Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 7 August, 2000

EPE Network Impact

Last month's issue presented an article on EPE (Enhanced Privacy and Encryption) by Bob Rance of Lucent. This month we continue our discussion by a look at the network impact with an article written jointly by Sharon Lim of Compaq and David Crowe.

EPE: A Network View

by Sharon Lim,
Compaq
and David Crowe
Cellular Networking Perspectives

TDMA Enhanced Privacy and Encryption (EPE) was designed to enhance a subscriber's privacy in two ways: Signaling Message Encryption (SME) and voice/user data privacy. Signaling message encryption prevents subscriber sensitive information, (e.g., calling party number), from being transmitted in the clear over the air. Voice and user data privacy prevents an intruder from eavesdropping on a subscriber's conversation on the air interface between the mobile station and base station. Currently, the wireless industry is using the Cellular Message Encryption Algorithm (CMEA) and Voice Privacy Mask (VPM) key generation procedure to protect a subscriber's privacy. Since these keys are static, TR-45 AHAG has proposed using the new EPE to provide dynamic session keys, Digital Control Channel (DCCH) and Digital Traffic Channel (DTC) keys, for every TDMA burst. EPE is targeted for mobile stations and wireless networks that support at least TIA/EIA-136B.

Figure 1 describes how DCCH and DTC keys are generated. The new DCCH and DTC key generation procedure is an extension to the current VPMask key generation.

Network Standards Support

TIA subcommittee TR-45.2 has agreed on protocols to support EPE, but the specification will not be published in a standard until TIA/EIA-41 Revision E.

Glossary

For any terms you are unfamiliar with, please consult:

www.cnp-wireless.com/glossary.html

…or the glossary of terms at the end of this issue.

Compatibility Considerations

It is always more difficult to add new capabilities to an existing system rather than designing from scratch. With EPE, there will be mobiles, base stations, MSC's, VLR's, HLR's and AC's that cannot execute EPE. However, only the MS and base station have to negotiate to determine whether EPE algorithms can be used. If the MS supports EPE then, by implication, its HLR and AC must also. If the base station supports EPE then the associated MSC's and VLR's must also. If these constraints are respected, EPE

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price – only $200 for delivery within the US and Canada or $250 elsewhere.

Back issues are available individually, or in bulk at reduced prices.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due

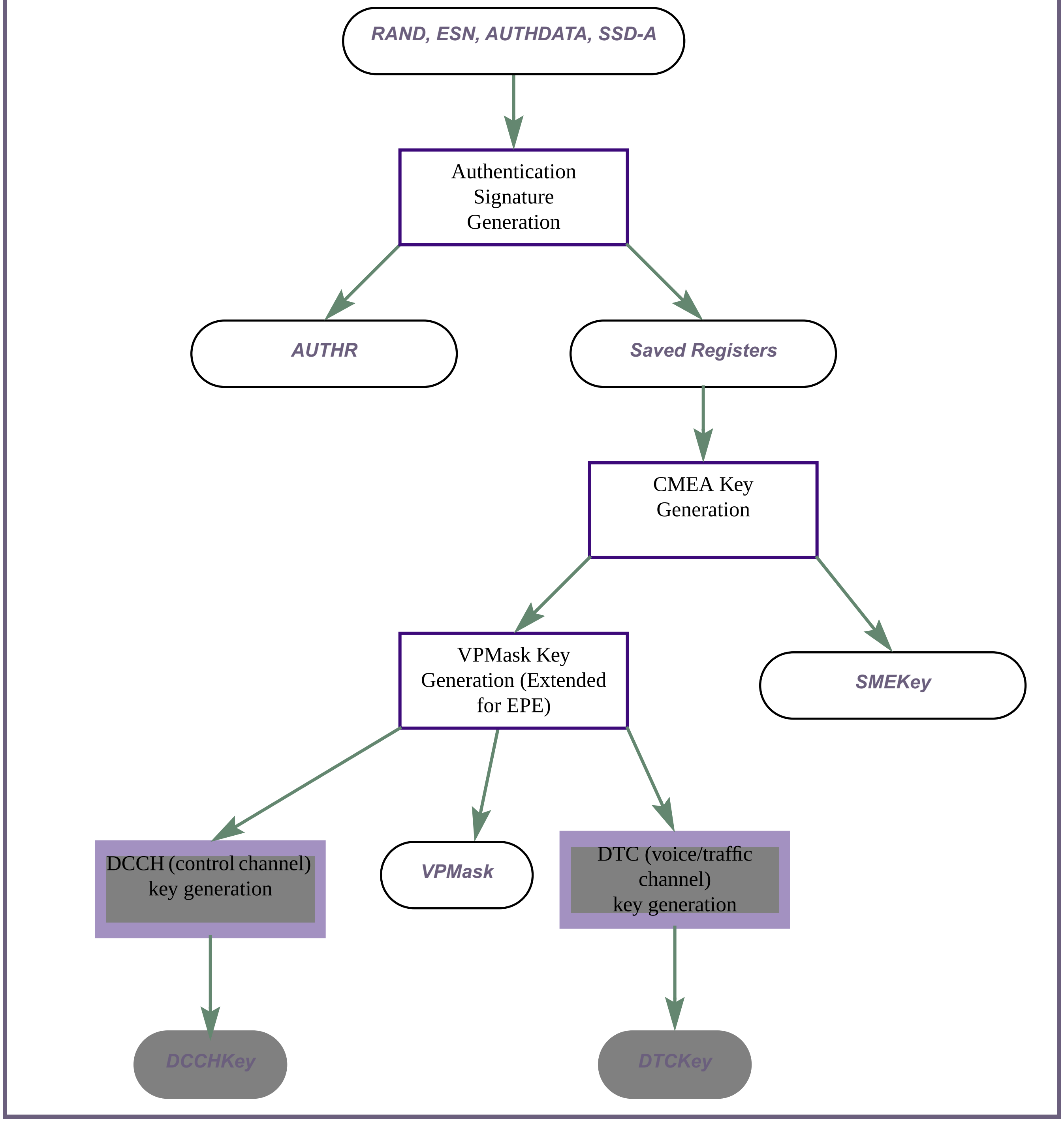
September 20th, 2000.

Future Topics

IP security • Public Keys & Wireless • Kerberos PKINIT• Public Key Infrastructure (PKI) • IKE • Wireless Data Security • Elliptic Curve Cryptography (ECC)• Abelian Varieties • IETF Security Standards

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/wsp.html. **Subscriptions:** $200 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Figure 1: EPE Key Generation (DCCHKey and DTCKey)

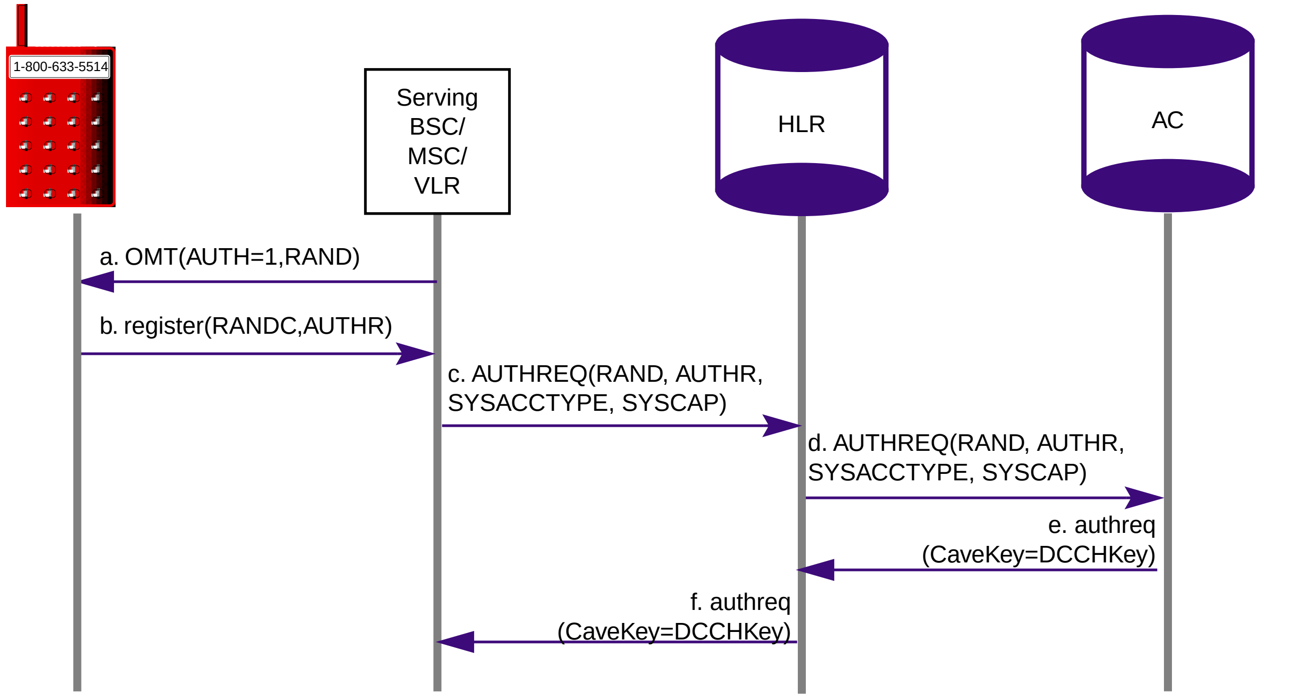

RAND, ESN, AUTHDATA, SSD-A
Authentication Signature Generation
AUTHR
Saved Registers
CMEA Key Generation
VPMask Key Generation (Extended for EPE)
SMEKey
DCCH (control channel) key generation
VPMask
DTC (voice/traffic channel) key generation
DCCHKey
DTCKey

can be introduced into a network without disruption.

DCCH Key Generation

A DCCH key is generated when a mobile station successfully registers, for example during a power up, upon an analog (FSK) control channel to DCCH transition, and whenever there is a forced or new system registration. The key remains valid until the mobile station performs a new registration, switches to a new SID, country code or network type, or is turned off. It is recommended that a new DCCH key be refreshed at least once a day. During registration, an MSC initiates a TIA/EIA-41 AuthenticationRequest INVOKE message (AUTHREQ) with system access type set to registration and forwards it to the VLR (if the SSD is shared) or via the VLR and HLR to the AC (if the SSD is not shared or upon initial registration). The VLR or AC will generate the DCCH key and return it to the MSC. Upon receipt of the DCCH key, the contents of all DCCH messages except for the proto-

Figure 2: DCCH Key Generation


1-800-633-5514
Serving BSC/ MSC/ VLR
HLR
AC
a. OMT(AUTH=1,RAND)
b. register(RANDC,AUTHR)
c. AUTHREQ(RAND, AUTHR, SYSACCTYPE, SYSCAP)
d. AUTHREQ(RAND, AUTHR, SYSACCTYPE, SYSCAP)
e. authreq (CaveKey=DCCHKey)
f. authreq (CaveKey=DCCHKey)

col discriminator and message type information will be encrypted if EPE encryption is enabled. Figure 2 shows how the DCCH Key is generated by the AC and then returned to the MSC during registration.

a. The MS determines from the Overhead Message Train (OMT) that authentication is required on all system accesses (AUTH=1). The Random Number to be used for authentication (RAND) may also be obtained by the MS at this time.

b. The MS executes CAVE using the currently stored SSD-A, ESN, MIN1 and the RAND value to produce a registration Authentication Result (AUTHR) which it sends to the serving system along with MSID, ESN and RANDC (a portion of RAND used for verification). The MS also generates the DCCH Key.

c. The serving system (MSC/VLR) sends the RAND, AUTHR, SystemAccessType (SYSACCTYPE), and SystemCapabilities (SYSCAP) in an AUTHREQ to the HLR. The SYSCAP parameter AUTH and EPE bits are both set to 1.

d. The HLR performs minimal validation (e.g. ensuring that the MSID and ESN are valid) and then forwards the AUTHREQ to its associated AC.

e. The AC verifies the MSID and ESN reported by the MS and then executes CAVE using the current values of SSD-A, ESN, MIN1 and RAND to produce a registration Authentication Result (AUTHR). The AC compares the generated AUTHR value with the AUTHR value received in the AUTHREQ and, if they match, generates the DCCH Key. It then includes the DCCH Key in the new CaveKey parameter before sending an authreq (AuthenticationRequest RETURN RESULT) to the HLR.

f. The HLR forwards the authreq to the serving system, which can now use the DCCH Key to protect further transmissions on the control channel.

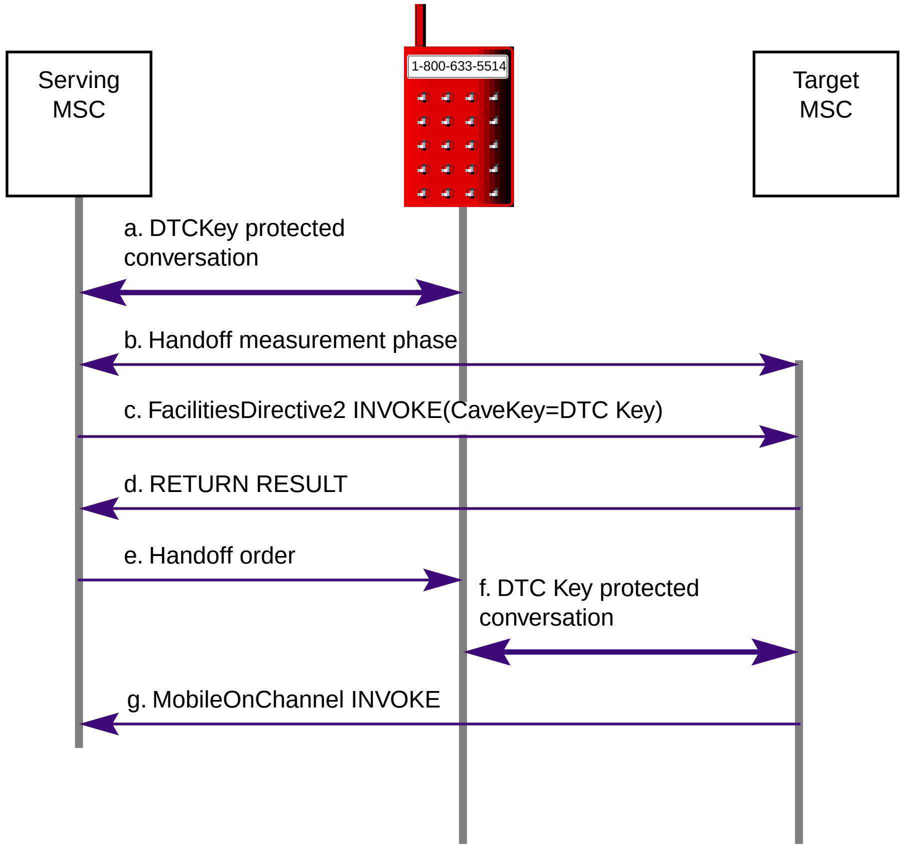
DTC Key Generation

A DTC (Digital Traffic (e.g. voice) Channel) key is generated when an EPE-capable MS makes or receives a call in an EPE-capable system. After an initial traffic channel assignment, an MS will start encrypting speech using the Enhanced Voice Privacy algorithm. The key is obtained in exactly the same way as the DCCHKey, the only difference is that the TIA/EIA-41 authreq CaveKey parameter contains the DTCKey instead of the DCCHKey shown in Figure 2.

SSD Sharing

Once initial authentication has been performed (e.g. at the first registration of an MS in a system) there is no need to continue to involve the AC in generation of new DCCH and DTC keys, although the home system can refuse to share the SSD (Shared Secret Data) to force this to occur.

Figure 3: Inter-MSC Handoff with EPE Encryption


Serving MSC
1-800-633-5514
Target MSC
a. DTCKey protected conversation
b. Handoff measurement phase
c. FacilitiesDirective2 INVOKE(CaveKey=DTC Key)
d. RETURN RESULT
e. Handoff order
f. DTC Key protected conversation
g. MobileOnChannel INVOKE

Inter-MSC Handoff

EPE support also requires modifications to inter-MSC handoff protocols. The new CaveKey parameter (containing the DTCKey) must be included in the FacilitiesDirective2 INVOKE message from the serving MSC to the target MSC to allow EPE voice or data encryption to continue after handoff.

Figure 3 illustrates how conversation is protected by the DTC Key before, during and after inter-MSC handoff:

a. The conversation is initially protected by the DTC Key obtained or calculated by the Serving MSC.

b. Due to a drop in signal strength, the Serving MSC initiates a request for handoff measurements (either from the network, or through mobile assistance).

c. The Serving MSC determines the target MSC for the handoff and initiates a FaclitiesDirective2 INVOKE with CaveKey set to the DTC Key.

d. The Target MSC responds with a RETURN RESULT to indicate that a new traffic channel has been assigned.

e. The Serving MSC tells the MS to handoff to the new traffic channel.

f. As soon as conversation starts on the new traffic channel it is protected by the DTC Key encryption.

g. The Target MSC tells the Serving MSC that it can release the old traffic channel, and now takes over as the Serving MSC.

Inter-System Call Setup

Another situation that is very similar to inter-MSC handoff is inter-MSC call setup which occurs when a call is delivered to one system but, due to border system anomalies, must be delivered to a cellsite in a neighboring MSC. By the time paging is completed, the DTC Key is already established, and must be provided to the neighbor MSC.

Summary of TIA/EIA-41 Impacts

Table 1 summarizes the TIA/EIA-41 operations that are impacted by EPE. Table 2 summarizes the parameters that have been added to TIA/EIA-41 or modified to support EPE.

Conclusions

EPE will provide additional security to wireless systems that support it (currently only TIA/EIA-136) with relatively modest network impacts, and will act as an interim method of enhancing the security of wireless phone calls until true 3G security systems are in place.

Table 1: TIA/EIA-41 Operations Impacted by EPE.

Operation	Modifications
AuthenticationDirective INVOKE	Addition of CaveKey parameter, set to either DCCHKey or DTCKey.
AuthenticationRequest RETURN RESULT	Addition of CaveKey parameter set to either DCCHKey (for registration accesses) or DTCKey (for origination or page response accesses).
AuthenticationStatusReport INVOKE	Addition of EnhancedPrivacyEncryptionReport parameter.
FacilitiesDirective2	Addition of CaveKey parameter set to DTCKey for use when a conversation or other user traffic is protected by EPE encryption.
HandoffBack2	Addition of CaveKey parameter set to DTCKey for use when EPE encryption is initiated following an initial handoff, or when the Anchor MSC does not retain the DTCKey.
HandoffToThird2	Addition of CaveKey parameter set to DTCKey for use during a path minimization handoff when EPE encryption applies.
InterSystemSetup	Addition of CaveKey parameter set to DTCKey for use when a call terminates at one MSC, but due to border cell problems, paging is successful in a neighboring MSC.
OTASPRequest	Addition of EnhancedPrivacyEncryptionReport for reporting over-the-air activation problems related to EPE.

Table 2: TIA/EIA-41 Parameters Impacted by EPE.

Operation	Modifications
CaveKey	A new parameter that contains either the DCCHKey or DTCKey.
EnhancedPrivacyEncryptionReport	A new parameter that describes the outcome of an attempt to initiate EPE, whether successful or not.
CallingFeaturesIndicator	A portion of the subscriber profile that was enhanced to indicate whether a subscriber (i.e. their mobile and home system) is capable of EPE.
ConfidentialityModes	Enhanced to indicate whether EPE is on for a current call (e.g. for transmission to a neighboring MSC during handoff).
SystemCapabilities	Enhanced to indicate whether an MSC is EPE capable (e.g. during initial authentication to indicate that an EPE key can be generated).