A MESSAGE HANDLING SYSTEM TO SIMULATE AN AUTHENTICATION CENTER NETWORK NODE IN A CELLULAR TELECOMMUNICATIONS NETWORK

Jey Veerasamy, Ross C. Creech, Jeffrey M. Doss, and Brett B. Stewart
Wireless Networks
Nortel, Inc.
M.S. D0210
2201 Lakeside Boulevard
Richardson, Texas 75082 USA
email:{jey | rcreech | jdoss | bretts}@nortel.com

KEYWORDS

cellular telecommunications, wireless, communication networks, authentication, simulation, IS-41

ABSTRACT

Cellular fraud is recognized as one of the most significant problems facing the cellular industry today. The Cellular Telecommunications Industry Association (CTIA) cites that losses in the United States as a result of cellular fraud aggregated to nearly $1.5 million per day in 1994. Authentication is an effective mechanism to combat this problem. North American Cellular Interim Standard 41 Revision C (IS-41C) defines the inter-system protocol for authentication and introduces a new network node called an Authentication Center (AC). An Authentication Center Simulator, ACSim, was developed to test the authentication functionality of Nortel's cellular switch. The operations of ACSim are fully controllable and provide a flexible environment to test a wide variety of scenarios, many of which are extremely difficult to test with an actual AC.

INTRODUCTION

Cellular Fraud

Cellular fraud is a tremendous problem for cellular providers and customers. The Cellular Telecommunications Industry Association (CTIA) cites that losses in the United States as a result of cellular fraud aggregated to nearly $548 million, or $1.5 million per day, in 1994; the 1995 loss is estimated at over $650 million (Jepson 1996). Cellular fraud can be divided into several categories; the focus of this paper is on combating cellular terminal fraud. One of the most common forms of cellular terminal fraud is the duplication of a valid mobile subscriber's Mobile Identification Number (MIN) and Electronic Serial Number (ESN). Subsequently, this allows cloned mobiles to make calls that are charged to the valid mobile subscriber. Mobile hijacking is another common form of cellular terminal fraud. By monitoring a weak on-air signal of a valid mobile, the call can be "hijacked" by overpowering the legitimate mobile's signal and use three-way calling to place a fraudulent call. Authentication is an effective mechanism to combat cellular terminal fraud.

Authentication

Authentication is the process by which information is exchanged between a mobile station and the entity performing the authentication for the explicit purpose of confirming the identity of the mobile. Its objective is to protect a cellular telecommunications network from unauthorized users, thereby ensuring only valid mobile subscribers are granted access to network services.

CELLULAR TELECOMMUNICATIONS

Network Nodes

North American Cellular Interim Standard 41 Revision C (IS-41C) defines the network nodes in a cellular telecommunications network. The nodes are shown in Figure 1.

Mobile Switching Center (MSC) The MSC is a node in the network that is responsible for activities such as call processing, cellular switching, and mobility man-

agement. MSC is the standard term for a cellular switch.

Home Location Register (HLR) The HLR is a node in the network in which a mobile subscriber's main database entry resides. Information in the HLR includes the mobile subscriber's profile and the mobile's current location. The HLR is essentially a database; it can serve multiple MSC/VLRs.

Visiting Location Register (VLR) The VLR is a node in the network used by MSCs to hold profile and location information for mobile subscribers currently being serviced by those MSCs. This information is required for the purpose of call origination and delivery. The VLR is essentially a local cache of HLR database entries.

Authentication Center (AC) North American Cellular Interim Standard 41 Revision C (IS-41C) defines the inter-system protocol for authentication and introduces a new network node called an Authentication Center (AC). The AC maintains per-mobile and system-wide authentication-related information, authenticates requests sent from MSCs, and initiates authentication-related operations for mobiles. The HLR is the only entity in the network that is connected to the AC. The AC can choose to share certain pieces of information with each VLR in its system, thereby allowing basic authentication services to be performed locally in VLRs.

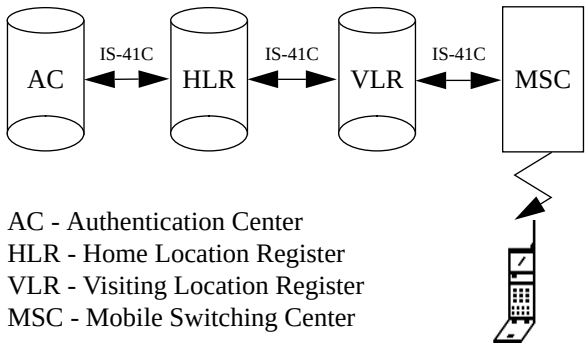

Figure 1 - Nodes in a Cellular Telecommunications Network

The nodes are depicted in Figure 1 as separate entities, and the industry views them as such. However, Nortel's DMS-MTX (Digital Multiplex System - Mobile Telephone eXchange) integrates the VLR with the MSC; optionally, the HLR and the AC can be integrated, as well.

Authentication Network Messaging

Authentication uses secret keys, encryption algorithms, and the concept of "challenges" to authenticate mobile accesses (Crowe 1996). The secret key should only be known by the mobile and the AC; it is used with other data including the Mobile Identification Number (MIN), Electronic Serial Number (ESN), and a random number to initiate the Cellular Authentication and Voice Encryption (CAVE) algorithm. The concept of challenges refers to the selection of a random number and the execution of the CAVE algorithm by the mobile and the AC or VLR. The results must match in order for service to be provided.

The CAVE algorithm is made secure because it is based on two secret keys. Each mobile has an A-Key which is known only by the AC and itself. The second key is known as Shared Secret Data (SSD). The SSD is generated by both the AC and the mobile; it can be transmitted around IS-41C networks and can be changed at any time. A cloned mobile with the correct A-Key, but not the SSD, can not respond correctly to challenges and is denied service. A cloned mobile with the correct SSD, but not the A-Key, can make calls until the SSD is updated. A cloned mobile with the correct A-Key and SSD can be eliminated by an automatic SSD update or having a new A-Key programmed into the valid mobile (Crowe 1996).

Authentication On Origination Authentication on origination is important to prevent fraudulent calls. When a particular cell's control channel information denotes that authentication is required, the mobile generates AUTHR by running the CAVE algorithm using the MIN, ESN, SSD, dialed digits, and a random number (RAND). This result is sent in an origination request message to the base station. The AC or VLR performs the same computation, generates AUTHR, and compares the two results. Call setup proceeds in parallel with authentication and is not delayed by the authentication process; the call is taken down if the AUTHR values do not match. For a pictorial representation of the network message flow for authentication on origination, please refer to Figure 3 at the end of this paper. This example illustrates an AUTHR mismatch.

Authentication On Registration Authentication on initial registration in a serving MSC is important

because it prevents location updates in the HLR due to fraudulent mobiles' registration attempts. This ensures that the HLR always contains the correct location of valid authentication-capable mobiles, thus improving the probability of reaching these mobiles when a call termination is attempted. Authentication on registration is very similar to that of origination. If the AUTHR values generated by the mobile and the AC match, then the mobile is registered in the HLR.

Authentication On Flash Authentication on flash is used to combat mobile hijacking. Even though the basic concept is the same, the process of authentication on flash is slightly different because the mobile is already on a voice channel. The mobile is challenged with a random number (RANDU) and computes AUTHU using the CAVE algorithm. This result is sent back to the serving MSC and the same computation is performed in the AC or VLR. Calls are taken down if the AUTHU values do not match. For a pictorial representation of the network message flow for authentication on flash, please refer to Figure 4 at the end of this paper.

Authentication On Termination Authentication on termination ensures that calls are only terminated to valid mobiles. The process is very similar to authentication on origination.

SSD Update Process The SSD update process updates the SSD that is associated with each mobile. It is generated and updated at periodic intervals. The SSD update operation is always initiated by the AC. If the SSD is shared with the VLR, the SSD is relatively less secure compared to A-key. Therefore, periodic SSD updates are necessary to limit the worth of SSD cloning. The SSD update process is a lengthy and computation-intensive process; it is designed to ensure that the SSD in the mobile and the AC are in synchronization with each other. The network message flow for an SSD update process on origination is shown in Figure 5 at the end of this paper.

AUTHENTICATION CENTER SIMULATOR (ACSim)

Description

The Authentication Center Simulator (ACSim) was developed to test the authentication functionality of Nortel's DMS-MTX switch. The operations of ACSim are fully controllable and provide a flexible environment to test a wide variety of scenarios, many of which are extremely difficult to test with an actual AC.

Users of ACSim develop test case processes that state the sequence of authentication messages sent between the DMS-MTX switch and the virtual AC. This gives the user complete control over the virtual AC in testing authentication scenarios.

Components

The ACSim architecture consists of both hardware and software components; see Figure 2. The T1 Link Manager and IS-41C Message Server components of ACSim were developed on the DCT-S platform designed by Catapult Corporation; it runs on a SUN Sparc workstation. The Catapult Corporation software provides the CCS7 MTP, SCCP, TCAP and IS-41C protocol stack. ACSim is built around DCT-S software which allows applications to be built by linking in C code. The user interface to ACSim consists of several components; all components were developed in the HP-UX environment. A description of each component is discussed in the following sections.

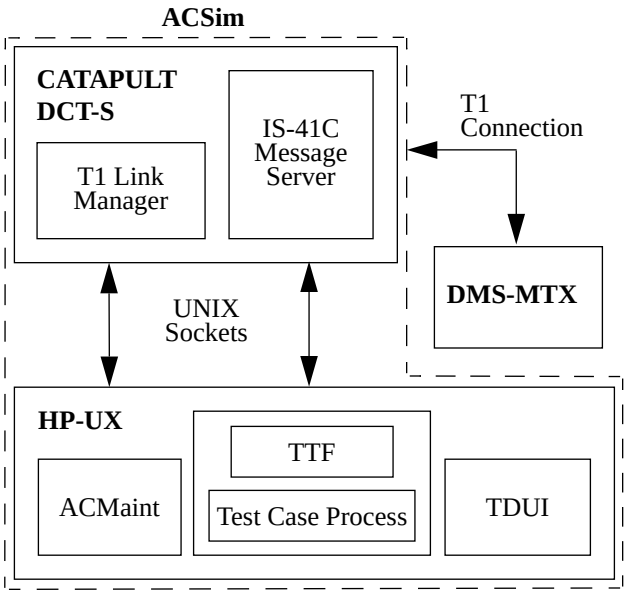

Figure 2 - Components of the Authentication Center Simulator (ACSim)

ACMaint and T1 Link Manager Processes The T1 Link Manager process starts and stops IS-41C Mes-

sage Servers for DMS-MTX switches upon request by a user running the ACMaint tool. Only one Message Server can be running per DMS-MTX switch under test. The ACMaint tool is a simple UNIX command-line tool with start, stop, reset, test and kill as its sole commands. A messaging interface specification that utilizes UNIX sockets was built for communication between ACMaint and the T1 Link Manager**.**

Test Tool Framework (TTF) The Test Tool Framework is a proprietary object-oriented test platform that allows C++ test case processes to utilize different hardware as test devices through instantiation of C++ objects. For the Authentication Center Simulator, the ACSim class was developed for creation of authentication message objects; the test device is the DCT-S which facilitates IS-41C messaging over a T1 interface between the IS-41C Message Server and the DMS-MTX switch. Communication is accomplished through UNIX sockets.

Test Driver User Interface (TDUI) The Test Driver User Interface is a UNIX utility used to run test case processes in the TTF environment. It allows execution of packages of test case processes, monitoring of test case processes at run-time, and recording of test case process run-time information for analysis by the user.

Test Case Process A test case process is an executing C++ program that is built using the ACSim and TTF class definitions. The ACSim class has methods that allow for the creation of IS-41C authentication messages, setting and retrieval of individual message parameters, and sending and receiving of messages between the DMS-MTX switch and the virtual AC. By using the ACSim class and its methods, the user controls the virtual AC at run time. Messages are sent between the DMS-MTX switch and the test case process using the IS-41C Message Server. The facility to actually send and receive messages is transparent to the developer of the test case process.

IS-41C Message Server The IS-41C Message Server handles run-time requests from the test case process running on the virtual AC to send and receive authentication messages to/from the DMS-MTX switch. A messaging interface specification that utilizes UNIX sockets was built for communication between the test case process and the IS-41C Message Server. The socket connection to the IS-41C Message Server is reserved during the entire execution of the test case process. The IS-41C Message Server records all of the messaging over the T1 link and sends it back to the test case process when the connection to the Message Server is released at the end of execution.

When the Message Server receives a request from the test case process to send a message to the DMS-MTX switch, it decodes the type of message and all of the parameters. It then constructs an IS-41C message via DCT-S facilities which sends the message down the protocol stack and out over the T1 connection to the DMS-MTX switch. The message begins at the DCT-S TCAP level, then to the SCCP level, and so forth, until the message is physically packaged by MTP and shipped over the T1 link to the DMS-MTX switch.

Messages are also received through the IS-41C Message Server. The message server, however, only waits a specified amount of time before terminating the test case process. When a message is received, the IS-41C Message Server has the capability to check the parameters in the message against the expected set of parameters indicated by the test case process. An indication is made as to which parameters, if any, did not match. In addition, the developer of the test case process may specify that any value is acceptable for a parameter in an incoming message or that certain parameter values must be empty.

GENERIC ACSim TEST CASE PROCESS (AuthGen)

Description

ACSim is a configurable environment where pre-written test case processes are executed which control the functionality of the virtual AC. AuthGen is a “generic” ACSim test case process that was developed for use with ACSim to eliminate the need for several specific test case processes.

Usage

The user defines a scenario and processing to be performed by the virtual AC using a sequence of keywords. These keywords allow the user to specify the sequence of incoming and outgoing network messages and associated parameters to be included in each message. Table 1 details the acceptable parameters for each authentication message; Table 2 provides an explanation of each parameter.

Table 1: AuthGen Parameters

Message	Valid Parameters
authreq	<sysacc> <ignore, auto, deny, nossd, uc, ssd, ssdus, ssduns, delay, reterr>
afreport	<ignore, auto, deny, nossd, uc, ssd, ssdus, ssduns, delay, reterr>
asreport	<ssduop | ucop> <ignore, auto, deny, nossd, uc, ssd, ssdus, ssduns, delay, reterr>
bschall	<ignore, delay, reterr>
authdir	<min> <deny, uc, nossd, ssd, ssdus, ssduns>

Table 2: AuthGen Parameter Explanations

Parameter	Explanation
sysacc	System access (orig, reg, flash, or unspecified)
ignore	Ignore the incoming message; do not send a response message
auto	Deny access if an authentication failure is detected. Otherwise, allow access.
deny	Force deny access in the response
uc	Initiate a unique challenge by including unique challenge parameters
nossd	Include the NOSSD parameter to revoke the SSD from the VLR
ssd	Share the SSD with the VLR
ssdus	Initiate a SSD update by including the parameters RANDSSD and SSD
ssduns	Initiate a SSD update by including the parameters RANDSSD, RANDU, and AUTHU
ucop	Expect the result for a unique challenge operation

Table 2: AuthGen Parameter Explanations

Parameter	Explanation
ssduop	Expect the result for a SSD update operation
delay	Delay the response message by 8 seconds
reterr	Send a return error response message with ‘System Failure’ indication
min	Mobile Identification Number

Examples

Table 3 lists some example AuthGen sequences used to test various authentication scenarios. The list is by no means complete, but it does show the flexibility of the AuthGen test case process.

Table 3: AuthGen Sequence Examples

Authentication Scenario	Sequence
Authenticate a registration access	authreq-reg-auto
Authenticate an origination access and share the SSD in the response	authreq-orig-auto-ssd
Force a call take-down for a flash access	authreq-flash-uc-asreport-ucop-deny
Perform a SSD update upon origination access (with the AC not sharing the SSD with the VLR)	authreq-orig-ssduns-bschall-asreport-ssduop-auto
Force sending a return error message to the VLR	authreq-reg-reterr
Verify call take-down after inter-system handoff	authreq-orig-delay-delay-deny
Verify message time-out handler in the MSC/VLR	authreq-orig-ignore
Revoke the SSD in the VLR for a mobile	authdir-5551231234-nossd

FUTURE ENHANCEMENTS

Authentication Center Simulator (ACSim)

ACSim provides the ability to send and receive IS-41C authentication messages. It includes basic reporting and debugging functionality, implementation of the CAVE algorithm, and the ability to have multiple users running test case processes. Future enhancements to ACSim will include the use of another test device to simulate mobiles, thereby allowing complex test cases to be executed quickly and automatically. In addition, ACSim can be enhanced to function as a full state machine AC simulator, suitable for running traffic.

Generic Test Case Process (AuthGen)

AuthGen can only support the existence of one message of each type at any given time. For example, it can not handle two AUTHREQ messages simultaneously; custom test case processes must be created for such scenarios. A future release of AuthGen will be able to dynamically create objects of the same message type in order to allow for such scenarios. Furthermore, AuthGen can readily be enhanced to cover end-to-end scenarios in the DMS-MTX switch, rather than just authentication transactions on the AC.

CONCLUSIONS

The development of ACSim and AuthGen proved to be an invaluable resource for testing the authentication-related software on the DMS-MTX switch. Their development provided a means to test a wide-variety of scenarios quickly and efficiently, many of which are very difficult to test with an actual AC. In addition, these tools allowed Nortel and Tandem to perform their respective development concurrently. Nortel was able to design, implement, and test authentication-related enhancements on their DMS-MTX switch in parallel with Tandem Corporation's development of the actual AC, thereby allowing a faster time to market for authentication services.

REFERENCES

Crowe, David. 1996. "The Secrets of Authentication." *Cellular Business, The Journal of Cellular Telecommunications*, vol. 31, no.12 (Nov.): page 68.

Doss, Jeffrey and Brett Stewart. 1996. "ACSim User's Guide," Release 1.4, Nortel Proprietary Document, (Oct.).

EIA/TIA IS-41C. 1995. "Cellular RadioTelecommunications Intersystem Operations." (Nov.).

Jepson, Robin. 1996. "Nortel Cellular Fraud Management." Nortel Proprietary Document, (Apr.).

Nortel, Inc. 1996. "Authentication and Voice Privacy High Level Design." Nortel Proprietary Document, (Mar.).

Veerasamy, Jey and Ross Creech. 1996. "AuthGen User's Guide." Nortel Proprietary Document, (Nov.).

BIOGRAPHIES

Jey Veerasamy is a Senior Member of Scientific Staff at Nortel. He has worked on advanced cellular services including flexible alerting and authentication. Recently, Mr. Veerasamy worked on several standards contributions related to authentication. He received a M.S. in Computer Science from the University of Texas at Dallas. He is currently a Ph.D. student in Computer Science at UTD.

Ross C. Creech is a Member of Scientific Staff at Nortel. He recently completed software enhancements to Nortel's DMS-MTX switch to support authentication. Prior to joining Nortel, he participated in programs involving emergency management simulation (Plowshares) and multi-chip microelectronics design and manufacturing. Mr. Creech received a B.S. in Industrial and Systems Engineering from the University of Florida and a M.S. in Computer Engineering, specializing in Software Engineering, from the University of Central Florida.

Jeffrey M. Doss is a Member of Scientific Staff at Nortel. He has developed the cellular automation and testing platforms used in the verification of the DMS-MTX switch. Much of his work has centered around the development of network protocol test tools. Mr. Doss holds a B.S. in Computer Science from Northeast Louisiana University.

Brett B. Stewart is a Senior Member of Scientific Staff at Nortel. He has developed the cellular automation and testing platforms used in the verification of the DMS-MTX switch. Mr. Stewart received his B.S. in Computer Science from Northwestern University. He is currently a M.B.A. student at the University of Texas at Dallas.

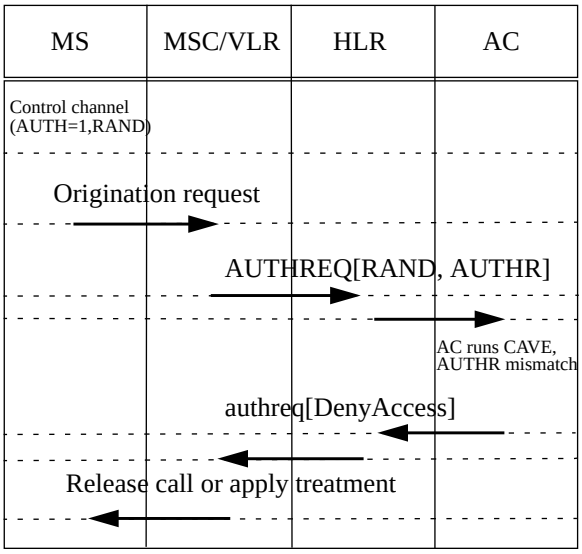

Figure 3 - Message Flow for Authentication on Origination

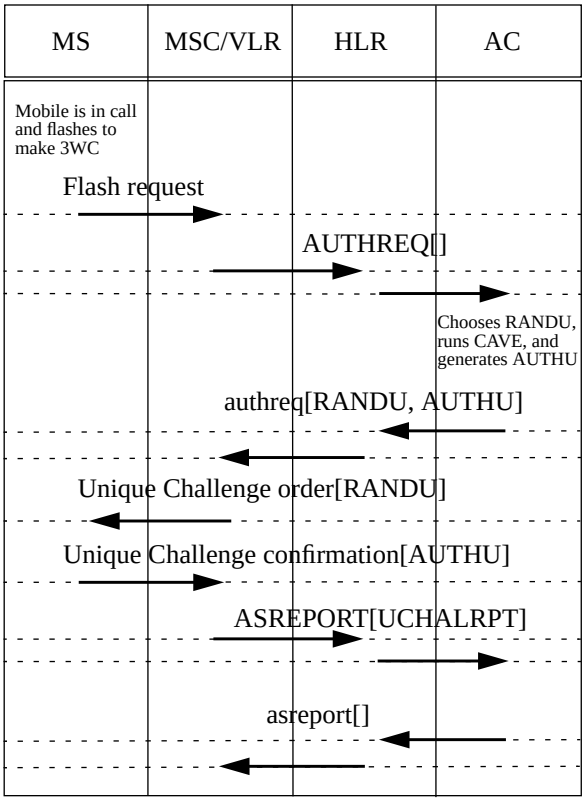

Figure 4 - Message Flow for Authentication on Flash

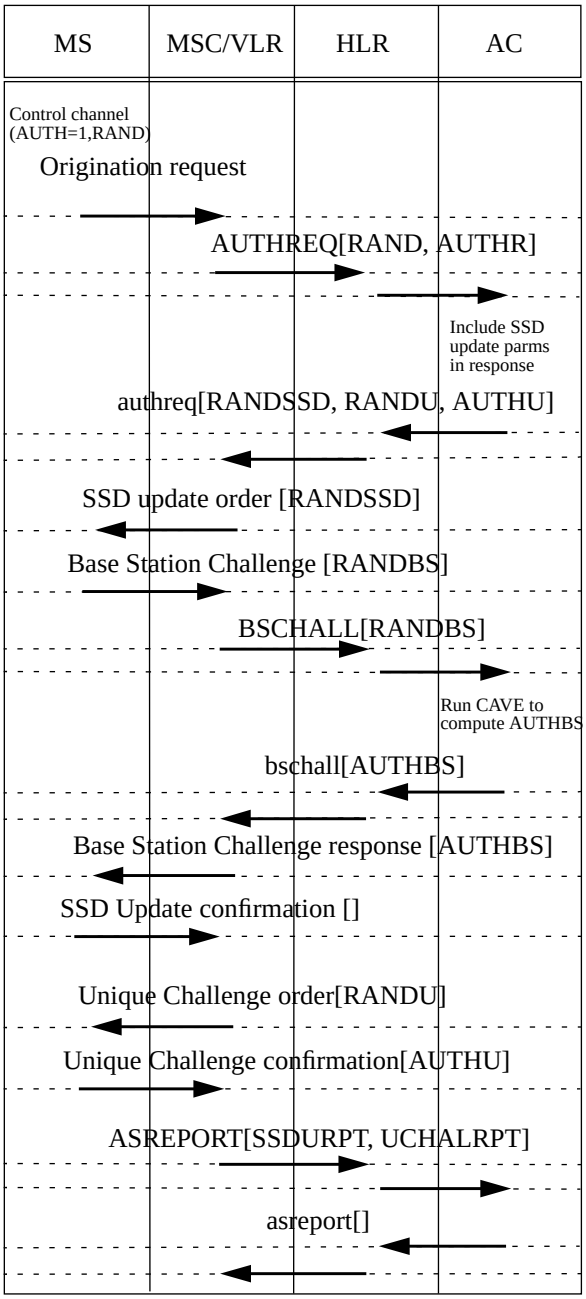

Figure 5 - Message Flow for A SSD Update on Origination