2022

Secure Communication for Contested Environments

Hale, Britta

Monterey, California: Naval Postgraduate School

NAVAL RESEARCH PROGRAM
NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SECURE COMMUNICATION FOR CONTESTED ENVIRONMENTS

EXECUTIVE SUMMARY

Principal Investigator (PI): Dr. Britta Hale, Computer Science (CS)

Additional Researcher(s): Mr. Jonathan Lussier, Systems Engineering; Dr. Amela Sadagic, Modelling Virtual Environments and Simulation; Dr. Duane Davis, CS; Dr. Wenschel Lan, Space Systems Academic Group; Dr. Anne Clunan, National Security Affairs; Mr. Joseph Lukefahr, Information Sciences (IS); Mr. Aurelio Monarrez, IS

Student Participation: LT Floyd Lewis, USN, CS

Prepared for:
Topic Sponsor Lead Organization: N4 - Material Readiness & Logistics
Topic Sponsor Name(s): CAPT Andrew Oswald, N4 - Fleet Readiness & Logistics
Topic Sponsor Contact Information: Phone: (703) 695-4758 email:
andrew.j.oswald2.mil@us.navy.mil

This research is supported by funding from the
Naval Postgraduate School, Naval Research Program (PE 0605853N/2098).

Project Summary

Many current communication channels rely largely on interactive cryptographic protocols to establish security. These protocols require real-time roundtrips of synchronous interaction between devices, which makes them susceptible to channel-tear down by adversaries as well as environmental effects—subsequently leading to additional set-up time and an increased electromagnetic footprint. Within a contested environment, such protocol use presents physical vulnerabilities to logistics due to the increased location detectability from the electromagnetic footprint as well as cyber security vulnerabilities. In particular, if an adversary compromises the communications channel, they can gain long-term access to the data. This research looks at addressing this problem through use of secure asynchronous protocols. Protocols supporting asynchronicity limit downtime, offering efficiency benefits under restricted communication. They furthermore have potentially attractive security features such as self-healing security in the event of adversarial compromise of a communications channel. This research applies the Common Aviation Command & Control System (CAC2S) as a case study, framing the environment concerns to the contested restrictions anticipated under contested environments.

Several protocols are identified which offer asynchronicity and could be adopted for naval use. A few cutting-edge protocols support asynchronicity while also implementing greatly increased security features, such as Forward Security (FS) and Post Compromise Security (PCS), which may be able to protect past and future data in the event of a compromise. The Signal and Messaging Layer Security (MLS) protocols are identified as promising candidates for command and control (C2) where asynchronous support or low probability of intercept/low probability of detection (LPI/LPD) are factors. For C2 operations in a contested environment with many different systems communicating with each other, MLS presents a highly promising choice for encrypted communication protocol.

Keywords: *command and control, C2, C2 comms, secure C2, contested environment, Common Aviation Command & Control System, CAC2S, cryptographic protocols, low probability of intercept/low probability of detection, LPI/LPD*

Background

Cryptographic protocols are a critical component in securing C2 links and enabling enhanced security capabilities. While the National Institute of Standards and Technology provides standards for the cryptographic primitives in use (e.g., Advanced Encryption Standard), the cryptographic protocols that bind together such primitives vary in source from proprietary protocols to standards by other organizations. As such, the DoD currently employs a mixture of open standard and proprietary-based protocols depending on the use cases, including the Transport Layer Security (TLS) protocol used for internet connections and 802.11 used in WiFi and for some autonomous device and sensor connections. Symmetric protocols based on manual distribution of keys through use of keyfill devices are also common.

Emerging DoD requirements call for joint C2 interoperability across the cyber domain to meet National Defense Strategy (NDS) objectives as adversaries continue to develop sophisticated anti-access/area denial (A2/AD) capabilities. In fact, not only interoperability of devices but interchangeability—where one device can be used as an ad-hoc replacement for a faulty alternative to achieve mission success—have become critical. The DoD's Joint All-Domain Command and Control (JADC2) concept; the Navy's Project OVERMATCH and the chief information officer

development, security, and operations task force (Weis & Geurts, 2021); and other service initiatives must effectively develop C2 technologies for this future operating environment that is called for by the NDS, this also applies to logistics (Hoehn, 2020). Consider, for example, a fleet unit that must maintain a clandestine posture where providing logistics information would be detrimental to identification by the adversary. Using an unmanned system as a relay, such information (as well as other intelligence) may be pre-loaded and sent to a separate location for C2 transmission, thus obscuring the unit's location.

The overall goal of this work is to present to relevant stakeholders a comparison of secure and sustainable solutions for mitigating emerging cybersecurity threats against C2 links and enabling secure C2 in contested environments. We frame case-study considerations under limited communication environments for the CAC2S—a US Marine Corps system for enabling C2 across multiple platforms. While the case study looks at CAC2S, the results of this work are applicable to multiple similar systems in the DoD. This research investigates both current and proposed alternatives for C2 security protocols to establish interoperability and standardization across the newly proposed Joint Force architecture. Some C2 security guarantees to consider include PCS and FS. PCS is both a newer security guarantee added to the analysis of key exchange protocols and one that has gained increasing prominence and demand in industry. It provides the ability to "lock out" an attacker after full system compromise, under certain conditions, thus allowing for advance planning against potential cyberattacks. It can even be achieved for groups of devices such as is expected under CAC2S operational contexts (Cremers et al., 2021). FS meanwhile ensures protection of data already transmitted, should such a cyberattack occur. These enhancements have the potential to harden security in any environment providing shared intelligence or other data from a known friendly platform.

Findings and Conclusions

This research confirms the applicability of recently developed C2 protocols in contested environments, and the unsuitability of traditional methods to provide security sustainability in LPI/LPD and contested environments. Encrypted C2 protocols of various types were reviewed within the context of current and emerging security concerns for communications in contested environments, as well as each protocol's ease of scalability, handling of lost messages, and recovery of communications after a connection is broken. While legacy style encryption using a single pre-agreed upon key was once thought to be nearly unbreakable, new attack methods and computer performance have changed the paradigm of encryption in the last decades, and the cybersecurity vulnerability window presented by use of such manual key changes presents a risk to logistical concerns.

Great advances have been made in the field of cryptography and cryptographic protocols, some of which enable alternatives to legacy C2 link security options. Techniques like double ratchet algorithms and Diffie–Hellman based key exchange can be used to make encrypted C2 protocols massively more resilient, secure, and able to greatly reduce data compromise in the event of a cyberattack. New and emerging protocols which take advantage of these techniques were reviewed for suitability for the Navy's use-case environment.

One notable emergent protocol, MLS, may be better suited to the Navy when multiple communication channels require C2 management. MLS provides support for message dropping and disconnection recovery, and data protection in the event of compromise via FS and PCS,

meaning that an attacker who successfully guessed a key would only be able to view a few current messages before being locked out (unless they successfully inject updates to keying material at the time of compromise), and would not be able to view any past messages. A Signal connection achieves limited entity authentication after the initial handshake, whereas MLS has authentication values that support optional epoch-level entity authentication (Dowling & Hale, 2021). MLS also offers scalability to large groups and a basis as an international standard, which may benefit the Navy by facilitating ease of adoption and interoperability.

Revised or replaced alternatives to legacy command and control protections is paramount for maintaining security. Cryptographic protocols should be adopted that are resistant to tear down and adversarial attacks.

Recommendations for Further Research

For Messaging Layer Security and other similar protocol candidates, further research is required to understand the pathway and costs towards updating current systems. Research on the potential security limitations of these new protocols and possible security hardening as needed is also suggested, to not only update legacy systems to competitive security levels but look towards future improvements.

References

Cremers, C., Hale, B., & Kohbrok, K. (2021, August 12). The complexities of healing in secure group messaging: Why cross-group effects matter. *30th USENIX Security Symposium*, 1847–1864. https://www.usenix.org/conference/usenixsecurity21/presentation/cremers

Dowling, B., & Hale, B. (2021, September). Secure messaging authentication against active man-in-the-middle attacks. *2021 IEEE European Symposium on Security and Privacy (EuroS&P), 54–70*. https://doi.org/10.1109/EuroSP51992.2021.00015

Hoehn, J. R. (2021). *Joint All-Domain Command and Control: Background and issues for Congress* (CRS Report No. R46725). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46725/2

Weis, A. D., & Geurts, J. F. (2021, January 15). *Department of the Navy DevSecOps Task Force* [Memorandum]. Department of the Navy Chief Information Officer. https://www.doncio.navy.mil/ContentView.aspx?id=14287

Acronyms

A2/AD anti-access/area denial
CAC2S Common Aviation Command & Control System
C2 command and control
FS Forward Security
JADC2 Joint All-Domain Command and Control
LPD low probability of detection
LPI low probability of intercept
NDS National Defense Strategy
MLS Messaging Layer Security

PCS Post Compromise Security
TLS Transport Layer Security