Journal of Strategic Security

Volume 4
Number 2 *Volume 4, No. 2, Summer 2011: Strategic Security in the Cyber Age*

Article 5

The Science of Mission Assurance

Kamal Jabbour , Ph.D.
Air Force Research Laboratory, Rome, NY USA

Sarah Muccio , Ph.D.
Air Force Research Laboratory, Rome, NY USA

Follow this and additional works at: https://scholarcommons.usf.edu/jss

pp. 61-74

Recommended Citation
Jabbour, Kamal , Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no. 2 (2011) : 61-74.
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4
Available at: https://scholarcommons.usf.edu/jss/vol4/iss2/5

This Article is brought to you for free and open access by the Open Access Journals at Scholar Commons. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Journal of Strategic Security
Volume IV Issue 2 2011, pp. 61-74
DOI: 10.5038/1944-0472.4.2.4

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

The Science of Mission Assurance

Dr. Kamal Jabbour
Dr. Sarah Muccio
Air Force Research Laboratory
Rome, NY USA

Abstract

The intent of this article is to describe—and prescribe—a scientific framework for assuring mission essential functions in a contested cyber environment. Such a framework has profound national security implications as the American military increasingly depends on cyberspace to execute critical mission sets. In setting forth this prescribed course of action, the article will first decompose information systems into atomic processes that manipulate information at all six phases of the information lifecycle, then systematically define the mathematical rules that govern mission assurance.

Introduction

Perhaps more so than any of its peers worldwide, the U.S. Department of Defense (DoD) depends increasingly on cyberspace to execute critical missions that are vital to maintaining American military superiority in the traditional domains of land, sea, air, and space. As a result, the U.S. is arguably more at risk to an asymmetric attack vector launched by an adversary that cannot, or chooses not to, confront the U.S. in a conventional conflict. In the end, the military advantages that net-centricity provides the U.S. military concomitantly offer an adversary affordable attack vectors through cyberspace against critical missions and advanced weapon systems.

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms,[1] defines cyberspace as "a global domain within the information

Produced by The Berkeley Electronic Press, 2011

environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," *and* cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."

When the U.S. Air Force and the DoD formally identified cyberspace as a legitimate war-fighting domain on par with land, sea, air, and space, the attention focused initially on computer networks and the information that traverses them, and the desire to deliver—and the imperative to defend against—military effects in cyberspace. Recent studies by the Defense Science Board, as well as congressional and White House reports,[2, 3] concurred on the urgent national need to shift the cybersecurity posture from defending computer networks to assuring critical missions.

Mission Assurance

DoD Directive 3020.40 defines Mission Assurance (MA) as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan.[4] It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy." In accordance with this directive, a principal responsibility of a commander is to assure mission execution in a timely manner. The reliance of a Mission Essential Function (MEF) on cyberspace makes cyberspace a *center of gravity* an adversary may exploit and, in doing so, enable that adversary to directly engage the MEF without the employment of conventional forces or weapons.

For the operational purposes of mission assurance, cyberspace operations occur when a signal affects an intelligent system. In this definition,

- *Intelligent system* refers to a stored-program computer—any central processing unit (CPU) that executes a sequence of instructions
- *Signal* refers to an information-modulated waveform

Thus, a cyber operation occurs every time an external signal modifies the flow of control or information in an intelligent system.

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

This article proposes adopting the operational definition of a cyber process as a *program executing in an intelligent system*. This definition provides a foundation for mission assurance in a contested environment. Using intelligent systems as building blocks, we can decompose a mission into logically interconnected components of intelligent systems.

We characterize missions by the security attributes of the execution environments of their cyber processes and their communication processes. Mission criticality and prioritization dictate the level of granularity of the decomposition of a mission into cyber processes. This decomposition permits measuring the assurance of a mission as a function of its constituent components.

Mission assurance can focus on each cyber process and its interactions with internal and external processes as having potential vulnerabilities to external signals. Thus, the elemental activity of information communication among processes provides a focal analysis point for both specification and implementation vulnerabilities.

Decomposing a mission into its atomic cyber processes provides the means for specifying operational mitigation measures through the imposition of security attributes on these processes and their inter-process interactions. An atomic cyber process refers to the lowest architectural level at which a system generates, processes, stores, or transmits data. Security attributes include the fundamental information assurance (IA) tenets of confidentiality, integrity, availability, authentication, and attribution, as well as state-of-the-practice provision of these tenets through cryptography, diversity, agility, and trust.

Principles of War in the Cyber Domain

This section introduces warfare in the cyber domain, identifies the weaknesses of the traditional approach to building reliable systems, and leads to an alternative approach that seeks to build secure systems.

Engineering focuses traditionally on designing, developing, building, testing, and deploying complex systems that operate reliably in a permissive environment, but fail catastrophically in a contested environment. Mistaking reliability for security characterizes a generation of military, industrial, and financial systems that make little to no provision for functional vulnerability to cross-domain cyber threats.

Produced by The Berkeley Electronic Press, 2011

Rule 1 – Reliability does not equal security.

In this context, cybersecurity focuses disproportionately on threats—hackers, criminals, terrorists, and states—instead of system vulnerabilities. The National Institute of Standards and Technology (NIST) defines *risk to information systems* as "a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event" and a *threat* as "the potential for a particular threat-source to successfully exercise a particular vulnerability."[5] Threat and vulnerability are dependent variables in the NIST definition; thus a threat requires the existence of a vulnerability to exploit.

Rule 2 – There is no threat without vulnerability.

Cryptography enables the Information Assurance attributes of confidentiality, integrity, availability, authentication, and attribution as they apply to information at rest or in motion. For the purpose of MA, we further break down the states of information.

Rule 3 – An information system acts on information at one or more stages of the information lifecycle:

1. Information generation

2. Information processing

3. Information storage

4. Information communication

5. Information consumption

6. Information destruction

To permit functional representation of relationships among processes within a mission, we define a hierarchy whereby a mission consists of functions, a function consists of systems, a system consists of subsystems, a subsystem consists of components, and a component consists of indivisible atomic nodes. The number of layers in a decomposition—set arbitrarily at six—and the granularity of abstraction depend on the mission at hand. However, the two ends of the spectrum present bookends to the decomposition.

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

Rule 4 – A critical function—and for that matter a system or a subsystem—consists of a set of cooperating processes executing on atomic cyber nodes that generate, process, store, communicate, consume, or destroy information.

Corollary – Every atomic cyber process belongs to a function.

Mission dependence on cyberspace consists of the dependence on atomic cyber nodes within the mission, the internal interactions among these nodes, and their external interactions with the outside world. The hierarchical mission decomposition outlined above exhibits certain fractal properties. Provable properties between a system and its subsystems are also provable between a mission and its functions, a function and its systems, a subsystem and its components, and a component and its nodes.

Rule 5 – If a system generates information, then at least one of its subsystems generates information.

Corollary – If no subsystem generates information, then the parent system does not generate information.

Rule 5 and its corollary apply equally to information processing, storage, consumption, and destruction. For the purpose of this decomposition, an Input / Output (IO) communication node is bidirectional if it is capable of both information transmission and reception.

Rule 6 – If a system transmits or receives information, then at least one of its subsystems transmits or receives information.

Corollary – The fact that a subsystem transmits or receives information is not sufficient to conclude that the parent system transmits or receives information.

Rule 7 – Information exchange between systems occurs through paired transmit-receive IO nodes.

Rule 8 – An external threat exercises an internal vulnerability only through an IO node.

Rules 6–8 permit focusing vulnerability mitigation on external transmit nodes. Thus, a system without an external IO node does not present a vulnerability to external threats.

Produced by The Berkeley Electronic Press, 2011

Rule 9 – An internal threat at a higher layer becomes an external threat at a lower layer.

This rule offers a new way to address the insider threat to a system, reducing it to an external threat against an IO node in a vulnerable subsystem.

Rule 10 – A vulnerability in a subsystem becomes a vulnerability in a parent system if and only if the IO node in the subsystem is an external IO node in the parent system.

This rule allows limiting the impact of a weak link on a system by isolating the vulnerabilities of the weak link from potential threats in the outside world. The vulnerability extends to multiple missions that share a common function, system, subsystem, component, or node; and multiple functions and systems may share a component or node.

Rule 11 – A vulnerable system supporting two functions renders both functions vulnerable if and only if the vulnerable system contains an IO node that connects one of the functions to an external system.

The success of a cyberattack that follows the kill chain of a traditional kinetic operation—consisting of the distinct steps of Find, Fix, Track, Target, Engage, Assess (F2T2EA)—requires information resources at the target system, including process, store, and IO nodes, for each step of the kill chain. This provides an effective defensive strategy against this class of cyberattacks.

Rule 12 – Breaking the threat kill-chain at any phase of F2T2EA denies threat success.

Corollary – Assuring the kill chain of a friendly cyberattack requires assuring the information lifecycle at all phases of the F2T2EA.

Mission Assurance End Game

The ultimate goal of mission assurance is to develop an engineering culture that mathematically represents the specifications of a critical MEF and verifies its implementation. Representing a MEF as a fractal system of cyber systems with the help of queuing theory provides a tool for reasoning on security properties and proving certain relationships among vulnerabilities and threats.

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

Traditional formal verification suffers from state-space explosion as soon as the size of the system under consideration exceeds trivial classroom examples. Conversely, a fractal approach to MA avoids state-space explosion by sidestepping discrete simulations in favor of analytical estimation. IBM's Research Queuing RESQ package achieved similar efficiency by representing communications networks as queuing systems rather than discrete systems.[6]

While availability and mean time between failures (MTBF) provide useful metrics to estimate the reliability of complex systems of physical components, mission assurance requires different metrics. The intertwined properties of vulnerability and threat offer an unbounded continuum across which to measure mission assurance in terms of cost, transforming MA metrics into the economics of security.

Rule 13 – MA relates (1) the cost of securing a MEF and (2) the consequence of security failure to (3) the cost to a threat intent on exploiting the MEF and (4) the benefit to a successful threat.

The cost of security as a metric applies equally to future systems and existing systems. For the latter, MA relates the cost of vulnerability mitigation to the cost of threat success and the consequences in the cost of a failed mission.

The secure engineering practices proposed above hold promise for future system design, yet offer little relief to legacy systems. The next section of this paper presents stopgap measures to assure existing systems in a contested cyber environment.

Methodology

Mission assurance in a contested cyber domain requires a four-step process: (1) prioritization, (2) mapping, (3) vulnerability assessment, and (4) mitigation:

1. Prioritization: Develop a list of MEFs, and prioritize them with respect to the overall mission of a command. For those MEFs deemed critical, systematic cyber mitigation must follow the steps below. This prioritization step belongs to the mission commander and relies primarily on the domain experts who own the mission.

2. Mission mapping: Decompose each critical MEF into a number of layers that represent sub-functions, relationships, responsibilities, and

Produced by The Berkeley Electronic Press, 2011

systems, culminating in a logical representation of the atomic cyber processes that enable the MEF. Mission mapping requires collaboration between mission owners and cyber advisors. The fidelity of the mapping depends primarily on the criticality of the MEF in question.

3. Vulnerability assessment: Through a tabletop war game by a combined blue team of cyber experts and mission domain experts, conduct a systematic assessment of MEF susceptibility to process failures, and the vulnerability of both atomic cyber processes and inter-process communication to accidents and attacks. The success of this step requires a current understanding of the cyber threats capable of exploiting identified vulnerabilities.

4. Mitigation: Develop operational measures to mitigate the vulnerabilities identified in Step 3. Specify these measures as security attributes applicable to the atomic cyber processes and the inter-process communications among them.

5. Red teaming (optional): An optional fifth step in this process brings in an external red team of cyber aggressors to test the effectiveness of the mitigation measures.

The evolution of the cyber threat landscape dictates conducting this MA process at all stages of weapon-system development. In the notional timeline of the Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System,[7] conduct MA analysis at the Material Solution Analysis Phase (Milestone A), Technology Development Phase (Milestone B), Engineering and Manufacturing Development Phase (Milestone C), Production and Deployment Phase (Initial Operating Condition), and Operations and Support Phase (Full Operating Condition.)

Prioritization

The prioritization step belongs to the mission commander and deals with identifying and prioritizing the critical functions, scoping the mission mapping activity, and establishing boundaries. MEF prioritization is fundamentally a non-cyber process and includes:

- Defining explicitly the scope of the study by enumerating the MEFs of interest
- Specifying the interfaces of the MEFs to their surroundings and the external world

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

- Prioritizing the MEFs as an initial assessment of acceptable risk
- Understanding the priorities of the mission commander permits the cyber engineer to estimate the granularity of the cyber mapping as a function of MEF criticality

Mission Mapping

Mapping mission dependence in cyberspace requires identifying the atomic cyber processes that make up the mission. Mission mapping includes the following steps:

- Decompose the mission into its constituent components.
- Identify all the stored-program processors in an MEF in the atomic cyber processes
- Identify the make and model of each processor, the fabrication technology, clock speed, storage architecture, amount of cache and primary storage, and input/output devices.
- Define the function of each processor—sensing, computing, storing, or transmitting data.
- Identify all data storage components within an MEF.
- Identify all data communication among cyber processes, and between the MEF and the outside world.
- List all the architectural layers that each processor implements.
- List all the programs that the processor executes at each layer.
- Characterize non-volatile storage in terms of pedigree, technology, and capacity.
- Document the data format, speed, and protocol for each data communication process.

Vulnerability Assessment

Mapping mission dependence on cyberspace generates a detailed diagram of the functionality of each atomic cyber process and the interaction among connected processes. This diagram facilitates and enables educated and informed cyber experts to conduct a meaningful and realistic

Produced by The Berkeley Electronic Press, 2011

tabletop blue team vulnerability assessment for each process based on known threats. The ultimate goal is to provide a quantitative risk assessment of each process and to use these assessments to compute an overall mission assurance. Vulnerability assessment includes the following steps:

- For each sensor, assess its potential malicious use as an entry vector into the system.
- For each processing unit, estimate the risk based on the software it executes and the documented vulnerabilities and threats.
- For each storage unit, estimate the vulnerabilities and threats.
- For each data communication channel, estimate the threats to protocol and implementation vulnerabilities.
- For each vulnerability, define its temporal and spatial properties and estimate their effects.
- Where feasible, combine into a larger cyber process those adjacent atomic cyber processes that share storage or communication resources.
- Compute an overall mission assurance metric as a measure of MEF susceptibility to cyber threats and as an input to inform a mission commander about risk management.

Threat Mitigation

Mitigation strategies focus on those atomic cyber processes, sensors, storage units, and inter-process communications that present the largest vulnerability surface for unintended cyber incidents and malicious cyber attacks. Mitigation strategies include measures to reduce the exposure to, and impact of, a cyber compromise, such as:

- Defensive posture realignment from intrusion detection to threat denial
- Physical and logical system isolation
- Virtualization and MEF recomposition
- Static threat avoidance by moving vulnerabilities out of band through system redesign

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

- Domain modification through protocol flattening, just-in-time implementation, and hardware-software tradeoffs
- Polymorphism through protocol and implementation modification
- Agility for real-time dynamic threat avoidance
- Hardening of the information assurance attribute of confidentiality through encryption
- Application of authentication measures
- Redundancy and artificial diversity to protect against monoculture vulnerability
- Compilation into hardware-critical software segments to protect against modification
- Selective insertion of Government Off The Shelf (GOTS) technology into Commercial Off The Shelf (COTS) systems to harden against common threats

Red Teaming (Optional)

The utility of red teaming is limited by the ability of the red team to accurately replicate the adversarial threat to a given mission. Aggressors have traditionally employed a three-step strategy that has been consistently effective over time, but has yet to be proven in the cyber domain. This strategy involves the following:

- Understand the threat
- Replicate the threat
- Exercise the threat

While this strategy works well against poorly-protected computer networks, it falls short in assessing the vulnerability of a critical MEF to cyberattack for two key reasons. First, aggressors have little documentation of threats against DoD MEFs that they can understand, let alone replicate and exercise. Second, aggressors typically lack domain expertise in specific MEFs, making their network attacks inconsequential to MEF execution.

Produced by The Berkeley Electronic Press, 2011

This optional step of red teaming serves to satisfy the misplaced belief in the usefulness of red team assessment of mission assurance. While red teaming has no drawbacks, its contribution remains inherently limited. The failure to compromise a system may be evidence of red team inexperience, not system resilience. We must not confuse the absence of evidence of vulnerability as evidence of the absence of vulnerability.

Multidimensional Dependencies

We have so far outlined in this article a methodology to map the dependence of MEFs on the underlying cyber infrastructure. Static mapping assumes that MEF dependence on cyber remains constant in time and location. This section examines MEF temporal and spatial dependencies.

Short-term temporal changes in mission assurance can occur in the normal course of mission execution. These changes occur when mission execution transitions among processes with different vulnerabilities. Long-term trends affecting mission assurance result from technology obsolescence, vulnerability discovery, and threat evolution. Long-term trends necessitate the reassessment of mission assurance on a periodic basis, especially over the lifecycle development of a weapon system.

Spatial dependencies occur when a system encounters different threats based on their geographic location. Kinetic threats unfold in a substantially different extent on a battlefield than in a home-base environment. Similarly, certain systems may encounter location-specific cyber threats that dictate a recomputation of mission assurance on a regional basis.

The granularity of the mission mapping may affect the fidelity of the mission assurance estimate. Too coarse a system-level decomposition may overlook device-level vulnerabilities. Too fine a device-level decomposition may miss system-level dependencies.

Conclusion

This article explored the critical vulnerability facing the Department of Defense, namely the dependence of critical MEFs on a contested cyberspace. Additionally, the article described the cyber environment, identified a method to catalog cyber vulnerabilities that may provide attack vectors against MEFs, and outlined a methodology to assure these MEFs in a contested cyber environment. The prescription for DoD MEF assurance laid out a series of steps, starting with prioritizing missions, mapping their dependence on the cyber domain, identifying vulnerabilities,

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4

and mitigating these vulnerabilities. Finally, it offered a set of rules to guide the design of future systems, as well as a stopgap approach for assuring legacy systems.

About the Authors

Dr. Kamal T. Jabbour, ST, (B.E. Electrical Engineering with Distinction, American University of Beirut; Ph.D. Electrical Engineering, University of Salford), a member of the scientific and technical cadre of senior executives, is the Air Force Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Rome, N.Y. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities, and industry.

Dr. Sarah L. Muccio (B.S. Mathematics, Summa Cum Laude, Youngstown State University; M.S., Ph.D. Applied Mathematics, North Carolina State University) is a mathematician for the Cyber Science Branch of the Information Directorate, Air Force Research Laboratory, Rome, NY. In the field of information assurance, Dr. Muccio works with scientists to mathematically model systems and analyze information. She conducts research on emerging technologies and maps mission-essential functions to their cyber assets. Dr. Muccio enjoys educating future cyber security leaders through several Syracuse University graduate courses that she co-created, as well as through the Advanced Course in Engineering (ACE) program.

Acknowledgement

This material is based upon work supported by the Air Force Office of Scientific Research under the Laboratory Research Independent Research Program under grant number FA8750-10-C-0116.

Produced by The Berkeley Electronic Press, 2011

References

1 Joint Publication 1-02, Department of Defense (DoD) Dictionary of Military and Associated Terms, September 2010, available at: *http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf*.

2 "Securing Cyberspace for the 44th Presidency," *Center for Strategic and International Security (CSIS)*, December 2008, available at: *http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf*.

3 White House, *Cyberspace Policy Review*, May 2009, available at: *http://tinyurl.com/nzdbjw (www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)*.

4 Department of Defense DoD Directive 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, July 2010, available at: *http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf*.

5 Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, NIST Special Publication 800–30, July 2002, available at: *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*.

6 C.H. Sauer, M. Reiser, E.A. MacNair, "RESQ: A Package for Solution of Generalized Queueing Networks," Proceedings of the AFIPS Joint Computer Conference, June 13–16, 1977.

7 *Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System*, Defense Acquisition University, December 2008.

https://scholarcommons.usf.edu/jss/vol4/iss2/5
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.4