CrossTalk would like to thank NAVAIR for sponsoring this issue.

As we see technology evolving, we are also bearing witness to the evolution of software development and software itself. These advances in software have been forged from the necessity of affordable improvements. From a programmatic perspective, it is not always cost effective to update hardware when there is an improvement. Therefore, we depend on software continuously leveraging that hardware to yield performance improvements. This ever-increasing reliance on software means that our requirements and the way we protect our systems cannot be a last-minute addition.

Newton's Third Law of Motion says that for every action there is an equal and opposite reaction. In the case of advancements in software, that opposite reaction is the advancement of threats against that software. Attacks continue to take advantage of technology and the dependence we have on software. In order to stay ahead of this curve, we must look to how we design and secure systems for tomorrow's threats.

The task of designing and securing systems is easier said than done. We are no longer dealing with network diagrams that can be drawn on one sheet of paper. Long gone are the days when your computer connected to a few other nodes in the network, then a single connection to the Internet. We are now faced with protecting systems that move in and out of multiple heterogeneous networks. The networks are scalable and rely more on near-real time or real time data. With multiple access points and ever changing users, we have to escalate to more than virus protection and firewalls.

When these nodes are aircraft and other military systems, the need for data on demand is even more critical. Information Assurance (IA) is therefore a key component to the protection and availability of our required data. However, we often regard the development of these IA requirements as an afterthought. Bringing the entire system performance in line with protecting its information has to be considered with both the risk and associated cost.

One approach to bring this field to the forefront is that of Real Time Information Assurance. This is increasingly important because our systems are in a constant state of flux. Changing users, conditions, incoming data and the need for that information to be processed and disseminated is making it harder to assign controls in the early stages of a project's design phase. We try to capture the flow of information in order to better secure it in the future. However, we cannot ever anticipate the demand and use of our systems at all times under all scenarios. Therefore, we need an adaptable manner in which to protect our systems depending on the complex state or states in which they are currently operating.

From the user perspective, the systems and the required information needed by those systems should be available at all times. With greater attention being focused on authentication, we cannot burden the users with additional wait times for validation. To the user, access of information and systems should be seamless. To an un-authorized user, access should be impossible or at the very least time consuming to the point that the information is no longer valid or useful. Analyzing these conditions in real time, can allow the best of both worlds.

The application of Real Time IA can aid a program in finding that ideal balance of cost, schedule and performance with security in mind. I hope you enjoy the articles in this issue of CrossTalk and consider their applicability to future programs. As you read, begin to think not only about Real Time IA, but to the future of Predictive IA.

Felipe Jauregui
Chief Engineer, H-1 Weapons System Support Activity
NAVAIR