



NIST - KMS Key Management Standard



User Perspectives/Requirements: Wireless Applications

Doug Rahikka
djrahik@alpha.ncsc.mil
NSA-R224
10 February 2000



Classes of Gov't Wireless Users

- **GOTS** (Government Off The Shelf)
 - High Grade crypto (end-to-end)
 - STU-III-compatible, CONDOR, FNBDT
 - Custom crypto and key management
 - Expensive \$\$\$\$
 - Just employ commercial wireless as 'transport'
 - Authentication, crypto, provided by GOTS overlay
- **COTS** (Commercial Off The Shelf)
 - Most gov't users !
 - Sensitive But Unclassified (SBU)
 - Rely on commercial wireless (cellular) infrastructure



End-To-End Security Challenge

■ Technology Enablers :

- Signaling Plan (**FNBBDT**)

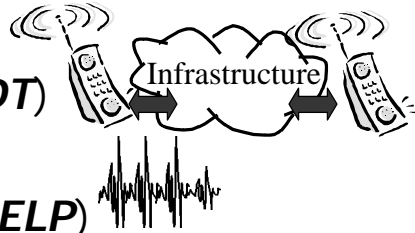
Protocol 'Lingua Franca'

- Common Vocoder (**MELP**)

Washington Post articles about Allied pilots talking in plain text during Kosovo crisis due to lack of interoperable secure voice radio equipment

2400 MELP requires less power than 16000 CVSD

(no signal fratricide as experienced by MSE in Bosnia)



STU-III Interoperability ?



- STU-III modem through 2G ACELP/VSELP/QCELP vocoders at 7-10% BER
- STU-III will not work over 2G digital cellular !!!
- Need for STU modem IWF in cell switches
- Failed business case !
- Use FNBBDT instead
- Iridium interoperability via red gateways (vocoder tandeming)

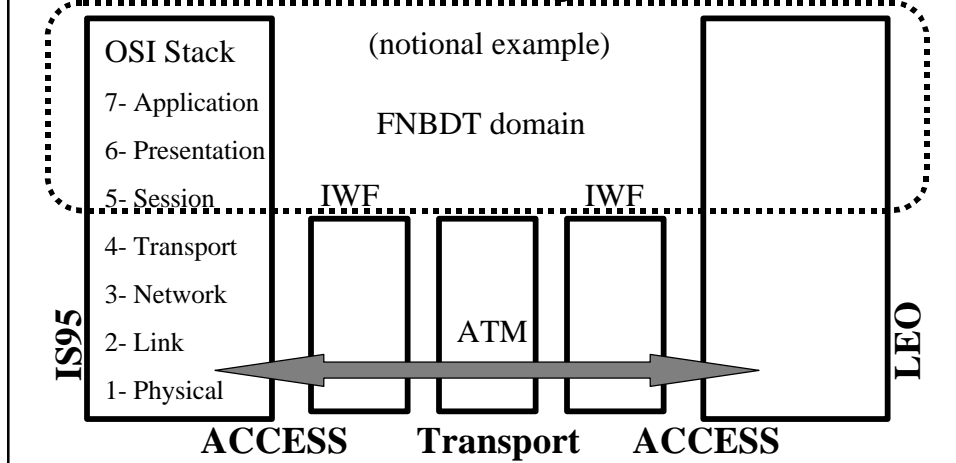
(R224's MATLAB sandbox)



STU-III QAM Modem Demod

FNBDT

■ "Future Narrow Band Digital Terminal"



What is FNBDT ?

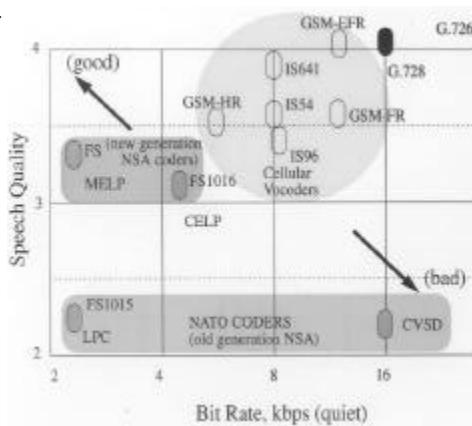


- Aging acronym - really a Digital Secure Voice Protocol
- Transport layer and above
- Operates over most data/voice network configurations
- Least Common Denominator for interoperability
- Many media (wireless, satellite, IP, ATM, ISDN, etc)
- Adapts to data rate
- Sync and Nonsync
- Negotiates security/application features
- Point to Point and Multipoint
- Realtime, Near Realtime and NonRealtime Apps

Interoperable Vocoder



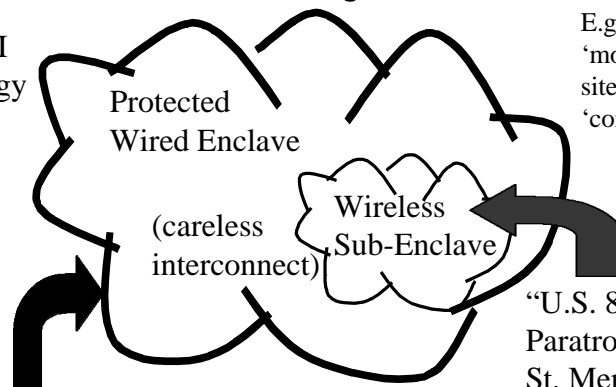
- Need common vocoder = MELP at 2400 bps
- 1200 bps MELP available also at quality ~CELP (for HF or combined data+voice over 2400 MILSTAR e.g.)



Wired to Wireless Convergence

- Take care when 'mixing' wired and wireless !

WWII analogy



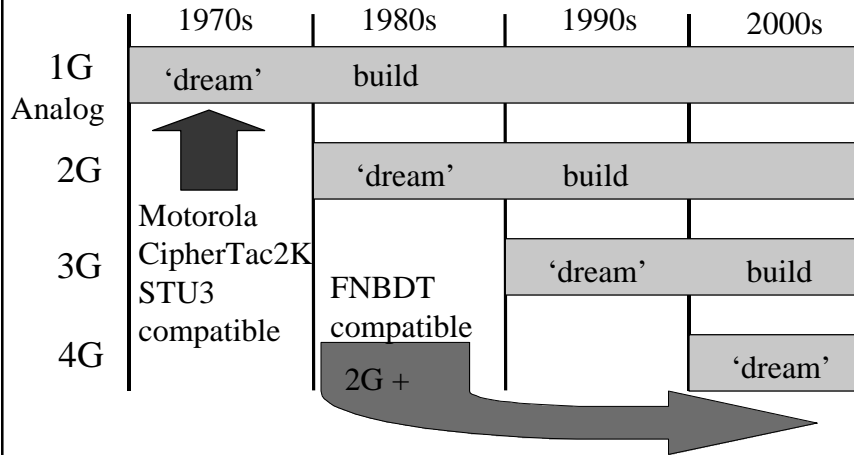
E.g. Bluetooth not for 'mobility' but for fixed site appliance 'convenience' = risky ?

"The Atlantic Wall" (firewall)

"U.S. 82nd Airborne Paratroopers at St. Mere Eglise"

Standards - 3G IMT2000

■ Evolution



3G IMT2000 Security Standards

- First Trilateral (NA+Eur+Asia) ITU mtg in Columbia MD April 1998 (organized by ITU-T SG7/11/4, NSA-CFS, and NSA-R2)
- First Bilateral European ETSI + North American TIA AHAG (Ad Hoc Authen Group) to be held in Stockholm April 2000
- TIA TR45 AHAG Projects (= Open & Public Process)
 - ESP Enhanced Subscriber Privacy (~5 candidates)
 - | (better than 2G Voice Privacy Mask algorithms)
 - ESA Enhanced Subscriber Authentication (~4 candidates)
 - | Adopting ETSI AKA algorithm (to be jointly used by 3GPP = GSM-compatible 'WCDMA' and 3GPP2 = IS95-compatible 'cdma2000')

(3G security stds continued)...

- 3G w/high data rates (no WWW 'world wide wait' mobile web access)
(~100kbps mobile, 384kbps outdoor, 2Mbps indoor)
Opportunities for multimedia, secure video conferencing
etc (FNBDT impact ?)
ETSI 3GPP slightly ahead of 3GPP2 schedule with GPRS
(General Packet Radio Service) trials underway now
- Export controls removed 15 Jan 2000 !
- 3G has satellite aspects (how relate to Bill Gates' Teledesic ?)



Cellular TIA TR45 ESA/ESP

- ESA = Enhanced Subscriber Authentication
- ESP = Enhanced Subscriber Privacy
- Develop crypto algorithms and key management/distribution schemes for 3G wireless
- Ensure security evolvability
- Investigate new services - public key certificates, ECC, key escrow, smart cards ...
- Work with ETSI and ITU !
Worldwide convergence
- Backdrop of U.S. export rules change

ESA Requirements

- Publicly scrutinized Protocols & Algorithms
- 128-bit authentication key (vs current CAVE 56 bit security)
- 128-bit privacy key (entropy reducible per gov't reqs)
- Privacy mandatory (a la GSM, unlike current North American IS136 and IS95 systems)
- Mutual/bilateral authentication (mobiles \leftrightarrow base)
 - Prevent false base station attacks (w/sequence #'s to prevent replay)
- Separate the ESN (electronic serial #) from auth calcs
- Backwards compatible w/older systems
- UIM (User Identification Module) a la GSM SIM cards
 - Removable or Fixed
- Negotiation of Air interface and network crypto algorithms

ESA Efficiency/Issues

- Cryptosync on air interfaces
- Increased message overheads
 - Reliability of error-free transmission
 - Time delay incurred
- Size of MAC message authentication code digest (signature)
 - Up to 160 bits
- Interoperability of 3GPP and 3GPP2

Weaknesses of Current Authentication

■ Data on the move ...

Sensitive information is transmitted in clear on vulnerable networks such as SS7 (SSD shared secret data, triplets, etc).

■ Data in storage ...

Secret keys are maintained in vulnerable network entities (HLRs, VLRs, etc)

ESA Candidates

■ Public-key

EPAC (from Certicom, w/optional key certification by home)

┆ Only mobile has private key, network has mobile public key

CipherIT (from CipherIT, w/implicit key certification)

┆ Each entity has own private key

■ Symmetric-key

LESA (from Lucent)

┆ A-key and SSD similar to current systems but with mutually authenticated session key agreement


AKA Authenticated Key Agreement w/Sequence Numbers (from ETSI 3GPP)*

** winner of late 1999 TR45 straw poll*

ESP Candidates

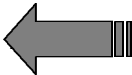
- Software-Oriented Stream Cipher 2 SSC2 (from GTE)
Combination Stream Cipher
- SOBER (from Qualcomm)
Stream Cipher with GF(2⁸) LFSR and non-linear clocking
- SHA-ZAM (from Lucent)
Feistel permutation using SHA-1 as stream cipher
- SCEMA (from Lucent)
CMEA descendant used as a stream cipher (IS136 TDMA only)
- ShaStream (from Qualcomm)

Adoption of NIST/NSA SHA-1

- It appears that a consensus has been built by both TIA and ETSI to adopt the NIST/NSA SHA-1 Secure Hash Algorithm as the preferred cryptographic primitive for 3G algorithms (as replacement for CAVE algorithm used in 2G) 
- Preferred cryptographic primitive of MACing shall be HMAC with SHA-1

AES

Advanced Encryption Standard

- May eventually replace ESP algorithm with NIST winner !! 
- AES is being designed with specs (speed etc) that are appropriate for wireless users



Conclusions



- Gov't wireless Type 1 security customers will always have custom end-to-end crypto and independent key management
- Need robust, efficient, and scaleable key management schemes to support vast majority of SBU users (with strong bilateral authentication etc)



Glossary/Acronyms

- ACELP/VSELP - 2G cellular vocoders for IS-136 TDMA systems
- AHAG - Ad Hoc Authentication Group
- AKA - Authenticated Key Agreement
- ATM - Asynchronous Transfer Mode
- BER - Bit error rate
- CAVE - Cellular Authentication and Voice Encryption
- CDMA - Code Division Multiple Access
- CELP - Codebook Excited Linear Prediction
- CMEA - Cellular Message Encryption Algorithm
- CONDOR - Government secure wireless program (originally "COunter Narcotics DEA Operations Radio", but now much broader !)
- COTS - Commercial Off The Shelf
- CVSD - Continuously Variable Slope Delta modulation
- ECC - Elliptic Curve Cryptography
- EPAC - Enhanced Public Key Authentication

Glossary/Acronyms (continued)

- ETSI - European Telecommunications Standards Institute
- FNBDT - Future Narrow Band Digital Terminal
- G - Generation (e.g., 3G = third generation)
- GOTS - Government Off The Shelf
- GSM - Global System Mobile
- HF - High Frequency (3-30 MHz band)
- HLR - Home Location Register
- IMT2000 - International Mobile Telecommunications-2000
- IP - Internet Protocol
- ISDN - Integrated Services Digital Network
- IS136 - TIA interim standard for the 2G cellular TDMA air interface standard
- IS95 - TIA TR45 interim standard for the 2G cellular CDMA air interface standard
- ITU - International Telecommunications Union
- ITU-T SG7 - ITU committee T, subgroup 7
- IWF - Inter Working Function

Glossary/Acronyms (continued)

- LEO - Low Earth Orbit satellite
- LESA - Lucent Enhanced Subscriber Authentication
- MAC - Message Authentication Code, or a process to generate a MAC
- MATLAB - Commercial signal processing and programming language tool
- MELP - Mixed Excitation Linear Prediction
- MILSTAR - DOD communications satellite system (2400 bps voice mode)
- MSE - Mobile System Equipment (DOD tactical wireless)
- NSA-CFS - National Security Agency Center For Standards
- OSI - Open Systems Interconnection
- QAM - Quadrature Amplitude Modulation
- QCELP - 2G cellular vocoder for IS-95 CDMA system (rate set 1)
- SBU - Sensitive But Unclassified
- SG7 - Study Group 7 of ITU-T
- SIM - Subscriber Identity Module
- SSC2, SOBER, SHA-ZAM, SCEMA, ShaStream - Encryption candidate algorithms

Glossary/Acronyms (continued)

- SSD - Shared Secret Data
- SS7 - Signaling System 7
- STU-III - Secure Terminal Unit III (3rd generation, see Tom Clancy novels !)
- TDMA - Time Division Multiple Access
- TIA - Telecommunications Industry Association
- TR45 - TIA committee concerned with cellular standards (TR = Transmit/Receive)
- VLR - Visiting Location Register
- WCDMA - Wideband Code Division Multiple Access
- 3GPP - cellular 3rd Generation Partnership Project