SAND2007-1563P

Cryptography for Information Barriers

US-UK Information Barrier Workshop

Keith Tolk

April 17, 2007

Cryptography for Information Barriers

- Problem – Verify the integrity of the software on an untrusted computer.
  - It is impossible to perform this verification using standard hash functions or with digital signatures on the software files, since a compromised computer will simply display the hash value or the digital signature verification result that the inspector expects.
- Solution – Use the keyed hash algorithm to compare the software on the machine to be tested to that on a trusted machine. (Variants of this process include Software Integrity Verification and Intrinsic Code Verification.)

Cryptography for Information Barriers (2)

- Problem – Verify that the contents of an external memory device have not been altered without revealing the contents to the inspector.
- Solution – Use a public/private key digital signature on the contents of the device. (Note that the computer performing the verification of the signature must be trusted.)

Cryptography for Information Barriers (3)

- Problem – Protect the contents of an external memory device from disclosure to an inspector who has physical access to the device.
- Solution – Encrypt the contents of the device, using either asymmetric or symmetric encryption algorithms.