# Multiple Independent Levels of Security:
## *The Changing Face of Range Information Management in the 21st Century*

**G. Derrick Hinton**
Central Test and Evaluation Investment Program (CTEIP),
Test Resource Management Center (TRMC), Arlington, Virginia

Imagine a test scenario where an aircraft is flying toward a target on a test range, and a millimeter-wave radar is illuminating the aircraft's low-observable profile as the aircraft launches a highly classified air-to-surface missile, which homes in on the target. Meanwhile, across the range, a coalition training exercise is underway, with an Airborne Warning and Control System (AWACS) aircraft using the test aircraft as a target of opportunity to vector German and British aircraft for a defensive counter-air intercept mission. Range controllers are simultaneously monitoring both events for safety and quality of data, providing real-time feedback such as achievement of test mission parameters and real-time kill notification. Information classified at multiple security levels (unclassified, Secret, NATO Secret, and Top Secret/Special Access Required) flows seamlessly to and from assets on the range, being used and processed by platforms at the levels for which the platforms are cleared.

Sounds far-fetched? Hardly. Range events and capabilities are already being designed to support just such a scenario. As the Global Information Grid becomes a reality, it is becoming less and less feasible to isolate a system under test, or a training participant, from the information-rich environment in which it operates. At issue is how Department of Defense ranges can effectively control and manage information across multiple access levels without compromising security, diminishing operational realism, or escalating the cost or complexity of effective range operations.

Ranges have traditionally taken the "system high" approach to data handling when multiple classification levels are involved, immediately classifying all data at the highest level of any data involved and requiring all participants to operate at that level. While such an approach mitigates the need for complex multiple security level processing, it can restrict the participation of systems and warfighters that cannot access data at the highest level.

Seamlessly sharing data among participants with different clearance levels is clearly a high-priority goal of operational system and range infrastructure developers. The increased demand to train and fight with coalition partners, using a mixture of "white-world" and highly classified weapons and information, has led the operational community to grapple with how to implement "multiple independent levels of security" (MILS) to share data among warfighters possessing various clearance levels.

A variety of MILS solutions have been considered in recent years. The optimum approach to MILS is the implementation of Multilevel Security (MLS), in which a single processing device is designed to segment and route data to the appropriate end user at each node in the network. Chipsets and devices have been developed to facilitate a true MLS network topology, but accreditation of MLS systems has proven elusive, largely due to design costs and

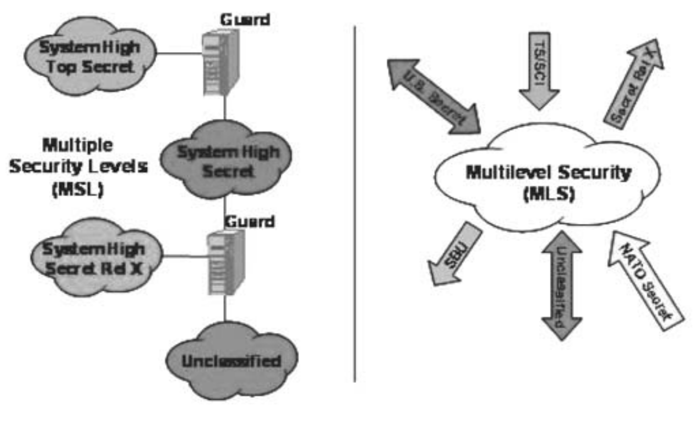

Figure 1. Multiple Security Levels (MSL) versus Multilevel Security (MLS)

the intensive testing required to verify the fidelity of MLS devices.

Due to the difficulty of implementing and accrediting MLS, many organizations have adopted a Multiple Security Levels (MSL) approach *(see left side of Figure 1)*. In the MSL approach, security point solutions, such as guards and firewalls, are placed in the system architecture to connect two or more security domains in the "system high" mode of operation. The advantage of this strategy is that "system high" operation is a relatively straightforward security implementation that has been used for many years. As a result, an MSL system can extensively utilize commercial off-the-shelf technology and offers less developmental and accreditation risk. On the downside, the MSL approach may degrade performance and may require the replication of hardware, software, staff and processes in each domain to accomplish the security gateway function at each classification level. Because the "system high" domains may not be entirely independent of each other, one or more guards may be needed to control the flow of any information between the domains.

An example of an MSL system that uses multiple single levels of security could include a "trusted guard" processor that sorts information by security level and routes it to an individual process where only that level of data (or lower) is handled. While the "payload data"—the key pieces of information to be passed over the network—are black (or encrypted), the header data remain red (or unclassified), and they contain information about the security level of the payload data. A similar topology simply uses different encryption keys to represent the different levels of security in a network. When messages are passed over the network, any message for which a participant does not have the appropriate key is rejected.

This improved approach allows for network message handling across different security layers; however, it invariably has critical limitations. One of those limitations is that any data, once introduced to a higher security level, are not readily downgraded to a lower level without human intervention. Second, it requires duplicate hardware components, often at multiple nodes, to be effective. This increases the cost of operation for computer platforms, cabling, maintenance and staffing. In contrast, an MLS system solution *(right side of Figure 1)* offers additional security functionality and assurance and requires little or no replication of hardware, software and processes. However, the cost of an MLS system may still be significantly higher than the cost of an MSL system, due to reliance on complex government off-the-shelf technology and management of increased developmental and accreditation risks.

Current MLS systems are custom, single-use designs that utilize very specific security protocols. To make MLS solutions practical for the test and evaluation community, new MLS technologies must be developed. Central to this effort must be a single security processor capable of handling and parsing data from multiple sources at different classification levels. This requires an advanced authentication and verification protocol that ensures information is distributed only to those with appropriate access. It also requires advanced intrusion detection algorithms to prevent unauthorized access or masquerading as an authorized user. Encryption and decryption will be central to all of these processes, and the processor must be able to account for multiple encryption schemes that may be employed at all levels of classification. On top of this, all of these functions must be implemented in such a way as to minimize processing delays, ideally in real time.

Regardless of the technological approach to MILS that is ultimately used, it is clear that ranges must adapt to this emerging requirement. Coordinated coalition warfare means sharing the right data with the right people at the right level. To test systems and train the forces to operate in this environment, the range community needs to position itself to take advantage of emerging MILS techniques and solutions as they become available. ❑

*G. DERRICK HINTON is program manager, Central Test and Evaluation Investment Program, for the Joint Investment Programs and Policy deputate under the Test Resource Management Center, Arlington, Virginia. He is also chairman of the ITEA Technology Committee* ***(itea@itea.org, Attn: G. Derrick Hinton, Chairman).***