

A Research Agenda for Survivable Systems

*Richard C. Linger, John McHugh, Nancy R. Mead,
Robert Ellison, Howard F. Lipson, Thomas Longstaff*
Software Engineering Institute
Carnegie Mellon University

Toward a Science of Information Assurance

Modern society exhibits pervasive dependency on large-scale information systems of unprecedented scope and complexity. Ever-increasing consequences of intrusion and compromise highlight the urgent need to assure survivability of these systems in adverse environments [1, 2, 3]. Unfortunately, the existing science base for information assurance in large-scale systems is inadequate to deal with this challenge.

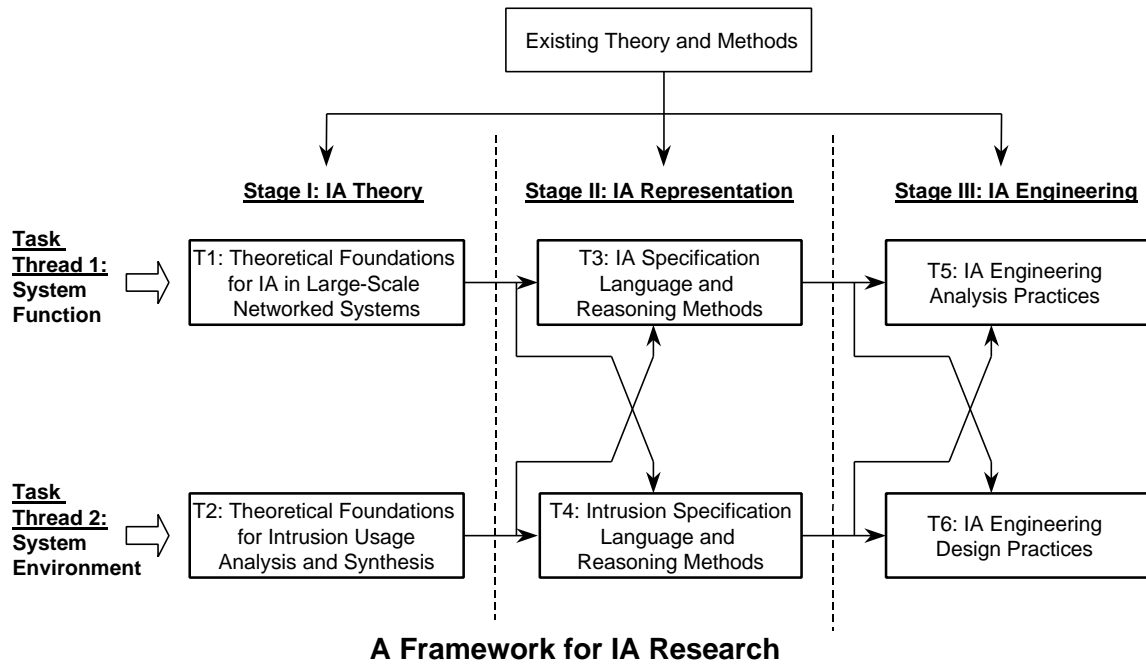
Many problems in information assurance today result from lack of theoretical foundations upon which to base an integrated IA engineering discipline. A scientific basis for IA will permit rigorous definition of the behavior and structure of large-scale systems and their intrusion usage. Survivable systems cannot be developed without engineering specifications of intrusion patterns, and intrusion vulnerabilities cannot be eliminated in the absence of engineering specifications for systems attacked. What is needed is to get beyond present natural language and graphical descriptions of systems and intrusions, toward a computational semantics for information assurance. Theoretical foundations will permit definition of specification languages to describe system IA capabilities and intrusion environments, development of methods and tools for automated IA reasoning, and creation of IA engineering practices. Improved methods for abstraction and decomposition are required to deal with the complexities of large-scale systems. Such methods must be essentially scale-free, and exhibit critical properties of compositionality and referential transparency.

As depicted in the figure below, two interdependent research threads are required, one for systems subject to intrusions and one for system environments from which intrusions arise. Each thread can progress through three stages. The first, IA Theory, defines scientific principles for information assurance. The second, IA Representation, defines specification languages and reasoning methods and tools based on the theoretical findings. The third, IA Engineering, defines engineering practices for analysis and design, based on the theoretical foundations, specification languages, and reasoning methods.

At present, no comprehensive theory of information systems exists that can guide construction and evaluation of IA in large-scale systems. As a result, creating an acceptable level of information assurance in these systems exceeds current capabilities. Scalable theoretical foundations for specifying, analyzing, and designing these systems are lacking. Without this theoretical basis, much IA research has resulted in localized point solutions whose extensive assumptions often swamp anticipated benefits. Moreover, many existing theories, in return for simplicity and elegance, abstract out the very complexities of a system that cause failures and vulnerabilities. For example, many system modeling approaches require that faults be independent, thereby preventing analysis of cascading and correlated failures.

An appropriate theoretical formalism will provide a basis for a wide range of activities. One of the most important of these is the construction of abstract models that can capture the essence of a

system under analysis so that one can reason about the presence (or absence) of critical IA properties. In the words of John Rushby, this ensures that a system is not required to be insecure. At the other end of the spectrum, theory must permit refinement down to the implementation level so that reasoning about details – for example, at the level of buffer overflows – is also possible, thereby protecting a system at the register level where it is vulnerable. In essence, the theory must be readily scalable, with mathematical reasoning methods employed at all levels of abstraction.



Research Objectives

Existing and well-understood, but little utilized, theoretical frameworks may well serve as a starting point for a science of IA. For example, it is well known that computer programs are rules for implementing mathematical functions or relations [4]. This is true regardless of program subject matter or language. This function-theoretic view permits information assurance problems and solutions to be expressed within the rigorous semantic framework of functions and relations.

Many vulnerabilities in programs are simply the result of implementing the wrong function. A common solution to the “wrong function” problem is to develop patches that, when mathematically composed with the original program, provide the correct function. Function-theoretic methods can permit reuse of decades of research and development in software function theory, representation methods, and engineering practices that have seen little application to IA problems.

The table below depicts a set of objectives and potential outcomes for the research agenda of defined in the figure.

| Activity | Objective | Potential Outcome |
|---|---|--|
| Task 1: Theoretical Foundations for Large-Scale Networked Systems | Mathematics-based logical systems incorporating theorems and principles for defining the behavior and structure of IA in large-scale systems. | Scientific basis for research, analysis, design, and measurement of information assurance. |
| Task 2: Theoretical Foundations for Intrusion Analysis and Synthesis | Mathematics-based logical systems incorporating theorems and principles for defining the structure and content of intrusions. | Scientific basis for intrusion research, analysis, enumeration, prediction, detection, and measurement. |
| Task 3: IA Specification Language and Reasoning Methods | Syntax and semantics of IA language structures, together with abstraction and composition methods for reasoning about IA. | Systematic representation and reasoning for IA research, specification, analysis, and design. |
| Task 4: Intrusion Specification Language and Reasoning Methods | Syntax and semantics of intrusion language structures, together with abstraction and composition methods for reasoning about intrusions. | Systematic representation and reasoning for intrusion research, enumeration, prediction, detection, and measurement. |
| Task 5: IA Engineering Analysis Practices | Set of CMM-style engineering and management practices for analyzing IA capabilities in existing and new systems. | Repeatable engineering discipline for IA analysis and improvement. |
| Task 6: IA Engineering Design Practices | Set of CMM-style engineering and management practices for designing IA capabilities in existing and new systems. | Repeatable engineering discipline for IA specification and design. |

Current research plans involve initiation of Tasks 1 and 2. We plan a parallel activity to apply the findings of these tasks to development of survivability architecture patterns. This work will serve as a validation vehicle for results achieved. We welcome partners and sponsors in this work.

References

1. *Survivable Network Systems: An Emerging Discipline*, Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, November 1997.

2. Linger, R.C., Mead, N.R., and Lipson, H.F., *Requirements Definition for Survivable Network Systems*, International Conference on Requirements Engineering, Colorado Springs, CO, IEEE Computer Society, Available online at <http://www.cert.org/research>, 1998.
3. Ellison, R.J., Linger, R.C., Longstaff, T., and Mead, N.R., *A Case Study in Survivable Network System Analysis*, CMU/SEI-98-TR-014, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, September 1998.
4. Prowell, S.J., Trammell, C.J., Linger, R.C., and Poore, J.H., *Cleanroom Software Engineering: Technology and Process*, Addison-Wesley, Reading, MS, 1999.