Unmanned Tactical Autonomous Control and Collaboration (UTACC) Threat and Vulnerability Assessment

18 May 2015

Captain D. R. Wimmer Jr, USMC
Captain L. Batson V, USMC

utacc@nps.edu
Agenda

• NPS Thesis Overview / Research Scope
• Methodology / Threat Template
• Threats/Vulnerabilities
• Conclusions
• Future Research Considerations
• Questions
Unmanned Tactical Autonomous Control and Collaboration (UTACC) is intended to be a decision-centric, semi-autonomous system that contains air and ground vehicles. UTACC will fail to accomplish its mission if the system is not built with security in mind from the outset. To improve the security of UTACC, this thesis conducts an analysis to identify threats and vulnerabilities in the system’s concept. The goal of this analysis was to mitigate threats and enable mission success to UTACC-supported missions.

Research Questions

• What threats exist that have the potential to affect the UTACC?
• What vulnerabilities are inherent in the UTACC concept?
• What can be done to mitigate those threats and vulnerabilities within UTACC?

Scope/Assumptions

• Treat UTACC system as a “teammate”
• Technology Agnostic
• UTACC is a decision support tool
• Marines carry weapons, not controllers
• Reconnaissance “team” missions
• Combat environment
Methodology

Threat Template

- A framework for threat and vulnerability analysis was developed based off the Cyber Security Matrix.
- This framework was used to create our threat template to analyze each threat facing UTACC and UTACC’s inherent vulnerabilities.
- The templates also include technical and non-technical security control strategies to mitigate each of the vulnerabilities within UTACC.
“People” Threats

Phishing

Attitude towards emerging technologies

Insider Threat

Autonomy as an Ethical Concern

Maintenance of the UTACC System

Demonstration | (Design/Development) | Employment
“Technology” Threats

- Denial of Service Attacks
- Eavesdropping
- Spyware
- Jamming C2 and Data Link
- Attack on Mobile Devices on a Wireless Network
- Computer Virus Attack on a Wireless Network
- Impersonation and Spoofing of a UGV/UAV
- Spoofing a MAC/IP Address of a UTACC System Component
- Unprotected Information Stored on the UTACC System

Demonstration | (Design/Development) | Employment
“Operations” Threats

- Airspace Integration
- Surface Space Integration
- RECON Team Employment
- Survivability Against EN WPNS
- Environmental Threat
- Terrain
- Shipboard Operations
- Operational Endurance

Human Machine Interaction

Demonstration | (Design/Development) | Employment
Conclusions

Non-Technical Security Controls:
- Policies, procedures and publications must be analyzed to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
- The UTACC system security policies and procedures must be developed to meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
- Adherence to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
- Training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
- Extensive testing with operational units.

Technical Security Controls:
- Remote zeroing of software, data, and cryptographic material.
- Employ tamper resistant technology.
- Independent UGV and UAV operations.
- Redundant and encrypted C2 and data links spread across the EM spectrum.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
Future Research Considerations

- Continuous monitoring and analysis of newly emerging threats, vulnerabilities, and their related security controls.
- New and emerging threats due to changing technologies and relevance to current technologies.
- The patterns of security controls for autonomous systems.
- Changes to the organizational and cultural behavior to accept this new technology.
- Ethical concerns.
- New and emerging technologies to mitigate threats.
Questions?

utacc@nps.edu