1. Introduction

Since the launch of its first satellite in 1958, the United States has been interested in protecting its on-orbit assets. In order to maintain custody of its satellite inventory, and to predict and prevent collisions, the United States monitors the locations of objects in orbit. This monitoring is accomplished by the Space Surveillance Network (SSN), which is managed by U.S. Strategic Command (USSTRATCOM) and staffed by 14th Air Force. The SSN currently tracks more than 20,000 orbital objects larger than 10 cm in diameter, and the data provided by the SSN form the most important source of space situational awareness (SSA) in the world.[1] While the SSN is one of the most important sources of data concerning the locations of objects orbiting Earth, data provided by the SSN have two significant drawbacks when it comes to tracking operational satellites. First, the tracking data obtained by the SSN are significantly less accurate than the active tracking information held by each satellite's operator. Second, operational satellites can perform active maneuvers, which cannot be predicted by a passive surveillance network. This means that the SSN will have inherent delays in detecting and processing such maneuvers, which, in certain cases, may result in the SSN temporarily losing track of the object.

Operational satellites are the most important satellites to track, but the passive tracking techniques used by the SSN do not provide the most accurate positioning information. The most accurate information comes from on-board instrumentation, such as star trackers and positional gyroscopes, but this information is available only to the satellite operator. Since satellite operators maintain accurate tracking information for only their own satellites, sharing this higher-fidelity information between satellite operators could provide significantly better tracking information than what can be obtained by non-cooperative means. As an example, a comparison of cooperative and non-cooperative tracking data for Global Positioning System satellites found that cooperative tracking data reduced mean positional error by 88 percent.[2]

[1] Brian Weeden, Paul Cefola, and Jaganathan Sankaran, "Global Space Situational Awareness Sensors," presented at the 11th Advanced Maui Optical and Space Surveillance (AMOS) Technologies Conference, Maui, Hawaii, September 16, 2010.

[2] T. S. Kelso, David A. Vallado, Joseph Chan, and Bjorn Buckwalter, "Improved Conjunction Analysis via Collaborative Space Situational Awareness," presented at the 9th Advanced Maui Optical and Space Surveillance (AMOS) Technologies Conference, Maui, Hawaii, September 19, 2008.

Cooperative Tracking and Data Sharing Today with Trusted Providers

In 2008, a group of commercial SATCOM (satellite communications) operators maintaining satellites in the geostationary belt joined together to share data in a prototype program run by the Center for Space Standards and Innovation (CSSI), a subsidiary of Analytical Graphics, Inc. (AGI). Operators shared their private data, and CSSI's software tool SOCRATES (Satellite Orbital Conjunction Reports Assessing Threatening Encounters in Space) generated automatic notification of close approaches.[3] This service was later expanded to incorporate tracking of satellites in low Earth orbit (LEO). This system requires that all participating operators trust CSSI with their private data.

This prototype system was extended in 2010, when AGI was selected by the Space Data Association to develop and run the new Space Data Center. The Space Data Center now uses the shared (private) data to perform 300 high-accuracy conjunction analyses twice per day for objects in both geosynchronous orbit and LEO.[4] Like its predecessor, this service requires participating operators share their data with a trusted third party.

Cooperative tracking is also provided by the Joint Space Operations Center (JSpOC) under USSTRATCOM. The JSpOC uses (passively obtained) SSN data to maintain a catalog of two-line element sets (TLEs),[5] which it makes public via the Space-Track website. In addition, the JSpOC maintains a high-accuracy catalog, which is not made available publicly. The high-accuracy catalog uses information from SSA sharing program partners (who have entered into an agreement with USSTRATCOM) to provide more accurate position information for satellites operated by program partners. The high-accuracy catalog is used internally by the JSpOC to perform conjunction analyses, and satellite operators are warned of potential conjunctions involving their satellites regardless of whether they are SSA sharing program partners.

Participation in these services indicates that operators place a high value on the ability to perform conjunction analyses on high-fidelity data.

Trust and the Need for Coordination

Sharing programs like those described above require satellite operators to trust the database operator (e.g., AGI, JSpOC). This provides a significant barrier to adoption and

[3] Center for Space Standards and Innovation, Satellite Orbital Conjunction Reports Assessing Threatening Encounters in Space (SOCRATES), online.

[4] T. S. Kelso, "How the Space Data Center is Improving Safety of Space Operations," presented at the 13th Advanced Maui Optical and Space Surveillance (AMOS) Technologies Conference, Maui, Hawaii, September 16, 2010; Space Data Association, "Space Data Center Attains Full Operational Capability Status," press release, September 9, 2011.

[5] A two-line element set (TLE) is a data format used to convey sets of orbital elements that describe the orbits of Earth-orbiting satellites.

hence decreases the utility of these systems. Some operators are unwilling to share their data with an outside party, and those that do must pay a premium for these services.

The need for cooperation among operators and the inherent problems of mutual trust have been widely recognized in the literature.[6] Although the problems caused by a lack of data sharing between operators are well-known within the satellite community, there are currently no solutions in place that do not require operators to agree on a trusted party with whom to share their private orbital information.

Purpose and Organization of This Report

In theory, cryptographic tools such as secure multiparty computation (MPC) have the potential to improve SSA. In practice, however, implementations of these cryptographic algorithms have been too slow to be useful in their intended application.

The primary research objective of this project was to determine whether modern implementations of MPC protocols could be made fast enough to present a practical alternative for computing conjunction analyses on private data.

This report begins with an outline of the cryptographic tools known as MPC protocols, which allow stakeholders to perform functions (such as orbital conjunction analyses) that utilize inputs from each party while maintaining the secrecy of the inputs. Although MPC is not currently in use by satellite operators, it has been the subject of intense study in the cryptographic community, and general-purpose software libraries for building MPC protocols currently exist.

Chapter Two provides a technical introduction and overview of the major protocols in the cryptographic literature. Chapter Three analyzes whether MPC protocols can be made fast enough to be practical for securely computing conjunction analyses. Chapter Four summarizes the key findings and discusses how the Air Force can take steps to implement them as part of its role in preventing orbital collisions. The Appendix reviews the mathematical techniques that are used to convert a continuous integral (e.g., a conjunction analysis calculation) into an arithmetic circuit using only addition and multiplication operations.

[6] Jeff Foust, "A New Eye in the Sky to Keep an Eye on the Sky," *The Space Review*, May 10, 2010; Institut français des relations internationals, "Assessing the Current Dynamics of Space Security," presented at SWF-Ifri workshop, Paris, June 18–19 2009; Tiffany Chow, "SSA Sharing Program," Secure World Foundation Issue Brief, October 5, 2010; Kelso et al., 2008.