Developing a Secure Framework for Space Domain Awareness (SDA)

William M. Allington, Kyle Bowen, Abigail Peterson
Center for Cybersecurity & Data Science, Ferris State University

ABSTRACT

This paper provides a high-level risk analysis of a theoretical Confederated Space Domain Awareness (CSDA) corporation. We utilize the Process for Attack Simulation and Threat Analysis (PASTA) framework to enumerate the threats that are posed to this structure of Space Domain Awareness and propose general risk mitigation solutions that CSDA stakeholders could utilize to reduce their attack surface. This will not be an in-depth exploratory examination of hard technical details, but a general overview of network structure and threats.

1. Literature Review

Due to the novelty of this paper, there are limited amounts of existing public research. However, at least two papers have been written regarding cybersecurity in Space Situational Awareness (SSA). James Pavur and Ivan Martinovic published a paper in 2021 for the ACM Asia Conference on Computer and Communications Security. [11] In it, they discuss using a Random Forest Classifier in conjunction with a voting mechanism to identify a hypothetical SSA provider falsely classifying their spy satellites as debris to conceal their nature. Also in 2021, Pavur published a doctoral thesis for the University of Oxford regarding Satellite Cybersecurity.[10] While most of the thesis lies outside of the scope of this paper, part three, chapter nine focuses on SSA. In this section, they expand upon the previous paper, discussing an alternative attack. An attacker may, if able to access an SSA repository, manipulate SSA data to falsely generate Conjunction Data Messages (CDMs) and force an operator to expend fuel maneuvering a satellite avoiding a collision that would have never occurred. In the same vein, an attacker could prevent CDMs from being generated for an operator, resulting in the destruction of a satellite. A key consideration of both papers is the threat of information integrity attacks, which will be further discussed during our risk assessment.

Outside of these two papers, SSA security broadly falls into two topics. The first relates to confidentiality. Most papers discuss the balance between secrecy requirements and useful data-sharing to avoid collisions. Brian D. Green discusses this in his 2014 paper, [4] proposing an increase in voluntary bilateral and multilateral agreements between SSA providers but doing so while preserving state secrets. Harvey Reed (et al) proposes using the Space Information Sharing Ecosystem to provide what they call the “Minimum Viable Information” to others in a decentralized system, keeping proprietary and sensitive information within the boundaries of the actor. The other topic relates to the accuracy of the data. Dr. Matthew Hejduk testified before Congress in 2022, [6] citing concerns with autonomous maneuvering of satellites (discussed later) and inaccurate uncertainty elements in commercial ephemerides. He also stated that, while with diminishing returns, tracking objects below 10cm (about 3.94 in) could be useful to certain members of the private industry. Laura K. Newman and her co-authors in their paper [9] inform us that NASA utilizes Conjunction Data Messages (CDMs) rather than Two Line Element sets (TLEs) when performing conjunction assessment and risk analysis, due to containing Covariance data, and higher-level modelling of orbital perturbations. Even CDMs contain some issues, including risk for cross-correlation errors in the covariance data, and covariance not in a normal distribution when assessed in a cartesian coordinate system.

2. Introducing the Confederated Model of Space Domain Awareness

The design of this research depends on a novel, hypothetical model for interconnected SDA systems. We are calling this idea a *confederated* model of SDA (CSDA). The CSDA model is distinguished at the organizational level. Entities that depend on space-domain assets as part of their mission would partake in managing and equipping a confederated SDA network. All participants would have access to frequent intelligence updates, as they pertain to

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

space traffic management or collision avoidance. A confederated SDA would act as a vendor within the collaborative domain of shareholder entities. The internal mission of a CSDA network would be the collection of space domain data, as well as the creation and management of channels for SDA data sharing. The primary mission would be the prevention of collisions between traveling space assets. Such an organization could assist in the responsible management of orbit space. Creating value for the benefit of aerospace and related industries, and public safety.

This model serves two purposes in this paper. Firstly, it is our assertion that this model is the most likely to develop as a sustainable enterprise outside of a military or government context. The cost of building an SDA network is outside the reach of most private organizations. A report from the Government Accountability Office (GAO) in 2015 stated that $5.5 billion would be used to enhance the national infrastructure for SSA [5]. This indicates that a cost-sharing model, such as CSDA, will be necessary for private organizations to participate in SSA/SDA activities into the near future. Secondly, the CSDA model presents a unique challenge for threat analysts. The interconnections mediated by such a system would require information sharing between competitors, and some form of reporting to non-participant entities to avoid collision. This makes a CSDA model a unique subject of threat analysis as it accentuates the natural threat boundaries inherent to any SDA/SSA network.

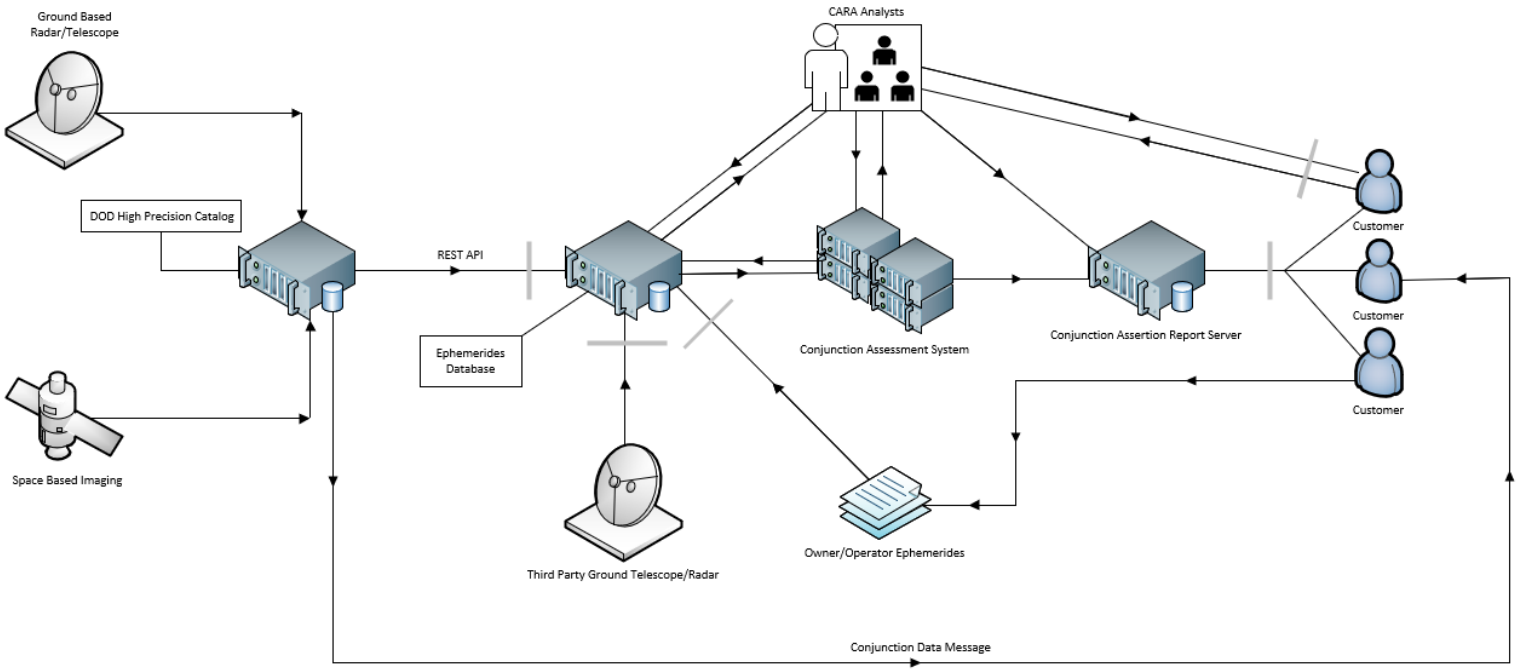

Fig. 1 An example diagram of a Confederated SDA Architecture

The above diagram is not designed to show the detailed network diagram of a specific organization. Instead, this represents a broad overview of the information flow, with external trust boundaries, illustrated by the gray lines in the diagram. Starting on the left, the U.S. Department of Defense gathers information from their assets. While ground based assets are the only items disclosed, space-based assets are not outside of the realm of possibility. From there, ephemeris data is placed into the High Precision Catalog. The commercial operator can then utilize a REST API to gather ephemeris data that corresponds to orbits their customers are in. This is placed into a database of ephemeris data gathered for the next few days, either from Owner/Operator Ephemeris files provided by their customers, or non-cooperative ephemeris data provided by third party assets. This would be ingested into a

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

database and run through a Conjunction Assessment System. The Conjunction Assessment System produces a probability of collision between all assets input into the system. The floor and ceiling are controlled by embedded operators within the software. Assets with a probability of collision above the ceiling are marked for analysts to evaluate, and work with customers to ensure appropriate action is taken. Assets with a probability below the floor are ignored, and those between the floor and ceiling are monitored closely for a change in probability. Reports are automatically generated and placed within a Conjunction Assertion Report Server for customers. There are several potential ways that these reports could be transmitted to the customers, either with another REST API, via email clients, or it could be accessed manually via a web interface.

The most important avenue of information flow within this model would be supplied through the Department of Defense. The sophisticated network maintained by the DOD provides the CSDA with a validating mechanism for integrity support. Advanced data analysis can be developed over time using data collected using CSDA and verified through public channels. For a CSDA network, Conjunction Data Messages are produced and communicated when triggered. This occurs when the conditions indicate a moderate probability of collision; given that the data shows a high degree of confidence based on the empirical data. Email or application alerts would be forwarded to stakeholders directly. They may also be contacted by the CSDA's Conjunction Assessment and Risk Analysis Team.

Communication with stakeholders continues through pre-determined channels, throughout the reporting process. Plans to maneuver the spacecraft out of harm's way are developed from a set of options identified by the automated system based on environmental data combined with the known limitations of the vehicle. These paths are verified as safe by the analyst team, and a set of commands is communicated via the system owner's ground station. The CSDA organization will not have the privileges needed to alter the spacecraft. This maneuver plan will be inputted into the Conjunction Assessment System, and new risk values are assigned to the asset. This continues until a safe maneuver plan is determined.

3. Methodology

The primary design of this research is to apply threat modeling procedures to the CSDA model of space domain awareness. Our hope is that by applying this design to a viable model of privately managed SDA, we can identify the areas where vulnerabilities in the design can be generalized. This will create a foundational basis, on which SDA enterprise solutions might rely when designing their architecture. We have chosen the PASTA method of threat analysis. PASTA is an acronym for Process for Attack Simulation & Threat Analysis. PASTA is a risk focused threat modeling process used to identify and prioritize evidence-based threats and their mitigation [8]. The PASTA threat model is well-suited to this design, because of its emphasis on risk analysis. Enumerating the potential threats, vulnerabilities, and vectors within a confederated model is a first step towards identifying any potential mitigations that could be built into the design of future SDA enterprises. This foundation could serve as the basis for building security into SDA from the onset.

4. Introducing PASTA

The creators of PASTA threat-modeling describe seven stages as the process of their design. These stages are as follows: *defining the purpose and objective(s) of the asset*, *defining the technical scope*, *deconstructing the data flow of the application*, *threat analysis*, *vulnerability analysis*, *attack analysis*, and *risk impact analysis* [8]. Within the PASTA framework, emphasis is placed on the business function of the information system [8]. An effective model of that business function will enumerate the communication channels within that system, including the internal boundaries found within the organization. Monitoring both internal and external communication boundaries allows threat analysts to classify potentially sensitive information transfers more easily, at all points in the system architecture. While also providing some basis for assuming the potential motivations of threat actors. Applying this unique model helps the analyst to determine the likelihood of a threat event occurring with the same level of granularity for insider threats as external threat actors. Prioritizing the analysis of actions occurring through stages of the business process facilitates the mitigation of risk in the most efficient and meaningful manner possible.

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

5. Applying the PASTA Model of Threat Analysis

Purpose and Objectives

Defining the purpose of any SDA system is a straightforward analysis. The confederated model does not fundamentally change the purpose. Space-Domain Awareness networks are designed for the specific and limited purpose of collecting accurate information regarding the environment of orbital space. The monitoring technologies are directed over a particular area of space and are limited to a particular distance. SDAs connect multiple instances of radar and optical devices, space vehicles, and ground stations to create a data fusion space. This aggregated data is cleansed of errors, and the results can be communicated as reasonably confident assertions of location. Due to the nature of orbital travel, it is relatively easy to make predictive assertions regarding an object's future location at a given time. By combining the probable locations of multiple objects, it is possible to detect and prevent collisions well before they become near-miss events or catastrophic incidents.

Following this simple operational model, we can safely claim that the purpose of a CSDA is to prevent collisions in orbital space by providing early detection and warning. This larger purpose can be weighed against the limitations of any business project, in the sense that it must create value for the business owners. In the case of CSDA, the value of such a system is generated by protecting the assets of stakeholder entities. Objectives must be integrated into the purpose of a system, and thus we can describe several that facilitate the mission of a CSDA network.

A well-functioning CSDA will generate assertions and make predictions that are reliable and accurate. These predictions must be produced and communicated to affected owners well before a potential collision or near-miss event occurs. Access controls must be implemented to prevent the unauthorized modification or delaying of data throughout each boundary within the information system. Redundancy and fail-over capabilities will protect the investment of the organization, and its stakeholders. Confidentiality of internal or architectural data must be protected from unauthorized disclosure, and the communication of data produced by the system should only be permitted to occur through the intended channels. Finally, these predictions must be accurate from the onset of production-level deployment but should also utilize the data generated and collected to become more accurate over time. The implementation of advanced analytics and machine learning solutions should be included from the onset of development planning stages.

Defining the technical scope of an SDA system

There are a few pieces of technology that are required to ensure CSDA operations are successful. Network gateways are required to ensure simple communication to the High Precision Catalog and to customers, while large databases are required to store aggregated data. A platform capable of supporting high resolution orbital predictions is required, given the amount of processing being performed it may leverage cloud computing. On top of this platform an application must be capable of performing this analysis. Analysts require high-performing personal computers and access to large parts of the SDA system. Firewalls are required for basic security needs, and likely an organization of this size has an Intrusion Detection System or Intrusion Prevention System.

Deconstructing the Data Flow

Data is generated in one of two ways. Non-cooperative ephemeris data is gathered by ground-based assets such as radars or optical telescopes. Cooperative ephemeris data is provided by Owner/Operators to the CSDA. This data can be provided in several formats, from Two Line Element Sets to Orbital Ephemeris Message files. This data is ingested by the CSDA and aggregated in a database. Once the necessary data has been gathered, automated software ingests this data and produces probabilities of collision between all objects in the system. Certain information is transmitted to analysts for analysis, while other information is automatically placed into reports by the software and transmitted to a database. Customers can access this database and gather reports for their space vehicles. Analysts may also open additional channels of communication to customers who operate space vehicles with high probabilities of collision.

Threat Analysis

Space assets are uniquely vulnerable to cyberattacks. This is due to many factors, but most importantly the high cost of developing, launching, and maintaining space systems, as well as the need to operate many space assets through exclusively remote channels. This combination of factors makes space systems a high-value target for threat

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

actors. Illicit access to space systems will generally target one or both primary subsystems. These subsystems will be either the control mechanisms that allow the spacecraft to maneuver while in orbit, or the payload mechanisms that allow the spacecraft to fulfill its mission function. Affecting the confidentiality, integrity, or availability of either subsystem will cause serious harm to the mission of the space system. In cases where a threat actor gains the level of access required to maneuver a spacecraft, this poses a serious threat to all space assets within that orbital space, as the resulting debris from collisions has potential to initiate a larger chain of collision events.

An SDA or CSDA system will face a similar threat landscape. Threat actors could view a vulnerable SDA network as an opportunity to exploit the SDA infrastructure for their own purposes. The most serious risk posed by threat actors to SDA systems is within the domain of affecting data integrity. Persistent and privileged access would allow threat actors to modify the assertions produced by an SDA system, thus resulting in unreliable and inaccurate data. A long-term strategy could take shape over time by poisoning training data before it can be digested by a machine learning system. If flight decisions are made based on this information, the result could be as severe as destroying space assets by manipulating a collision.

The types of threat actors most likely to attack an SDA system include, in rough order of likely success: Advanced Persistent Threats, criminal organizations, organized hacking groups, and script kiddies. APT organizations carry the highest level of risk and the most severe impact if successful. The threat organization known as Fancy Bear is reported to have successfully targeted space systems in recent years (Vasquez, 2022) APTs are generally funded or supported by nation-state actors to support political objectives through espionage, ransoming, or destruction of assets [3]. The level of access to space systems afforded to a CSDA system would represent a high value target due to the model's inherent function as a bridge between multiple organizations. The large pool of resources available to APTs allows them to operate with more patience than other threat actors. They are more inclined to deploy a more effective strategy of long-term exploitation [3]. This form of attack is generally hard to detect and even more difficult to eradicate upon detection [3].

Criminal organizations and organized hacking groups will generally operate with similar levels of resources and technical expertise [2]. The illegality of their actions creates an incentive to minimize the time investment for attack campaigns. They generally prefer to target low-hanging fruit to maximize their return-on-investment. An SDA organization must take the necessary precautions to avoid making themselves an easy target. The most typical intention of illicit access by criminal entities is a ransomware attack. Thus, the intention is to affect the availability of assets to extort money from the victim. A CSDA organization would be especially vulnerable because the data generated by the information participates in the protection of assets. Also, the cooperative nature of a CSDA implies that each stakeholder will seek to minimize their losses in the event of an outage. This would result in increased pressure to pay a ransom if affected by ransomware.

The term *script kiddie* refers to amateur black-hat threat actors with minimal expertise or access to resources [1] Similarly to organized hacking groups, they are inclined to target low-hanging fruit to exploit systems. Generally, they act without regard for any specific target because their primary intention is to affect a system to demonstrate their prestige as an amateur [1]. The impact of an attack will range from minimal to severe, depending on the individual level of expertise. It is less likely that a threat actor at this level will have the technical skill to cause serious, long-term damage to an SDA. It is also unlikely that they will operate within the system for a considerable time without detection.

Vulnerability Analysis

Any number of vulnerabilities may be found throughout an SDA network. These points of weakness on the attack surface can be identified by locating the trust boundaries within an architecture. These boundaries are significant within a CSDA framework, as the coordination of organizations within this model requires additional trust boundaries that delineate the limits of communication between entities with competing missions. Vulnerabilities may exist on the external or internal boundaries of an information system. In cases where the vulnerability is identified on an external boundary, exploitation will result in network intrusion. For vulnerabilities within the functional boundaries of a system, exploitation can result in privilege escalation, arbitrary code execution, and or data exfiltration. Organizations embed multiple layers of security controls into their architecture to prevent a single point of vulnerability from leading to a catastrophic security breach. This principle is known as *defense-in-depth.* The Confederated model of SDA encourages an organization to build an architecture with this principle in mind, because doing so helps to prevent any accidental disclosure of proprietary data to other stakeholder

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

organizations. This reinforcement of trust boundaries helps to proactively mitigate the impact of extant vulnerabilities within a CSDA network.

The architecture of an SDA will ultimately determine the vulnerabilities within the network. However, there are essential qualities that will be shared by all SDAs, and the CSDA model is intended to accentuate these boundaries. As a cyber-physical system, an SDA relies on complex sensory equipment, radio transmission hardware, networking technologies, analytics software, machine learning software, database software, server equipment, interface technologies, and human effort to operate. Vulnerabilities identified within these components are most likely to be identifiable at the margins of operation. The points of interconnection within the system.

The hardware used for sensory data collection is unlikely to be the initial access point for an attacker. While this equipment initiates the SDA functional process, it cannot be reached without prior access to a networked component, or through physical access and exploitation. The same can be said of radio transmission equipment, except when considering risks to the availability of information produced through radar emission. Radio transmission is susceptible to jamming by threat actors with the ability to generate a more powerful signal within the same frequency bandwidth [7]. These could be viewed as downstream targets for a successful threat actor. Hardware vulnerabilities can be difficult or impossible to patch, but they also require physical access to a device. They may be inaccessible to threat actors, outside of corrupt or malicious employees.

The most likely boundary to target for initial access would be human actors. Social engineering tactics such as phishing attacks can be used to gain a foothold into an SDA network. An organization is vulnerable to social engineering when employees lack the training, time, or incentive to identify these threats as they occur. Software is also a potential source of vulnerabilities within an SDA system. Upstream supply-chain attacks can affect any computer system that depends on the software to complete its business function. Vulnerabilities may also be present in any version of a software program, which may be undetectable until the time it is discovered and patched. These situations are the preconditions for *zero-day* attacks. Nearly all organizations are vulnerable to zero-day attacks, so controls such as defense-in-depth and other mitigating techniques should be deployed.

Attack Analysis

The breadth of what we have defined here has opened many doors for attempting to access SDA systems. There would likely be two major end goals for an attacker accessing SDA systems. The first would be deployment of ransomware onto mission critical systems, earning the attacker a large amount of income. The second would be an APT attacking data integrity, manipulating data to their own ends. We will start with the low technical options for an attack, and work towards more highly technical options that require nation state resources to attack.

An attacker may begin with social engineering, with the goal of compromising the analyst accounts. The 2023 Verizon Data Breach Investigation Report states that social engineering is one of the top three attack patterns detected in 2023 [12]. To effectively analyze data, analysts are required to have broad privileges, and phishing with the goal of compromising the account and pivoting to other devices on the network is a straightforward means of attacking the CSDA system. Another form of attack may be an SQL injection against the ephemerides database, allowing for injection of malicious content, or may result in data required for SDA disappearing [12]. An attacker with low technical skill may be able to launch a denial-of-service attack between the CSDA system and the customers, preventing necessary communication from being able to be received.

More complex attacks may require significant investment but reap high rewards. An APT could interfere with the software development pipeline of the Conjunction Assessment system, allowing for any number of results, from backdoor access to arbitrary remote code execution. This would be on a similar technical scope to the SolarWinds attack in 2019. An APT could also attack the ephemerides in the database, manipulating the data to produce false Conjunction Data Messages. The severity of this attack could range from overwhelming analysts, meaning real conjunctions may be missed, to encouraging a collision between two space vehicles as the best maneuver in the false data forces a conjunction event.

A key aspect of an APT attack would be avoiding detection and establishing persistence. Subtle changes to the data would be preferred, and one may spend substantial amounts of effort to avoid detection, from erasing certain log files to living off the land. If an attacker wanted to just observe data passing through, and be as transparent as possible, ARP cache poisoning may be the best solution as it would allow interception of every packet that runs through the network. An attack that becomes more noticeable would be poisoning the training data for machine learning algorithms, which actively interferes with the progression of the algorithm.

Risk and Impact Analysis

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Combining the information derived from all other steps in our application of PASTA throughout this report. We can start to draw conclusions about the lingering risks within a CSDA model. From there, we can derive a strategy for addressing those risks. Though we must acknowledge that solutions will be dictated according to the risk appetite of the organization in question. We may be able to assume that a cooperative venture, such as CSDA, would tend towards a low-risk appetite. At least in part because each stakeholder would prefer to maximize the return on their portion of the cost burden for development and maintenance of the organization.

The analysis within this research can assert with a high degree of confidence that the highest risk inherent to an SDA network is the integrity of data. Any component within the system that contributes to the forming and communication of space domain information must employ controls that facilitate information assurance. Reliability and accuracy are the cardinal virtues of an SDA network. Examples of controls that contribute to mitigating risks to data integrity would include, but are not limited to, the use of encrypted and digitally signed transmissions across trust boundaries, file integrity monitoring, and federated user authentication mechanisms. These controls must be implemented at all levels and with defense-in-depth considerations embedded into the architecture. Levels of implementation should include administrative, technical, and physical controls.

To protect the availability of CSDA data, a strategy of risk avoidance and mitigation is recommended. Risk avoidance may be best achieved using redundant configurations and data backup practices. Risk mitigation to protect the availability of SDA data involves the early detection of intrusion, and thus includes controls to be implemented at all levels, as well as strong incident response procedures. The ability to recover from a security incident will minimize the time when operators are unable to monitor space assets. At the policy and planning levels, the creation of business continuity and disaster recovery procedures are integral to a speedy recovery following an outage.

The primary focus of efforts to protect the confidentiality of information within an SDA should be focused on internal and architectural information on which the system relies. The data produced through SDA operations should be controlled, but absolute confidentiality is not a priority. The data is intended to be communicated to both internal and external parties. Digital signatures and encryption should be deployed, but primarily to ensure that authenticity is verifiable for information recipients. Access control mechanisms and similar internal security technologies must be deployed effectively, as they protect the internal boundaries and integrity of CSDA information.

6. Research Limitations

This research is based on an imperfect representation of an emergent technology. The novelty of connected space technology, and the high cost-burden of operating in the space sector contribute to a dearth of available data on near-miss incidents in orbital domains. There are few sources of SDA information that are available to the public. Due to the confidential nature of many space technologies, in part due to their use as instruments of national security, we were unable to identify the full range of specific technologies deployed across modern SDA systems. Additionally, the application of threat modeling frameworks to cyber-physical systems can be difficult without significant financial resources. We were unable to procure the technology that would be required to perform real-life attack modeling, and thus we relied entirely on speculative claims. Future research in this area will allow for a more realistic examination of the potential attack landscape for SDA networks as the technology becomes more developed and accessible to researchers.

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

References

[1] Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

[2] Cloud Security Alliance. (2022, December 4). *Threat #10 to cloud: Organized crime, hackers, and apt: CSA*. Threat #10 to Cloud: Organized Crime, Hackers, and APT | CSA. https://cloudsecurityalliance.org/blog/2022/12/04/top-threat-10-to-cloud-computing-organized-crime-hackers-and-apt/

[3] Cybersecurity & Infrastructure Security Agency. (n.d.). *Advanced persistent threats and nation-state actors*. Advanced Persistent Threats and Nation-State Actors | Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors

[4] Green, B. D. (2014). *Space Situational Awareness Data Sharing: Safety Tool or Security Threat?*

[5] Gruss, M. (2015, October 19). *U.S. plans $6 billion investment in Space Situational Awareness*. SpaceNews. https://spacenews.com/planned-u-s-investment-in-space-awareness-is-6-billion-gao-says/

[6] Hejduk, M. (2022). *SPACE SITUATIONAL AWARENESS: GUIDING THE TRANSITION TO A CIVIL CAPABILITY HEARING BEFORE THE SUBCOMMITTEE ON SPACE AND AERONAUTICS HOUSE OF REPRESENTATIVES ONE HUNDRED SEVENTEENTH CONGRESS SECOND SESSION*. https://www.congress.gov/event/117th-congress/house-event/114695/text

[7] Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* Chatham House. The Royal Institute of International Affairs.

[8] Morana, M. M., & Vélez, T. U. (2015). *Risk centric threat modeling process for attack simulation and threat analysis* (1st ed.). John Wiley & Sons, Inc.

[9] Newman, L. K., Mashiku, A. K., Hejduk, M. D., Johnson, M. R., & Rosa, J. D. (2019, August). *Nasa Conjunction Assessment Risk Analysis Updated Requirements Architecture*. In AAS/AIAA Astrodynamics Specialist Conference (No. AAS 19-668).

[10] Pavur, J. (2021). *Securing New Space: On satellite cyber-security* (thesis).

[11] Pavur, J., & Martinovic, I. (2021). *On detecting deception in space situational awareness*. 280–291.

[12] Verizon. (2023). (rep.). *2023 Data Breach Investigations Report*.

Copyright © 2023 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com