MLS for Tactical Soldier, Sensor and Munitions Networks

September 10, 2003

MITRE

Outline

- **Purpose / Background**
- **Statement of the Challenge**
- **Additional Security Discussion**
- **Emerging Communication Network Architectures**
  - **Secure Gateway**
  - **MLS**
- **Secure Computing Card**
- **Summary**

MITRE

Purpose / Background

- **Purpose**
  - **The purpose of this briefing is to explore the challenges, and a potential solution of Multi Level Security for Tactical Soldier, Sensor and Munitions systems**

- **Background**
  - **The potential solution that will be discussed in this presentation was initially explored through the Anti Personnel Landmine Alternative (APLA) Track 1 Non-Self Destruct Alternative, Spider System**

MITRE

Statement of the Challenge

- **Networked Communications for the future force will require a seamless architecture ensuring information exchange capabilities between all nodes, including those of dissimilar classification levels**
  - **This type of network architecture requires Multi Level Security (MLS) in order to facilitate information exchange at the lowest possible level**
- **MLS is a complex and intricate challenge that has yet to realize a fully effective tactical solution**
- **An effective tactical solution for Soldiers, Sensors and Munitions is critical for the Networked Centric Warfare concepts of the Objective Force**
  - **This solution MUST be capable of being handled as an unclassified, non Crypto Graphic Controlled Item (CCI) in order to meet current policy and future operational and performance requirements**

MITRE

Additional Security Discussion

- **Even if a non-CCI algorithm is approved for the protection of classified information during transmission, protection of classified information in an unencrypted state is still a major challenge for unattended and unclassified systems**

- **The availability of small, affordable, unclassified device that is capable of protecting classified information while remaining unclassified will facilitate a true MLS architecture**

  - **Such a device would only release classified information when authorization was confirmed via password and/or physical key (or other approved method) is supplied**

- **A device such as that listed above in addition to the approved use of a Type III algorithm for the protection of classified information will facilitate true MLS functionality by allowing unclassified through Top SECRET Soldier, Sensor and Munitions nodes to be connected to the same network**

MITRE

Notional Communication / Networking Architecture using Secure Gateway

Security

Either a ***High Assurance Guard /Secure Gateway*** is required between the classified network an the unclassified Warriors, or the network needs to be multi level secure

High Assurance Guard /Secure Gateway

The backbone network is classified, so a secure gateway is required between the backbone and the unclassified node (warrior)

- Where will the gateway be?
- All nodes *below* the gateway will only have access to unclassified Information and every message coming in to the gateway will have to be filtered by that Gateway node

Sensor UAVs

Comm UAVs

Missiles

LAM/PAM

LAM/PAM

LAM/PAM

"JTRS" Network

Filter integrated into Squad Leader equipment

——	***Classified Net***
——	***Unclassified Net***

UGS

Dismounted

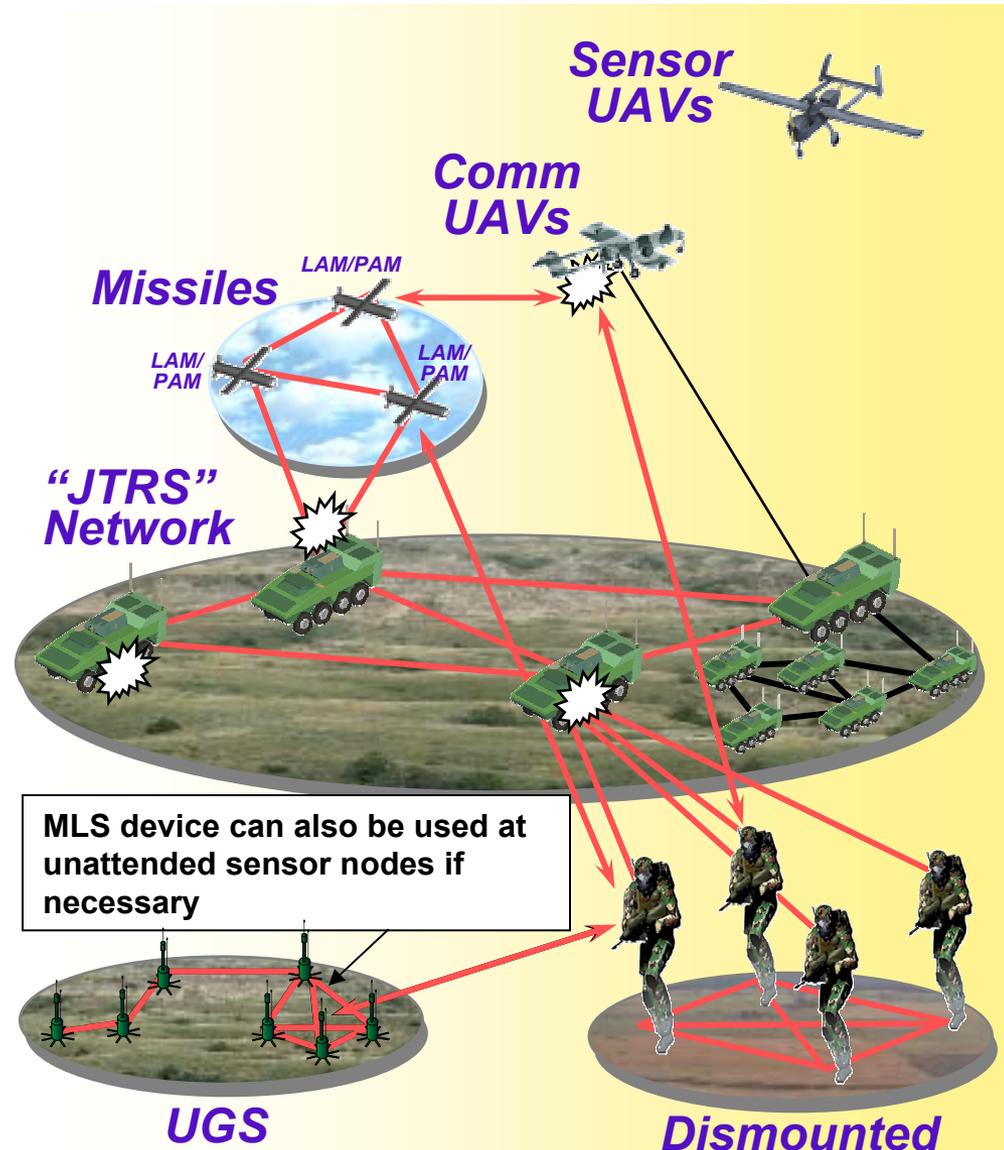# Notional Communication / Networking Architecture using full MLS solution

Security

Either a High Assurance Secure gateway is required between the classified network an the unclassified Warriors, or the network needs to be *Multi Level Secure*

Multi Level Security

The network is classified, but now each node (Warrior) has the same equipment that is configure for that soldiers clearance.

No choke point for message filtering.

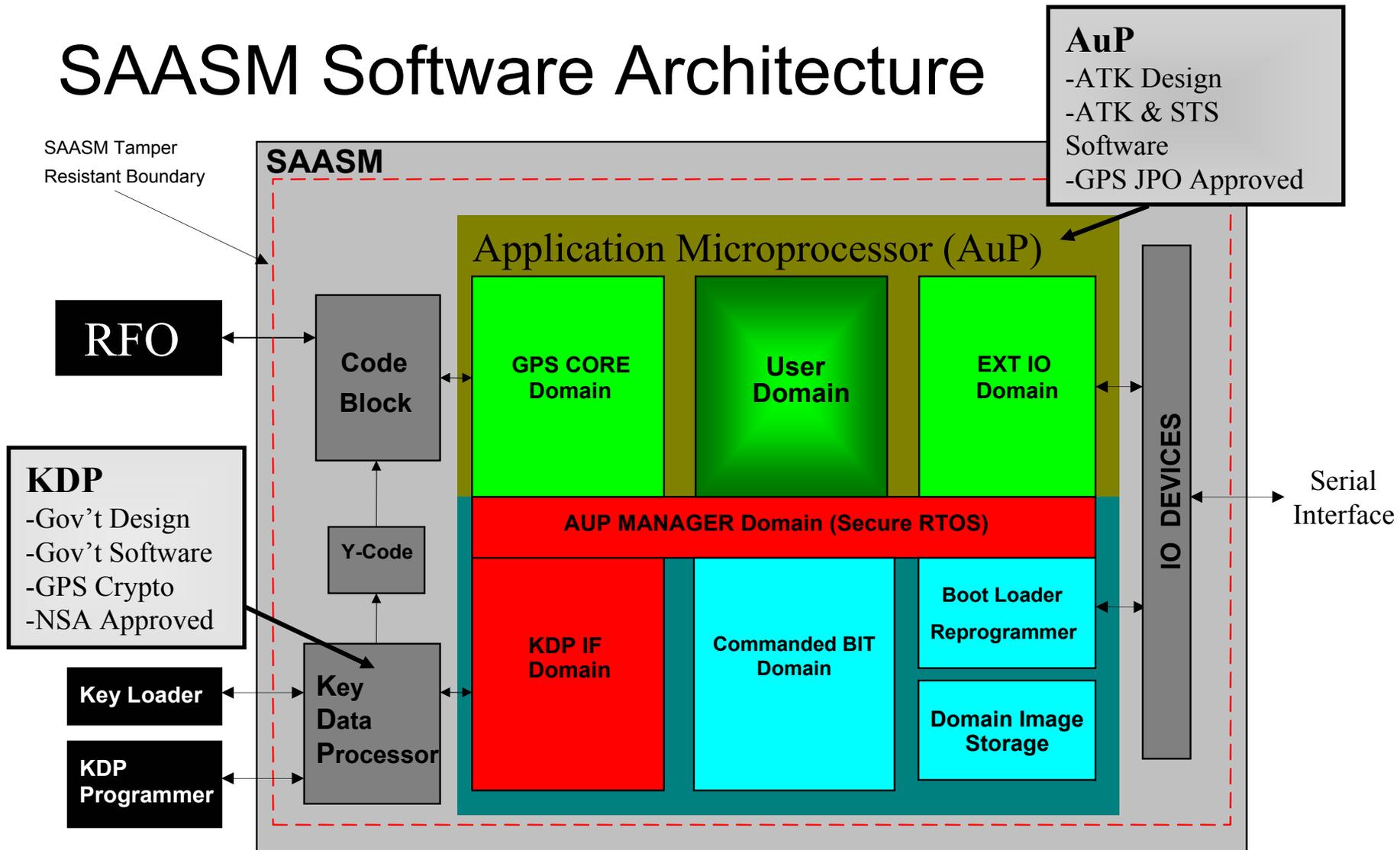Each messages is filtered at its destination

Sensor UAVs

Comm UAVs

LAM/PAM

Missiles

LAM/PAM

LAM/PAM

"JTRS" Network

MLS device can also be used at unattended sensor nodes if necessary

— Classified Net
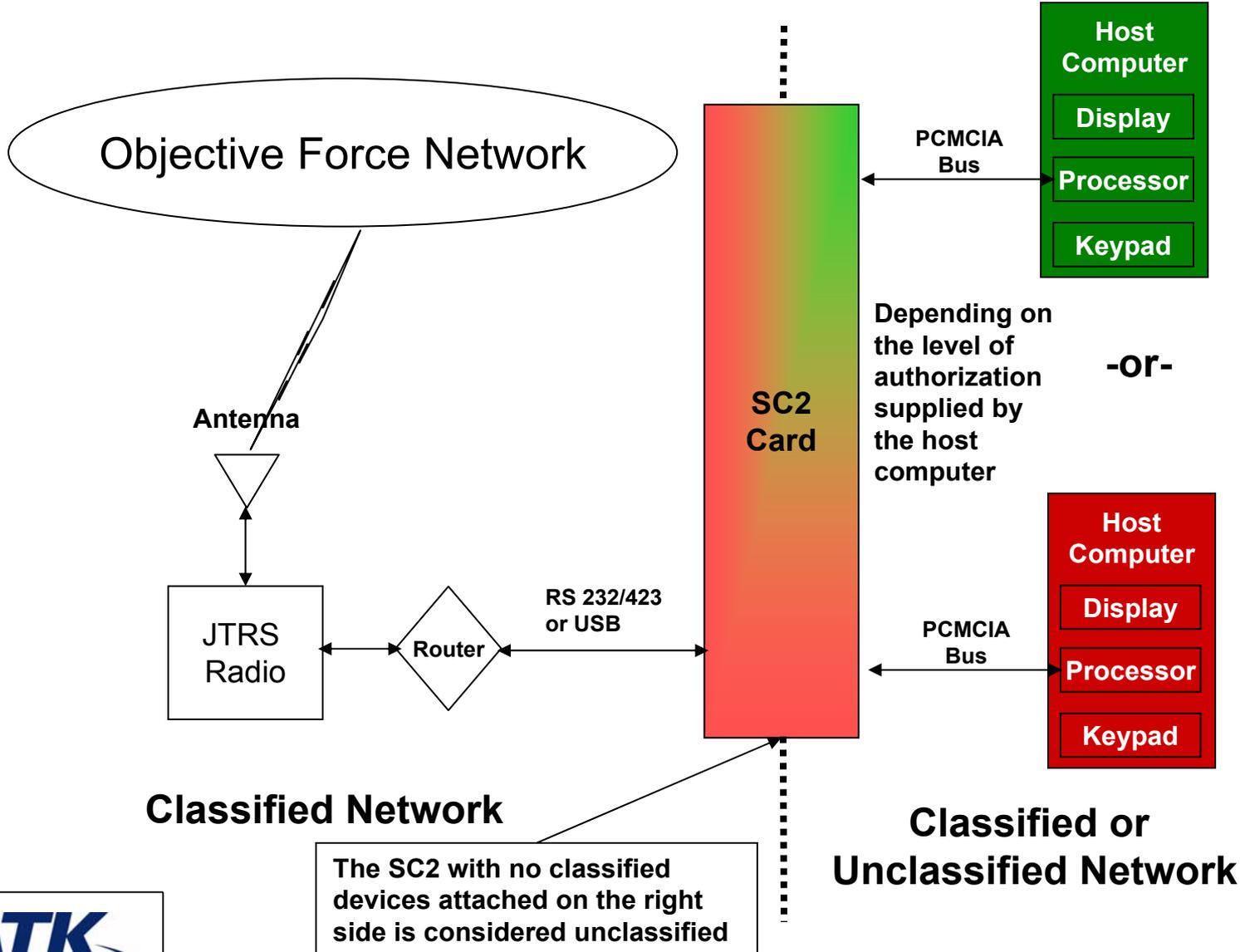— Unclassified Net

UGS

Dismounted

Secure Computer Card (SC2) Background

- **During early development of the Spider APLA system, there was a derived requirement for the manned portion of the system to contain/protect classified information while being operated by an unclassified user**

- **The proposed solution to meet the above requirement was to use the Secure Computer Card (SC2), which used the same technology used by the Selective Availability Anti Spoofing Module (SAASM), the security module for the emerging military GPS systems**

  - **The SAASM module uses physical and software protective measures that allowed it to contain and process classified information, while the module itself remains unclassified**

- **Due to Landmine Security Doctrine change, the SC2 functionality is no longer required by Spider**

  - **A prototype exists that will filter messages based on format and JVMF message header**

MITRE

SAASM Software Architecture

AuP
-ATK Design
-ATK & STS Software
-GPS JPO Approved

SAASM Tamper
Resistant Boundary

SAASM

Application Microprocessor (AuP)

RFO

Code Block

GPS CORE Domain

User Domain

EXT IO Domain

IO DEVICES

Serial Interface

KDP
-Gov't Design
-Gov't Software
-GPS Crypto
-NSA Approved

Y-Code

AUP MANAGER Domain (Secure RTOS)

KDP IF Domain

Commanded BIT Domain

Boot Loader Reprogrammer

Domain Image Storage

Key Loader

Key Data Processor

KDP Programmer

ATK
ALLIANT TECHSYSTEMS

MITRE

SC2 Functional Architecture

Objective Force Network

Host Computer

Display

Processor

Keypad

PCMCIA Bus

Antenna

SC2 Card

Depending on the level of authorization supplied by the host computer

-or-

JTRS Radio

Router

RS 232/423 or USB

PCMCIA Bus

Host Computer

Display

Processor

Keypad

Classified Network

The SC2 with no classified devices attached on the right side is considered unclassified

Classified or Unclassified Network

ATK
ALLIANT TECHSYSTEMS

MITRE

Summary

- **A full MLS solution must be achieved to facilitate the Network Centric Warfare concept of the Objective Force**
  - **This solution should be pushed down to the lowest possible level**
- **The proposed protective measures of the SC2 could allow for it to be handled as an unclassified device based on the level of the authentication**
  - **It can maintain segregation of data of multiple classification levels and release that data only with the appropriate authorization**
- **Network, radios would be Classified at the highest required level, the SC2 would be MLS, and the host computer would operate in a single level of security**

MITRE

Summary (concluded)

- **Would require interaction with NSA and CIO/G6 to approve connection (authentication) between network radio and SC2 card, unless SC2 handles the encryption / decryption**
  - **Additional Authentication may be required between radio and SC2**
- **SC2 concept still needs to be certified and accredited**

MITRE

Acronyms

- **AES – Advanced Encryption Standard**
- **APLA – Anti Personnel Landmine Alternative**
- **CCI – Controlled Cryptographic Item**
- **JTRS – Joint Tactical Radio System**
- **JVMF – Joint Variable Message Format**
- **MLS – Muli Level Security**
- **NSD-A - Non Self Destruct Alternative**
- **NSA – National Security Agency**
- **SAASM – Selective Availability Anti Spoof Module**
- **SC2 – Secure Computer Card**
- **UAV - Unmanned Air Vehicle**
- **UGS – Unmanned Ground Sensors**

MITRE