SPAWAR Systems Center (SSC) Pacific Unmanned Vehicle (UV) Information Assurance (IA) Support

15th Annual INCOSE Region II Fall Mini-Conference
30 October 2010

John Yen
Unmanned IA Support Team
SSC Pacific
619-553-9404
john.yen@navy.mil

Jason Ricks
SSC Pacific
Key Management Architectures and Information Systems Branch Head
jason.ricks@navy.mil

SPAWAR Systems Center PACIFIC

Agenda

- Background
- Assumptions
- DoD Encryption Policy for UAS
- Certified Cryptography in UV Environments
- Cross Domain Issue
- Data at Rest (DAR)
- Summary

SPAWAR Systems Center PACIFIC

Excerpt from the Wall Street Journal

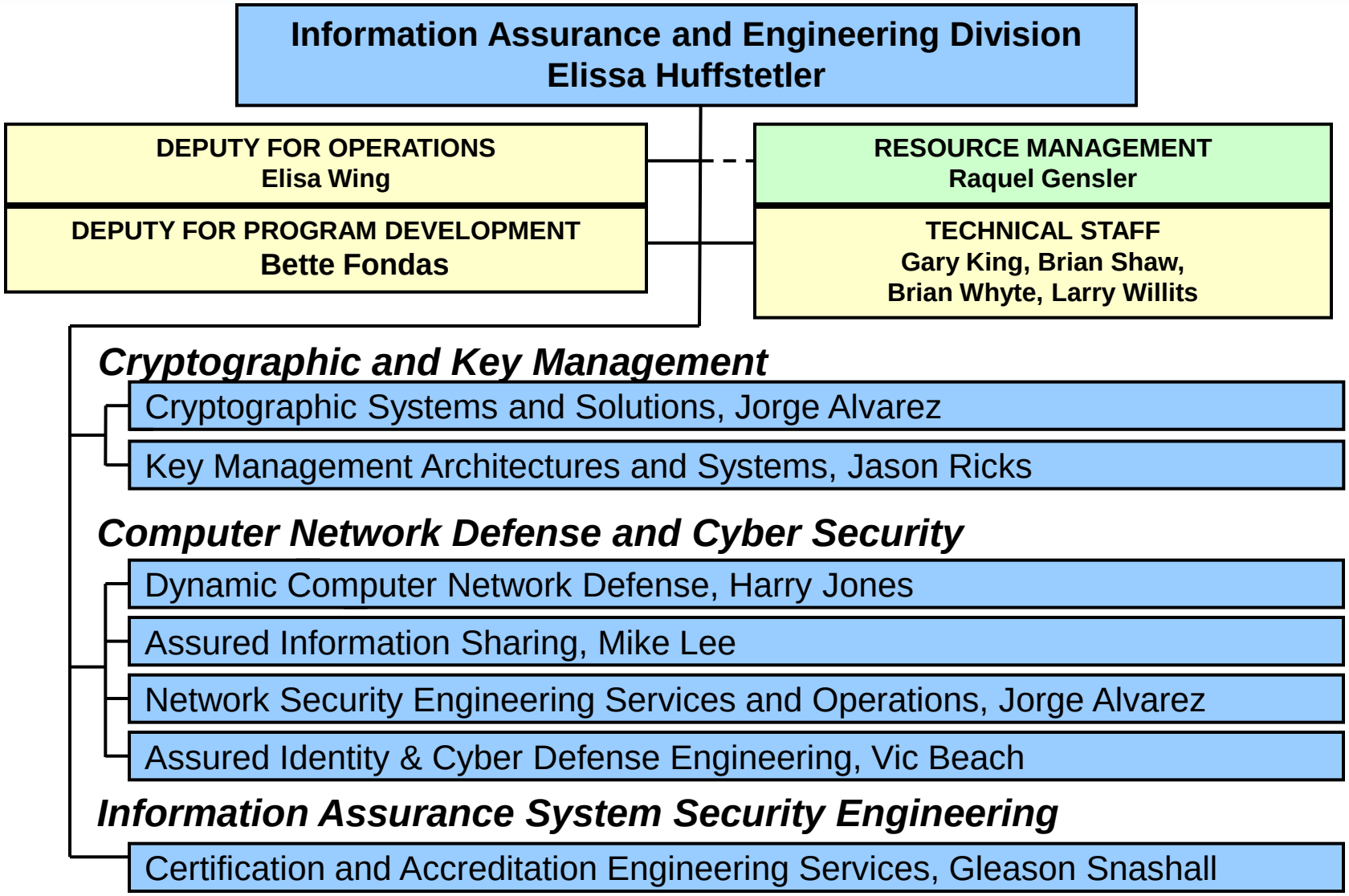
- WASHINGTON -- Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations. - *Wall Street Journal, 17 December 2009*
- Senior defense and intelligence officials said Iranian-backed insurgents intercepted the video feeds by taking advantage of an **unprotected communications link** in some of the remotely flown planes' systems. Shiite fighters in Iraq used software programs such as Sky-Grabber -- available for as little as $25.95 on the Internet -- to regularly capture drone video feeds, according to a person familiar with reports on the matter.

Who We Are, How We Can Help

- SSC Pacific IA & Engineering Division provides acquisition program IA and systems engineering support for Navy and other activities to include:
  - Cryptography and Key Management Architectures
  - Certification & Accreditation (C&A)
  - Computer Network Defense (CND)

- Currently supporting 3 Navy programs deploying Unmanned Vehicles (UV)
  - Common IA lessons learned from these UV implementations

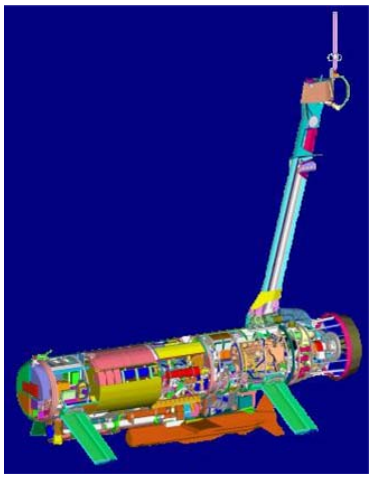
SSC Pacific Information Assurance (IA) Division



Littoral Combat Ship (LCS) Mission Modules (MM)

- SSC Pacific provides IA and cryptographic systems engineering support to NAVSEA PMS 420 for the Littoral Combat Ship Mission Modules (LCS MM)
- Mine Countermeasures (MCM) Mission Module includes two UVs

Remote Multi-mission Mine-hunting Vehicle (RMMV)



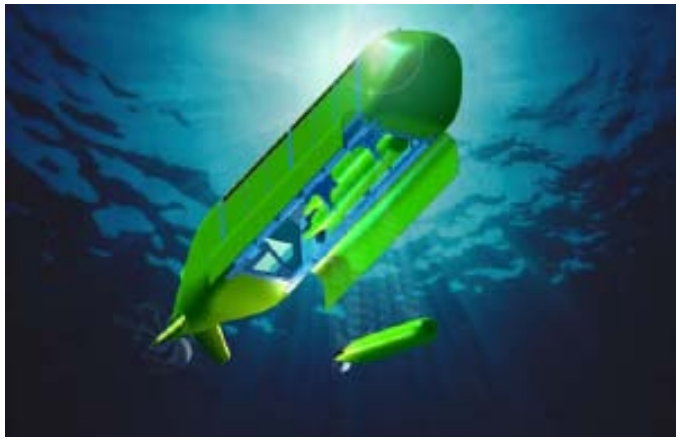
MCM Unmanned Surface Vehicle (USV)

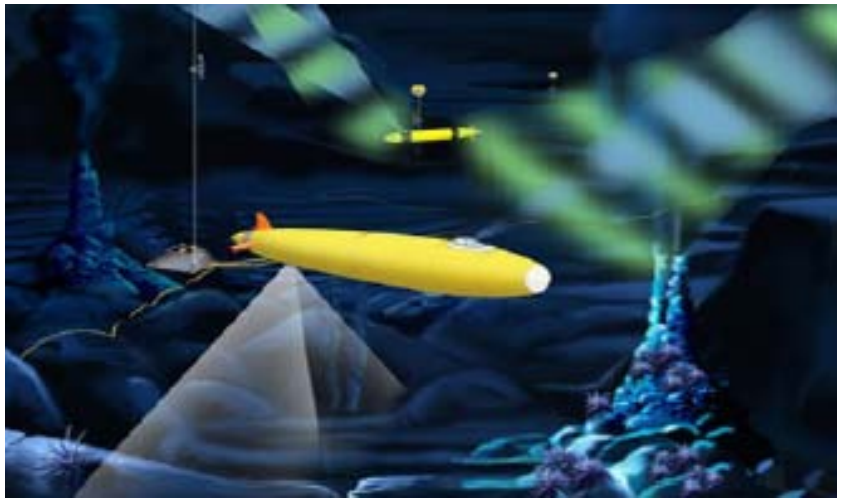
BAMS UAS

- SSC Pacific provides IA and cryptographic systems engineering support to NAVAIR PMA 262 for the Broad Area Maritime Surveillance (BAMS) Unmanned Aircraft System (UAS)

LD UUV

- SSC Pacific also provides IA and cryptographic systems engineering support to Office of Naval Research (ONR) for the Large Displacement Unmanned Underwater Vehicle (LD UUV)





SPAWAR Systems Center PACIFIC

Assumptions

- Information onboard UV is National Security Information (NSI)
  - NSI: Information that has been determined, pursuant to Executive Order 12958 (as amended) or any predecessor order, to require protection against unauthorized disclosure – *CNSSI 4009, June 2006*
  - National Security Agency (NSA) is the single authority for cryptography protecting national security systems
    - *Executive Order 12333, 04 December 1981*
    - *National Security Directive 42, 05 July 1990*
- NSI stored, processed, transmitted and/or received onboard UV must be protected in accordance with its classification level:
  - Classified information must be protected with Type 1 (NSA) cryptography
  - Unclassified sensitive NSI must be protected with Type 2 (NSA) cryptography
  - Unclassified US government information can be protected with Type 3 (National Institute of Standards and Technology (NIST)) cryptography
  - Categories defined by *CNSSI 4009*
- Protection of NSI onboard UV must be approved by the Navy through the DoD Information Assurance Certification & Accreditation Process (DIACAP)
  - *DODD 8500.1, 24 October 2002*
  - *DODI 8500.2, 06 February 2003*

SPAWAR Systems Center PACIFIC

DoD Encryption Policies for Unmanned Aircraft Systems (UAS)

- Cryptographic Methods for Protection of Unmanned Aircraft Systems (UAS) Wireless Communications
  - Classified ASD NII policy memo dated 06 Aug 2009
    - Applicable to Airborne UVs only
  - Establishes encryption solutions for protection of DoD UAS wireless communications in new DoD developments

- Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications
  - DoD Instruction currently being staffed at OSD
    - Approval at end of 2010?

Certified Cryptography in UV Environments

- Cryptographic devices previously certified by NSA were based on expectations that they would be operated in controlled environments
  - Radio rooms, command posts, manned aircraft
- The UV environment was not “anticipated” in prior NSA cryptographic certifications
  - Cannot remove and smash Crypto Ignition Key (CIK) on a UV
  - How to implement a remote/autonomous key zeroization process
    - Emergency key and related data zeroization
- NSA will reassess earlier cryptographic certifications with respect to the UV environment
  - NSA triage process for validated requirements
    - Will NSA allocate resources to support the requirement?
  - Security engineering assessment of UV environment

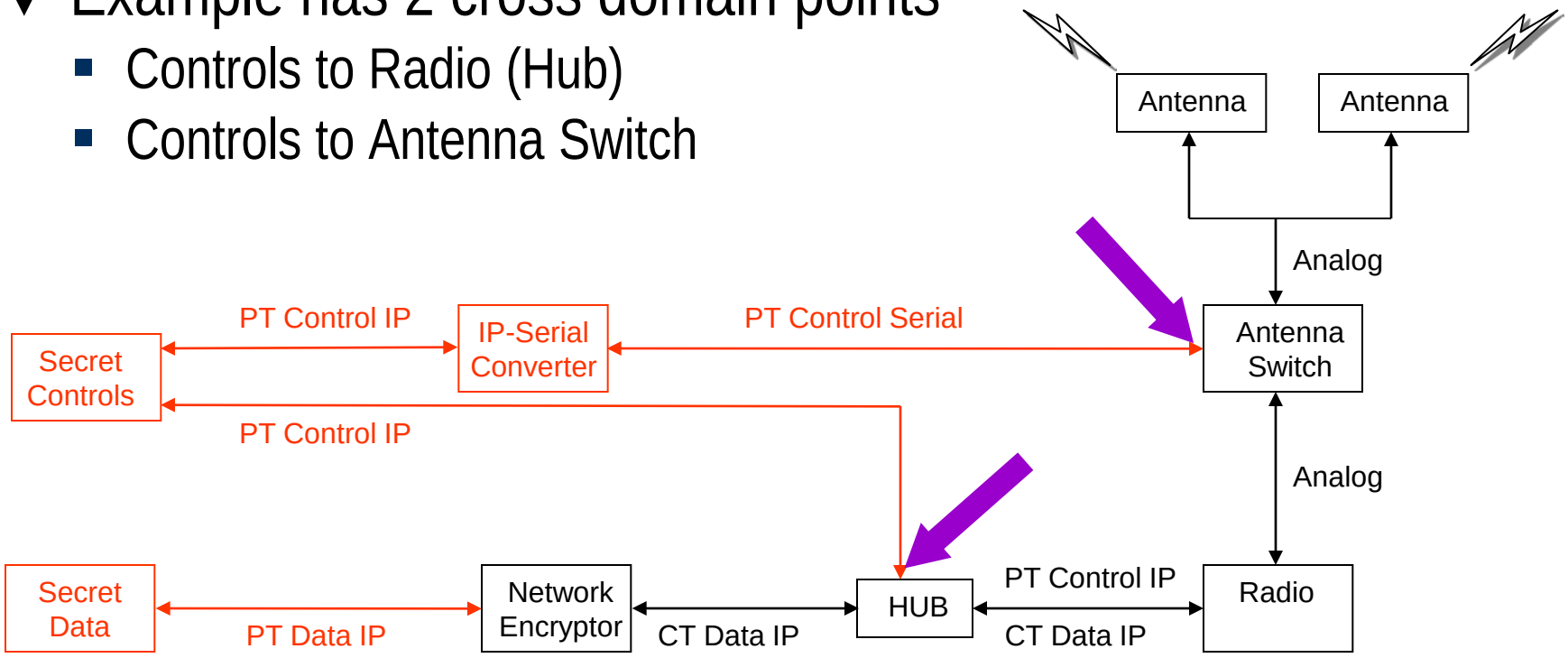
SPAWAR Systems Center PACIFIC

Cross Domain Issue

- Desire to control unclassified devices (radio, antenna, sensor, etc…) from a classified network
- This is a cross domain issue since **plaintext information** is moving between classified and unclassified domains
  - Capability to access or transfer information between two or more security domains – *CNSSI 4009, June 2006*
  - High Assurance Guard (HAG) such as Radiant Mercury is overkill given the low risk level
- Working with Navy Cross Domain Solutions Office (NCDSO) towards a Very Low Attack Risk (VLAR) cross domain filter
  - Information being transferred is usually limited in size
  - Information being transferred is usually well formatted
  - Risk level is generally low

Example Basic Functional Diagram

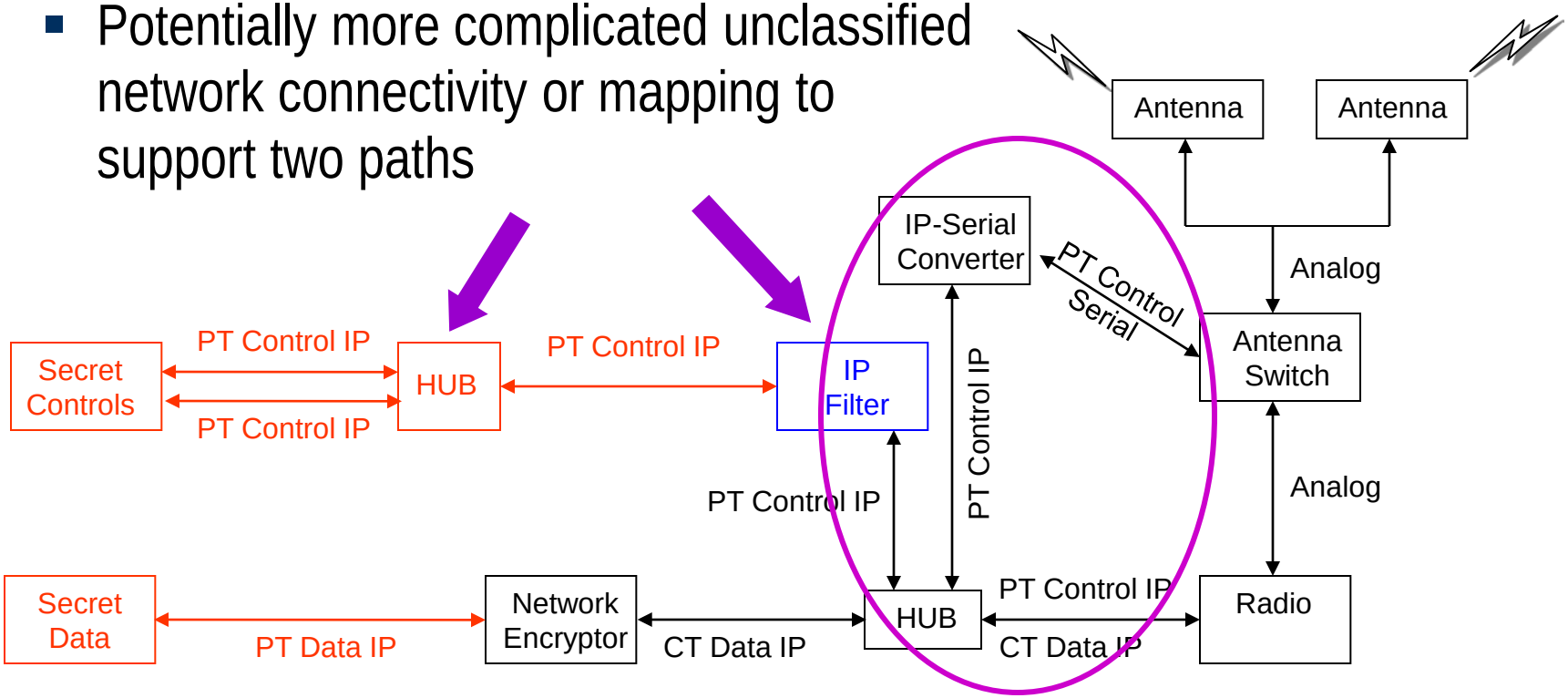
- Management & control information must be plaintext for radio and antenna switch to understand commands
  - Cannot go through the network encryptor
- Example has 2 cross domain points
  - Controls to Radio (Hub)
  - Controls to Antenna Switch



RED=Classified Black=Unclassified PT = Plaintext = Unencrypted CT = Ciphertext = Encrypted

Example Solution Architecture

- Single cross domain filter that supports IP-only traffic
  - Potential addition of a classified hub
  - Potentially more complicated unclassified network connectivity or mapping to support two paths



SPAWAR Systems Center PACIFIC

Data at Rest (DAR)

- Classified data collected and stored on UV risks compromise if the UV is lost or captured
  - Imagery, ELINT collections, processed information
  - NSA cryptographic devices generally protects only **data in transit** (COMSEC and TRANSEC)
  - Zeroization generally applies to small amounts of data
    - Crypto key material
    - ELINT processing algorithm databases
  - Insufficient power or time to wipe potentially gigabytes of data
- Data at rest protection is needed to ensure that classified data is not exposed if UV is lost or captured
  - Encrypt stored DAR
  - Ensure DAR encryption keys are zeroized on UV loss or compromise

SPAWAR Systems Center PACIFIC

Summary

- Developers of DoD UVs need to consider these IA systems engineering issues and work towards solutions acceptable to the approving authorities
  - SSC Pacific IA Division can provide technical expertise to help resolve these issues

  - John Yen
    - 619-553-9404 desk
    - 619-888-0302 cell
    - john.yen@navy.mil
    - yen@spawar.navy.smil.mil
    - yenj@spawar.navy.ic.gov