Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-800-633-5514 • Fax 403-289-6658 Vol. 6, No. 5 May, 1997

In This Issue ...

Next issue due: June 2, 1997

New TIA TR-45 Standardization Efforts: CDPD and Number Portability

Two new groups have been formed within TIA standards committee TR-45. Subcommittee TR-45.6 has been formed for standardization of "Adjunct Wireless Packet Data Standards" - CDPD in other words. Up to this point, the CDPD specification has been controlled by a closed industry group. TIA standardization may not result in large changes to the standard, but will open the process to more companies. Mark Munson of GTE is the chairman.

A second group that has been formed is an ad-hoc group to study number portability, within the TR-45.2 subcommittee. With the CTIA requirements just received, and FCC deadlines for compliance in 1998/1999, this group is going to have to work extremely quickly. Achieving the goal of a quality standard that can be published in time for implementation by network infrastructure vendors might not even be possible. Peter Musgrove of AT&T Wireless is the chairman.

Cellular Networking Perspectives in Spanish

Cellular Networking Perspectives will be available in Spanish, starting with this issue. A sample package is also available *en Español*. Please email us at cnpsales@cnp-wireless.com or phone us at 800-633-5514 (+1-403-274-4749) to have your subscription changed.

Mail Backup Available

Email and fax subscribers to *Cellular Networking Perspectives* can now receive a backup copy by mail every month, for a modest additional fee. If you are concerned that faxes disappear from a shared fax machine before you get to them, or that your email disappears into a virtual pothole - then, for only $50 a year ($75 outside the US and Canada) you can arrange to have an additional copy sent by slower, but more reliable, first class mail. Please call us at 1-800-633-5514 or email to cnpsales@cnp-wireless.com to arrange for this additional service. We are still committed to 100% customer satisfaction, so if your mail version arrives and you have not received your email or fax copy, let us know and we will resend them (even if it isn't our fault!).

"Predictions Best Forgotten" Department

"Demand for cellular services [in the USA] will increase dramatically from 13 million subscriptions in 1993 to 33 million in 1998." From the *PCIA 1994 PCS Market Demand Forecast.*

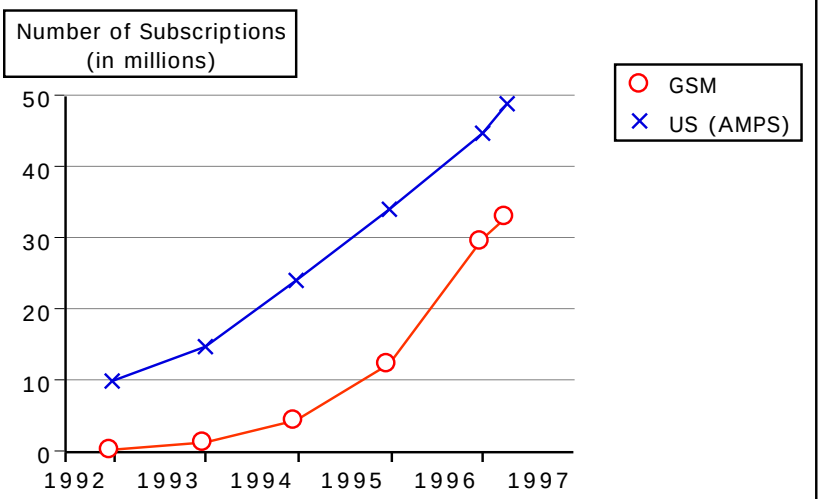
While this prediction seemed optimistic at the time, according to the most recent CTIA industry survey, there were actually over 45 million cellular phones active at the end of 1996. By the end of 1998 there could be close to double the subscribers estimated in 1994 (according to growth estimates from Paul Kagan Associates).

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/. **Language Editions:** English - Español.

Growth in GSM and AMPS Compared

On the subject of the number of subscriptions, recent statistics from the GSM MoU Association show the gap between GSM and AMPS is narrowing, although AMPS is still well ahead when just the numbers from the single largest AMPS market, the USA are considered (see Figure 1). Other large markets employing AMPS-compatible technologies (including IS-54/IS-136 TDMA digital and IS-95 CDMA digital) are Korea, Australia, Canada, Taiwan and Brazil. These probably account for at least another 20 million subscriptions (source: US Dept. of Commerce).

Figure 1: Growth in GSM and US AMPS Subscriptions



Digital Cellular Encryption "Cracker" Responds

We are pleased to publish a response to our April 1997 article "Has Digital Cellular Been Cracked?", by David Wagner, a graduate student at UC Berkeley, one of the team that exploited a weakness in the TIA CMEA algorithm used to protect the transmission of credit card numbers and short messages in the IS-95 CDMA standard. While we do not endorse his position, we believe that his response provides a useful insight into the attitudes of the cryptography community.

I enjoyed reading the article [April 1997 *Cellular Networking Perspectives* "Has Digital Cellular Been Cracked?" -- it is refreshing to see a report on the subject with significant technical content -- but I do have complaints about the way several issues were characterized:

Closed Design Process in TIA

Perhaps TIA was not *deliberately* secretive -- I have no personal knowledge of their intentions -- but the design process was certainly not open, either. *[Cellular Networking Perspectives]* said the TIA process is "open to all companies with an interest in the technology being standardized"; however, joining costs at least $1,000. As a grad student, I do not have access to that sort of money. Furthermore, the TIA is open only to companies; I am not incorporated (references: http://www.industry.net/c/orgunpro/tia/join-mem).

Even though I am not a TIA member, I can still get copies of the standards, right? It is not that easy. I have over a thousand dollars worth of specifications, and I still do not have everything relevant (I have IS-54-B, IS-136, EIA-627, and more, but not IS-95, for instance); and those funds were made available only by a gracious donation from a concerned citizen, to whom I am very grateful. Remember, I am doing this research as a public service; I have no financial interest in the matter. I am merely a grad student; I do not have large sums of money to throw around on a whim.

Also, the TIA goes out of its way to prevent proliferation of the authentication and encryption specification and make distribution to other interested cryptographers very difficult, by aggressively protecting its copyright. (I do not have any special reason to believe it is TIA's intention to prevent independent review of the algorithms, but that is the effect.) I can give you an example, for instance, where TIA lawyers threatened to sue when someone made a 1992 document describing the IS-54-B authentication and encryption algorithms available on the Internet -- even though it was later learned that:

i. the document was already available for free from TIA themselves upon request, and
ii. the document was already obsoleted by much newer specs.

One would think the TIA would recognize the time-proven value of independent evaluation and peer review, and would contact the cryptography community at large for help in making sure their algorithms are strong before deployment, but they do not. The end result of all this (whether deliberately intended or not) is that these cryptographic algorithms have languished for over 5 years in an effectively-closed design process without serious independent peer review from the cryptographic community. The CTIA admitted there were problems in the design process. In his NY Times article covering the issue, John Markoff wrote: "Carroll, head of the industry's privacy committee, said it planned to revise the process for reviewing proposed technical standards."

ITAR Restrictions Exaggerated

The supposed "ITAR (US International Traffic in Arms Regulations) restrictions" which prohibit foreigners from attending committee meetings are fabricated out of thin air. These regulations, which prohibit export of the documents describing the cryptographic documents are purely phony as well. Textual descriptions of encryption algorithms, even including pseudo-code and figures, are not controlled -- or so the State Department told Judge Patel in open court. Technical talks on cryptography are not controlled, even if foreigners attend; US cryptography conferences have welcomed foreigners for years. The cellphone industry needs to learn to listen to the NSA's dissembling with a skeptical ear.

Strong Encryption is Practical

The *Cellular Networking Perspectives* article claims that "Strong encryption not needed." Well, that is what the NSA would like us to believe, anyhow. In practice, building strong encryption into cellphones is merely good engineering practice. Like any other engineering discipline, in cryptography if you want robustness, you build more strength than you think you need and leave an extra margin for error. When building in more strength is extremely cheap, you build in lots of extra strength; when building strength is expensive, you do not go so far. In practice, building extra strength into your encryption algorithms is extremely cheap -- strong encryption is no more expensive than weak encryption.

Robustness is critically important. The cellular industry is deploying a new infrastructure for digital phones, and they had a chance to get the technology right. Instead, they blew their chance, and we will be stuck with these weaknesses for quite some time to come. If the TIA had built in extra strength for robustness, then quite likely we would still have good protection, and the TIA would look foresighted. Instead, the industry now looks shortsighted and foolish.

The phone industry did not develop phones with unbreakable security because they chose not to. It is possible, with today's technology, to implement digital cellular algorithms in cellular phones without affecting the phone's weight, power consumption, voice quality, or call setup. It takes more computer processing power to digitize the voice than it does to encrypt the digital voice.

TIA Voice Encryption is Weak

The *Cellular Networking Perspectives* article claims that "Voice encryption is unaffected." It is true that our paper did not discuss voice encryption, but that does not mean that the TIA system is any good. As early as 1992 others -- including noted expert Whitfield Diffie -- pointed out fatal flaws in the new standard's voice privacy features. The underlying technology is the Vigenere cipher, which was broken by the Union Army during the American Civil War. One cryptographer was quoted in the July 1992 Communications of the ACM calling the voice privacy protection "pitifully easy to break." This stuff is Cryptology 101. It is one of the first things you learn about when you study cryptography; the second thing you learn is how easy it is to break.

NSA Role Criticized

The NSA "did not .. mandate an algorithm to be used." No, they merely threatened the industry with denial of export approval and other such niceties. They did not mandate; they strong-armed. As far as I can tell, the cryptographers in the industry knew full well how terrible the voice privacy protection was. There is at least one documented example of an industry cryptographer who felt forced to speak on condition of anonymity, because he feared NSA reprisals to his company. That should tell you that there is something wrong with the situation.

Cloning and Authentication

It is true that our attack does not affect phone cloning. The TIA put more effort into preventing cellular fraud, because that directly affects their bottom line. Cellular privacy is much less of a concern to them, so they did not bother doing a good job.

Many of these points were made in Bruce Schneier's rebuttal to the CTIA's press release (see http://www.counterpane.com/cmea-response.html); it is unfortunate that they were not taken into account before press time. Much of the article was worth reading for its high-quality technical information, but I am disappointed that the article was littered with so many misleading statements.

Cracking CMEA: An 'Inside' Job?

The cracking of the TIA CMEA algorithm is a more complex story than originally thought. As reported in the April issue of *Cellular Networking Perspectives*, the CMEA algorithm protects credit card numbers and PIN codes (and other digits dialed within a call). It also protects the contents of short messages for the IS-637 standard (an option for IS-95 CDMA digital cellular and PCS).

The formerly obscure CMEA algorithm received much press recently when Schneier *et al* reported that they had 'cracked' the algorithm (see previous article). In fact, they were not the first to crack the algorithm, nor is their method the most efficient. Greg Rose of Qualcomm, whose assistance was acknowledged in the Schneier paper, has developed a much more serious attack. It apparently can achieve high success levels and near real-time performance.

What benefit would there be to a company that chairs the TIA *ad hoc* Authentication Group (AHAG) in breaking an algorithm developed by this group (although prior to Qualcomm's involvement)? The answer lies in the denial of export approval for IS-95 base stations which include CMEA protection for short messages (in IS-637). The US government prevented exports because they believed that CMEA was strong (although they had earlier verbally indicated that this would not be cause to deny exports), and that short messages could be used to encrypt significant amounts of user data. Soon after word got out that CMEA had been cracked, export approval was granted.

Qualcomm may have done everyone a favor. By proving that CMEA is weak now, they may have prevented greater embarrassment later. The current stir opens a window of opportunity to freshen not only the encryption provided by CMEA, but also voice and data encryption which were intentionally made weak to obtain export approval.

Status of IS-41 Rev. B Implementation

Cellular Networking Perspectives

Phone 1-800-633-5514 (+1-403-274-4749) • Fax +1-403-289-6658 *Last published 11/96*

Vendor1	Vendor2	Status	Date	Type	Location
Alcatel SEL	EDS PC	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Lucent	Commercial	2Q'95	H V D S	Orlando, Florida (BellSouth)
	Motorola	Commercial	2Q'95	H V D S	Richmond, Virginia (BellSouth)
	Nortel	Commercial	2Q'95	H V D S	Mobile, Alabama (BellSouth)
Astronet	***connectivity using IS-41 Rev. A plus TSB-55 only***				
Celcore	Alcatel SEL	Commercial	05/96	V D S	Yorkville, TN
	Ericsson	Commercial	06/96	V D S	Chicago (Cellular One)
	Lucent	Field Trial	09/95	H V DX	Cleveland, Ohio (GTE Mobilnet)
	Motorola	Commercial	12/95	V DX	Little Rock, AR (Alltel)
	Nortel	**Commercial**	**12/96**	**V D S**	**Knoxville, TN (USCC)**
	Tandem (HLR)	Field Trial	11/95	V D S	Seattle (AT&T-WS)
EDS PC	Alcatel SEL	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
Ericsson	EDS PC	Planning		V X	*location not announced*
	Motorola	Field Trial		H V D S	*location not announced*
GTE TSI	*connectivity using IS-41 Rev. A plus TSB-55 only*				
Harris	**NACN**	**Field Trial**	**08/96**	**V DX**	**NACN testing complete**
Lucent	Alcatel SEL	Field Trial	03/95	H+V D S	South Florida (BellSouth)
	NEC	Commercial		H V D S	Brazil
	Nortel	Planning		H+V DX T	*location not announced*
Motorola	Alcatel SEL	Commercial	2Q'95	H V D S	*Multiple locations*
	EDS	Commercial		H V D S	*Multiple locations*
	Ericsson	Commercial		H V D S	NACN
	Lucent	Commercial		H V D S	*Multiple locations*
	NEC	Commercial		V D S	Brazil
	Nortel	Commercial		H V D S	NACN
	Plexsys	Commercial		V D S	*Multiple locations*
NEC	Lucent	Commercial		H V D S	Brazil
	Motorola	Commercial		V D S	Brazil
Nortel	Alcatel SEL	Commercial	4Q'95	H V D S	Orlando, FL & Jackson, MS
	Lucent	Lab Trial	TBD	H V DX	Windsor (Bell Mobility)
	NEC	Commercial	2Q'94	H V D S	Brazil
Phoenix	***several***	**Commercial**	**3Q'97**	**V D SI**	**Bermuda via NACN/Brazil**
Plexsys	Ericsson	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Lucent	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Motorola	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	NEC	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
	Nortel	Commercial	12/95	V D S	Sao Paulo, Brazil (Telebras)
Telos	Lucent	Field Trial	3Q'96	V D S	Vancouver, BC (BC Tel)
	Nortel	Lab Trial	04/96	V DX	Vancouver, BC (BC Tel)

Explanation:

Status:	Development, Planning, Lab Trial, Field Trial or Commercial.
Date:	Date of actual or expected completion of listed phase of testing.
Code	Capability Being Tested
H	Handoff forward and back ('+' indicates path minimization & flash handling)
V	Validation ('+' indicates authentication using TSB-51).
D	Includes call delivery.
X/S/I	X.25 / ANSI SS7 / ITU-T(CCITT) SS7 datalink protocol.
T/C	Uses TDMA(IS-54, IS-136) / CDMA(IS-95) digital mobiles.
Location:	Location of test and carrier. Usually listed for first trial only.

Status of IS-41 Rev. C (ANSI/TIA/EIA-41) Implementation

Cellular Networking Perspectives

Editor David Crowe • 403-289-6609 • Fax 403-289-6658

Last published 01/97

Vendor1	Status	Date	Features	Other Vendors	Carriers	Locations
Alcatel SEL	**Field Trial**		**A N S**	***n/a***	**BellSouth**	***several***
Ericsson	**Commercial**		**S**	**Tandem*, Lucent***	***several***	***several***
	Field Trial	**3Q'96**	**A P**	**Tandem*, Lucent***	***n/a***	***n/a***
	Field Trial	**02/97**	**P T**	**Nortel**	**AT&T/Palmer**	**Atlanta**
GTE	Field Trial	2Q'97	**A**	*n/a*	*n/a*	*tbd*
Lucent	Field Trial		A	*n/a*	*n/a*	*tbd*
Motorola	Field Trial	4Q'96	A	Lucent	BANM	Charlotte, NC
Nortel	**Commercial**	**4Q'97**	**A N S V**	***n/a***	***n/a***	**MTX06 generic**
	Field Trial	**02/97**	**P T**	**Ericsson**	**AT&T/Palmer**	**Atlanta**

Explanation:

Status:	Development, Planning, Lab Trial, Field Trial or Commercial.
Date:	Date of actual or expected completion of listed phase of testing.
Features	Features Being Tested
A	Authentication
C	CDMA digital terminal support (IS-95)
N	Calling Number Identification
P	Cellular/PCS inter-band operation (TSB-76)
S	Short Message Service (SMS)
T	TDMA digital terminal support (IS-54, IS-136)
V	Voice Mail Notification (not SMS-based)
Other Vendors:	Other equipment vendors involved in trials. (*) indicates that this information has not been officially confirmed.
Carriers:	Carriers involved in trials.
Locations:	Locations of trials.

Note: IS-41 Revision C is in the early stages of implementation, and some vendors have not yet revealed their plans for implementation. There are several differences in the implementation of IS-41 Rev. C versus IS-41 Rev. B:

i. IS-41 Revision C implementation will occur in subsets, with the early candidates being Authentication (kills fraud dead), Calling Number Identification (sells digital), Message Waiting Notification (sells air-time) and Short Message Service (sells digital).

ii. Complete vendor-vendor pairwise testing will not be required, a trend that emerged towards the latter stages of IS-41 Rev. B implementation. Vendors and carriers have more confidence in their ability to install IS-41 solutions after testing with only selected vendors, and the ability to resolve compatibility issues in the field.

iii. ANSI/TIA/EIA-41 Revision 0 has not been published yet. For all practical purposes, implementations of this ANSI standard will be indistinguishable from IS-41 Rev. C.

iv. Additional extensions to IS-41 Rev. C and ANSI-41 will become available over the next several months. The first of these, TSB-76 for PCS/Cellular inter-band operation, has already been published, and standards to provide support for enhanced digital features (TDMA and CDMA), digital data, over-the-air service provisioning, enhanced emergency services (E9-1-1), international roaming and number portability are under development.

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 *Last published 09/96*

CDMA Digital Air Interface Standards - First Generation (Cellular)

Standard	Description	Status
IS-95	CDMA Dual-Mode Air Interface Standard	Published 07/93
IS-96	CDMA Option 1: Voice Coder	Published 04/94
IS-97	Base Station minimum performance standards	Published 12/94
IS-98	Mobile Station minimum performance standards	Published 12/94
IS-126	Service option 2: Loopback	Published 12/94

CDMA Digital Air Interface Standards - Second Generation (Cellular & PCS)

Standard	PN/SP	Description	Status
IS-95-A		IS-95 Revised	Published 05/95
IS-96-A		CDMA Voice Coder	Published 05/95
IS-97-A		**Base Station minimum performance standards (incl. J-STD-019)**	**Published 07/96**
IS-98-A		**Mobile minimum performance standards (including J-STD-018)**	**Published 07/96**
IS-99		Data Services (Fax and Circuit Switched Data)	Published 07/95
IS-125		Voice coder minimum performance standards	Published 05/95
IS-637		Short message service (rate set 1)	Published 12/95
J-STD-019	**SP-3383**	**Base station minimum performance standards**	**Pub. est. 05/97**
J-STD-008	**SP-3384**	**IS-95 adapted for 1800 MHz frequency band**	**Pub. est. 05/97**
J-STD-018	**SP-3385**	**Mobile minimum performance standards (for J-STD-008)**	**Pub. est. 05/97**
TSB-58		Administration of parameter value assignments	Published 12/95

CDMA Digital Air Interface Standards - Third Generation (Cellular & PCS)

Standard	PN/SP #	Description	Status
IS-95-B	PN-3693	IS-95 for 800 MHz and 1800 MHz frequencies (including J-STD-008)	Development
IS-96-B		CDMA Voice Coder (8 kbps)	Published 07/96
IS-126-A		**Mobile station loopback service option**	**Published 07/96**
IS-127		**Option 3: enhanced variable rate voice coder (EVRC)**	**Published 01/97**
IS-657		Packet data services	Published 07/96
IS-658		Data inter-working function interface (e.g. modem pool)	Published 07/96
IS-683	**PN-3569**	**Over the air activation and service provisioning**	**Published 02/97**
IS-707	**PN-3676**	**14.4 kbps data services (including STU-III voice encryption)**	**Development**
~~**n/a**~~	~~**n/a**~~	~~**STU-III (strong voice encryption)**~~	~~***see IS-707***~~
IS-xxx	PN-3648	Minimum performance standards for EVRC voice coder	Development
IS-xxx	**PN-3682**	**Bit exact description for EVRC (IS-127)**	**Development**
TSB-74		14.4 kbps radio link protocol and inter-band operations	Published 12/95
TSB-79	**PN-3823**	**IS-637 update for 14.4kbps SMS, service negotiation and Year 2000**	**Published 02/97**
IS-683-A	**PN-3889**	**OTA update: Roaming system selection and programming lock**	**Development**

Note: 1. IS- TIA Interim Standard, J-STD- TIA/ATIS Joint Technical Committee standard (ANSI), PN- TIA Project Number, SP- ANSI Standards Proposal, TSB- TIA Telecommunications Systems Bulletin.

2. **Bold Type** indicates modification since the previous publication of this report.

- Thanks to David Ott of OKI and Dr. Ed Tiedemann/Sam Broyles of Qualcomm for their assistance.