ACN | Alerting and Coordination Network

ACN*Report*

Spring 2004 Vol. III, No. 1

Published Exclusively for Members of the Alerting and Coordination Network

In this issue...

View from the Inside: A Stakeholder's Look at ACN

Rosemary Leffler, Director of National Security and Emergency Preparedness with SBC, has been active with the Alerting and Coordination Network (ACN) since its inception in 1983. When the National Telecommunications Alliance (NTA), which had been operating ACN, dissolved in December 2000, the NCS assumed operational control of the ACN and SBC continued its participation in ACN. Ms. Leffler met recently with the *ACN Report* editor to discuss ACN.

In 2001, Ms. Leffler became the SBC representative to the National Coordinating Center (NCC) for Telecommunications under the National Communications System (NCS) and helped facilitate the transition from the NTA to the NCC-Telecom ISAC. She remembers discussions during policy meetings and working groups with other NCC industry representatives on the importance of enhancing

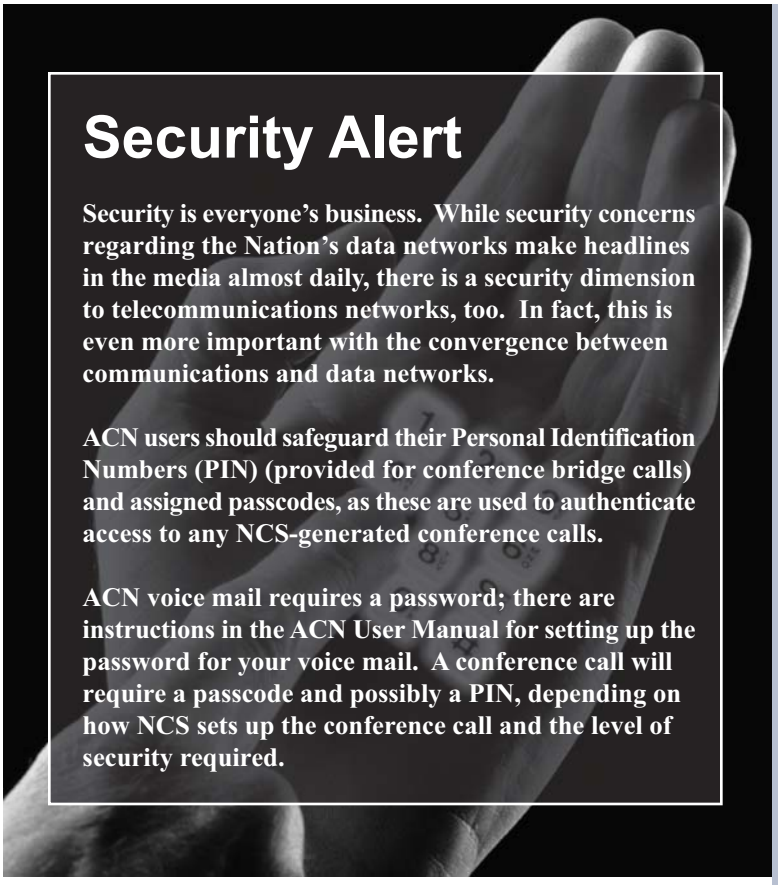
continued on page 2

Keeping ACN Traffic Safe: VoIP Encryption

Encryption is the scrambling of data so only the intended recipient can read or use it. Data encryption is used to protect information that streams through Voice over Internet Protocol (VoIP) technology that would otherwise be vulnerable to malicious activity. Depending on the particular network or system structure, a series of protective measures may be included. Virtual Private Network (VPN), Internet Protocol security (IPSec), and Data Encryption Standard (DES) are some of the protocols that encrypt data across private networks.

VoIP technology provides the ability to speak over either a traditional phone or a VoIP phone; however, the VoIP protocol processes the signals in a manner dramatically different from the way an analog phone processes signals. When a user speaks into a VoIP phone receiver, the internal electronics convert the analog voice signal into a digital stream of 1's and 0's. The digital bit stream is packaged according to the protocol in use, and sent through the routers and servers to the backbone network. The voice packets are treated exactly like data packets because that's exactly what they have become! At the other end, the router and servers will pass through the packets to the IP phone, where they are converted back to the analog signal. Now the signal can be heard by the person holding the receiver.

continued on page 3



Security Alert

Security is everyone's business. While security concerns regarding the Nation's data networks make headlines in the media almost daily, there is a security dimension to telecommunications networks, too. In fact, this is even more important with the convergence between communications and data networks.

ACN users should safeguard their Personal Identification Numbers (PIN) (provided for conference bridge calls) and assigned passcodes, as these are used to authenticate access to any NCS-generated conference calls.

ACN voice mail requires a password; there are instructions in the ACN User Manual for setting up the password for your voice mail. A conference call will require a passcode and possibly a PIN, depending on how NCS sets up the conference call and the level of security required.

View *continued from page 1*

ACN's capability under NCS leadership. She commented that the transition was necessary and valuable for both Government and industry, since "ACN is an excellent addition to the toolkit of NS/EP resources."

Noting the value ACN has provided as a back-up communication resource, she recalled an event in 2003 when the public network was disrupted and ACN was used by industry and Government to coordinate mitigation activities. She recalled, "Even with other options of communications such as SHARES, cell phones, and satellites, ACN has proven to be dependable and has worked when needed."

"There is always room for improvement," she added, suggesting that the monthly tests should be supplemented. "It would be really useful to see more interaction with ACN within the telecommunications sector, involving both Government and industry, through the introduction of operational drills and exercises," she commented. Concluding, she noted, "It's a good tool and we all should be more familiar with its capabilities."

Welcome Kevin C. Piekarski, ACN Program Manager

Kevin C. Piekarski is the new ACN Program Manager, replacing Ron Thomas who retired from Government service in February 2004. Mr. Piekarski adds great depth to the ACN program with experience that spans both the private sector and Federal service. Mr. Piekarski joined the National Communications System (NCS) in December 2002 as an Information Technology (IT) Specialist in Information Security. His background includes ten years in the Navy and positions in IT and telecom with Verizon and iDirect. Mr. Piekarski understands the importance of converging IT and telecommunications capabilities and he brings that appreciation to the ACN program.

Noting that the ACN program is a key component within NCS, he commented, "My job now is to make sure that it continues to thrive by guiding its technological evolution and expanding its membership to ensure that all critical players within the telecom community participate."

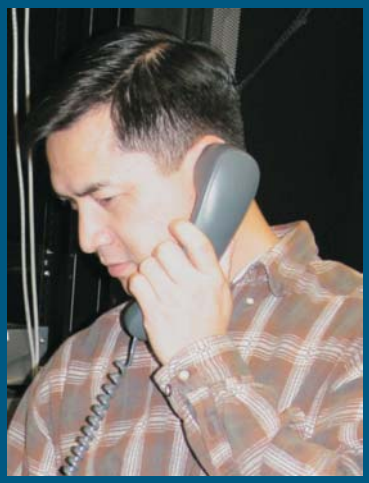
Mr. Piekarski began his IT career in 1989 as a Navy Data Systems Technician. Among other career highlights, he spearheaded a mission in Bahrain to provide 100 commands access to the Department of Defense global Non-classified Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET) based on dial-in WAN technology. Mr. Piekarski's role in developing, configuring, and installing these two networks provided direct support to the Navy during the attack on the USS Cole in October 2000.

Mr. Piekarski sees ACN's value to the NCS and its customers. "The ACN is a vehicle for both Government and telecom industry decision-makers to restore as well as mitigate the effects of national emergencies to the telecom infrastructure. It's important to make sure that the best IT and telecom technologies are being used." Mr. Piekarski is committed to ACN's continued contribution as a dependable vehicle for telecom restoration.

Engineer's Corner: *Conference Calling on the Conference Bridge*

As we announced in the last ACN Report, ACN now has new Compunetix Mini-Contex conference bridges. A conference bridge allows multiple users to dial into a central location using either the VoIP phone or an analog ph one from the public network. The Mini-Contex provides a secure conference calling capability.

If you receive a notification that a conference call will be held, do you know what to do? Here are procedures to get started.



1. The NCS will initiate the conference call.
2. Contact will be made to the necessary participants via e-mail or phone. Time and date will be provided.
3. A PASSCODE number will be provided when the conference call is announced. A PASSCODE defines the specific conference to which the ACN user belongs.
4. You may be required to enter a Personal Identification Number (PIN), which will come from the NCS administrator, to identify yourself to the conference bridge. This allows access into the system.
5. If you lose your PASSCODE or PIN (or you believe either has been compromised), you will not be allowed to use the conference bridge. (Contact the ACN Program Manager immediately to generate a new PASSCODE or PIN.)
6. At the predetermined time of conference, pickup your ACN phone and dial the appropriate access numbers. Enter the conference PASSCODE and PIN if applicable.
7. You have now entered a conference.

Typically, it will take an authorized ACN user less than 30 seconds to connect to a conference. If you have any questions or concerns, contact Kevin Piekarski, the ACN Program Manager.

VoIP *continued from page 1*

Analog signals can be intercepted by wiretaps, which must be placed physically on the line. Digital information can be manipulated by tampering with the 1's and 0's or the packets of information. However, physical access to the line is not necessary for a phone hacker, or phreaker. All he or she needs is (logical) access to a layer 2 switch port, or a router. That is why any data that can be potentially intercepted by malicious users must be encrypted for security purposes. As explained in the Fall *ACN Report*, 128-bit point-to-point encryption is used for all ACN VoIP phones. Digitally encrypting the voice portion of the VoIP call reduces the risk of electronic eavesdropping.

Media encryption utilizes symmetric cryptographic algorithms in VoIP endpoints. This form of encryption uses a 'shared' secret or 'private key' to ensure that both endpoints will understand how to decrypt the voice packets sent from phone to phone. Since the very privacy of the key is required to be protected as well, the key is also encrypted before it is distributed to either endpoint. Also, a new key is generated each time a VoIP session is initiated.

The encryption process does not alter the voice quality in a phone call, and neither party is aware of the encryption.

ACN Newsletters Available on NCS Web Site

NCS is currently in the process of adding its collection of ACN publications to the recently redesigned NCS web site. Past and current volumes of the ACN newsletter "ACN Report," published in hardcopy each quarter, are now posted on the NCS site's Library page.

You will find publications relating to a variety of NCS programs and services there, including ACN. Although electronic versions of the ACN newsletter are e-mailed to its users each quarter, these publications are now available for public download. Look for interesting articles in these volumes dating back to 2002 including: network upgrades, interviews with ACN staff, engineering information, equipment support, and community issues.

To enjoy these newly available resources, please visit the NCS Library at http://www.ncs.gov/library.html.

Did You Know?
Ring that Thing!

In order to ring your analog phone, the telephone company sends out a "ringing signal" to either a warbling ringer driven by integrated circuits, or a gong ringer (older style bell) powered by the telephone line itself.

A telephone's ringing cadence - the timing of ringing vs. pause - varies from company to company. In the United States the telephone cadence is normally two seconds of ringing to four seconds of pause. An unanswered telephone in the United States will keep ringing until the caller hangs up. But in some countries, the ringing will "time out" if the telephone call is not answered.

While an ACN phone's ring is activated by digital bits, and not a ringing signal, it is designed to simulate the familiar ring tone of a traditional phone.

2004 Test Schedule

The monthly ACN test occurs on the third Monday of each month between 10am and 2pm EST.

24/7 Help Desk
877- 441- 9330

ACN ON NET
Ext. 4357 (HELP)

Contact Us

National Communications System
ACN Program Manager
Tel: 1-866-NCS-CALL (1-866-627-2255)
E-mail: acn@ncs.gov
Web: http://www.ncs.gov/acn/

Department of Homeland Security
Information Analysis and Infrastructure Protection
National Communications System
701 South Courthouse Rd., Arlington, VA, 22204-2198

Technical Support, Service Management Center (SMC)
ACN Ext: 4357 (HELP)
Tel: 1-877-441-9330
E-mail: smc@ags-inc.us