The Challenge in Developing an SCA Compliant Security Architecture that Meets Government Security Certification Requirements

Ronald Bunnell
Senior Systems Engineer
The Boeing Company
Anaheim, CA
ronald.r.bunnell@boeing.com
(714) 762-2838

John Trinidad
Senior Systems Engineer
Harris Corporation
Rochester, NY
john.trinidad@harris.com
(585) 242-3664

Introduction

- The Joint Tactical Radio System is being developed to be Software Communication Architecture (SCA) version 2.2 compliant
  - Open Architecture
  - Open Standards
  - Portability
- The JTRS is also being developed to provide secure communications for the US Military
  - Meet Government security requirements
  - Protect Voice, Data and Network

SCA Security Supplement

- The SCA Security Supplement (SS) version 1.1 defines a number of security requirements for the SCA (approximately 260)
  - Enhances Security
  - Generic in nature
  - Doesn't address issues with classified systems
- Other Government Security Requirements total over 1300

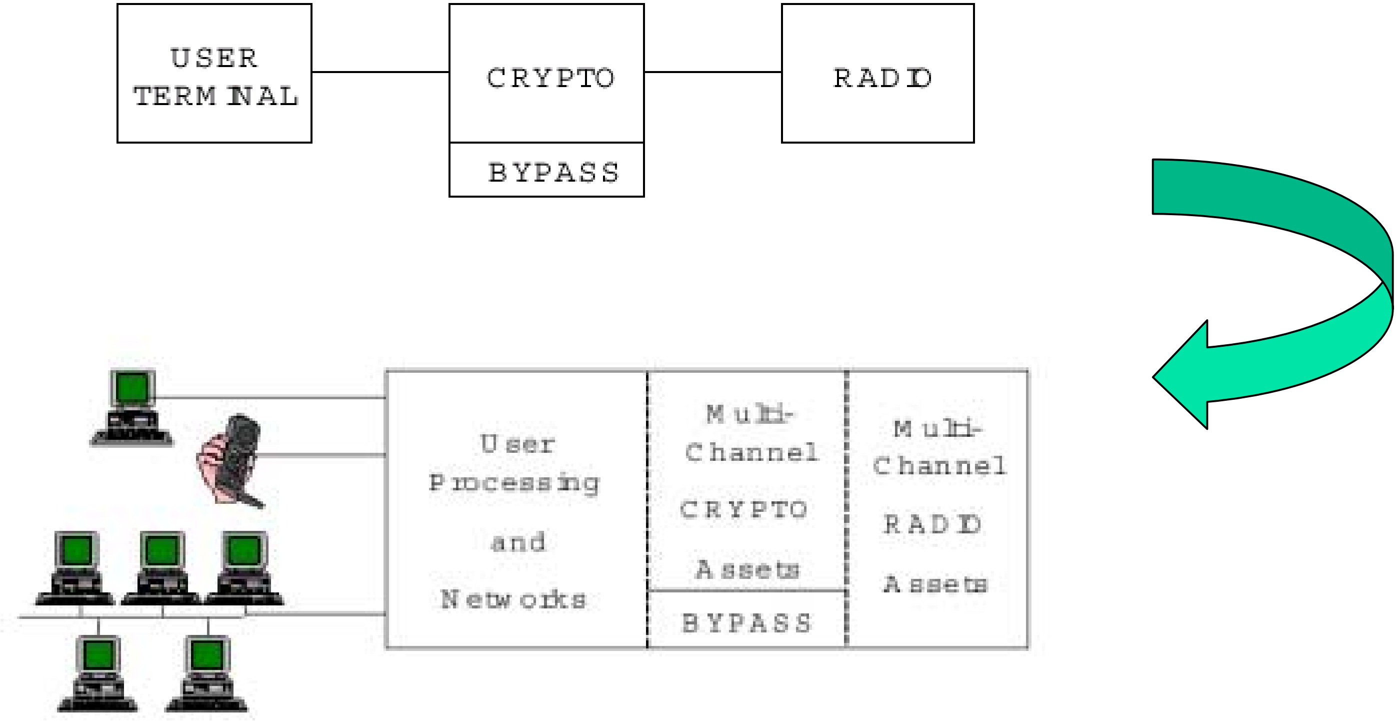
SCA SS (cont'd)

- Some contradiction between requirements exist
  - Multiple requirements documents generated by multiple authors
  - Some requirements assume a specific implementation
- Challenge is to meet intent of SCA and still provide a secure system

Example Security Functions

- Encryption for confidentiality
- Authentication of users, commands, software, radio parameter files
- Integrity of keys, software, files
- Transmission security to protect the communications channel
- Protection of network topology

Approach



USER TERMINAL

CRYPTO

BYPASS

RADIO

User Processing and Networks

Multi-Channel CRYPTO Assets

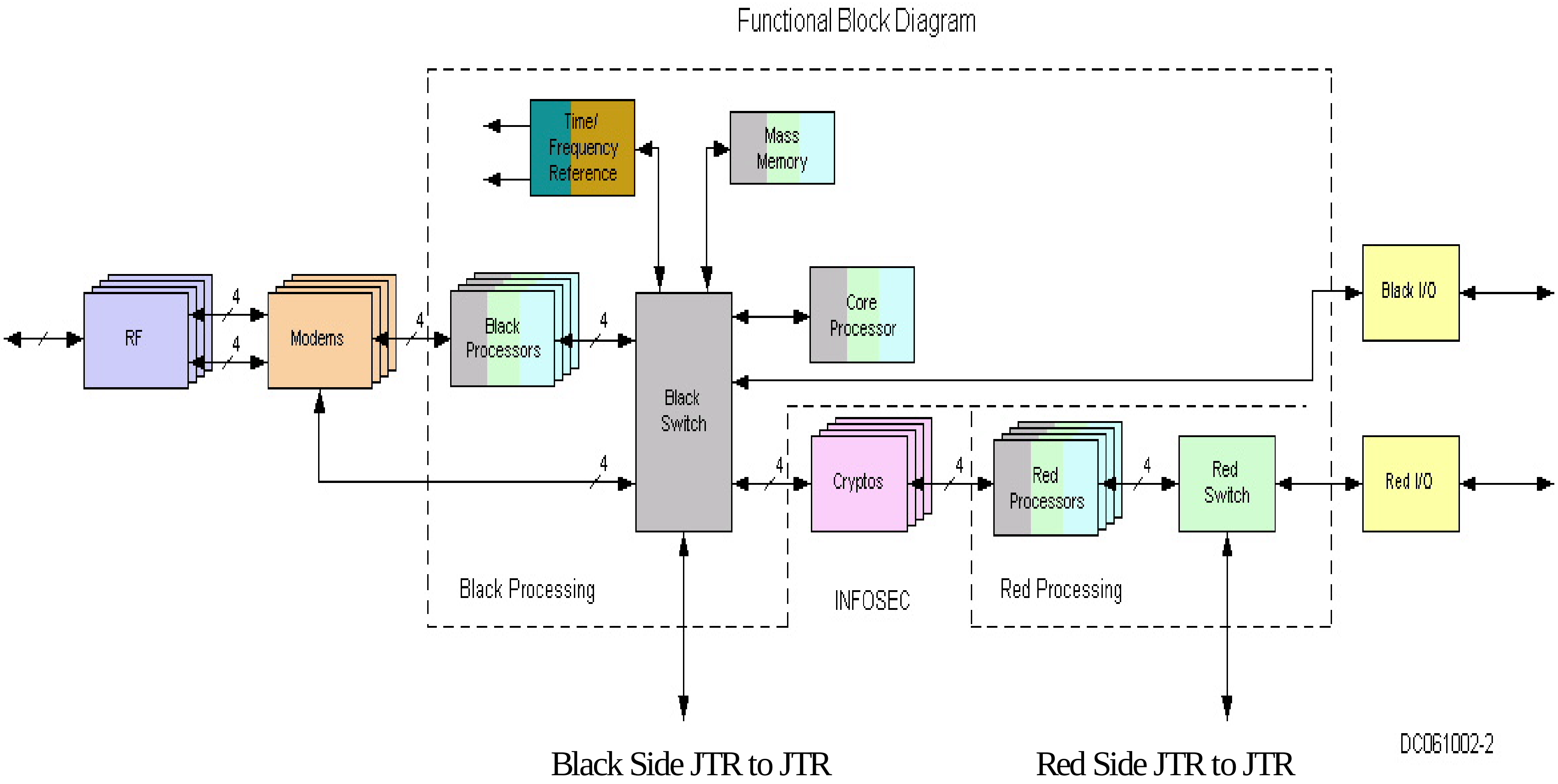
BYPASS

Multi-Channel RADIO Assets

Implementation Approach

- Our Approach to meeting Multiple Single Levels of Security (MSLS) includes providing four channels, each with its own transceiver, cryptographic channel, and processors (RED and BLACK). The JTR allows for the capability to operate simultaneously four instantiated waveforms. Waveforms can be torn down or re-instantiated as required.
- Two radios connected together can provide for an 8 channel radio.

Functional Block Diagram



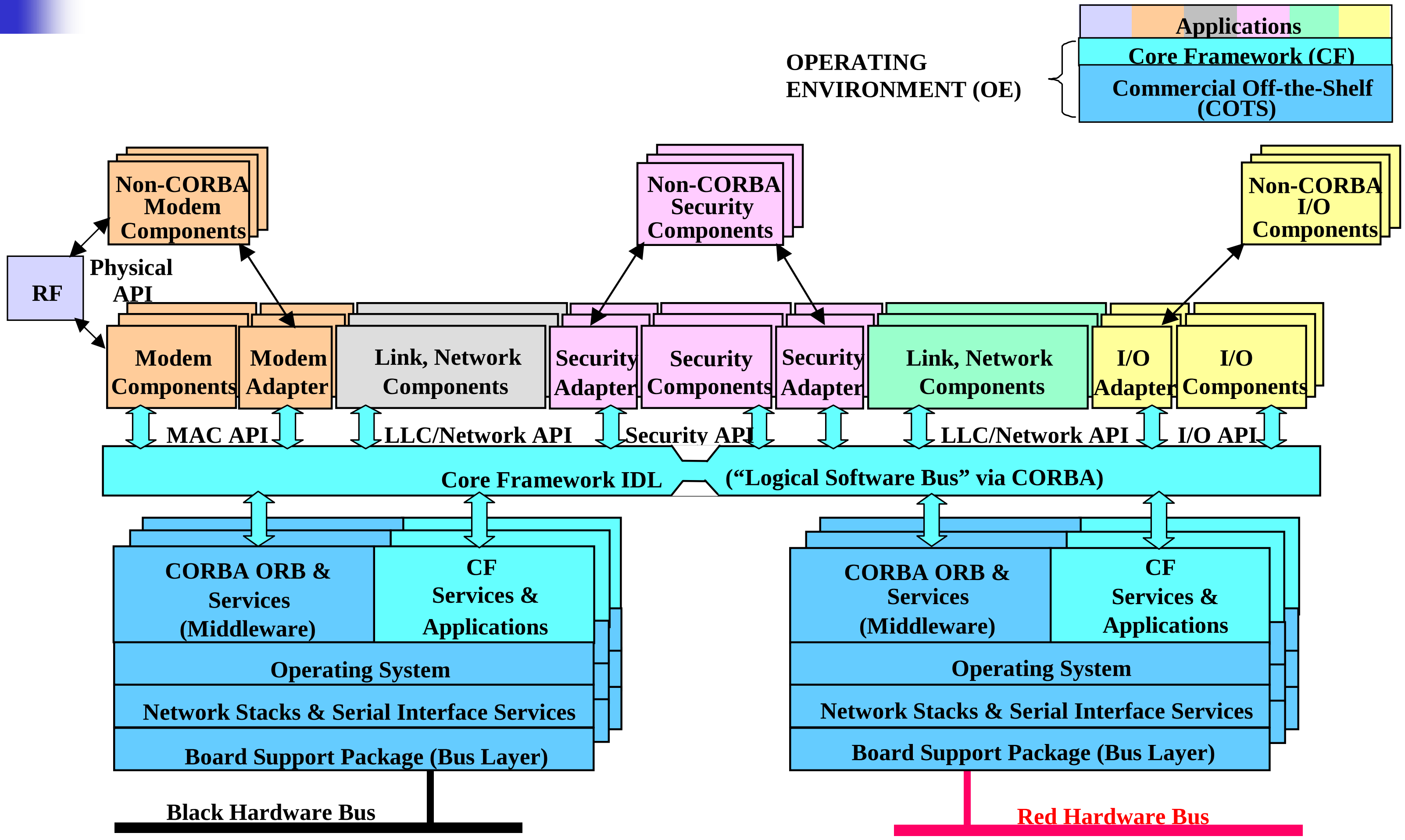
Joint Tactical Radio System Cluster One

- Security adapter components use Security APIs per the SCA Security Supplement
- Strict adherence to the SCA maximizes Waveform Application’s portability
  - Adherence to the AEP
  - Constraint of minimum CORBA
  - Use of CF:Devices (i.e., Radio Devices) to interface with hardware
  - Use of existing APIs

JTRS Cluster One (cont'd)

- A set of common Radio Security Services for non-waveform and waveform applications to use.
- Consists of SCA components that are persistent, SCA-compliant Resources or Devices that reside within the JTR Set and execute on a General Purpose Processor
- Compliance to the SCA to provide portability and reuse for other Clusters

Software Structure


Applications
Core Framework (CF)
Commercial Off-the-Shelf (COTS)
OPERATING ENVIRONMENT (OE)
Non-CORBA Modem Components
Non-CORBA Security Components
Non-CORBA I/O Components
RF
Physical API
Modem Components
Modem Adapter
Link, Network Components
Security Adapter
Security Components
Security Adapter
Link, Network Components
I/O Adapter
I/O Components
MAC API
LLC/Network API
Security API
LLC/Network API
I/O API
Core Framework IDL
("Logical Software Bus" via CORBA)
CORBA ORB & Services (Middleware)
CF Services & Applications
Operating System
Network Stacks & Serial Interface Services
Board Support Package (Bus Layer)
Black Hardware Bus
CORBA ORB & Services (Middleware)
CF Services & Applications
Operating System
Network Stacks & Serial Interface Services
Board Support Package (Bus Layer)
Red Hardware Bus

Waveform Porting

- Security Architecture must support porting of waveforms
  - Eleven legacy waveforms in addition to the WNW
- Design guidance given to waveform developers in meeting porting, bypass and other security related issues

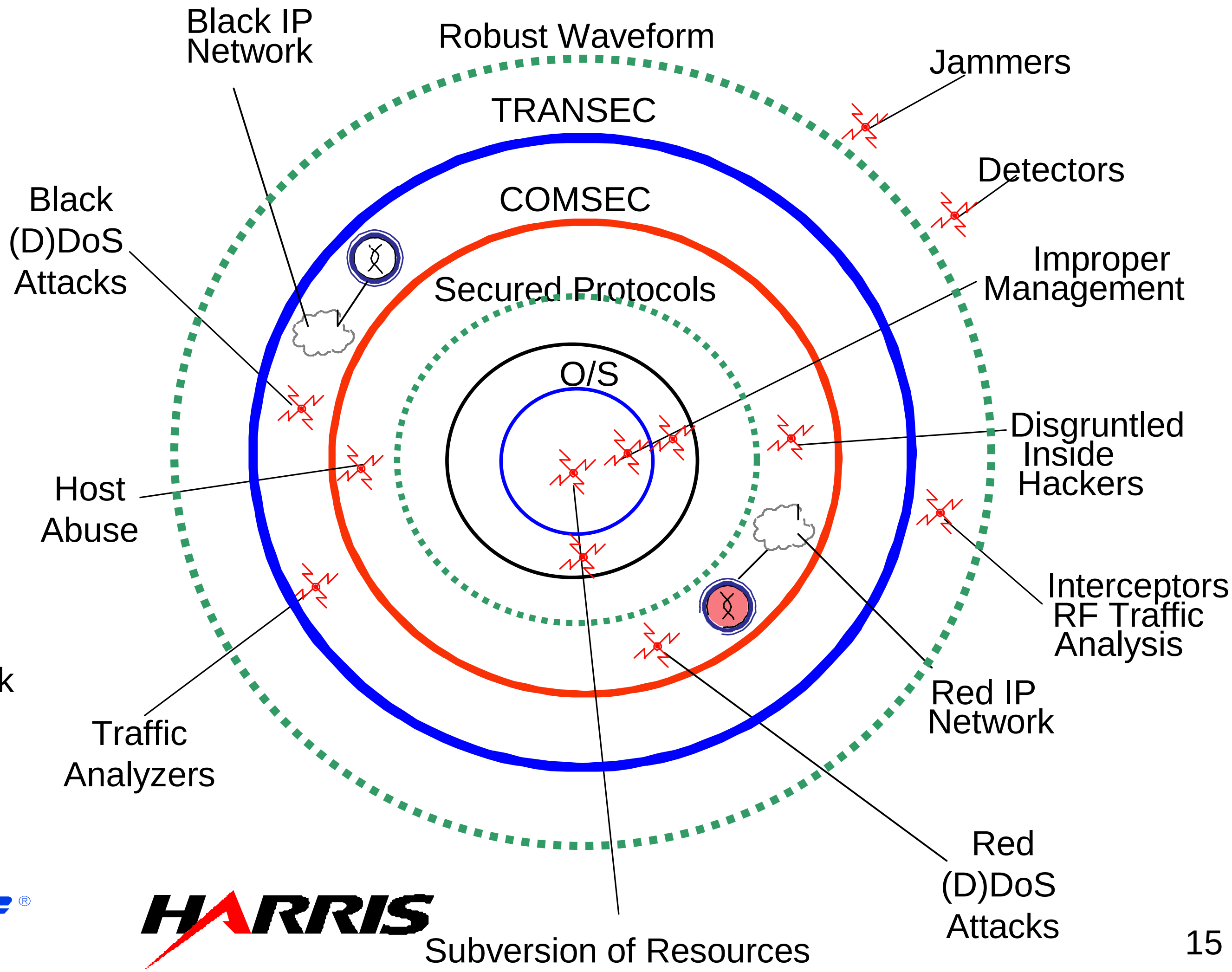
Network Security

- JTRS is designed to provide transformational communications in the form of the JTRS Networking capability
- Waveforms provide tremendous connectivity to each Radio node
- With this improved connectivity, comes greatly increased exposure to threats. Threats now are also network centric and can affect JTRS nodes *from anywhere on the planet*.

Network Assurance

- SCA mandates separate network stacks (TCP/IP) for internal software transactions and for external waveform support
- Information Assurance approach must Prevent/Detect Network attacks
  - Provide protection to Detection System

Defense in Depth



● Packet Filtering Red Router

○ Packet Filtering Black Router

⚡ Risks

BOEING®

HARRIS

Limitations

- Control placed on CORBA calls and other data bypass of the Cryptographic Unit
  - Mainly concerned with Red to Black bypass
  - Some concern with Black to Red
- Limits need to be placed on amount and type of Bypass data
  - Limit free text for example

Cryptographic Bypass

- Four types of bypass:
  - Header bypass
  - Waveform control/status bypass
  - System control/status bypass
  - Plain text bypass
- Each Application will have a Bypass policy
  - Guidelines for Applications established. Waveform developers are defining

Conclusion

- While providing a complete open architecture is not totally possible, given our need to protect data as well as the radio from attack, standards can be applied to the Security Architecture that support portability across a number of different platforms