2019

Cybersecurity Planning for Artificial Intelligent Systems in Space

Gary Langford
Portland State University, gary.langford@pdx.edu

Lucas Beaulieu
United States Air Force

Jeffery Carpenter
United States Air Force

Ian Watkins
United States Air Force

Brock Marsh
United States Air Force

See next page for additional authors

Citation Details

G. O. Langford et al., "Cybersecurity Planning for Artificial Intelligent Systems in Space," 2019 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 2019, pp. 1-8.

Gary Langford, Lucas Beaulieu, Jeffery Carpenter, Ian Watkins, Brock Marsh, Teah Heidorn, and Chris Chase

2019 Proceedings of PICMET '19: Technology Management in the World of Intelligent Systems

Cybersecurity Planning for Artificial Intelligent Systems in Space

Gary O. Langford[1], Lucas Beaulieu[2], Jeffery R. Carpenter[3], Ian Watkins[4], Brock Marsh [2], Teah Heidorn[2], Chris Chase[1]
[1] Engineering & Technology Management, Portland State University, Portland, Oregon, USA
[2] United States Air Force
[3] United States Air Force (Ret)
[4] United States Air Force, 9th Bomb Squadron, Dyess AFB, Abilene TX

***Abstract*—CubeSats continue to proliferate and are an excellent low-cost method of remote sensing. A key piece of intelligent systems is sensory input, data storage, and data communications. With the continued miniaturization of technology, CubeSats will increase their sensory inputs with future miniaturization and enhance their robustness for autonomous operations if data and communications are secure. These futures inspire an intelligent system solution to on-orbit communications. This paper explores a dual-microprocessor approach to improve hardware cybersecurity of intelligent systems, with a view toward intensional intelligence as a means of adjudicating access to sensitive data onboard the CubeSat. With enhanced cybersecurity, Artificial Intelligent Systems (AIS) will add vital utility to otherwise vulnerable, autonomous systems. Using Systems Models-Based Thinking, we shed light on our plan to apply artificial intelligent system concepts to advance CubeSat technology. Managing technology for AIS reduces some of the uncertainties and risks associated with the space environment.**

I. Introduction

Outer space is inherently hostile and unforgiving. Beyond the ever-present space radiation that damages all materials, particularly harmful ionizations impact computer operations, including data collection and storage, data movement and communication. Adding to those hazards, keeping data safe from human misuse, theft, destruction, and denying others access is a key concern. The advent of unattended, autonomous operations necessarily suggests Artificial Intelligent Systems (AIS) for space-based, cybersecure applications. A concern for AIS in space immediately focuses attention on a problem not yet solved – the significant consequences of losing control of highly sensitive data. Systems engineering graduate students in the Engineering & Technology Management Department at Portland State University are using Systems Model-Based Thinking (SMBT) [1], [2] , [5] to secure the lifecycle of data in CubeSats [6] against nefarious access. Figure 1 depicts the size and shape of two NASA CubeSats, with 3 units, each with dimensions of 10x10x10 cm^3 and total mass of ~ <5 kg per unit, significantly greater now than the 1.33kg mass proposed in 1999.

This paper reports on early stage planning to build a cybersecure CubeSat – a model for all satellites that communicate to other satellites and to ground, regardless of size or mission.

II. CubeSat Design and Operations

CubeSats are small, nano-sized satellites constructed in cubes (termed a unit or "u" size) with common sizes for standardization. Less expensive research in space can be and is carried out by these very small satellites, opening up space for students from high school to graduate school, and countries who are blocked by the cost of the multi-million-dollar satellites of the recent past.

The Portland State CubeSat is planned to have 1 u, incorporating electrical power, Electromagnetic Pulse (EMP) sensor, and additional control and communications capabilities to provide for cybersecure communications. Of primary importance to secure data that has been collected and stored in the CubeSat memory is the ability to maintain a secure communications link to ground stations to protect the integrity of the data so that it cannot be destroyed or manipulated or intercepted and stolen".

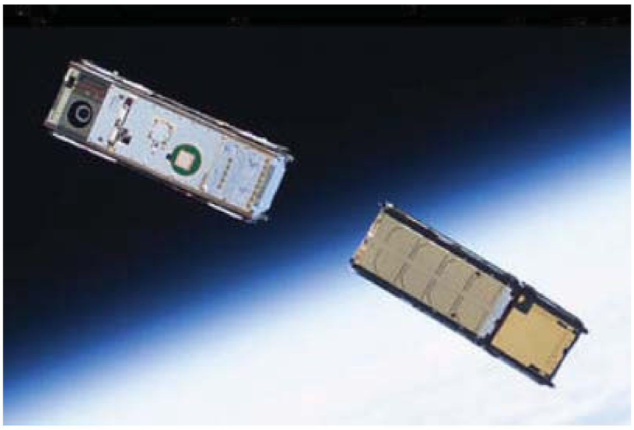

Fig. 1. NASA CubeSat

III. Systems model-based thinking (SMBT)

The primary issues in defending a satellite that is not in constant, real-time communications with human guardians of security, center on the amount of time in which the unattended satellite can be interrogated and profiled by cybercriminals.

978-1-890843-39-7 © 2019 PICMET

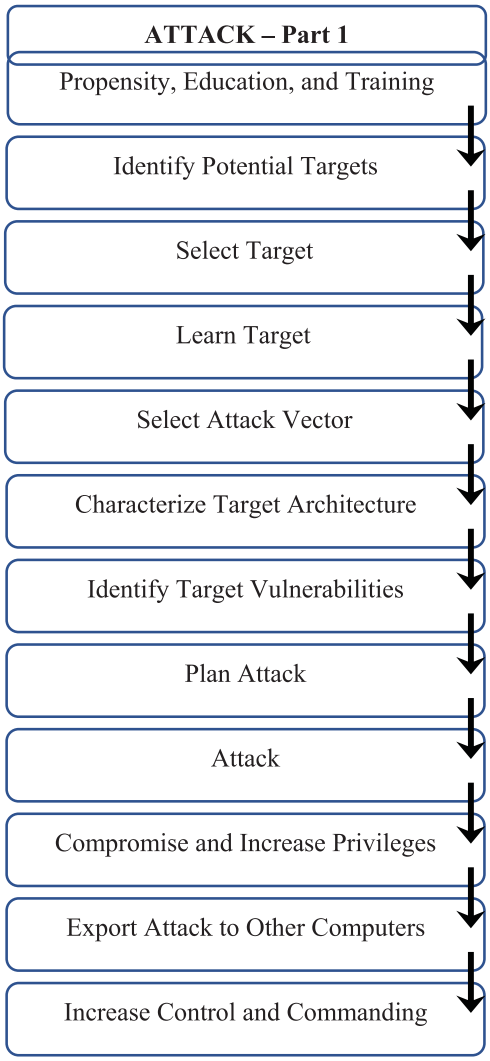
ATTACK – Part 1
Propensity, Education, and Training
Identify Potential Targets
Select Target
Learn Target
Select Attack Vector
Characterize Target Architecture
Identify Target Vulnerabilities
Plan Attack
Attack
Compromise and Increase Privileges
Export Attack to Other Computers
Increase Control and Commanding

Fig. 2. The Lifecycle of a Cyberattack

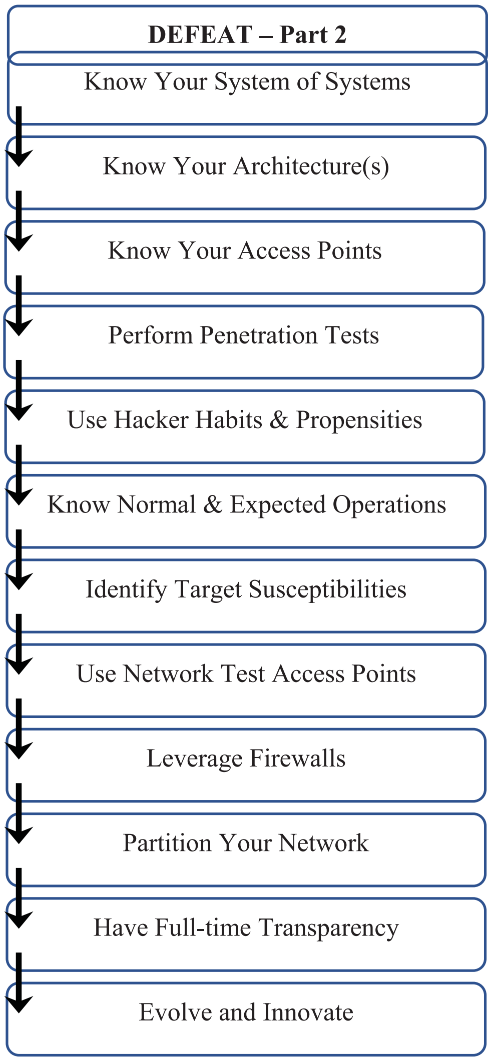
DEFEAT – Part 2
Know Your System of Systems
Know Your Architecture(s)
Know Your Access Points
Perform Penetration Tests
Use Hacker Habits & Propensities
Know Normal & Expected Operations
Identify Target Susceptibilities
Use Network Test Access Points
Leverage Firewalls
Partition Your Network
Have Full-time Transparency
Evolve and Innovate

Fig. 3. The Cyber-Defender Preparation for Attack

We adopt a view that cybersecurity involves people, machines, economics, and malicious intent. Consequently, a sophisticated socio-technical system of systems confronts solving cyber-problems with only a limited set of traditional approaches, including for example: engineering, defense-centric, attacker-centric, response dominated, data-centric, punishment focus, constructivist, collaborate, lone wolf, problem-based, learning-centric, needs-based and requirements-based. Each approach fails to adequately capture the diversity of views represented by hundreds of stakeholders who impact the lifecycle aspects of a cyberattack. Little exists in the way of formal, principle-based approaches to securing data against surreptitious cyberattacks on satellites. To ensure security against cyberattacks or cyber mishaps an approach accentuates the difference and relatedness of strict ontologies will better portray the relationships between cybersecurity and operational priorities. Applying SMBT to that emphasizes systemic relations between inputs and outputs; stresses succinct boundaries and boundary conditions; and organizes and highlights lifecycle stages.

A. Hacking and Jacking

The focus of this SMBT use is the lifecycle of an attack on a satellite. Specifically, the concern is the topology of interactions, i.e., the objects that exchange Energy, Matter, Material wealth, and Information (EMMI) [2] as part of the request for data and the response to that request. Figure 2 & 3, derived from Joe Zott [3] illustrates the lifecycle stages of a cyberattack. communications processing (including software, hardware, data storage, connectivity, and protocols).

Figure 2 shows relational dependencies on resources available to hackers, knowledge at time of the hacking, premise under which attack is to be carried out, technology, and resources available to defender. The left column describes the attack – in lifecycle fashion from pre-attack training to identifying potential targets of interest, target selection and learning how the target reacts to various queries. Once target architecture is reasonably characterized in terms of types and number of nodes, types of processes that are enacted, and priorities that can be established by probing, the plan vector is selected to try to break into a part of target system. Further details about target architecture are laid-out to identify vulnerabilities of the target. The plan of attack is then formalized and the attack is initiated. With compromise of the target system by various attacks, the notion is to increase the level of privileges. With increasing levels of privileges, the attacker may tamper with the system, disable it, steal intellectual property, or export data to other computers, thereby increasing control and commanding within one or more computers. The attack lifecycle ends when the objectives and goal of the attack are completed or when the attack is terminated by the attacker or the defender.

B. Defending and Mending

Figure 3 views the defense against a cyberattack as the essentials for preparing for a cyberattack without describing the tools that may be used to interdict or preempt an attack. The goal is to protect data such that the intended use of the data is inviolable. The objectives are to discourage, dissuade, disrupt, defend, delay, minimize attack surface area, and destroy attacks. Here, we assume that the target of the attack that needs protecting is a system of systems. SMBT provides an in-depth assessment and evaluation of the physical objects that do or could interact with the defender and the attacker; the processes and mechanisms enabled to carry out the defender's objectives and the processes and mechanisms used by the attacker; the boundaries and boundary conditions that govern the defender's and attacker's respective domain; and the types and locations of emergence that may be unexpected, yet possible. The defender should anticipate an attacker's target architecture, including access points. Tests should be performed by the defender to try to penetrate the architecture, interrogate access points, and defend against an extremely wide range of attack vectors. The defender needs to learn the hacker habits, propensities, and preferences so they can be factored into the defense strategies to defend. For the attacker's targets, the defender should be aware of the sets of normal operations as well as the range of expected operations. There are metrics which can be monitored to determine if some computing operations are allowable or not. The attacker's targets should have all susceptibilities acknowledged and back-up with security, including reliable review by human or AIS, third-party monitoring, or means of isolating (e.g., air-gap with shoe-leather interface) to protect highly sensitive data. The network should be configured with test access point so that data flow can be monitored and compared with expected usage given normal circumstances. Firewalls should be maintained, inspected, and managed. The network should be set up for partitioning to close and open various portions. And, the defender should provide for full-time transparency across *all* network and computing nodes.

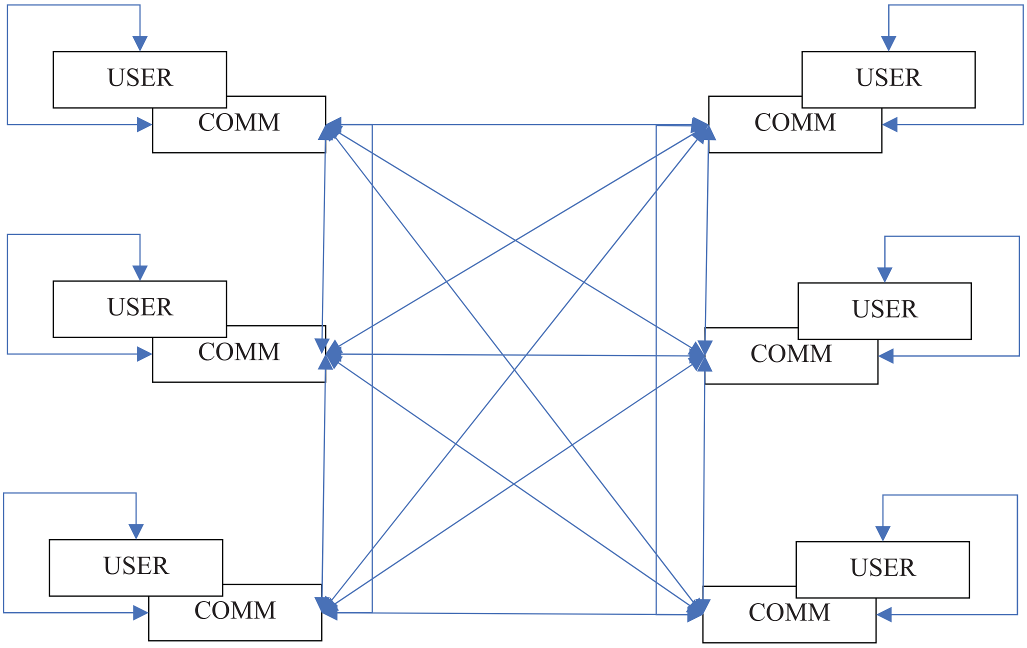

Fig. 3. ASMP for CubeSat Cybersecure Operations

IV. The Fundamentals of Systems and Systems of Systems

A. *Systems*

Systems and systems of systems are distinguished by fulfilling a set of criteria. A group of objects and processes that is bounded and dynamically stable is a system, if the objects are adaptively to their environment, show irreversible or nonreciprocal actions, exhibit objects that change from one state to another and then revert to their first state using a different process than before (i.e., metastability); and have agility to exchange Energy, Matter, Material Wealth and Information (EMMI) in response to stimuli.

B. *Systems of Systems*

A system of systems is an integrated, interoperable set of constituent systems that function as a system (with one exception). That exception is that no constituent systems shall be harmed or irreparably degraded by joining, participating, or leaving a system of systems or systems of systems.

C. *Intelligent Systems*

Only humans and animals (and perhaps alien sentient beings) are considered to be intelligent systems. Intelligent systems can perceive, create action, and learn in an autonomous fashion, i.e., without external supervisory intervention for an extended amount of time (here restricted to only humans and animals) [7]. Artificial Intelligent Systems (AIS) are made to mimic intelligent systems. The distinction between artificial and non-artificial intelligent systems (with sentient functions and faculties) will remain a governing discriminant, as we similarly distinguish between human genetics and chimpanzees, and bonobos – with close, extant similarities [8]).

V. Discussion of Cybersecurity Issues

Just because something is unobservable does not mean that it is empirically untestable. The ontic nature of properties cautions us to consider that every object must be tested for its properties, traits, and attributes before affording it with the trust that may be implied by the name and use of the object. An object is anything that is physical or has agency in physical form [2]. For example, a rock and the idea of a rock are both an object – rock. An idea, physical object, model or representation, or concept are all objects. For cybersecurity, every object shall be subjected to test, verification, and validation. Intensional and extensional logic are essential factors in test, verification, and validation. Getting to the essence of semantical meaning, Rudolf Carnap proposed a new approach that extended the then 1940's thinking from a word, a phrase, or a sentence representing the name of something to two meanings – one about a thing, proposition, or fact (extensional); and the other meaning about the "necessity and contingency, possibility and impossibility" [9].

A. *Intensional and Extensional Meaning*

We adopt the meaning of a concept as formed by Carnap's components – intension and extension. Extension is determined by empirical analysis. By extension illustrates the range of a term or concept as measured by the objects which it denotes or contains. Objects occupy space. For cybersecurity, the concern is for categories that can be used to help identify a requestor for data.

We use several sources of information in cybersecurity to determine and check credentials of requestors for data, including (1) knowledge that is specific to the data or need for the data; (2) domain knowledge represented by deductive logic, that includes policy, rules, regulations, and integrity constraints; and (3) corroborated "facts" about the requestor.

The first source of such information includes basic ontological knowledge of the data (processes, physical objects, functions, performances, behaviors, cognition, mechanisms, models that are consistent with or indicative of the data (none of which discloses data). Specifically, why does the requestor need access to the data requested? Why is that data necessary? The intent is for each request to include reference to specifics in the data that the requestor would know because of the tasking authorized for use by the requestor. The same level of interrogation is used in systems engineering work to verify that each person working on a task is authorized to work on that task. Furthermore, results of that task tie to a specification and then directly to a sanctioned requirement, i.e., the process of verification is by independent means from an end-to-end perspective with complete traceability and transparency [10]. The resulting extensional (logic by the same line of argument) set of direct answers can be designed to cover or incorporate answers to intensional questions.

The second source of information includes knowledge about specific access to only those parts of the data that the requestor is authorized to handle and store (no other use is intended or authorized). The requestor is expecting access within x time following the requestor's request for data from an authorized third-party (i.e., one who has granted the requestor permission to handle and to store the requested data). The set of intensional questions from this source of knowledge may result in extensional and intensional answers.

The third source of information includes facts about the requestor e.g., country, location, specific IP address, organization, name, password, and answers to questions with inclusion of confidential content and information that is to be taken from an email sent to requestor on the same day as the requestor's request to access data. The set of intensional questions result in intentional answers.

Test on information and knowledge to determine its extensional make-up relies on verification to determine its intensional implications [10], and validation to determine its fitness for use [2]. In support of this schema for cybersecurity, Carl Hempel stated, "…the verifiability criterion implies that existential generalizations are meaningful, but that universal generalizations are not, even though they include general laws, the principal objects of scientific discovery" [11]. The condition, "authorized to access data" must be contingent on satisfying both intensional and extensional means of determining trust. Here, we determine that relative frequencies of trust verifications in finite sequences of requests are meaningful, but thresholds of verifications in infinite sequences is specious. The logic of negation must be satisfied – the standard of reference must be an objective statement that someone is untrusted in the following situation. In other words, there are no absolutes, no standard set that determines trust, and certainly no algorithmic means to sift conditions by which a particular request is acceptable. Artificial objects today do not satisfy AIS requirements.

The essence of security should not enforce an absolute standard, but rather a conditional, intensional standard that delves deeper into meaning and intent of an individual's request and that individual. Moreover, cybersecurity should not be premised on deductive logical inferences that are meant to partition and disassemble a request for data without first recognizing the emergence that is lost in the process of determining trust. Each individual component that derives from "password", "IP address", "user authentication" (for example), by themselves are insufficient, but included in the extensional set from which authorization for accessing data is given. No extensional set should be considered secure. Instead, the emergence that arises when the parts are constructed (prior to forming the objects, "password", "IP address", and "user authentication").

It is difficult to cope with the full extensions of concepts on a computer, since some concepts have an infinite extension (e.g., successor), some have a fuzzy extension (e.g., hill, large), and some (like extension) arguably cannot be assigned an extension. Therefore, we incorporate partially described extensions for use with computers. Extensional structures can never hope to capture the inherent complexity of natural language, whereas Intensional reasoning can include all instances of ideas and concepts.

In spite of the fact that human reasoning is extensional and intensional, all knowledge today is extensional, enforced by formal representations that are amenable to automated reasoning on the Semantic Web. The reason we use extensional reasoning is there is no formal computational system that can handle intensional reasoning quickly and with a high degree of comprehensibility. An excellent example of extensional prowess is an IBM computer beating Ken Jennings in Jeopardy – still, a shard less than essential intensional logic.

Most human reasoning is highly intensional, i.e., involving belief, desire, knowledge, action, intention, perception, and communication. In contrast, standard reasoning in mathematics or the natural sciences is extensional. Systems engineering thinking is a mix of intensional and extensional logic (as indicated by strong measures and practice for verification to requirements through specifications).

Intension is made clear by that which is apprehended by understanding of the concept. Intensional intelligence is defined as "by comprehension". By comprehension rather than by extensional intelligence through "referential meaning".

Combined, intensional and extensional descriptors and usage narrow the comprehensibility more quickly than intensional and more accurately than extensional logics. When using both intensional and extensional responses to requests for data, security is increased. The amount of increase in security (as measured by the number of nefarious accesses relative to standards determined to be "secure safe") compared to the time it takes to catch a nefarious access request, in conjunction with the time it takes to allow a legitimate access request to process and send data, is a future project for graduate students at Portland State University.

VI. Intensional Intelligence Planned for CubeSat

To strengthen computer security, we plan to incorporate a greater sensitivity to physical, compliance, and logical cybersecurity than is currently in place anywhere. At the most critical of all data repositories – for individuals, finance, health, and national security, data is at risk of compromise by reading, removing, destroying, denying, or changing. Halting raiders from accessing sensitive files and data sources is a mission objective for our CubeSat project. We are implementing a hardware/software computer sentry to secure physical access to only legitimate users who are authorized by duly appointed and trained personnel, sanctioned to perform to security policy by following a set of rules, certified to have the requisite knowledge, skills, and abilities, properly acknowledged to have a need that is sanctioned by an approved work task.

A three-fold mix of physical, compliance, and logical security is planned for the CubeSat. With regards of the interplay between compliance and logical security techniques, we add intensional logic to improve security. With regards to the interplay between physical and the combination of compliance and logical security, the physical security enforces separation between functions of receipt of request and the release of sensitive data.

A. Physical Security

Multiprocessing was first implemented as asymmetric processing through the use of two distinct processors that did not share memory or other resources. Consequently, two operating systems were implemented, one on each processing platform. The peripherals were allocated to one or the other processor, thereby partitioning various functions to one or the other processing units. We plan to implement pairs of multiple processing units, any number of which can be connected into a network of multiple processing units. Each processing unit will have identical architectures. Each processing unit will operate with the same software operating system. Each processing unit will be connected to other processing units. This Asynchronous, Symmetric Multi-Processing (ASMP) configuration will operate either as individual unit pairs or as an integrated set of unit pairs, depending on the type of communications that is dictated by the contexts for cybersecure operations. Figure 4 diagrams the ASMP Asynchronous, Symmetric Multi-Processing Configuration.

From the perspective of physical security, first and foremost, there is no centralized repository of data. While the data is decentralized physically, its access, mediated through sentry software, has two layers of software to enhance invulnerability. The first layer interrogates for intensional and extensional information structures (to include intensional and extensional questions that must be answered. The second layer collects and compares the analytics for deviant behaviors.

B. *Software Security*

Data infringements are often perpetrated by accessing and using legitimate credentials. Behavior analytics that derive from the capture, analysis, and evaluation of patterns of behaviors are used to monitor computer activity that originates from a non-authorized location, recognize and shut down a service account has been compromised, watch for and correct a non-compliant account configuration, and surveil outgoing data for duration and destination. These methods are meant to handle the significant deviations from expected behaviors, i.e., compliance, across accesses networked to sensitive data. A form of compliance security is embodied in using intensional logic to interrogate credentials, authorization, appropriateness, and legitimacy for accessing data.

At the center of logical security are the terms, terminology, and structures governed by semantics and syntax – the logic of meaning and the arrangement of words and phrases, respectively. Interactions between the cyber system and requests for data and information will be managed by implementation of formal logic. Definitions of the terms, terminology, and discourse for access to data will be sorted into two major categories based on logic: Intensional logic that puts forward intensional definitions stating the essences of a word; and extensional logic that offers definitions listing the objects within categories that are described by the word. For example, extensional definitions are used to compile all objects in association by title, book, author, publisher, and date. Currently, all knowledge on the Internet and World Wide Web are represented in categories of structured taxonomy to facilitate automated search by category. Use of only extensional logic by a computer hampers full and rapid search since categories, alone, do not capture all aspects of search.

As yet, no formal artificial computing demonstrates intensional logic for either fast or accurate search. However, intensional logic can readily define intensions as functions and relates those functions to the physical world for accessing data files. We will apply Montague semantics to describe, predict, and interpret the intensional semantics when requesters communicate their intention to access data. All data stored and used on the CubeSat will be protected by a tuple associated with security questions and answers, circumstances and contexts, authorizations and sanctioning, certifications and legitimate need. Properly orchestrated intensional questions will formulate a short list of conditions that will reflect on the requestor's actions. If those actions are nefarious in nature, intensional logic will betray the requestor's intentions. By correlating the answers to intensional questions, access to data will either be granted or denied. For example, intensional semantic logic treats 'access today to project X' and 'Jeff (the data file custodian who is known by a legitimate requestor) agrees to your accessing project X today' as having the same intensional meaning. Posed dichotomous and trichotomous intensional questions to requestors should ensnare or at least improve capability to detect and thwart would-be nefarians. The degree of familiarity with the particulars of the requested data as well as its context and circumstances of the generation, storage or use will depend on how the requestor believes the posed statements could be true. Through a series of intensional questions and answers, the knowledge of the requestor is meant to distinguish between access and denied access to data. After a person experiences and observes a phenomenon, an intensional definition begins to instill a sense of what belongs to the situation and what is appropriate. The observer knits the intensional logic with the highly structured extensional forms of categories to form a set of necessary conditions that apply to the situation encompassing the lifecycle of the data. From first instantiation of the data to the last vestiges of the use or repurposing of the data, the lifecycle is replete with opportunities to employ intensional and extensional structures of logic.

This application of intensional logic is not new to cybersecurity, but as yet is not implemented in a computer hardware/software configuration. Security investigators use a combination of both intensional and extensional logic to discern behaviors and intentions. For the CubeSat, analysis using SMBT suggests several actionable ways to stage and manage an intensional exchange to provide the foundation and substance necessary for a credible and warranted need for particular data. In practice, the intensional logic differentiates the behaviors of requestor and hardware sentry's response to requestor's answers both prior to and after their interactions to request protected data. The temporal nature of intensional logic is an essential aspect to establish and describe the sequence of events surrounding the data and its use. For example, knowing the logic format of the data when either stored or used, knowing the circumstances for when the data is used, and knowing the limits of validity for data use, are discriminates that aid in protecting data. The list of intensional interactions with a data requestor is estimated to be less than ten, only three to four of which will require the requestor to respond to unique questions. Therefore, requests for data will necessarily require personal, interactive attention with the computer sentry. No automated or scripted requests will be successful.

The condition for intensional logic being equal or higher in value as compared to extensional logic (the current mainstay of structures used for cybersecurity) is key to improving sentry-protected data.

VII. Rule of Equivalence

Here, causal intension concerns the logically necessary conditions that apply qualitatively to defined terminology within the structure of questions for cybersecurity. Intensional definitions that are too broad in their scope mean a short list of conditions. Definitions that are said to have restrictive extensional structure are narrowly scoped with a long list of categories stipulated. Logic dictates and practice confirms that causal intension cannot be applied rigorously; restrictive extensional definitions should be refined to the higher level of intension; and that an operational definition needs to be developed to simplify, characterize, and clarify use to yield an academically rigorous, reproducible result [12], [13].

After experiencing and observing a phenomenon, the intensional definition begins to knit the logically necessary conditions that apply to the word being defined. Without a classically intensional definition, any observed emergent phenomenon may be ill-expressed and inefficiently communicated. Classifying emergence according to the intensional approach – first, differentiates the behaviors of objects before interaction from that of behaviors of the same objects due to or after interaction. Second, distinguishes between individual objects and their known properties and traits before interaction from the phenomenon that is observed during or after interaction. These two differences stipulated in genus and differentia give rise to the intensional definition of emergence. The essential characteristic of the phenomenon that is captured in the intensional definition of emergence is that a change in behaviors of objects before, during, and after interaction may be observed. However, the rule of equivalence is broken when the definition includes more or less specification than required. This situation is the case with the historical and recently promulgated definition of emergence. The rule of equivalence is a check that follows from the inclusion principle – only that which is necessary is included, all else, not.

Rule of Equivalence: an object x is a mereological sum of the group W if and only if every W is part of x and every x is compatible with some W.

VIII. Mereological Sum

The rule of equivalence is built on the definition of a mereological sum which means that because every object is subordinate to itself, no class of objects is not subordinate to itself. A mereological sum is not the numerical result of a mathematical process, but rather the imbuement of properties of objects with spatially or temporally continuous traits with mixed kinds of things and stuff. According to Tim Ferris, "The word 'stuff' is deliberately used with its Jacobean era definition as including both the material of which things are made and the things themselves" [14].

The mereological sum is imbedded in the cybersecurity schema which is premised on the sum of all objects that comprise the answers to questions posed by the two processors as compared to the sum of all objects that make up the "answer key" used to determine if access to data is to be granted, denied, or delayed. These objects include both intensional and extension types. The distinct benefit of using the mereological sum of intentional and extensional logic structures is there may be both apparently disjoint responses from requestors for data (typically precipitating a further request for information from the requestor) and responses overlapping the answer key. With conventional set theory, i.e., not Leśniewskian mereology, the logic terms indicate uniqueness, i.e., either the person provides the password or not, the partial answer is unacceptable [19]. However, with Leśniewskian mereology, there can be partial answer that when overlapped offer a different way of authentication and means to provide rightful access to secured data. The mereological sum is the ultimate test for authorization – far in excess of simple set-theoretic answers. In other words, a purely extensional response will not be sufficient to access sensitive data. The additional intensional logic is an integral part of the mereological sum and consequently a sufficient difficult barrier to those who have neither proper credentials nor permission.

The mereological sum was first described and made relevant by Stanisław Leśniewski [15], [16], and expanded by numerous logisticians [17]–[24]. The mereological sum has been notionally corrupted with too many interpretations without proper representations of the basic underlying theory [18]. The term *synthetic sum* is deemed to be a more descriptive expression of the state before interactions that change that state. The essence of the synthetic sum is that it is contrived or sentient constructed and given pseudo-meaning.

IX. Conclusion

Since mereology is regarded as the theory of collective classes, intensional logic is tied to the mereology of objects and processes within the collective of descriptions and not venerated solely in either or both of the ontology of objects or the ontology of processes. This distinction between intensional and extensional logics positions the synthetic sum by provenance and previous interaction, very differently from that of emergence, i.e., emergence is the results of sustained interaction between objects. The result is a simple way to differentiate between valid users of data using questions based on intensional logic that are intermixed and posed to requestors of data.

Coupling the two logics, the mereological sum is apply to all requests for data that is meant to be secure. The answer key is constructed into the software *and* hardware of the two-processor configuration that manages access to sensitive data on the CubeSat. The mereological sum is the adjudication schema that thwarts nefarians. The COMM and USER processors carry out the tasks of interrogating, comparing, and communicating for the requestor, the manager of the answer key, and the recipients of the data, respectively.

The COMM processor manages and determines legitimacy of user requests through interactions with the requestor. Those requests that are accepted as valid are communicated to the USER processor. The USER process has its own set of extensional and intensional protocols used to further interrogate the requestor of data to mediate the flow of data. These mediations include determining priority and bandwidth, and scheduling and interrupts. Limits are imposed by both the COMM and USER processors. Systems Model-Based Thinking provides the formal model for the artifacts of cybersecurity used for CubeSat protection of data.

Applying a combination of hardware to separate the control of incoming communications that request access to data and the control of how and when data is to be released, the cybersecurity of a network of Asynchronous, Symmetric Multi-Processing units should improve over simple extension security schemas. Combining intensional and extensional logic is expected to dramatically improve cybersecurity.

The simplicity of the CubeSat, its low cost to demonstrate space-borne communications security, and the managed access by the mereological sum provide a convenient means to provide a platform to test a solution to the number one problem faced by all users of space-platform data – that of loss of sometimes vitally important data.

The next steps in the research are to build and orbit the CubeSat, run the defined battery of test cases to check out the on-orbit two-processor configuration, collect and store data from a simulated EMP signature in a USER board, then deluge the COMM process with legitimate and illegitimate requests by varying sequences, concurrency, partial and complete requests, and other structures and delineations.

Disclaimer

Any views, opinions, findings, conclusions, or recommendations expressed or implied in this paper are those of the authors and do not reflect or represent the official policy or position of the United States Government, the United States Department of Defense, the United States Air Force, or the National Aeronautics and Space Administration, and nor do they reflect or represent the official policy or position of Portland State University, the Maseeh College of Engineering & Computer Science, or the Engineering and Technology Management Department.

References

[1] G. O. Langford and T.S-Y. Langford, “The making of a system of systems: Ontology reveals the true nature of emergence,” in Conf. Proc. 2017 12th Annual System of Systems Engineering Conference IEEE Int.

[2] G. O. Langford, *Engineering Systems Integration: Theory, Metrics and Methods*. Boca Raton, Florida, CRC Press/Taylor & Francis. 2012.

[3] J. Zott, Lecture Notes on Cybersecurity, “Attacking Joe’s Network,” Systems Engineering Program, Portland State University, 2018.

[4] G. O. Langford, “Toward a General Theory of Systems Integration: Research in the Context of Systems Engineering,” Ph.D. dissertation, Defence and Systems Institute, School of Electrical and Information Engineering, University of South Australia, Mawson Lakes, Australia, 2013.

[5] G. O. Langford, “System of Systems Process Model,” Chapter 6, Phenomenological and Ontological Models for Predicting Emergence, L. Rainey and M. Jamshidi, Eds. Boca Raton, Florida: CRC Press/Taylor & Francis. 2018.

[6] G. O. Langford, J. Carpenter, I. Watkins, B. Marsh, L.Beaulier, “Novel Approach to Managing Technological Entrepreneurship Using A Model-Based Systems Approach To Develop Low Cost Earth Orbiting Satellites,” Paper 18R0104, Portland International Center for Management of Engineering and Technology (PICMET), Managing Technological Entrepreneurship: The Engine for Economic Growth, 19-23 August 2018, Waikiki, HI.

[7] J. Spatz and S. Schaal, “Intelligent Systems Research,” Max Planck Institute for Intelligent Systems. https://www.mpg.de/9330879/intelligent_systems_basetext.pdf

[8] K. Prüfer, K. Munch, I. Hellmann, K. Akagi, J.R. Miller, B. Walenz, S. Koren, G. Sutton, C. Kodira, R. Winer, J. R. Knight, J. C. Mullikin, S. J. Meader, C. P. Ponting, G. Lunter, S. Higashino, A. Hobolth, J. Dutheil, E. Karakoç, C. Alkan, S. Sajjadian, C. R. Catacchio, M. Ventura, T. Marques-Bonet, E. E. Eichler, C. André, R. Atencia, L. Mugisha, J. Junhold, N. Patterson, M. Siebauer, J. M. Good, A. Fischer, S. E. Ptak, M. Lachmann, D. E. Symer, T. Mailund, M. H. Schierup, A. M. Andrés, J. Kelso and S. Pääbo, “The bonobo genome compared with the chimpanzee and human genomes, " 28 June 2012, V. 486, NATURE, 527 https://www.nature.com/articles/nature11128.pdf

[9] R. Carnap, *Meaning and Necessity*. Chicago University Press, Chicago, 1947.

[10] G. O. Langford. “Verification of requirements: system of systems theory, framework, formalisms, validity. 27th Annual INCOSE International Symposium,” IS 2017, International Council on Systems Engineering, Adelaide, Australia, July 15-20.

[11] J. Fetzer, "Carl Hempel", The Stanford Encyclopedia of Philosophy (Fall 2017 Edition), Edward N. Zalta (ed.) citing Hempel (1950), “Problems and Changes in the Empiricist Criterion of Meaning” Revue Internationale de Philosophie, 41(11): 41–63. 1951, “The Concept of Cognitive Significance: A Reconsideration”, Proceedings of the American Academy of Arts and Sciences, 80(1): 61–77. doi:10.2307/20023635 (1950, 1951)).

[12] N. Swartz, “Definitions, Dictionaries, and Meanings,” Philosophia Vol. 3:2-3:167-178 April-July 1973. http://www.sfu.ca/~swartz/definition.htm.

[13] I. M. Copi, Eds. C. Cohen, and K. McMahon, Introduction to Logic. 14th ed. New York: Routledge, 2014.

[14] J. Martin and T. Ferris, “On the Various Conceptualizations of Systems and Their Impact on the Practice of Systems Engineering.” INCOSE. Journal of Systems Engineering, 2008.

[15] S. Leśniewski, 1916, ‘Podstawy ogólnej teoryi mnogosci I’ [Foundations of a General Theory of Manifolds], Prace Polskiego Kola Naukowe w Moskwie, Sekcya matematycznoprzyrodnicza, 2, Moscow.

[16] S. Leśniewski, 1927–30, ‘O Podstawach Matematyki’ [On the Foundations of Mathematics], Przeglad Filozoficzny, 30 (1927), pp. 164–206; 31 (1928), pp. 261–291; 32 (1929), pp. 60– 101; 33 (1930), pp. 75–105; pp. 142–170.

[17] H. Leonard and N. Goodman, “The Calculus of Individuals and Its Uses,” Journal of Symbolic Logic 5, pp. 45–55, 1940.

[18] D. Lewis, Parts of Classes, Oxford: Basil Blackwell, 1991.

[19] P. Simons, Parts: A Study in Ontology, Oxford: Oxford University Press, 1987.

[20] J. J. Thomson, ‘Parthood and Identity Across Time’, The Journal of Philosophy 80, pp. 201–220, 1983.

[21] B. Smith and K. Mulligan, “Pieces of a Theory,” in: B. Smith ed., Parts and Moments: Studies in Logic and Formal Ontology, Munich: Philosophia Verlag, 1982.

[22] B. Smith, Formal ontology, common sense, and cognitive science, International J. of Human-Computer Studies 43, 641-668, 1995.

[23] B. Smith, Basic Concepts of Formal Ontology, in Guarino (1995) pp. 19-28, 1998.

[24] B. Smith, Les objets sociaux,Pilosophiques 26:2, 315-347, 1999. English version at http://wings.buffalo.edu/philosophy/ontology/socobj.htm