Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 4, No. 11 November, 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. ❒

Look for your next issue on: December 1, 1995

Fraud and Countermeasures, Part II: Clones

Cloning is such a serious problem for the cellular industry (an estimated $500 million in the USA in 1995) that an explosion of innovative countermeasures have arisen to combat it. Unfortunately, cloning is so simple to perpetrate and so hard to detect, that there is no single effective answer. In this part of our series we focus on techniques that attack cloning in the tens of millions of phones that lack the capability to authenticate.

In part III (December, 1995), we will focus on authentication, the ultimate solution to cloning.

Cloning

Cloning is sometimes described as counterfeiting, which is perhaps a more accurate name. Whatever the name, it can be defined as the complete duplication of a legitimate mobile identification. This involves replicating the MIN and ESN of a mobile and, in systems that use it, the PIN. An entire mobile identification has to be replicated to qualify as cloning, and to slither by the IS-41 pre-call validation checks. Replicating only a MIN or only an ESN can easily be detected.

Cloning is performed for three different reasons:

a. To steal service.
b. To maintain anonymity.
c. For an 'extension phone' service.

While all three motivations for cloning are a serious problem, the first two cause the biggest loss of revenue. People that duplicate their own MIN and ESN still pay their own airtime and toll charges, with carriers just losing subscription revenue for additional phones. However, companies that claim to clone for extension phone services may be a cover for hardcore criminal cloning.

Most cloners will use a MIN and ESN until it is no longer allowed by the system, especially if they have paid others for the stolen mobile identification, or if reprogramming is difficult. Only when service is denied will they move to another combination. Sophisticated cloners using advanced clone phones may reuse MINs and ESNs even before they are detected to avoid triggering alarms.

Obtaining Mobile Identities

The first step in cloning is to obtain a complete mobile identity. Unfortunately, this information can easily be obtained as it is transmitted on the control channel every time a mobile registers, originates a call or receives a call. The PIN is transmitted on the voice channel, but this is only a barrier to the unsophisticated cloners, a barrier that only a computer, software and the right model of cellular phone is required to overcome.

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.

Modifying an ESN

According to FCC rules (Part 22.919), a cellular phone ESN should be virtually impossible to modify. However, cloners have discovered that to clone some models of cellular phones, modifying the ESN is not necessary, phone software is simply modified to replace the real ESN by another value whenever it is read from memory. Other cloners have discovered that some manufacturers have left a trap door for service technicians to modify ESNs. This was intended as a way to provide replacement phones without a switch service order and is just one indication of the generally negative interaction between customer service and fraud prevention.

Clone Detection Techniques

There are many clone detection techniques, the most common of which are described below and summarized in Table 1. For each, we will pay particular attention to the customer service impact and the effectiveness for counterfeit home and roamer mobile identifications. We categorize the cost of each method as low (e.g. MSC software changes only), medium (e.g. additional MSC hardware and network capabilities) or high (e.g. additional base station hardware). Table 2 lists some of the products being marketed as clone countermeasures. Figure 1 points out the impact of each countermeasure on the the cellular network.

Pulling Exchanges

If a large amount of fraud attacks MINs from a few switches, one of the simplest ways to prevent this is to "pull the exchange". This involves removing the NPA-NXX of the switch from the roamer agreement tables stored in every MSC. Unfortunately, while this technique bars all cloning fraud using these MINs, it also bars all legitimate roaming. While cloners can simply use MIN and ESN combinations from a different MSC, roamers remain without service. Carriers may reduce the loss of revenue to cloners, but have to accept the loss of profitable roaming revenue. This is absolutely the worst approach to fraud management, but sometimes is necessary to stem near fatal bleeding.

Pulling Call Types

Instead of eliminating all service for blocks of roamer MINs, it is possible instead to just remove privileges that are most abused by cloners, including international calls and 3 way calling. This has somewhat less impact on legitimate roamers, but has the worst effect on the most desirable roamers and, again, cloners can just move to different MIN/ESN blocks while roamers are stuck with reduced service. Carriers temporarily reduce cloning losses and permanently reduce roaming revenues.

Call Pattern Analysis

A knowledgeable person scanning call records can often detect cloning fraud within a few calls. Unfortunately, the person power required to do this for every subscriber would be prohibitively expensive. A few companies have recognized that computers can do this almost as effectively as humans, and without demanding coffee breaks or overtime. Several products provide continual analysis of calling patterns based either on real time analysis of call records or IS-41 validation transactions (see Table 2). Patterns of fraud can be detected from analyzing different combinations of the following information:

- MIN (the fundamental key to all subscriber based pattern analysis).
- Dialed number (either individual phone numbers or geographical locations commonly associated with criminal dealings, such as Colombia and Wall Street).
- Calling location (e.g. from cells in high crime areas in high crime cities, such as Los Angeles, Miami and New York).
- Duration and frequency (lots of long calls are most suspicious).
- Velocity (a call from Los Angeles, followed 2 minutes later by a call from New York City indicates that either Superman is making calls or a mobile has been cloned).
- Time of day (off hours are most suspicious).
- Previous subscriber calling patterns (sudden changes are suspicious).

Software can maintain a profile for subscribers and then rank calling behaviour for each MIN based on a combination of call characteristics and previous subscriber calling patterns. Fraud investigators can manually investigate behaviour from the most suspicious MIN on down. When cloning is verified, the subscriber's MIN, ESN or PIN must be changed and the existing mobile identification turned off.

PIN

A PIN is a short numeric code (usually at least 4 digits) that a subscriber must enter to receive service. When a mobile is cloned, a new PIN can be given to the subscriber. PINs are either entered on every call (by a prompt once the phone is directed to a voice channel) or as a lock code to turn service on or off. PINs have had a large impact on fraud where they have been implemented, but they are also a large annoyance to customers. The beneficial effect is temporary, because obtaining a PIN is not a lot more difficult than obtaining a MIN and ESN and no modifications to clone phones are required to use a PIN. The reduction in fraud is because cloners have been thrown off balance and need slightly more sophisticated equipment to obtain PINs. Another drawback to PINs is that they will not be supported by IS-41 until Revision C is published, and consequently are not applicable to roaming fraud from markets using different MSC equipment vendors.

The long term advantage of PINs is that they allow service to be given to a cloned subscriber immediately after cloning is discovered and the subscriber is contacted, without the subscriber needing to visit a service centre to have their MIN reprogrammed or phone swapped.

Law Enforcement

The CTIA has put a lot of effort into educating law enforcement to find and prosecute cloners. They have also lobbied successfully to have US law clarified to clearly make cloning illegal. However, using law enforcement will be no more successful than the war on drugs has been. For every cloner caught, more will enter this lucrative criminal enterprise. And, for every amateur caught by their own sloppiness, professionals associated with multi-layered criminal gangs will

become more successful. If cloning remains simple, the enormous financial rewards will attract many people willing to take a risk. Cloners sent to jail will just educate fellow inmates so that they can have a supply of pawns when they get out, and move up to a safer perch on the totem pole themselves.

RF Fingerprinting

Three companies with a history of US defence radio R&D claim that they can recognize most phones by an individual pattern of radio transmission.. The claims of Coral (with Applied Signal Technology), Corsair and CTS appear to be true, with a high success rate at recognizing fraudulent mobiles (80% - 90%). The drawbacks to this technique are an impact on customer service through false positives (1% - 2%), the possibility that cloners may find certain models of phones that this technique does not reliably work on and difficulties with roaming. Roaming troubles occur because the three techniques being used are incompatible, and not every market may be able to afford RF fingerprinting. The first problem is being examined by the industry and could be solved by a network that transmits a digitized RF transmission from a home system to visited system. However, RF fingerprinting will not stop cloners picking MINs from systems that cannot afford this expensive technology. Unfortunately, systems that cannot afford RF fingerprinting, are also least able to absorb the cost of fraud which has nothing to do with their system. In the worst case scenario, subscribers from these systems would lose roaming privileges, causing a further loss of revenue, and causing subscribers to sign up with systems that have RF fingerprinting (and therefore more roamer agreements), causing a further loss of revenue.

Voice Prints

Voice recognition technology has been promoted as an adjunct to the PIN method. It would require each subscriber to pick a word that they would have to speak whenever a PIN is required. This method will increase the customer annoyance factor, make it inconvenient to lend a phone to a friend or colleague and also suffers from the roaming problem of RF fingerprinting. The benefit of voice recognition technology is that the cost will be quite low, particularly for carriers that plan on using voice recognition to provide enhanced services.

ESN Hardening

The FCC required that ESN protection within a cellular phone be toughened in a modified Part 22 that became effective on January 1, 1995. The CTIA may soon follow suit by including ESN hardening in their Gold Seal program. While ESN hardening is good to a limited extent, it will not have a significant impact on cloning and has the potential to significantly increase the cost of manufacturing and servicing cellular phones. While it may be worthwhile to remove the ability to modify an ESN by connecting a cable to a phone, millions of phones already exist with this capability (which has customer service benefits). And, even if an ESN was made impossible to modify within a phone, it would do nothing to prevent the ESN from being used in an older phone without hardening. Since greater ESN protection can only be applied to new phones, this technique has no advantages over authentication, and will not work nearly as well.

Table 1: Clone Counter measures Compared

Counter-measure	Home Effectiveness	Roamer Effectiveness	Customer Impact	Cost
Pulling Exchanges	n/a	High	High	Low
Pulling Call Types	n/a	Medium	Medium	Low
Call Pattern Analysis	Medium	Low to Medium	Low	Medium
PIN	Medium	Low	High	Medium
Law Enforcement	Low	Low	Low	High
RF Fingerprinting	High	Low to Medium	Low	High
Voice Prints	Medium	Low	High	Medium
ESN Hardening	Low	Low	Medium	High
Authentication	High	High	Low	Medium

Table 2: Clone Counter measure Products

Counter-measure	Company	Product	Contact
Pulling Exchanges	*MSC/HLR vendors*		
Pulling Call Types	*MSC/HLR vendors*		
Call Pattern Analysis	Coral Systems	FraudBuster	+1•303•772•5800
	GTE Telecommunication Services	CloneDetector	1•800•892•2888
	IBM	WFMS	1•800•753•4426
	Subscriber Computing	FraudWatch	+1•714•588•3700
	Systems/Link	FraudTec	+1•908•928•4900
PIN	*MSC/HLR vendors*		
Law Enforcement	CTIA	Fraud Task Force	+1•202•785•0081
RF Fingerprinting	Coral Systems/Applied Signal Technology	veRiFier	+1•303•772•5800
	Corsair Communications	PhonePrint	+1•415•842•3300
	CTS	Blackbird	+1•206•443•6400
Voice Prints	Brite Voice Systems	VoiceSelect Sentry	+1•316•652•6648
ESN Hardening	US Federal Communications Commission		
Authentication	*Phone/Infrastructure vendors*		

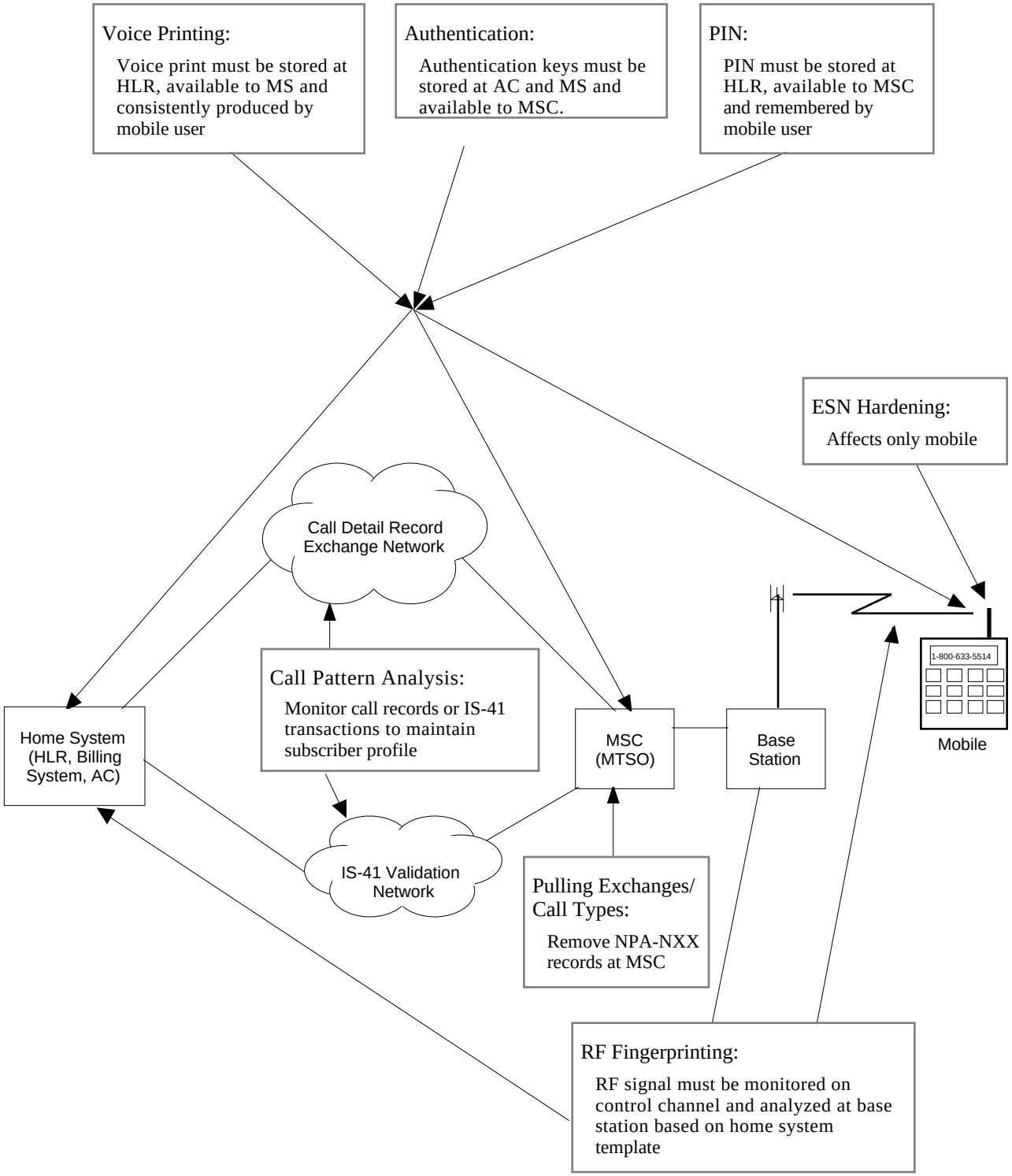

Figure 1: Cloning Fraud; Points of Defence

Summary

Countermeasures to cloning are available, but vary widely in their cost, effectiveness and impact on customers. None of the countermeasures are as effective as authentication, but due to the lack of this capability in most cellular phones, they will continue to be used for several years until authenticating phones (hopefully promoted by laws making authentication mandatory in new phones) significantly outnumber the older non-authenticating phones. Even then, cloners will focus on the diminishing numbers of non-authenticating phones and, at some point in the far distant future, all non-authenticating phones will have to be recalled and either upgraded, if possible, or replaced at no cost before the bleeding finally stops. ❒

TIA TR-46 Committee
Public 1800 MHz PCS
Project Status Report

Published Interim Standards

IS	Title	Publication
IS-104-A	PCS Service Descriptions	in press
IS-651-0	SS7/GSM A Interface (RS/PCSC)	TIA review
IS-652-0	Intersystem Operations - DCS1900 (GSM) MAP based	TIA review

Published Telecommunications Systems Bulletins (TSBs)

TSB	Title	Publication
TSB-68	Intersystem Operations - IS-41 MAP based	in press

Projects in Ballot Process (SP = Standards Proposal Number)

SP	Title	Status	IS/TSB
3344	ISDN A interface (RS/PCSC) Second ballot includes PN-3585, adding SS7 transport as an option	second ballot	IS-653

Active TR46.1 and TR46.2 Projects (PN=TIA Project Number)

PN	Title	Completion	IS/TSB
3167	System Requirements, Revised (was PN-3368)		*Internal*
3212	DCS1900(GSM)/IS-41 PCS Network Interoperability (I&I) Seamless interoperability between IS-41 MAP and DCS-1900 MAP networks	4Q'95	
3368	System Requirements, Revised		
3436	Advanced Network Reference Model The network reference model is being enhanced to accommodate IN, OA&M, 911 and lawful intercept network elements		
3513	SS7 Signaling and Network Routing Translation type 10 has been reserved by T1S1, for SS7 network routing using an E.164 directory number, specifically for DCS-1900 systems.	4Q'95	TSB-
3567	Intersystem Operations - DCS1900 MAP (revised) This revision will add Call Barring, Intercept, Multi-way Calling, Data, Fax, 911, Equal Access, ITU-T TCAP and E.164 GTT (see PN-3513)	1Q'96	IS-653-A
3568	Frame Relay A Interface (RS/PCSC) Pending formal TR46 approval to move this work to TR-45.4		*see IS-652-A*
3596	SS7 A-Interface (Revision A) This revision will contain only the DCS-1900 (GSM) interface. CDMA work is expected to move to TR45.4.		IS-651-A
3808	Lawful Intercept A new joint project with TR-45.2		
3809	Emergency Services A new joint project with TR-45.2		
n/a	Privacy and Authentication Requirements (P&A) An internal document set describes: (1) generic requirements, (2) IS-41 authentication and possibly (3) GSM authentication		
n/a	PCS Service Descriptions, Revision B This revision will align IS-104 with IS-53 (Cellular feature descriptions)		IS-104-B

Status of IS-41 Rev. B Implementation

Vendor1	Vendor2	Status	Date	Type	Location
Alcatel SEL	Astronet*	Commercial	08/94	H V D S	Mobile, Alabama (BellSouth)
	AT&T	Commercial	2Q'95	H V D S	Orlando, Florida (BellSouth)
	EDS PC	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	GTE TSI	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Motorola	Commercial	2Q'95	H V D S	Richmond, Virginia (BellSouth)
	Nortel*	**Commercial**	**2Q'95**	**H V D S**	**Mobile, Alabama (BellSouth)**
Astronet		Development			
AT&T	Alcatel SEL	Field Trial	03/95	H+V D S	South Florida (BellSouth)
	GTE TSI*	Planning		V DXS	Location not announced (BAM)
	NEC	Commercial		H V D S	Brazil
	Nortel	Planning		H+V DX T	location not announced
Celcore	Alcatel SEL	Lab Trial	05/95	H V D S	Yorkville, TN RSA
	AT&T	**Field Trial**	**09/95**	**H V DX**	**Cleveland, Ohio (GTE Mobilnet)**
	Ericsson	**Field Trial**	**09/95**	**V D S**	**Chicago (Cellular One)**
	GTE TSI*	**Commercial**	**10/95**	**V DX**	**Yorkville, TN RSA**
	Nortel	**Lab Trial**	**12/95**	**V D S**	**Toronto (Bell Mobility)**
EDS PC	Alcatel SEL	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Ericsson	Planning		V X	location not announced
Ericsson	EDS PC	Planning		V X	location not announced
	Motorola	Field Trial		H V D S	location not announced
GTE TSI*	Alcatel SEL	Commercial	08/94	V D S	Mobile, Alabama (BellSouth)
	Others	**Commercial**	**3Q'95**	**V DXS**	**Rev. A plus TSB-55 compatibility**
Motorola	Alcatel SEL	Commercial	2Q'95	H V D S	Orlando, Florida (BellSouth)
	Astronet*	Commercial	4Q'94	V DX	Several locations
	AT&T*	Commercial		V D S	Several locations
	EDS PC*	Commercial		V X	Dedham, MA
	Ericsson*	**Commercial**		**V D S**	**Several locations**
	GTE TSI*	**Commercial**		**V DX**	**Several locations**
	NEC	Commercial		V D S	Brazil
	Nortel (MTX)*	Commercial		H V DX	Denver, CO
	Nortel(800CM)*	Commercial		V DX	Raleigh, NC
NEC	AT&T	Commercial		H V D S	Brazil
	Motorola	Commercial		V D S	Brazil
Nortel	**Alcatel SEL**	**Commercial**	**2Q'95**	**H V D S**	**Pensacola, Florida**
	AT&T	Lab Trial	TBD	H V DX	Windsor (Bell Mobility)
	NEC	Commercial	2Q'94	H V D S	Brazil
Plexsys	**AT&T**	**Field Trial**	**11/95**	**V D S**	**Sao Paulo, Brazil**
	Ericsson	**Field Trial**	**11/95**	**V D S**	**Sao Paulo, Brazil**
	GTE TSI*	Commercial	2Q'95	V DX	San Maarten(V) / Tennessee(D)
	Motorola	**Field Trial**	**11/95**	**V D S**	**Sao Paulo, Brazil**
	Nortel	**Field Trial**	**11/95**	**V D S**	**Sao Paulo, Brazil**

Explanation:

*	Other vendor is using IS-41 Rev. A with TSB-55 for compatibility.
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	X.25 datalink protocol.
S	ANSI SS7 datalink protocol.
C	Uses CCITT SS7 datalink protocol.
T	Uses TDMA (IS-54) digital mobiles.
W	Uses CDMA (IS-95) digital mobiles.
Location:	Location of test and carrier. Usually listed for first trial only.