CyberSecurity for Aerospace Autonomous Systems

Jeremy Straub*
Department of Computer Science, University of North Dakota, Grand Forks, ND, USA, 58202-9015

ABSTRACT

High profile breaches have occurred across numerous information systems. One area where attacks are particularly problematic is autonomous control systems. This paper considers the aerospace information system, focusing on elements that interact with autonomous control systems (e.g., onboard UAVs). It discusses the trust placed in the autonomous systems and supporting systems (e.g., navigational aids) and how this trust can be validated. Approaches to remotely detect the UAV compromise, without relying on the onboard software (on a potentially compromised system) as part of the process are discussed. How different levels of autonomy (task-based, goal-based, mission-based) impact this remote characterization is considered.

Keywords: Times Roman, image area, acronyms, references

1. INTRODUCTION

High profile breaches have occurred across all types of information systems: from business systems to systems that manage and support guidance, navigation and control. One area where these attacks are, perhaps, among the most problematic is autonomous control systems. Unlike manual control approaches, where typical verification and non-repudiation techniques can be used to verify that the two communicating parties are who they claim and transmissions have not been altered in route, autonomous systems present a distinct challenge. An autonomous system can, prospectively, be compromised by attacks against the AI (which seek to control it, overwhelm it or otherwise) as well as attacks against the supporting systems which the AI relies upon.

This paper considers the aerospace information system with a particular focus on elements that interact with autonomous control systems (e.g., onboard UAVs). It discusses the trust that is placed in the autonomous systems and supporting systems (such as navigational aids) and how this trust can be validated and if it is well placed. It considers technologies that would support reducing the reliance of the next generation of autonomous control software on these external information suppliers and validation techniques that could be used to determine when to transition from the less computationally expensive (and prospectively more accurate) external positioning technologies to other positioning systems. It also discusses approaches to remotely detect the compromise of UAVs, without relying on the onboard software (on a potentially compromised system) as part of the process and how different levels of autonomy (task-based, goal-based, mission-based) impact this remote characterization. The paper concludes with a discussion of the impact of information warfare on autonomous systems and their efficacy and ethical questions regarding their deployment when their security may be questionable.

2. BACKGROUND

Complete coverage of the topic of cybersecurity is far beyond the scope of this article; however, several key elements are introduced which inform and serve as components of the proposed solution for a MWPT system. Cybersecurity necessarily takes a system-of-systems approach [1], with numerous areas of system functionality being required and presenting opportunities for the malicious to prospectively exploit. The complexity of systems has led to the use of game approaches [2] and simulation [3] for identifying prospective vulnerabilities and defects – an implicit acknowledgement that formal verification techniques are not practical for ill-defined and complex systems.

Cybersecurity processes can be subdivided into two categories: those that aim to create barriers for security purposes (such as firewalls [4] and some anti-virus [5] functions) and those that seek to detect anomalies [6-8] and attacks underway [9-11]. Security has been extensively considered in the context of Supervisory Control and Data Acquisition (SCADA) systems [12-14], many of which were developed long before the modern security landscape evolved and have been retrofit for network connectivity. While SSPS and MWPT would not have the retrofitting problem, prior work on securing power systems informs this current work.

Unmanned Systems Technology XVII, edited by Robert E. Karlsen, Douglas W. Gage,
Charles M. Shoemaker, Grant R. Gerhart, Proc. of SPIE Vol. 9468, 94680M

3. EXAMPLE USE SCENARIO – SPACE SOLAR POWER

Cybersecurity is part of a larger area of consideration: system assurance. This section, thus, considers the assurance needs of a MWPT system, identifying which raise non-cybersecurity considerations, considerations that partially relate to (or are resolved / mitigated through) cybersecurity and fully cybersecurity considerations. The next section discusses each of the identified cybersecurity needs in greater detail and the subsequent section discusses how the can be resolved.

Assurance can be subdivided into two categories which can be effectively summed up as (1) making sure that required actions happen and (2) preventing prohibited actions from happening. Considering the needs of a MWPT system from this category identifies a number of items in each category.

Required actions that must be assured to happen include supplying power at times to locations required of the requisite level and generating power of the amount required. Communications capabilities must be assured. Onboard computing, which is required for controlling the spacecraft, must also be guaranteed. Finally, the position determination and control system must be assured to work as must the attitude determination and control system.

Prohibited actions that must be prevented begin with the important goal of preventing overheating. The assurance process must also prevent any discharge of transmitted power to unintended targets or at incorrect times. The assurance process must also insure that power transmission does not occur within requisite safety margins. It must also prevent transmission when non-participating craft are in the way, when an attitude or position fix problem exists, or another problem is occurring.

The cybersecurity needs of a MWPT system are a subset of the assurance needs of the system. While a subset, they relate to all of the aforementioned categories. While a wide variety of occurrences can impair system performance and must be proactively assured against or assured to happen, cybersecurity is primarily concerned with three areas: onboard software operations, ground station software operations and transmission link security. In the first two categories, malware or other attack could prospectively cause the system to be activated at incorrect times, either via changing the definition of when appropriate operating times and locations are or be confusing the system in to believing that the time or its position, orientation and other characteristics are different than they are. An exploit in either of these areas could also result in the system being directly commanded into an override mode where assurance mechanisms to prevent against unintended operations are bypassed.

Transmission link security could cause similar issues. It may result in incorrect position, time or orientation knowledge and breaches could provide a vector for attacks against and the exploitation of vulnerabilities in either the ground or onboard software.

Also problematic is the fact that an exploit in any of these areas may place the spacecraft into an inconsistent state where further command is not possible but anyone, or where the owner/operator's command capabilities are denied, but a third party attacker retains control. This last situation is perhaps the most problematic as it not only loses in the usability of the asset, but may result in some or all of the desired actions not occurring (e.g., supplying power to required locations) as well as any number of the undesired actions (e.g., sending power to an incorrect location) occurring. Finally, the spacecraft may be used to impair the operation of other spacecraft through physical collision, if third-party control is gained.

4. SOLUTION FOR EXAMPLE USE SCENARIO

A multi-faceted cybersecurity solution is proposed for the MWPT system discussed. This system is comprised of multiple parts (in the parlance of space mission design, these parts are referred to as segments, which may be comprised of one or more components). An overview of these parts is presented in Figure 1 (and loosely based on the system architecture presented in [15]) First, the ground segments (command/control stations and receiving stations) must be secured against unauthorized physical and electronic access, tampering and the loss of critical security credential information (credential information security may also involve third party credential issuers). Second, the communications pathways to and from the ground must be secured to prevent denial of service, misuse or the loss of critical information (including security credential information). Third, third-party systems on which the spacecraft (or ground / communications systems) relies on for information must be secured against providing incorrect information or being impersonated by a malicious party. Forth, the spacecraft itself must be secured against actioning unauthorized commands and providing sensitive data (including security credential data or data that could allow credentials to be determined or reduce the credential impersonation search space) to unauthorized parties. Standard techniques exist for

virtually all of these areas (some may be impractical or beyond the control of system developers, particularly in the context of test missions). These include standards for data encryption/decryption, access control and credential management, intrusion detection and such.

While best practices should be utilized for securing all of the foregoing, this is insufficient for a system that has the properties of a MWPT system. These properties include:

- System operations are mission (possibly human life / safety critical)
- System maloperation can possibly cause human injury / death / damage to property
- System cannot be directly accessed by human operators (i.e., without relying on cyber component) to correct catastrophic error
- System relies on information that may be interpreted different ways in light of other information

To meet the needs of this type of a system, a more robust security mechanism must be utilized that evaluates system operations holistically and makes both operations-level and systems-level decisions in light of a broader picture view. This is, of course, analogous to how a human would make decisions (given the requisite level of information and intellect) in such a situation.

To this end, all critical commands will be subjected to a review by an onboard autonomous system, based on the concepts of expert systems (see e.g., [16]) and the Blackboard Architecture [17, 18]. This system will be tasked with evaluating the command, in context, to determine whether it should be actioned, or not. Commands and data that impact critical commands will also be vetted, either by this system or a command/data specific algorithm which will feed trust value information into this system. It is important to note that, while this system can override virtually any command transmitted to the spacecraft, it cannot initiate key (i.e., potentially dangerous) activities on its own. However, it can (1) generate requests for information or instructions to human controllers and (2) make decisions about onboard configuration (e.g., engaging the radio outside of believed transmission windows) to attempt to communicate with controllers or respond to urgent onboard problems. The second part of this system is beyond the scope of this discussion (as it relates to spacecraft operating and not security software); the first part can be effected through the use of actions within the context of the Blackboard Architecture-based version of the system. Note that actions taken by the second part of the system (e.g., allowing communications when not expected) will be considered as part of one or more trust metrics of the security command review system.

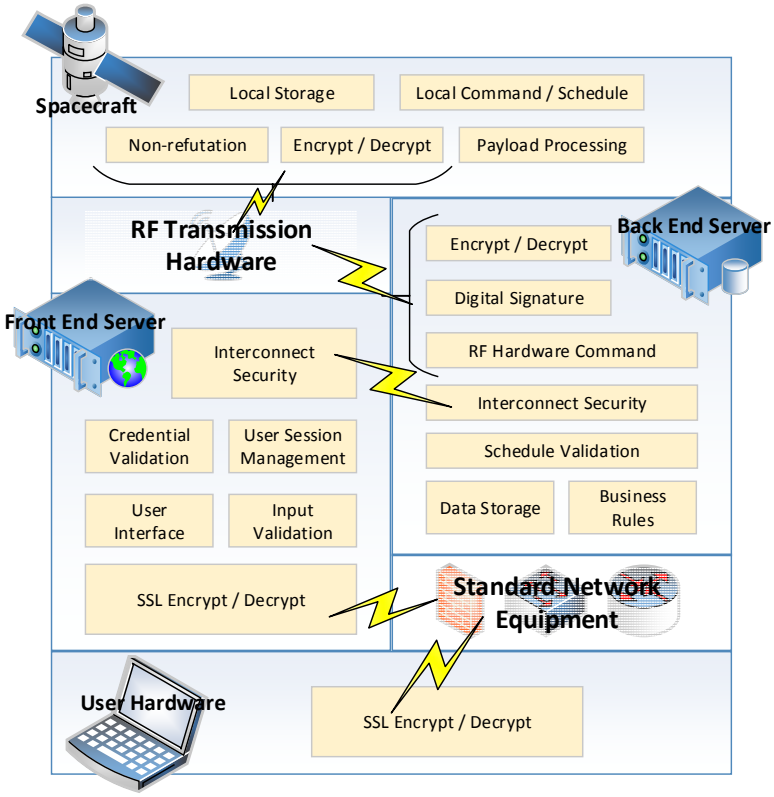

Figure 1. Security System Diagram [15].

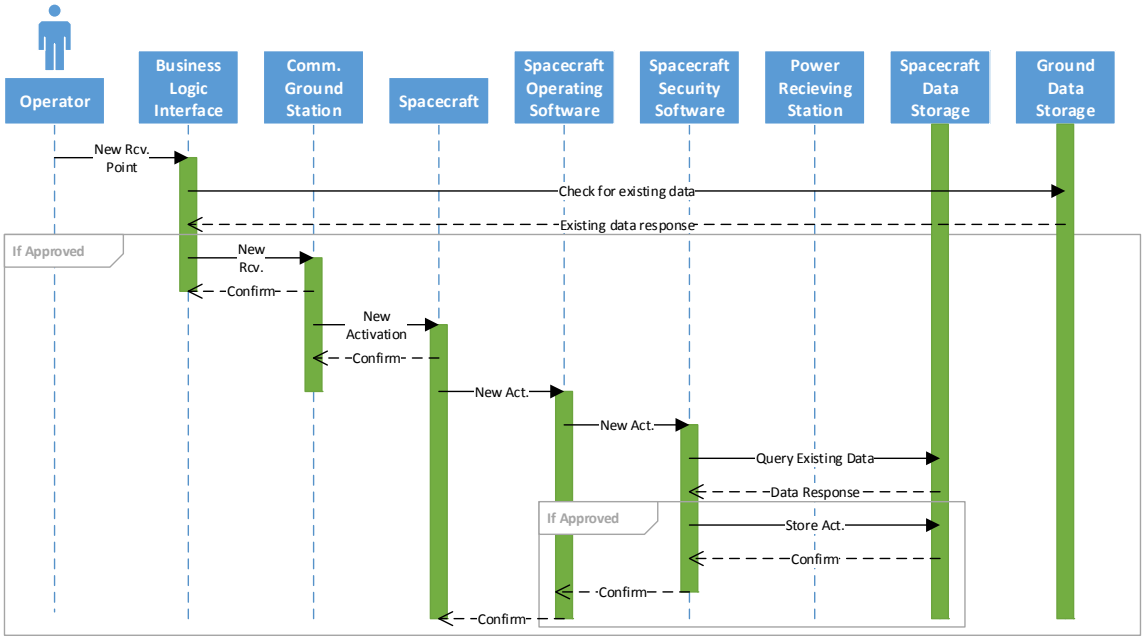

Figure 2. System Use Scenario for Adding a Receiving Point [19].

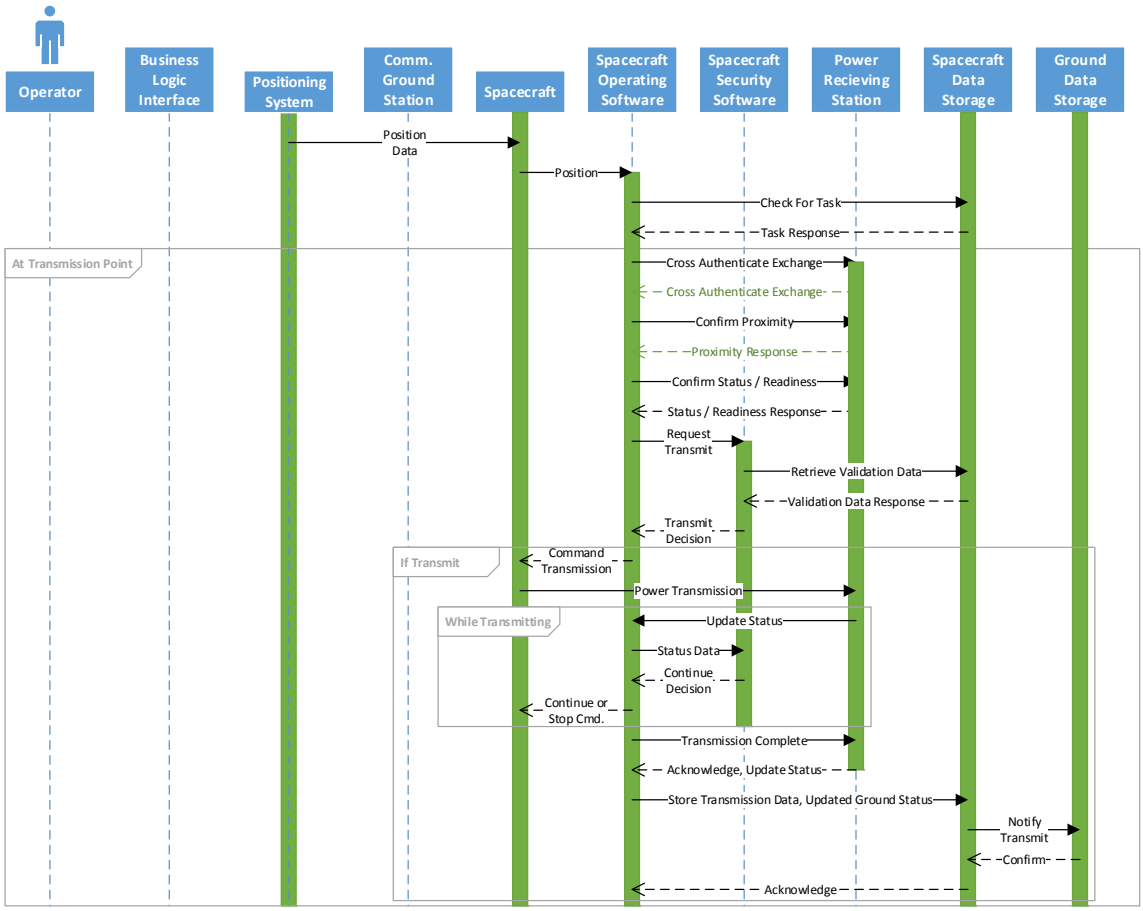

Figure 3. System Use Scenario for Power Transmission [19].

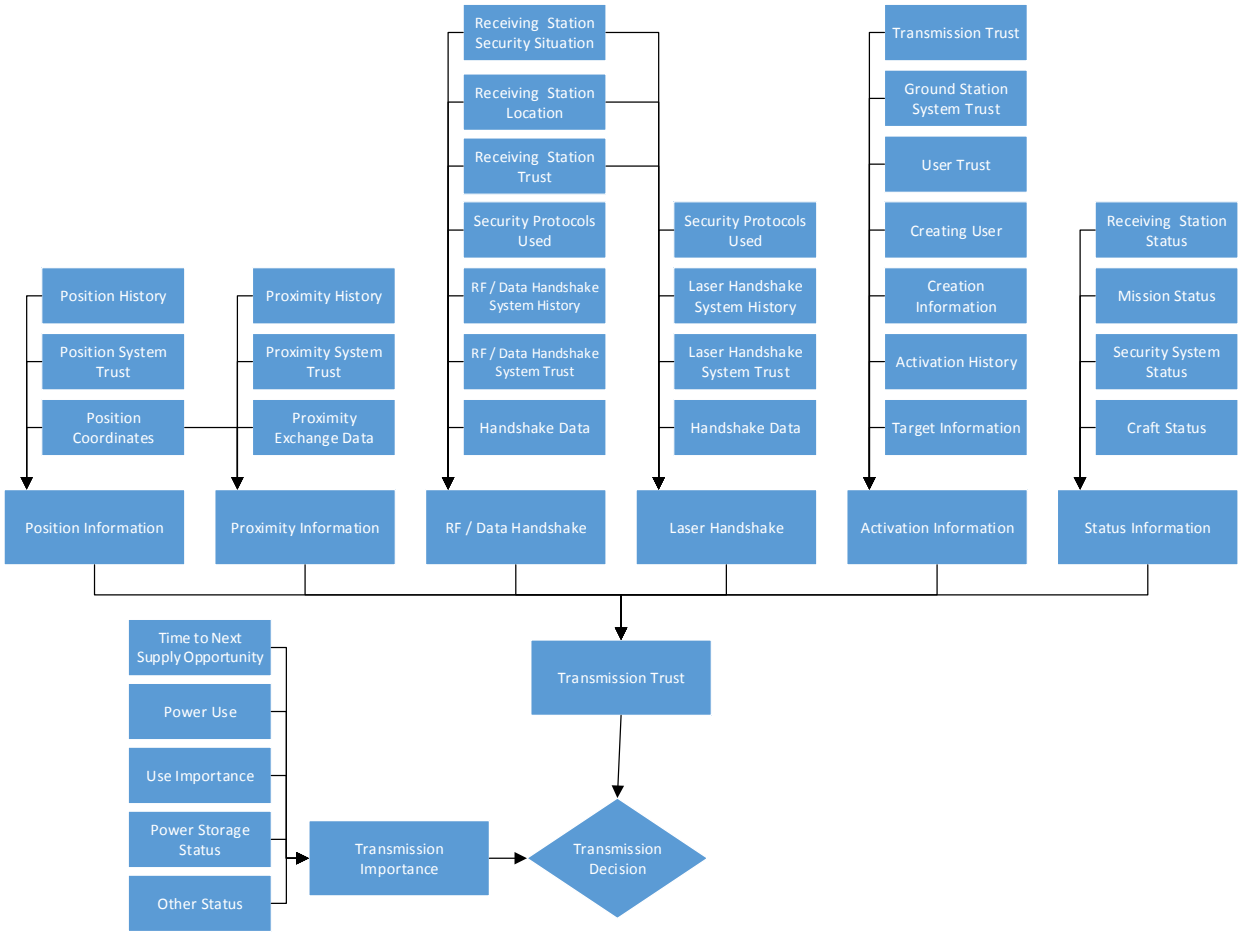

Figure 4. System Logic Diagram [19].

5. CONCLUSIONS AND FUTURE WORK

This paper has presented an overview of a proactive cybersecurity solution for use by autonomous aerospace systems and demonstrated its application to one specific area (which is of particular interest, due to its potential for catastrophic results, if compromised): space solar power. Future work will involve the development, operations simulation and testing of the proposed system and its refinement.

REFERENCES

[1] Amin, M. In *System-of-Systems Approach;* Kyriakides, E., Polycarpou, M., Eds.; Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems; Springer: New York, 2014; pp 317-354.

[2] Hewett, R.; Rudrapattana, S.; Kijsanayothin, P. In *In Cyber-security analysis of smart grid SCADA systems with game models;* Proceedings of the 9th Annual Cyber and Information Security Research Conference; ACM: 2014; , pp 109-112.

[3] Straub, J.; Huber, J. A Characterization of the Utility of Using Artificial Intelligence to Test Two Artificial Intelligence Systems. *Computers* **2013***, 2*, 67-87.

[4] Cheswick, W. R.; Bellovin, S. M.; Rubin, A. D. *Firewalls and Internet security: repelling the wily hacker;* Addison-Wesley Longman Publishing Co., Inc.: 2003; .

[5] Nachenberg, C. Computer virus-coevolution. *Commun ACM* **1997***, 50*, 46-51.

[6] Lane, T. D. Machine learning techniques for the computer security domain of anomaly detection. **2000**.
[7] Lane, T.; Brodley, C. E. In *In Sequence matching and learning in anomaly detection for computer security;* AAAI Workshop: AI Approaches to Fraud Detection and Risk Management; 1997; , pp 43-49.
[8] Hu, W.; Liao, Y.; Vemuri, V. R. In *In Robust Support Vector Machines for Anomaly Detection in Computer Security.* ICMLA; 2003; , pp 168-174.
[9] Hochberg, J.; Jackson, K.; Stallings, C.; McClary, J.; DuBois, D.; Ford, J. NADIR: An automated system for detecting network intrusion and misuse. *Comput. Secur.* **1993***, 12*, 235-248.
[10] Rowland, C. H. *Intrusion detection system* **2002**.
[11] Maddox, J. F.; Kadonoff, M. B.; Robert, W. G. I.; Wendt, R. A. *Intrusion detection system* **1988**.
[12] Igure, V. M.; Laughter, S. A.; Williams, R. D. Security issues in SCADA networks. *Comput. Secur.* **2006***, 25*, 498-506.
[13] Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. SCADA security in the light of Cyber-Warfare. *Comput. Secur.* **2012***, 31*, 418-436.
[14] Pollet, J. In *In Developing a solid SCADA security strategy;* Sensors for Industry Conference, 2002. 2nd ISA/IEEE; IEEE: 2002; , pp 148-156.
[15] Kerlin, S.; Straub, J. In *In Small Satellite Communications Security and a Student Ground Station;* Submitted for publication in the Proceedings of the IEEE Aerospace Conference; 2015; .
[16] Waterman, D. A guide to expert systems. **1986**.
[17] Erman, L. D.; Hayes-Roth, F.; Lesser, V. R.; Reddy, D. R. The Hearsay-II speech-understanding system: Integrating knowledge to resolve uncertainty. *ACM Computing Surveys (CSUR)* **1980***, 12*, 213-253.
[18] Hayes-Roth, B. A blackboard architecture for control. *Artif. Intell.* **1985***, 26*, 251-321.
[19] Straub, J. Cybersecurity Considerations and a Prospective Solution for Microwave Wireless Power Transfer Missions. *Submitted to the International Journal of Electrical Power & Energy Systems* .