

# Intrusion Tolerant Systems

Jaynarayan H. Lala  
Defense Advanced Research Projects Agency  
[jlala@darpa.mil](mailto:jlala@darpa.mil)

The United States Department of Defense mission is becoming increasingly dependent on the correct functioning and availability of Defense Information Infrastructure (DII). At the same time, the threats posed to DII from hackers to nation-states are becoming more serious at an alarming rate. The Defense Advanced Research Projects Agency (DARPA) has initiated a major new research and development effort, entitled "Third Generation Security (3GS)", to take on this challenge of national importance. Major technical thrusts of this effort include system survivability and resilience in the face of information attacks, capability to see, control and maneuver in cyberspace, and an assessment and validation of these properties.

The DoD information systems currently are potential targets of attackers exploiting vulnerabilities via malicious and mobile code, distributed denial of service and other multiplier attacks, misuse and malicious insiders, and wireless and non-IP attacks. The DoD needs operational systems that can operate through attacks, gracefully degrade functions and capabilities in the face of attacks while keeping as many critical functions going as possible, and be able to dynamically configure themselves to optimize performance, functionality and security.

DARPA is sponsoring a number of advanced research and development projects to address the DoD system vulnerabilities and create fundamentally sound architectures to possess the desired survivability attributes. In particular, the Organically Assured and Survivable Information Systems (OASIS) program has about 30 projects that are researching the means for tolerating intrusions and attacks.

First generation security systems relied on cryptography, trusted computing base, authentication, firewalls, access control, and other perimeter defenses to keep intruders out. Although this approach was successful for a highly selected set of users, the current inter-networked environment makes it unaffordable and impractical. Furthermore, it does not provide adequate defenses against malicious insiders, life-cycle threats, mobile code, and widespread use of commercial off-the-shelf components of unknown trustworthiness. Second generation security involved intrusion detection systems to flag the now commonplace breaches of defenses. We have come to the realization now that despite all the defenses, some of the attacks will inevitably be successful. We must build systems that can operate through these attacks. Intrusion tolerant systems will provide the third generation security.

There is no silver bullet that will provide intrusion tolerance. Multiple layers of tolerance must be built into the systems. The first of these layers is the Real-Time Execution Monitors. This is a set of mechanisms that, in general, is invoked at run time. Before the software module executes or as each instruction executes, its consequences are determined. If security policy will be violated, the execution is preempted. Examples of these mechanisms include proof-carrying code, in-line reference monitors, wrappers, and sandboxes.

Execution monitors will not have 100% coverage. Some attacks will leak through. The next tolerance layer will detect errors and prevent their propagation. Value and time domain checks, comparison of redundant computations are some of the means successfully employed in fault tolerant systems to detect errors. However, to detect errors caused by intentional faults, one must take into account the common vulnerabilities of redundant computations, as has been done for other potential common mode failures.

To provide continued correct operation, error propagation must be prevented, damage must be repaired, and system resources reallocated so that mission-critical functions are given prioritized use of remaining trustworthy components, and system functionality degrades gracefully. Fundamentally new architectures, employing temporal, spatial, and data redundancies, agile reconfiguration, and real-time quality-of-service trade-offs have the potential for providing the last layer of intrusion tolerance. Again, unlike random hardware failures, intrusions and attacks pose challenges akin to software errors, environmental effects and other common mode failures. Design diversity, randomness and uncertainty are some of the additional weapons to be employed against intentional faults.

Intrusion tolerant systems herald a new era of survivability in the face of malicious insiders, intruders and attackers. The third generation secure systems will shift the security paradigm from keeping intruders out at all costs to a more cost-effective and affordable combination of avoidance/prevention, detection, and tolerance.