SAND2007-3813P

Authentication and Certification Approaches for Information Barriers

Keith Tolk

7th Meeting of the Norwegian Study Group on Disarmament and Non-Proliferation

20 June 2007

National Nuclear Security Administration

Sandia National Laboratories

Information Barriers

- An *Information Barrier* consists of technology and procedures that prevent the release of Host-country classified information to a Monitoring Party during a joint inspection of a sensitive item, while promoting assurance of an accurate assessment of Host country declarations regarding the item.
- The Monitoring Party must be assured that the displayed results are authentic.
- The Monitored Party must be assured that no sensitive information is inadvertently disclosed.

Authentication and Certification

- Authentication – Procedures used to verify that the equipment functions as specified and that there have been no modifications that compromise the authenticity of the results
- Certification – Procedures applied by the owner of the items being measured to verify that the measuring equipment does not reveal sensitive information

Basic Principles

- Source code for all software and firmware must be available for inspection.
- All design features must be thoroughly documented.
- The system must be designed for authentication beginning with the conceptual design.
- The system should be
  - Simple
  - Modular
  - Inspectable
  - Verifiable

Authentication Measures

- “Blind Buys”
- Random Selection
- Inspection
- Performance testing
- Software Integrity Verification
- Tamper Indicating Devices and Tamper Indicating Enclosures
- Vulnerability Assessments

Blind Buys

- When possible, all hardware and software should be purchased anonymously to avoid purchasing items that have been altered by an adversary.
- The compilers used for the application and system software should be included in the blind buy program.
- Whenever possible, enough of the security critical devices such as microprocessors and read-only memories should be purchased to provide an adequate supply for the entire inspection regime. When practical, these devices should come from a single lot to simplify inspection.

Random Selection

- A procedure in which randomly selected devices or systems can be taken to a trusted laboratory for further inspection or testing.
- This testing is often destructive and the sample taken is never returned for use in an operational system.
- This procedure can be used at any point in the authentication process but cannot be applied once the system has taken measurements on a sensitive item.

Inspection

- Hardware is inspected using visual, X-ray, and/or microscopic techniques to verify that the devices are identical to a “golden copy” that has been purchased through a trusted channel.
- The source code for all software and firmware is inspected using automated and manual techniques to verify that no exploitable vulnerabilities are present.

Performance Testing

- The system should be thoroughly tested to verify that it performs as specified.
- Note that this testing will **NOT** detect “hidden switches”.
  - A hidden switch is a feature that will allow the adversary to control the equipment so that it performs correctly during testing but gives altered results during actual use.

Software Integrity Verification

- This is a cryptographic process that allows verification that the software and firmware in a device matches a trusted copy.
- This process can often be applied without opening the tamper indicating enclosure.

Tamper Indicating Devices and Tamper Indicating Enclosures

- These technologies are used to provide assurance that a device or a system has not been altered while out of the control of the concerned party.
- Effective TID and TIE technologies can minimize the amount of inspection required on operational systems.
- Obviously, the best possible TID and/or TIE must be used on systems that cannot undergo authentication procedures after making sensitive measurements.

Vulnerability Assessments

- All parties involved in the transparency agreement will perform vulnerability assessments on the systems to be used.

Certification Procedures

In addition to the authentication procedures, the following will be implemented:

- Emissions testing (radio frequency, high frequency signals on cables, acoustic, etc.)
- Inspections for side-channel attacks (e.g. a short radiation spectrum counting time would indicate a stronger source)
- Access control – only trusted personnel will have unsupervised access to the equipment once it has been certified.