Extended Abstract
Quantifying the vulnerability of tactical data networks

Andy Loebl, James Nutaro, and Teja Kuruganti
Oak Ridge National Laboratory
{loeblas,nutarojj,kurugantipv}@ornl.gov
Rajanikanth Jammalamadaka
University of Arizona
rajani@ece.arizona.edu
September 22, 2006

Overview

Experience with the first five generations of modern military data networks has shown a need to address physical and operational security of computer based functions. The sixth generation of large scale, complex systems software represents a major change in how computing and communications will support military operations. This new paradigm requires that network security and information assurance be addressed in the earliest phases of the system life cycle. An affordable and deployable system must begin with an analysis of security requirements in the context of anticipated operational use. How the network is used and operated is likely to have a significant impact on its intrinsic security. This paper takes a first step towards establishing requirements oriented models to assess security needs in the context of overall system performance objectives. This paper presents an abstract and, in this first issuance, a simplified view of network security and information assurance as it pertains to the evolving vision of network centric warfare. When system requirements can be quantified, it is possible to make informed technical decisions concerning development options and expected functionality. If important functional requirements can be broadly understood and quantified, then accurate and precise answers concerning a design's adequacy can be given early in the design lifetime. This, in turn, will significantly reduce the overall cost of the system.

.

Introduction

Cost reduction and expected reliable performance are two goals of model based system design. This is especially true for the design of weapon systems and command and control systems, which are particularly difficult to test in situ. The coming generation of complex systems, and the Future Combat System in particular, will be tested

piecemeal prior to their combat debuts. This makes model based studies the only way to predict the overall performance of these systems prior to their critical use. Informative model based studies must be built on quantifiable definitions of performance metrics.

The ability to share data is a critical feature of the Future Combat System. In the absence of heavy armor, superior situational awareness and understanding are essential for an engaged unit to survive and complete its mission. Because the Future Combat System is a highly mobile force, data sharing will be enabled by an ad hoc, wireless data network. This network will need to be robust, reliable, and carry a great quantity of information. It will, therefore, be expensive.

Stringent performance requirements and the anticipated high cost of the Future Combat System data network strongly motivates careful identification of its functional requirements. The most essential requirements must be quanifiable to allow for early, model based studies of proposed designs. Network security is one of these critical requirements, and one that should be subjected to early, detailed, and methodical scrutiny. This paper recommends a research effort to develop a methodology for analyzing network security and information assurance requirements for network centric combat systems. A security focused requirements analysis methodology is essential if affordable and deployable network centric systems are going to be produced.

The remainder of this paper presents a preliminary model that serves to illustrate how security related requirements analysis might be conducted. However, only a few of the many security and performance attributes1 of modern systems (or system of systems) are empirically understood. A comprehensive analysis methodology is beyond the scope of this paper; a complete methodology will require an intensive and focused research effort.

The benefit of pursuing such a research agenda will be a quantifiable understanding of security and assurance requirements as they relate to modern tactical data networks. If successful, there will be two long term benefits. First, a substantial reduction in the lifetime cost of these systems will be possible due to a reduction in experimental development, improved system of systems testing and validation, and reduced maintenance and configuration management costs. Second, the operational performance of network centric systems (or system of systems) will be improved. These benefits will be the result of a precise understanding and articulation of system performance requirements.