roaming problems caused by the current 10 digit MIN identifier. Initially, these modifications were going to be published as part of ANSI/TIA/EIA-41 Revision A, but as this standard has been delayed by the onslaught of separate annexes to Revision 0 (see above), it has been decided to publish an annex against ANSI/TIA/EIA-41 Rev. 0.

Wireless Number Portability (WNP; PN- *pending*) • Wireless number portability will allow telephone subscribers to keep their directory number when churning from one service provider to another. Churn is possible between any carriers, wireless or wireline. The wireless industry, by US FCC mandate, must support this capability in the 1998/1999 time frame. Yet, work on a standard is only in the CTIA requirements-setting stage. Clearly, this project will become a high priority very soon.

TIA TR-45.4 Subcommittee
BS-MSC "A" Interface Standards
Project Status Report

Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 *Last published June, 1996*

Published Documents

Standard	Description	WG	Published
EIA/TIA-634	MSC-BS "A" Interface Standard	II	12/95
IS-94	Mobile Station - Land Station Compatibility Specification for Analog Cellular Auxiliary PCS (CAPCS)	III	05/94
TSB-80	**IS-634-0 Addendum (corrections, SMS, subrate voice frame format)**	**II**	**11/96**
TSB-104	PCS Service Description (now IS-104 in committee TR-46)	I	06/94

Completed Internal Documents

PN	Description	WG	Editor
3142	Cellular Microcell/Microsystems Requirements Document	III	Steve Jones
3296	MSC-BS Interface (A-Interface) Requirements for Public 800 MHz	II	Mike Burke

Active TR-45.4 Projects (PN=TIA Project Number)

PN	Description	Editor	IS/TSB
PN-3539	MSC-BS Interface (A-Interface) Standard, including support for: • IS-136-A (TDMA DCCH) • IS-95 Rev. A (CDMA) • IS-91 Rev. A (analog) • EIA/TIA-553 Rev. A (analog) • IS-41 Rev. C and IS-53 Rev. A • Short message service • Data services for CDMA/TDMA (IS-99, IS-130, IS-135) • Frame Relay • 1800 MHz • Optimization	Steve Jones	IS-634-A
PN-3746	ISDN based A-Interface, adding • address alignment with Mobility Management Application Protocol (MMAP) • CDMA and TDMA support, and • support for architectures with separate mobility management and call control functions		IS-653-A
PN rejected	~~**Use of A-Interface standards in Wireless Local Loop (WLL)**~~		***n/a***