PNNL-13941

Pacific Northwest
National Laboratory
Operated by Battelle for the
U.S. Department of Energy

Introduction to Methods Demonstrations for Authentication

RT Kouzes WK Pitts
RR Hansen

July 2002

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm


This document was printed on recycled paper.
(8/00)

Introduction to Methods Demonstrations for Authentication

R.T. Kouzes, R. Hansen, W.K. Pitts
Pacific Northwest National Laboratory, Richland, Washington

During the Trilateral Initiative Technical Workshop on Authentication & Certification, PNNL will demonstrate some authentication technologies. This paper briefly describes the motivation for these demonstrations and provides background on them.

Radiation measurement systems are central to the affirmation of a variety of arms control and non-proliferation regimes. A number of radiation measurement systems are under development for this purpose, and the correct functioning of these systems is to be authenticated. In the U.S. bilateral community, *Authentication* is the process by 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 provides assurance that measurement systems are assembled as designed, function as designed, and do not contain hidden features that allow the passing of material inconsistent with an accepted declaration.

A joint U.S. DOE-DoD Authentication Task Force (ATF) was established in September 2000 to elaborate upon the requirements for authentication of instrumentation that may be used as part of future verification or confidence building activities. The ATF, consisting of technical experts from the DOE National Laboratories, the Defense Threat Reduction Agency, and other governmental organizations, considered authentication in general as potentially applied to multiple regimes of non-proliferation. Four working groups of the ATF developed reports on aspects of authentication: specifically, Procedures and Integration, Hardware, Software, and Policy.

There are two basic requirements for a monitoring system: protection of classified information, and assurance of credible performance of the system for the measurement. The technology used to protect classified information is referred to as an *information barrier*. An information barrier consists of technology and procedures that prevent the release of host-country classified information to a monitoring party during an inspection of a sensitive item. Information Barriers impact the system design and the authentication methodology.

When sensitive items are to be inspected, the most likely scenario is one of "host supply." Under this scenario, where the host country would supply the system to be used by the monitoring party in a host facility, the crucial authentication issues are that a measurement system correctly measures the attributes, and that there be no hidden features in the system that allow it to pass out-of-specification items. To authenticate a host-supplied system, a set of approaches are used:

- Evaluation of Documentation. Thorough examination of documentation and a comparison to the as-built system are important tools to determine the correct operation of a system and to define sensitive design points for targeted authentication. Such targeted authentication could provide a means for effective 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 thorough examination of software, including a

search for hidden switches, is central to authentication. Software reliability is especially important to 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 would be one of the principle tools used during an on-site authentication process. Examples include random selection of computer modules, memory units, or software disks.
- Functional Testing Using Trusted Calibration Sources. Radiation sources play an important role in verifying the correct function of a system. Functional testing can show that a system performs correctly, but only for a limited set of conditions. This drives the need for the other approaches given below to fully authenticate a system.
- Tamper-Indicating Devices. Tags, seals, 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 measurement systems.

Measurement systems need to be authenticated throughout their lifecycles, including during system design and fabrication, off-site and on-site authentication, and authentication following repair. The most important of these is the initial design of the system. Hardware and software design criteria and procurement decisions can make future authentication relatively easy 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 monitored items as measurement systems, spare equipment, and reference sources. Certification of systems by the host must also be performed in a manner that provides for the requirements of authentication.

Radiation measurement based monitoring systems are being developed in the United States and the Russian Federation. Pacific Northwest National Laboratory is leading the authentication effort for the U.S. Department of Defense's Defense Threat Reduction Agency Cooperative Threat Reduction program.

Demonstrations

During the workshop, demonstrations of PNNL work will be provided on the following four topics.

1. Methods for Software Authentication – Confirmation (On-Site)

Due to the sensitive nature of the location where some monitoring systems are used, it may be unlikely that the monitor will have adequate access to extensively authenticate an installed system. This problem is compounded by the need to have a secure system approved by the host's information security groups prior to its use. Less invasive means can be used for authentication if it can be confirmed that the installed system or component is consistent with those validated off-

site. This allows the confirmation activities to leverage the results of the validation activities. It is important to remember that only the confirmation activities are performed on the actual system, therefore they are the true measure of the system authenticity. The rest of the activities are just support activities.

Perhaps the most powerful tool for authenticating measurement systems is random selection. During random selection the host party provides two or more copies of a system, sub-system, or component to the monitoring party. The monitoring party then selects one for the installed system and another to take home for private examination. It is important that the host party's right to privately examine the measurement system be terminated coincident with the exercise of random selection. This means that certification and attestation activities requiring private access will have to be performed prior to random selection.

The goal of software confirmation is to confirm the software on the system matches the code that was validated, and assures that the memory is functioning properly. To confirm that the software on a system matches a trusted code, the binary image of the system is compared to the trusted code (the 'gold' copy). The expectation is that the comparison should be exact – each bit in the binary images must match. Two methods were chosen to compare the binaries: a hash function when the comparison must be made onboard the target system; and a byte-for-byte compare when it is possible to dump the memory contents to another computer.

A hash function is a mathematical algorithm that is designed to reduce an arbitrary sized file to a fixed sized digest. A secret key is also input into the algorithm to insure the reduction is secure. The goal of the reduction is to make it mathematically infeasible to use a different input and obtain the same digest without the secret key. This is referred to as a collision resistant algorithm. Three common algorithms are the Secure Hash Algorithm – 1 (SHA-1), Message Digest – 5 (MD-5), and the Advanced Encryption Standard (AES). A hash function is especially well suited for in-situ or onboard software confirmation.

A byte-for-byte comparison simply compares corresponding bytes from two files to insure they are identical. Byte-for-byte comparison is better suited for comparing software that is not currently installed on the system, since it requires that both the actual software and trusted copy be on the same machine. So either the trusted copy would have to be copied onto the measurement system or the software from the measurement system would have to be copied onto some other system. These requirements make byte-for-byte comparison an unlikely choice for onboard confirmation, however it would be very useful for authenticating a randomly selected software-bearing component.

2. Methods for Software Authentication – Validation (Off-Site)

Validation activities are essential for the effective authentication of an instrument. When the monitor arrives on site, the off-site validation preparatory work allows the installed system to be authenticated to a reasonable level of confidence using just a few, relatively noninvasive examinations. A number of important validation activities also need to be conducted after the on-site visit. Through the process of random selection, the monitor obtains copies of the components that comprise the measurement system. Thorough validation of these components is an important

element of the monitor's overall confidence that the results of the measurement system are authentic.

Validation activities require a complete set of detailed documentation. Due to the vast number of vendors, the small quantities purchased, the manufacturer's desire to protect their intellectual property, and the fact that many of the vendors are from foreign countries, this documentation can be difficult and time consuming to obtain. The level of detailed documentation required exceeds the standard level of detail commonly distributed as product documentation. Manufacturer representatives contacted for this case study said that their detailed documentation was unavailable. When pushed further, only two of the eight vendors contacted were willing to initiate nondisclosure agreements that would allow the release of more detailed documentation. After four months, only one nondisclosure agreement has been implemented.

All system software can be placed into one of two groups. Software that can be anonymously purchased in a mass market is referred to as "commercial software," and all other software is referred to as "custom software." A medium level of confidence in the commercial software can be achieved by digitally comparing a version of software provided by the host to a version purchased anonymously by the monitoring party. Even though an item of commercial software passes the digital comparison test, it may still have pre-existing vulnerabilities. However, it is likely that some trigger will be required to exploit this feature. These triggers could be buried in the custom code; therefore, to have any confidence in custom code, it must be analyzed in detail.

Line-by-line examination is probably the preferable method for analyzing or vetting the source code. Line-by-line examination can be a very time consuming process, however this can be minimized by providing complete and fully commented source code. It is also helpful to avoid the use of massive I/O libraries and unused code, and use best engineering practices. Periodic design reviews involving the host and monitoring parties will also facilitate source code analysis.

This process can also be aided with the use of automated code coverage tools. These automated tools are designed to analyze source code and look for unreachable code, generate a diagram of the program flow and variable usage, and identify common error conditions. Code coverage tools will not replace the human vetting activity, but they help focus the activity.

One approach for the human vetting approach is shown by the following five step process: 1) conducting a review of the software's functional requirements document; 2) generating a flow diagram based upon the functional requirements document; 3) generating a flow diagram directly from the source code (the code should also be scrutinized and analyzed for acceptable coding practices, remarkable features, and errors); 4) comparing the two flow diagrams, noting and investigating further additions, deficiencies, and remarkable features; and, 5) functionally testing the code, including limit, boundary, failure, and error testing as appropriate.

Authentication of radiation measurement systems will include an evaluation of the physics analysis software with special attention to the correctness and robustness of the algorithms. One authentication issue for this analysis code is its robustness for variations in input data such as resolution, gains shifts, and interfering peaks. Such effects can be produced by thermal damage, vibration, other environmental effects, or aging. These effects may or may not show up in normal

functional acceptance testing, depending on the seriousness of the test regime. One method for validating analysis software is to test the limits and the associated failure modes. These tests can be conducted using experimentally gathered data, but synthesized data simplifies the construction of large and diverse data sets.

3. Methods for Hardware Authentication – Validation (Off-Site)

Validation activities off-site are essential for the effective authentication of an instrument. When the monitor arrives on site, this off-site preparatory work allows the installed system to be authenticated to a reasonable level of confidence using just a few, relatively noninvasive examinations. A number of important validation activities also need to be conducted after the on-site visit. Through the process of random selection, the monitor obtains copies of the components that comprise the measurement system. Thorough validation of these components is an important element of the monitor's overall confidence that the results of the measurement system are authentic.

Validation activities require a complete set of detailed documentation. Due to the vast number of vendors, the small quantities purchased, the manufacturer's desire to protect their intellectual property, and the fact that many of the vendors are from foreign countries, this documentation can be difficult and time consuming to obtain. The level of detailed documentation required exceeds the standard level of detail commonly distributed for product documentation.

Depending on the complexity of the system, hardware validation can be a very time consuming activity. Each component or subsystem is in turn constructed from different parts and devices. The different parts and devices can be manufactured by numerous companies, and some of these companies will surely be foreign. An added difficulty is the need to remove some of the individual electronic components and test them independently.

With the manufacturer's desire to reduce the size of electronic devices, visual inspection can be very difficult. The boards can be stacked in very cramped enclosures, and the parts are usually on both sides of the board and tightly grouped.

The digital components that are available today have dramatically reduced the effort required to produce an application specific integrated circuit. With relatively inexpensive software and a personal computer, a device can be programmed to perform specific tasks. In the extremely competitive market of electronic equipment, devices that are easy to reconfigure are used extensively to speed products to the marketplace. The flexibility that makes these devices attractive to engineers also makes these devices a liability in a trusted system. It is easy to reprogram or replace a device and although they look identical, they function very differently. One alternative is to use the same tools that are used to program these devices to interrogate or readout the original design or program. However, since these programs represent valuable intellectual property for the company that develops them, the programmable device manufacturers have worked diligently to insure the program in the device is secure. These devices have integrated features that can be used at the discretion of the designer to limit the amount of information that can subsequently be read from a programmed device.

One alternative is to test various combinations of inputs and insure the correct output is produced. The process of testing various combinations of inputs and verifying the correct output is commonly called "vector testing." Vector testing is a common step during the design and testing phases for newly designed chips. Vector testing is usually performed using the same specialized hardware and software designed for programming the chip. An appropriate vector testing campaign can produce an adequate level of confidence, but the detailed design documentation must be available. The documentation provided by the host is required for the generation of the test vectors.

4. Photographic Change Detection

Intrinsic characteristic properties of any item may be used to label or tag the item. High-resolution photographic recording and comparison may be used to (1) record intrinsic characteristics without physical contact and/or (2) detect change to an item through comparison to earlier photographs. Intrinsic tagging could monitor a sufficiently unique item for some classes of tampering without the need for physical contact with the item.

Comparing photographs using blink or flicker comparison allows examination of images too complex for unaided visual examination. Applying blink comparison to inspection applications has been difficult since the technique relies upon images with well-matched fields of view. The Change Detection System (CDS), produced at the Idaho National Engineering and Environmental Laboratory, solves this problem by transforming the images to match common features well enough for successful blink comparison. The CDS enables high-quality inspection even with hand-held cameras. Combining CDS with a high-end digital camera results in a highly capable toolkit to inspect items and detect tampering with or counterfeiting of seals.

For example, these tools allow fine details of handwritten signatures to become an intrinsic feature. Several examples will be presented.

Acknowledgement

This work was supported by the U.S. Department of Energy and by the U.S. Defense Threat Reduction Agency. Pacific Northwest National Laboratory is operated for the U.S. Department of Energy by Battelle Memorial Institute under contract DE-AC06-76RLO 1830.