International Authentication Program
At Pacific Northwest National Laboratory

Authentication is a process for establishing Monitoring Party trust in monitoring systems, often provided by a Host Party, for use in gaining confidence in compliance with non-proliferation or disarmament agreements. Authentication helps assure the Monitor that accurate and reliable information is provided by monitoring systems and that any irregularities are detected. PNNL researchers are developing the procedures and tools to be used for the authentication of systems now planned or contemplated for arms-reduction, arms-control, and non-proliferation applications.

BACKGROUND

Attribute measurement systems are being developed or are planned in support of various arms-reduction agreements and negotiations. Under one bilateral agreement, the Department of Defense's Defense Threat Reduction Agency Cooperative Threat Reduction (DoD DTRA/CTR) program is constructing the Fissile Material Storage Facility (FMSF) at Mayak, Russia, to hold 50 tons of plutonium, and possibly highly enriched uranium, from the disassembly of nuclear weapons. Negotiations are being held with the Russian Federation for cooperative development of attribute measurement systems for use at the FMSF. PNNL has played a role in the development process for the attribute measurement systems, with a leading role involving the design-basis for the information barriers (IB) of such systems.

PNNL is providing authentication services for the CTR program to satisfy the need for an authentication team and an Authentication Laboratory where U.S. and Russian Federation attribute measurement systems can be evaluated, tested, and validated.

AUTHENTICATION APPROACHES

Authentication is defined as "the process through which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item." Authentication of a system means the use of reference unclassified calibration sources, evaluation of complete design documentation for all hardware and software, tamper indicating devices, and/or random selection of system hardware and software modules to gain confidence that the system functions to accurately report the results of measurements and to protect classified information.

The Monitoring Party would plan to completely examine and independently authenticate each component or module of a host-supplied system. There are two basic requirements of an monitoring system: protection of classified information during and after measurements, and credible performance of the system for the measurement. Under the "host-supply" scenario, where the Host would supply the system to be used by the Monitor in a Host facility, the crucial authentication issues are that a measurement system correctly measures the attributes, and that there be no hidden switches in the system to pass erroneous information. To authenticate a system, a set of approaches and tools are used:

- Functional Testing Using Calibration Sources. Radiation sources play an important role in verifying the correct function of a monitoring system. Functional testing can only show that a system performs correctly for a limited set of conditions. This drives the need for the other approaches given below to fully authenticate a monitoring system.
- Evaluation of Documentation. Thorough examination of complete documentation and a comparison to the as-built system is an important tool to determine the correct operation of a system and to define sensitive design points for targeted authentication. Such targeted authentication can provide a means for effective and efficient on-site examination of crucial system elements.
- Evaluation of Software. Software exists at several levels in any system, from firmware to analysis software to the operating system. A complete examination of all software, including a search for hidden switches, is central to authentication. Software reliability is especially important for unattended operations.
- Evaluation of Hardware. A variety of hardware makes up a system, from detectors to computers to shielding. An examination of

all hardware is necessary for authentication. Simplicity, robustness, and no extraneous functions are examples of hardware design principles for authentication.

- Random Selection of Hardware and Software. Random selection of hardware and software components is one of the easiest authentication tools to implement and one of the most crucial tools. It will be one of the main tools used during on-site authentication. Examples include random selection of computer modules, memory units, or software disks.
- Tamper-Indicating Devices. Tags, seals, enclosures, video monitoring, and other tamper-indicating devices are important methods for verifying physical integrity.
- Procedures. Procedures will be defined for all aspects of authentication and for any other activities on-site that affect the reliability of monitoring systems.

Monitoring systems need to be authenticated throughout their lifecycles, starting with the system design, moving to off-site authentication, on-site authentication, and continuing with authentication following repair. The most important of these is the initial design of systems. Hardware and software design criteria and procurement decisions can make future authentication possible or impossible. Facility decisions can likewise ease the procedures for authentication since reliable and effective monitoring systems and tampering indicating devices can provide the assurance needed in the integrity of such items as measurement systems, spare equipment, and reference sources. Host certification requirements also impact authentication.

WHY PNNL?

The PNNL authentication program is a natural outgrowth of the information barrier and detector technology development work that has been carried out for a number of years. PNNL has led the reviews of the IB for U.S. systems and has demonstrated the ability to collect and evaluate information in a manner leading to efficient discovery of potential problems with IB systems. In the arena of attribute measurements, PNNL has demonstrated the limitations of proposed oxide attribute determination method, demonstrated the robustness of PU600 analysis against potential spoofs, and studied a number of neutron and gamma detector technologies for monitoring systems. PNNL is uniquely positioned in the National Laboratory system to provide authentication services in an environment easily accessible by the international community.

AUTHENTICATION LABORATORY

PNNL has created an Authentication Laboratory dedicated to DTRA and DOE program needs, utilizing the expertise of the staff in the Laboratory's National Security Division. The Authentication Laboratory houses the instrumentation, nuclear material, and other sources, to perform U.S. certification-type testing and evaluation of system components and assemblies. The dedicated Authentication Laboratory can receive monitoring systems and perform authentication procedures that can give the U.S. the confidence it requires in the function of these monitoring devices. The Authentication Laboratory is sited in the 300 area and in the Plutonium Finishing Plant where technologies can be tested both privately (classified) and with international collaborators. The requirement for accessibility by an international community is one reason why PNNL, as a non-defense programs national laboratory, is ideally suited to host the Authentication Laboratory.

The Authentication Laboratory at PNNL has areas where measurement systems can be housed for thorough physical inspection and component testing, and areas where test sources can be utilized for functional testing. The Authentication Laboratory has highly controlled areas where large plutonium oxide sources can be used to perform subsystem and full system functional tests. The Authentication Laboratory is a Category-III *nuclear* facility and a Category-III *safeguards* facility on the basis of the quantity and form of plutonium used.

The PNNL authentication program is prepared to respond to future requirements in the area of authentication. The laboratory and team are positioned to handle the need for validation and demonstration of U.S. attribute and template measurement systems including systems for highly enriched uranium measurements. The laboratory is able to address the requirements of future treaty developments such as START III.

Richard Kouzes, Bruce Geelhood, Karl Pitts, James Fuller
P.O. Box 999, MS P8-20
Richland, WA 99352
Telephone: (509) 376-2320
Facsimile: (509) 376-3868
Email: rkouzes@pnl.gov
http://authentication.pnl.gov