Computer Security Aspects of Dependable Avionics Systems: Position Paper

Jim Alves-Foss

Introduction

Information assurance addresses issues of confidentiality, integrity and availability. In avionics systems, information integrity and availability have been key aspects of system certification. However, most certification practices have dealt with verification and validation of systems in the presence of non-malicious faults. Computer security addresses issues of malicious behavior, where system faults are introduced through deliberate behavior. Now, where we used to use fault predication probabilities, we have to assume high probability of attack from uncertified or untrusted systems. Although there are tremendous needs in many research aspects of certifiably dependable avionics systems, I will specifically address concerns related to computer security.

Important Challenges:

Certification of security aspect of systems is a difficult task. In addition to showing that the system does all the right tings, it is necessary to show that the system does not do the wrong things, even in the presence of multiple, dependent malicious events. Researchers have shown that they can prove small tractable components are secure, but have difficulty when it comes to proving system security. Here I highlight three main areas that I believe will have the most impact on certifiably dependable systems with respect to security.

Compositionality of certified components

One of the most difficult problems facing computer security certification activities, is the ability to compose certified components such that we are guaranteed a system that satisfies the desired properties, even when the properties are emergent. Composition must include three types of composition

- peer-to-peer composition, where two certified components communicate with each other, possibly relying on each other's correct behavior
- hierarchical composition, where one certified component relies upon the correct behavior of another component when they are composed through layering
- and extensional composition, when one component encapsulates another (such as inclusion of as a trusted library)

In the malicious security world there are so many possible interactions between components that we must be able to evaluate all of them. However, certification artifacts may not provide sufficient information or even address all the security parameters or aspects that we are interested in. Paul Karger of IBM has provided a good summary of these problems in some of his talks.

Maintenance of security certification

In addition to composition of security components, there is a need for V&V technologies that can be applied incrementally throughout the product life-cycle. It is essential that we learn how changes to a system affect the certification and how to re-certify a component or system that has undergone changes.

Impact of security on performance

For avionics systems or other real-time systems it is imperative that security technologies do not impair performance to the point where the system becomes unusable. At the same time, we can no longer afford to allow developers to ignore security concerns with claims of performance loss. There is a need for development of security metrics that determine the strength of specific security technologies as well as performance impacts. These technologies may include new architectural approaches, and new certification technologies that reduce the need for high impact run-time mechanisms.

Information Technology Research Needs

Development of large-scale exemplary systems for academic use
There is a strong need for academic researchers across the nation to have access to large scale software systems of reasonable complexity. There are many talented researchers around the nation, many at small schools where they may be the only researcher in their area. These researchers do not have the resources or contacts that larger universities enjoy. If these researchers had access to exemplary software, simulation systems and other commercial-grade systems, they could help make substantial in-roads to the current challenges. Also, large scale exemplary systems would reduce costs in redevelopment at each lab.

Merger of security, safety and avionics communities
Although there are instances of interdisciplinary work, there is still a strong need for cross-education. From the security side I am often disappointed when I see proposed solutions or analyses that show a lack of fundamental understanding of computer security. One recent paper assumed that there was a direct correlation between computation time and strength of cryptographic algorithms, which is not true.

Open-minded funding programs
As a researcher at a small university, I am disappointed when research proposals come back with comments such as: "researcher's teaching load is too high to conduct high impact research", or "the researchers should look at/spend time at 'big-name' university to understand the problem". I served on an NSF panel recently where one panelist said "this researcher has an excellent track record on obtaining funding, we should fund him." We need program managers and panelists to take more risks in funding small exploratory projects at academic institutions of different sizes, and not just continue funding those who have been funded in the past. Innovation can come from out-of-the way places.

Optimistic Road Map for Next 5-10 Years

1-4 years out
- Architectures and design processed to reduce composition and life-cycle based certification costs
- Development of small-scale exemplary sub-systems (for UAV's, Command and Control)
- Distribution of operational data (data rates, throughput needs, real-time data measurements)
- Development of interdisciplinary venues and curriculum materials

4-8 years
- Provable mathematical models of composition and life-cycle based cost reduction.
- Development of medium-scale exemplary systems for researchers
- Certification standards based on new technologies
- Preliminary adoption by industry

8-10 years
- Feedback from industry and revision of certification technologies
- Modified standards and full adoption by industry

Biography:

Dr. Alves-Foss is the Director of the University of Idaho's Center for Secure and Dependable Systems and is a professor of computer science. He received his BS degree in mathematics and computer science and physics from the University of California at Davis in 1987, and his MS and PhD degrees in computer science from the University of California at Davis in 1989 and 1991 respectively. His main research interests are in the design and analysis of secure distributed systems, with a focus on formal methods and software engineering. Dr. Alves-Foss is a senior member of the IEEE.

Dr. Jim Alves-Foss, Director, Center for Secure and Dependable Systems, University of Idaho, POBOX 441008, Moscow, ID 83844-1008, jimaf@uidaho.edu, (208)-885-5196