Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-403-289-6609 • Fax 403-289-6658 Vol. 6, No. 8 August, 1997

In This Issue ...

Next issue due: Sept. 4, 1997

"These flaws effectively nullify authentication" … Or do they?

This bold statement is quoted from the abstract of a paper by Sarvar Patel of Bellcore entitled "Weaknesses of North American Wireless Authentication Protocol" published in the June 1997 issue of IEEE Personal Communications. Can Patel claim that "In this article, we show the IS-41 authentication protocol to be unsound by pointing to multiple flaws in the protocol which allow a network impersonator to gain service *without breaking the CAVE algorithm*"?

We are responding to this article because we believe Patel's argument to be academically correct, but unsound in practice. The security limitations of a public radio based protocol are also, in some cases, its strengths, an observation obviously missed by Patel.

Patel's theoretical attacks on authentication are modelled around a cloner (which he calls "HI") and a network impersonator (which he calls "NI"). It is the requirement for a network impersonator (basically a fraudulent base station) that is the main weakness of his paper attack.

In order for the Patel attack to work, the cloner has to command the NI to launch an air interface message to a previously chosen victim mobile. This mobile will then respond with an authentication response that can be used by the HI to gain access. There are several flaws with this method, which are listed below.

Method not Passive

When the NI transmits a message, it is raising a red flag to the carrier, and to regulatory authorities. Unlicensed transmitters are not a new problem, and they can be detected quite easily, even when they do not broadcast continually. So , this method could only work for a while, until the transmitters are located and shut down, with the operators fined or in jail.

Not only is the NI an illegal transmitter, but it can be detected in several ways other than monitoring for spurious transmissions on the control channel. The mobile that is sent a message to the NI will respond with a message that will be detected by the legitimate base station. If the number of such spurious messages from mobiles exceeds a threshold, the presence of an NI can be inferred. Also, the transmission of a message by an NI may corrupt legitimate transmissions, elevating the error rate, which can also be the spoor of an NI. If this attack ever becomes a real problem, which is doubtful, it would be easy to design a device that would monitor for transmissions on the control channel that are not from the base station. And, with the location technology required for the FCC 9-1-1 order, the spurious transmitter could usually be automatically located within 125 meters.

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. Additional charges apply for international fax delivery. **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.

Coordination of NI/HI

The Patel attack requires close coordination between the cloner (HI) and the network impersonator (NI). Every time the HI is challenged, it will have to communicate with the NI, the NI will have to initiate a message to the victim mobile, receive the response and forward it to the HI, which will respond to the challenging system. This takes time, which will increase the likelihood of a timeout failure. More importantly, it requires the ability for the NI and HI to communicate.

Just how are the NI and HI going to communicate? If a wireless method is used, the distance between the NI and HI will be restricted and transmissions can be monitored. If a wired method is used, the NI and HI are forced to be stationary. Most likely, the NI and the HI would be the same device because of this problem.

Tracking the Victim is Not So Easy

One of the security advantages of a cell-based system is that it is hard to monitor a single mobile for long. The Patel attack would require the NI to follow a victim mobile (which would be impossible if the NI is stationary, and merely difficult if it is mobile). The only solution would be for the NI to pick on a mobile that happens to be around at the time the cloner decides to make a call. This creates its own set of problems, because the NI needs to continually feed MIN/ESN pairs to the cloner, so that a 'fresh' pair is available at the time the cloner wants to make a call.

Victims Won't Cooperate

Even if all the problems listed above were solved, the victim would not always be available for this attack. The victim mobile may move outside the cellsite between the time it is observed by the NI and when its identity is used by the cloner. The victim may be in a call, or in another call state that does not allow it to respond to a message on the control channel. These limitations will increase the error rate of this type of attack, forcing multiple attempts for many calls, and further increasing the level of communication required between the NI and the HI.

Inability to Sell ID's

Currently, cloners can obtain a MIN and ESN pair in one market and sell them days later in another. The Patel attack must be performed in real-time, so that information obtained in this way has no value on the black market.

Other Criticisms

The Patel paper also outlines the need for truly random numbers to be used for authentication. While this is important, even a flawed random number received by a mobile phone is made more random by unpredictable changes in the location of the mobile. An attack on the random number generator would have some chance of succeeding in a fixed wireless system, without the additional source of randomness provided by mobility.

Patel also criticizes the need for distribution of authentication A-Keys by mail. While this process is known to have vulnerabilities, it is far from the only method available. A-Keys can also be programmed by secure programming cradles, by over-the-activation or by querying a manufacturer's database, indexed by ESN. While these methods are not all available at present, neither is the need for this level of security. High security methods for handling A-Keys are not crucial until the number of easily cloned analog phones declines much further.

Conclusions

The Patel attack on IS-41 authentication is purely an academic exercise, with no practical application. There are realistic network based attacks being resolved in ANSI-41 by TIA TR-45.2 and the AHAG, but these were not addressed by the Patel paper. You can continue to rely on the security of the CAVE algorithm and also the IS-41 support for authentication by roamers.

CTIA Requests FCC Decision on SP-3580

On July 16th 1997, the CTIA, representing most US wireless carriers, requested that the FCC adopt ANSI Standards Proposal SP–3580 as the technical standard for implementation of the US CALEA law. In articles in our June and July, 1997 issues, we have discussed some of the controversy surrounding two competing proposals (both TIA's SP–3580 and US law enforcement's ESI). Articles in our July 1997 issue and the current issue provide a summary of the capabilities provided in the ballot version of SP-3580.

It was expected by many that if SP–3580 was approved as a standard, that the FBI would appeal to the FCC to prevent its recognition as "safe harbor". However, it was a surprise when the CTIA, obviously believing that a good offence is a good defence, leapt into the lap of the FCC before the standards process was completed.

The term "safe harbor" refers to a provision in CALEA that treats affected companies as in compliance with the statute "if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the [Federal Communications] Commission".

The CTIA move may be designed to ensure that carriers and manufacturers know what capabilities are required to meet the October 1998 CALEA deadline, or to try to have the deadlines extended by the FCC. The review of SP–3580 ballot comments will continue, with the possibility that the relevance of the resulting standard will be known sooner, rather than later.

Another outstanding problem is that the October 1998 deadline covers capability, not capacity (as final capacity requirements have not been made available). While these terms have distinct legal meanings, it is hard for system designers to separate capability from capacity.

FCC to Revisit Wireless 9-1-1 Decision

On July 21st, 1997 the FCC announced that it is going to revisit its Wireless Enhanced 9-1-1 rule-making based on comments received recently from GTE Wireless, the Wireless E911 Coalition (representing carriers) and the Ad Hoc Alliance for Public Access to 911 (representing public interest groups).

The most controversial issue is the requirement to allow 9–1–1 calls from uninitialized mobiles. Providing some 9–1–1 services (such as callback) to an uninitialized mobile may be technically difficult or impossible, and may only invite abuse of the system and anonymous harassment of 9-1-1 personnel. Uninitialized phones may have a meaningless identity or one that is the same as a legitimate mobile. Also, charging wireless subscribers a monthly fee to pay for the 9-1-1 infrastructure may be less palatable to consumers, if methods of avoiding the fee are sanctioned by an FCC rule-making.

US Law Enforcement Surveillance Standard Part II: The Protocol

The controversy over the requirements for the US CALEA law have overshadowed the fact that a standard is still being developed, and does have at least the basic requirements for the surveillance of suspects by law enforcement. The first part of this article, in the July 1997 issue, provided an overview. This part describes the messaging protocol (see Table 1 for a summary of SP-3580 messages). In all cases messages are sent from the carrier to the law enforcement agency.

Starting & Stopping

Whenever a call is initiated, a call identity must be assigned. All subsequent messages are associated together by the use of the same identity. If a call is being made to a subject of surveillance, a *TerminationAttempt* message is transmitted. If the subject initiates a call, an *Origination* message is transmitted.

At the end of a call a *Release* message must be sent.

Mid-Call Events

A few events are detected during a call, resulting in other messages being transmitted:

- Answer

  When a call is answered, the *Answer* message is initiated.

- Redirection

  When a call is forwarded, directed to voice mail or routed to another MSC for call delivery, the *Redirection* message is initiated, indicating the new destination of the call (e.g. the call forward number).

- Merging/Splitting Calls

  In some complex call scenarios, calls may be merged or split. Complex features such as 3 way calling, call transfer, conference calling and call waiting may need to invoke the *Change* message to associate a set of current call identities with their replacements. The number of calls being monitored may be increased or reduced in this way.

Role of the HLR

When a surveillance subject registers in a system, the HLR must send a *ServingSystem* message to the monitoring law enforcement agency. This is not intended to track the subject (as the geographical area covered by a single system could be hundreds of square miles), but to allow the law enforcement agencies to determine whether surveillances need to be set up in other systems.

Monitoring Voice

Relatively few surveillances involve the recording of calls. In most cases, only the call identifying information is required. However, in cases where the contents of a conversation are authorized for surveillance, the Call Content Channel (CCC) between a switch and law enforcement must be controlled (see Figure 1 in the June 1997 issue).

Two messages are required to perform this function, *CCOpen* and *CCClose*. *CCOpen* associates a specific call that is being monitored with either one or two CCC's. Two call content channels are required when both the conversation of the subject and the other party to the call are of interest, and when it is important to know which party said what.

These messages are not likely to be used to turn recording on and off, as this could result in clipping of calls. Instead, simple signaling on the CCC (equivalent to on-hook/off-hook) can be used. This eliminates clipping, under the assumption that the law enforcement agency will be informed of the identity of the surveillance subject within a few seconds (at most) of recording starting.

Monitoring Data

Circuit mode data can be handled like a voice call by the carrier, although the law enforcement agencies will obviously have to deal with determining what kind of data is being transmitted (e.g. modem tones) over the CCC.

Table 1: SP-3580 Messages

Message	Indicates...
Answer	Call has been answered.
CCClose	Stop recording on a CCC.
CCOpen	Start recording on a CCC.
Change	Change in call identities (e.g. 3 way calling).
Origination	Subject has made a call.
PacketEnvelope	Packet data has been transmitted.
Redirection	An incoming call is redirected.
Release	A call has ended.
ServingSystem	Subject has registered.

Packet data can either be handled in a similar fashion, with the subset of packets belonging to a surveillance subject being transmitted over a CCC, or packets can be transmitted over the CDC. In this case, the *PacketEnvelope* message is used to transmit both the identity of the subject and the contents of the packet. This method is expected to be used for the transmission of wireless short messages and for ISDN user-to-user signaling.

Parameters

Each SP-3580 message contains a number of parameters. The most important are described below:

- Surveillance Identity

  The *CaseIdentity* parameter is a string of characters that uniquely identifies a specific surveillance, and, by implication, a specific subject.

- Call Identity

  The *CallIdentity* parameter is an internal identifier for a call within a switch. Some complex call scenarios may require more than one call identity, or even the merging and splitting of these identifiers during a call (see the *Change* message, above).

- Access Identity

  The *AccessLocation* parameter identifies the telecommunications network element that is transmitting the message. This will be most useful in cases when several independent elements share the same CDC. This does not locate the subject of the surveillance.

- Party Identity

  The *PartyIdentity* parameter identifies a party to a call, via dialed digits, calling number identification, the MIN and ESN of a mobile or other means. This parameter is usually included twice to identify both the calling and called parties to a call.

- Subject Location

  The *Location* parameter identifies the location of the subject being monitored when they originate, receive, answer or disconnect a call. This will most likely the cell or sector that the mobile is connected to. Location is not reported when a handoff occurs, or a reshuffling of parties in a call takes place (e.g. in a 3-way call).

- CCC Identity

  Each CCC, used for monitoring voice or data transmissions, has a unique identity which is reported in the *CCCIdentity* parameter whenever a CCC is allocated through the use of the *CCOpen* message.

- Date and Time

  The *TimeStamp* parameter records the time at which the message is generated. This is somewhat redundant, as the law enforcement agency should receive the message shortly afterwards, but may be important in a system with significant delays or to establish the sequence of events reported by multiple network elements over a single CDC.

- Other parameters

  A number of other parameters report information of lesser significance, such as the format of a CCC transmission and the nature of incoming calling party numbers.

Message Encoding

The encoding of SP-3580 messages is defined by the ASN.1 language. This is simply a formal method for specifying the parameters that are allowed in a message, whether they are mandatory or optional, what size and type of data they are composed of and how to distinguish them from other parameters.

The SP-3580 protocol differs from IS–41 in several ways. Firstly, it can be defined by ASN.1, which indicates it is a cleaner protocol which should result in less complex software to create or interpret its messages. Secondly, parameters are numbered as they are listed for each message, rather than having the same identity for all messages. This is more efficient (as all parameter identifiers are 1 byte long, rather than the 3 bytes required for most IS-41 parameters) and more flexible (e.g. the same parameter can be used twice in one message without ambiguity). Also, all parameters are defined as ASCII characters (i.e. plain text), rather than the binary format used for the majority of IS-41 parameters. This makes equipment to view the information in messages somewhat simpler, although the benefits are limited because parameter ids and other 'envelope' information is still in a binary format.

What's Missing?

SP-3580 comments received from the FBI (and other law enforcement agencies) recommend the inclusion of several additional capabilities. So far the TIA TR-45.2 subcommittee has not agreed to modify the protocol to provide any of these:

- Changes in the subscription or activation status of features.
- Transmission of DTMF digits during a call.
- Reception of call progress tones.
- Commands to activate visual or audible indicators on a phone (such as a call waiting indicator).
- The addition, removal or sidelining (hold) of a party to a call.
- Regular confirmation that surveillance for a subject is still in place.

Why the Objection?

The telecommunications industry generally believes that the additional requirements of law enforcement are beyond the scope of CALEA, and will result in extra costs. In particular, costs not mandated by CALEA will not be reimbursed for any switches, even those installed before 1995. Also, adding these requirements could expose carriers to lawsuits from civil liberty organizations.

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 05/97

Vendor1	Status	Date	Features	Other Vendors	Carriers	Locations
Alcatel SEL	**Field Trial**	***complete***	**A N S**	***n/a***	**BellSouth**	***several***
Ericsson	**Commercial**		**A ST**	**Tandem*, Lucent***	***several***	***several***
	Field Trial	***ongoing***	**P**	**Lucent, Nortel**	***several***	***several***
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
Telos	**Field Trial**	**4Q'97**	**A N S**	**Lucent, Nortel**	**n/a**	**n/a**

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 has not been published yet, although it was submitted to the TIA for publication in July, 1997. For most 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 February, 1997*

Superseded Interim Standards and TSBs

IS/TSB	Description	Published
IS-41-B	Cellular Radiotelecommunications Inter-System Operations	12/91
IS-52-0	Cellular Subscriber Dialing Plan and Service Codes	11/89
IS-53-0	Cellular Features Description	09/91
TSB-41	Technical Notes for IS-41 Revision B	11/94
TSB-51	Inter-System Authentication, Signaling Message Encryption and Voice Privacy	05/93
TSB-55	IS-41 Rev. A/B Forward Compatibility	05/94
TSB-64	Wideband Spread Spectrum Intersystem Operations	02/94
TSB-65	Mobile Border System Problems	04/94

ANSI Standards and Annexes

ANSI #	SP #	TIA IS-	Subject	Published
ANSI/TIA/EIA-41	**SP-3588**	**IS-41-C**	**Intersystem Operations**	***in press***
ANSI/TIA/EIA-660		IS-52-A	Dialing Plan	09/96
ANSI/TIA/EIA-664		IS-53-A	Features	09/96
ANSI J-STD-025	**SP-3580**	**n/a**	**Lawfully authorized electronic surveillance**	**Ballot**
ANSI/TIA/EIA-xxx	**SP-3581**	**n/a**	**Enhanced Wireless 9-1-1, Phase I**	**reballot**
ANSI-41 annex	**SP-3892**	**n/a**	**International Mobile Station Identity (E.212 IMSI)**	**Ballot**

EIA/TIA Interim Standards

IS-	Description	Published
IS-41-C	Cellular Radio Telecommunications Intersystem Operations	02/96
IS-52-A	Uniform Dialing Procedures for use in Cellular Radiotelephone Systems	03/95
IS-53-A	Cellular Features Description	04/95
IS-93-0	Ai and Di Interfaces Standard (PSTN/MSC)	12/93
IS-124-0	Cellular Inter-System Non-Signaling Data Communications	11/93
IS-124-A	**Cellular Inter-System Non-Signaling Data Communications**	***in press***
IS-725	**IS-41 support for Over-the-air Service Provisioning (OTASP)**	***in press***
IS-728	**Inter-System Link Protocol**	***in press***
IS-730	**IS-41 Support for IS-136 DCCH (TDMA digital control channel)**	***ballot***
IS-xxx	**IS-41 support for data services for digital terminals (TDMA and CDMA)**	***ballot***

Telecommunications Systems Bulletins (TSBs)

TSB-	Description	Published
TSB-29-A	International Implementation of Cellular Systems Compliant with TIA-553	09/92
TSB-29-B	International Implementation of Wireless Systems	*ballot*
TSB-56-A	Application Level Testing for IS-41 Rev. B, IS-53 Rev. 0 and TSB-51	06/94
TSB-76	PCS Multi-Band Support	09/96

Active TR-45.2 Projects (PN = TIA Project Number)

PN/SP	Description	Editor	WG	Standard
PN-3295	**Ai and Di Interfaces Standard**	**David Crowe**	**VII**	**TIA/EIA-93-A**
PN-3362	**Cellular Features Description (Rev. B)**	**Terry Watts**	**I**	**TIA/EIA-664-B**
SP-3590	Intersystem Operations	Terry Watts	II,III	TIA/EIA-41-A
PN-3619	IS-41 Support for IS-95-A (advanced CDMA)	Sam Broyles	II	n/a
PN-3661	Wireless Intelligent Network	Terry Jacobson	II	TIA/EIA-41-A
SP-3725	Call detail/billing record transfer for data and enhanced services	Peter Larsen	IV	TIA/EIA-124-B
PN-3890	**Enhanced 9-1-1, Phase II (125 m. location accuracy)**	**Terri Brooks**	**0**	**n/a**
PN-3980	**Wireless Number Portability, Phase I (database query)**	**Chuck Ishman**	**II**	**n/a**
n/a	**Authentication enhancements**	**n/a**	**II**	**n/a**
n/a	**Broadcast/Multicast Short Message Service**	**n/a**	**I,II**	**n/a**
n/a	**Calling Name Presentation/Restriction**	**Terry Jacobson**	**I,II**	**n/a**