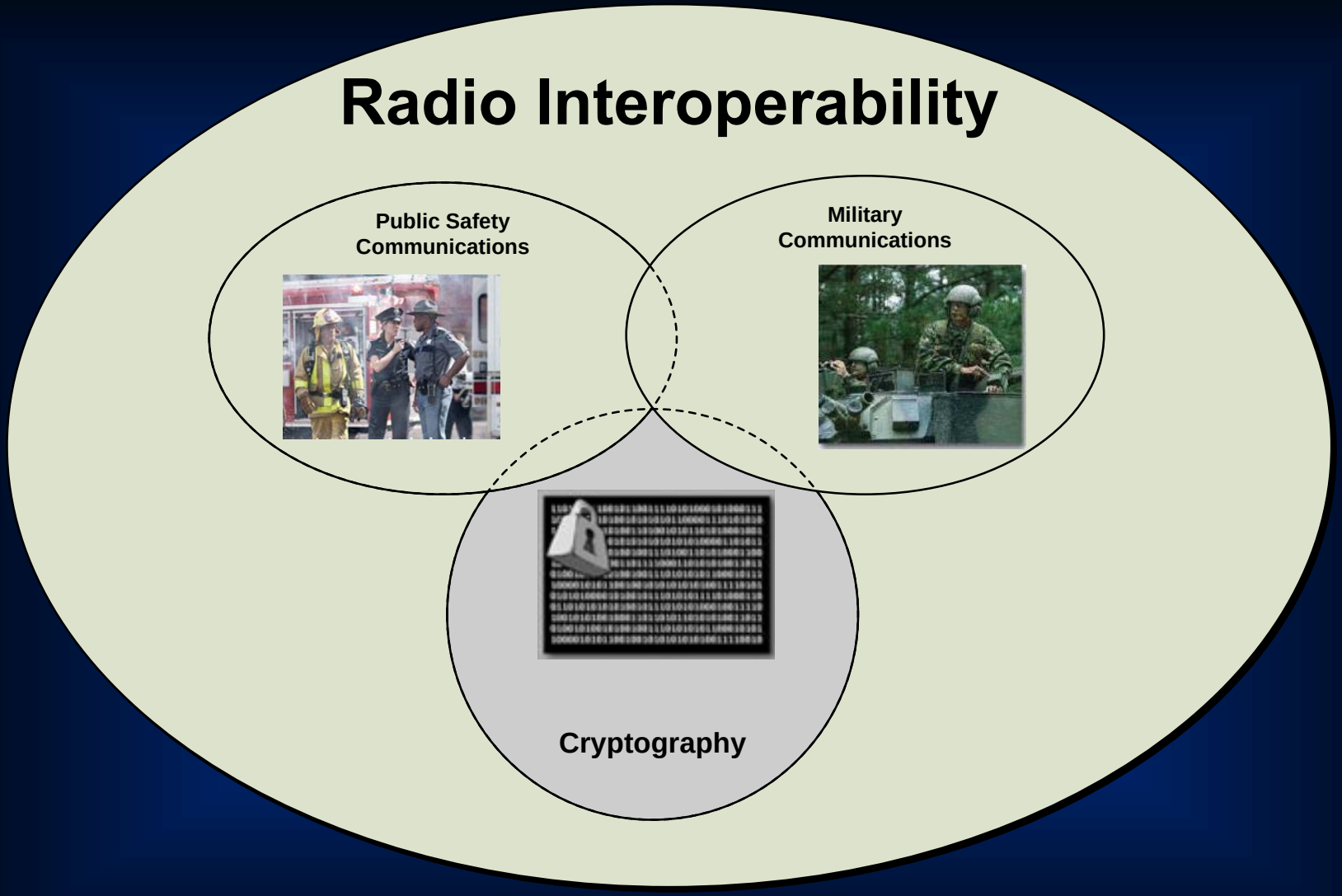
Suite B Compatible Tactical Radio

Igor A. (Tony) Spivak – Sr. Principle Engineer

Presentation Overview

- Cryptographic Interoperability problem statement.
- Department of Defense Suite B initiative.
- Harris RF-310M-HH Suite B Multiband Handheld Radio.
- Interoperability scenarios

Cryptographic Interoperability



What is Suite B?

Set of Cryptographic Algorithms based on a set of strong commercial algorithms.

- Encryption/Confidentiality - Advanced Encryption Standard (AES) – specified in FIPS 197 (key sized 128 and 256 bits).
- Digital Signature/Authentication – Elliptic Curve Digital Signature Algorithm (ECDSA) – specified in FIPS 186-3 (using the curves with 256 and 284 bit prime moduli).
- Key Exchange – Elliptic Curve Diffie-Hellman (ECDH) – specified in Draft NIST Special Publication 800-56 (using 256 and 384 bit prime moduli).
- Hashing – Secure Hash Algorithm (SHA) – specified in FIPS 180-2 (using SHA-256 and SHA-384).

Algorithms are not enough

- AES sub-mode specifications
  - Electronic Codebook (ECB) Mode
  - Cipher Block Chaining (CBC) Mode
  - Cipher Feedback (CFB) Mode
  - Output Feedback (OFB) Mode
  - Counter (CTR) Mode
- Initialization Vector (IV) definition
  - Format
  - Size
- These parameters are typically defined in the higher level Waveform or Protocol Specification (APCO P25, SCIP, etc.)

Complete Interoperability Solution

Cryptography

+

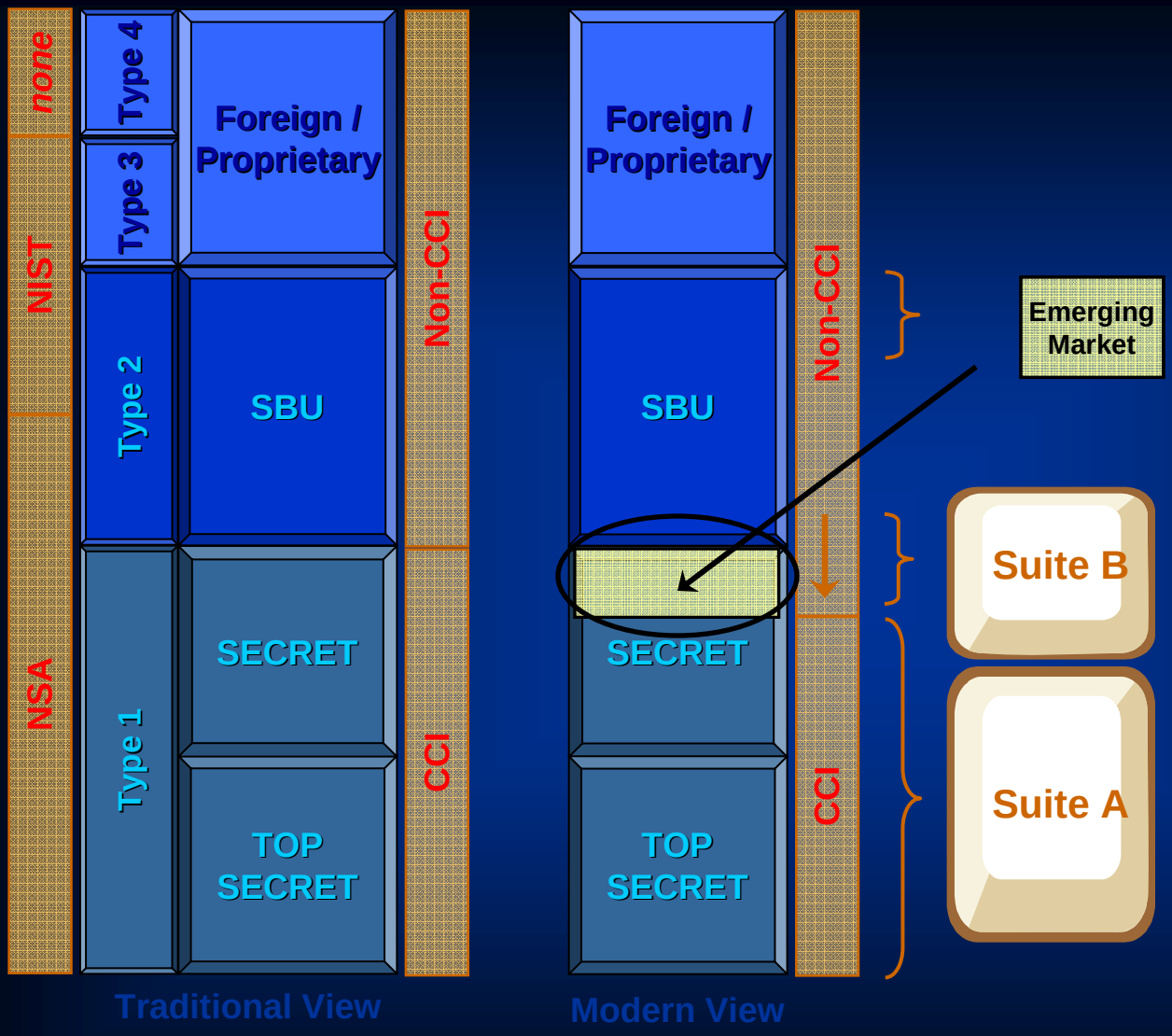
Protocols

Modem Signaling Schemes

=

Complete Voice and Data traffic Interoperability Solution

Crypto Standards Migration



Harris Software Defined Radio (SDR) Product Evolution

1988 1990 1992 1996 1998 2000 2002 2006 2007 2008 2009

Falcon I (HF) | Falcon II (HF, V/UHF) | Falcon III (HF, V/UHF, Microwave)

Proprietary SDR | Proprietary SDR | JTRS-SCA, Exportable-SCA

RF-5000

AN/PRC-138

AN/PRC-117F(C)

AN/PRC-150(C)

AN/PRC-152(C)

AN/PRC-117G(C)

RF-310M-HH (Suite B)

Falcon III AN/PRC-152 and AN/PRC-117G Tactical Radios (Dual Mode)

AN/PRC-152 SCA-based Multiband Handheld Radio

- 30 - 512 MHz
- JTRS SCA v2.2 Operating Environment
- Waveforms:
  - VHF/UHF LOS
  - SINCGARS
  - HAVEQUICK II
  - MIL-STD-188-181B SATCOM
  - High Performance Waveform (HPW)
  - APCO P25 option
- Type-1 Sierra II Programmable Encryption
  - DS-101/102 fill: AN/CYZ-10, KYK-13, KYX-15..
  - Modes: KY-57, ANDVT, KYV-5, KG-84C,
  - Suite B AES
- NSA / JTEL certified

AN/PRC-117G SCA-based Multiband Manpack Radio

- 30 – 2 GHz
- JTRS SCA v2.2 Operating Environment
- Waveforms:
  - VHF/UHF LOS
  - SINCGARS
  - HAVEQUICK II
  - MIL-STD-188-181B SATCOM
  - High Performance Waveform (HPW)
  - ANW2 Wideband Networking
- Type-1 Sierra II Programmable Encryption
  - DS-101/102 fill: AN/CYZ-10, KYK-13, KYX-15..
  - Modes: KY-57, ANDVT, KYV-5, KG-84C,
  - Suite B AES
- Certified HAIPE 3.0 legacy subset
- NSA / JTEL certified

RF-310M-HH Suite B, non-CCI Radio

Key Features:

- **30-512 MHz**
- **Selectable RF Output, up to 5 watts**
- **JTRS SCA v2.2 Operating Environment**
- **Sierra IIB Programmable Encryption**
  - Suite B algorithms, interoperable up to US SECRET voice & data
  - EKMS (DS-101/102) fill interface
  - Dedicated key fill / programming interface
- **Initial Waveforms:**
  - VHF/UHF AM/FM
  - APCO P25
- **Future Waveforms**
  - SCIP (AES) – NATO STANAG implementation
  - Quicklook (VHF ECCM waveform)
- **Built-in GPS (optional)**
- **Integrated speaker & microphone**
- **Alphanumeric keypad & LCD display**
  - Same as AN/PRC-152
  - NVG Compatible
- **Multiple Fill File Storage**
- **Common accessories with AN/PRC-152**
  - Including RF-300M Vehicle Adapter Amplifier

Military Coalition Scenario

AN/PRC-117G(V)1(C)
CCI Type 1 Dual-Mode

AN/PRC-152(V)1(C)
CCI Type 1 Dual Mode

Type 1, Suite A Net

Military Coalition Scenario (cont.)

AN/PRC-117G(V)1(C)
CCI Type 1 Dual-Mode

AN/PRC-152(V)1(C)
CCI Type 1 Dual Mode

RF-310-HH
non-CCI Suite B

Type 1, Suite A Net

Type 1, Suite B Net

DHS Mission Scenario

Conclusions

- Radio systems interoperability is critical in both military and public safety/first responder communications scenarios.
- Cryptographic interoperability is an important aspect of the overall interoperable radio communications solution.
- Suite B defines a set of interoperable cryptographic algorithms.
- The Harris Falcon III RF-310M-HH multiband handheld radio is the first SCA based Suite B compatible radio product certified by NSA for secret and below traffic.
- The RF-310M-HH Suite B radio is able to support a number of mission critical communications scenarios, both in the battlefield and in the area of public safety communications.

Contact Information

Igor A. (Tony) Spivak

Senior Principle Engineer

Harris Corporation
RF Communications Division
1680 University Ave.
Rochester, New York 14610

Telephone: (585) 242-3034
ispivak@harris.com