SECURED BY SPYRUS®

TRUSTED MOBILITY SOLUTIONS

Solving The Digital Chain of Custody Problem

Problem Statement

We live in a digital world, and so does the criminal element. When it comes to collecting, processing, disseminating, and storing digital evidence, the processes and procedures used for a hundred years no longer will do.

Whether from a suspected terrorist Web site, a surveillance video; the audio/video record of a suspect's interrogation; or a statement provided by a whistle blower, informant, or a concerned citizen, the evidence consists of bits of magnetic or electronic fields that are easy to modify or delete without detection.

Although the use of digital technology has simplified the distribution of intelligence, the ease with which such information can be manipulated, or at least be alleged to have been manipulated, is proving problematic in providing an auditable secure chain of custody. It is simply not practical to store every computer or hard drive in a vault and use the traditional forms of access control and signature cards for sign in and sign out. Every time someone signs out a computer or hard drive to examine it, there is one more opportunity to alter the record—or at least that is what any defense attorney would argue.

For nearly 30 years, experts have recognized that the solution to the problem of non-repudiation lies in the use of so-called digital signatures that are based on Public Key Infrastructure (PKI) . Assuming that the private key is held securely by the individual to whom it is associated, it is possible to provide strong mathematical proof that only the person in possession of that key could possibly have signed the particular document, as verified using the corresponding public key.

Mathematics notwithstanding, there are other obstacles to proving that the private key only was held securely by the individual to whom it is associated. Most Public Key Infrastructure (PKI) applications are software-based, and virtually every current operating system has a wide variety of verifiable security holes and flaws in it. In most IT deployments, the system administrator has virtually unrestricted rights to access the user's computer, either directly, perhaps after hours, or indirectly, over the network. It is even possible that a hacker could penetrate the network and access the user's keys. Of course, it is not necessary for the defense to prove that such an attack actually did occur, it is sufficient merely to show that it COULD have occurred, in order to raise reasonable doubt in the minds of a jury.

This problem can be mitigated by using dedicated, secure, and portable hardware, where the private keys are generated in hardware within the device itself and can never be exported or altered, and by prohibiting the importation of externally generated private keys. This ensures that the private keys have never been disclosed to anyone, including the device holder.

The SPYRUS Hydra PC Solution

Hydra Privacy Card® (Hydra PC™) high-assurance cryptographic products by SPYRUS, and specifically the combination of Secure Pocket Drive and Digital Attaché, are uniquely suited to protect the confidentiality, integrity, and non-repudiation of digital evidence with the highest-strength cryptographic technology available today.

Secure Pocket Drive is a Hydra PC device that provides an entire securely protected, self-contained, and portable native Windows® environment. Simply connect it to the USB port of almost any PC and securely boot into Windows with your applications and data files. The host PC supplies the keyboard, display, mouse, memory, and CPU; and its hard drive and network card can be blocked unless permitted by policy. When the device is removed, nothing is left behind. The entire operating environment is encrypted, protecting information from alteration or theft.

Digital Attaché provides file encryption capabilities that extend off of the device itself. Files and folders encrypted by Digital Attaché can be placed anywhere, including the Internet, because only authorized users with their own Digital Attaché can decrypt them. At the time of encryption, both the plaintext and the resulting cipher text are digitally signed and time stamped, the originator's credentials are embedded, and an access control list (ACL) can be put on the file that allows read-only sharing of the information with additional recipients. The encrypted file or folder becomes the sealed document of record because, once encrypted, nothing, including who has access to it, can be altered. The contents, time of encryption, recipients, and the device used to encrypt the information can all be independently verified.

In addition to its file encryption capabilities, Digital Attaché also works just like a traditional encrypting flash drive, protecting files and folders stored on it without individually encrypting them. This feature can be useful when storing an unencrypted file received from some-

one else or for temporary storage while preparing a report or document. At the end of the working session, the plaintext files and folders can be deleted, and Digital Attaché ensures that they never can be recovered.

Digital Attaché is unique. No other encryption device offers these features and benefits:

- High-assurance, hardware-based Suite B encryption for confidentiality.
- Note: Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program designed to create an interoperable cryptographic base for both unclassified and classified information.
- Secure file sharing between one or more designated Digital Attachés, using algorithms and key strengths that are expected to resist attack for at least the next 100 years.
- The ability to restrict access to encrypted data to specifically designated computers, providing strong data containment.
- The ability to circulate previously encrypted and digitally signed data, eliminating the need for "sanitizing" processes that destroy the original signature and non-repudiation protection.
- The ability to store secure, encrypted backup copies off-site and be certain that they cannot be read or modified by unauthorized individuals, either accidentally or deliberately. Because the plaintext and cipher text are digitally signed, the integrity of the backup file can be verified without decrypting the data or performing a bit-by-bit comparison of the primary and backup files.

A Real-World Example

A citizen contacts law enforcement with information that may be relevant to an on-going investigation. Because the individual's life could be endangered if the suspects discover that he is talking to law enforcement, it is absolutely essential that confidentiality be maintained for the rest of the individual's natural life—perhaps 60 to 70 years—even if the informant eventually goes into the witness protection program.

At present, only the highest-strength Suite B algorithms are considered strong enough resist cryptanalytic attack for such a long period of time. RSA 2048, which is widely used, is expected to resist attack for only the next twenty years, if that long.

In addition to maintaining the confidentiality of the data, it is essential to protect the integrity of the data from the first moment it is captured and to provide unambiguous and provable data showing time of encryption, list of recipients, and the device used to encrypt the information.

In the past, the original document could be locked in a safe, and the records custodian could testify that the chain of custody had been maintained. Because data is gathered and stored electronically today, it is much more difficult to guarantee that only authorized individuals had access to it and that no changes or alterations occurred since the time the information was first captured.

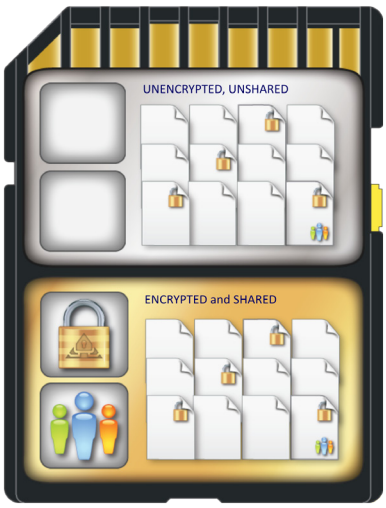
The Solution

Use Secure Pocket Drive to capture or collect the information and the Hydra PC Digital Attaché to encrypt and seal it. The process works like this:

1. Process the initial data by a computer made secure by booting it from Secure Pocket Drive, blocking all malware, including software key loggers. The information to be protected might be a recording of an interview with the informant, an e-mail or text message, the contents of a suspect's hard drive, or information collected from a suspicious Web site.

Secure Pocket Drive

2. To ensure that unprotected data is never stored anywhere, even temporarily, store the input data initially in the encrypted partition (shown as gold below) of a Digital Attaché.



Digital Attaché Memory Card

3. When the information is ready to become part of the permanent record, Digital Attaché encrypts it, creating a time stamped, unalterable sealed document of record.
4. The encrypted and sealed file can now be stored anywhere. It should also backed up to an off-site storage facility for safekeeping without the risk of an unauthorized person accessing the data.
5. After the file is encrypted, sealed, and properly backed up, the plaintext file should be securely deleted to protect the confidentiality of the data.
6. When the file is first encrypted, it can be designated for sharing, while still in encrypted form, with specific authorized individuals in accordance with well-defined policies. Authorized users can decrypt the file with their own Digital Attaché without breaking the chain of evidence.
7. Before decrypting a file, the Digital Attaché hardware verifies that the cipher text has not been corrupted or modified in any way. After decryption, Digital Attaché reverifies that the digitally signed plaintext has not been altered since the file was sealed as the document of record. The originator's credentials are embedded in the file header and can be used to confirm the originator's identity beyond reasonable doubt.

If and when it becomes necessary to produce the original evidence in court, any authorized recipient of the original encrypted file can decrypt the data (again using Secure Pocket Drive and Digital Attaché), and prove beyond a shadow of a doubt that the decrypted data is exactly as it was initially recorded and processed, and that no alteration could have taken place. SPYRUS experts can provide details of the encryption and sealing process to corroborate the soundness of the evidence.

Intelligence and law enforcement communities must often share highly sensitive data, often over classified, compartmented networks, while preserving the original evidence within a strict chain of custody. The Hydra PC Digital Attaché allows the original, encrypted files to be exchanged with verifiable evidence that the original, presumably unclassified, contents remain unaltered and uncorrupted.

About The Authors

Robert R. Jueneman

Mr. Jueneman has over forty years of computer and communications security experience. In addition to his commercial experience, he has extensive experience in providing security services to various US government agencies including NSA, CIA, FBI, Secret Service, Department of State, Department of Commerce (NIST and BXA),NASA, Department of Energy, and HEW; as well as the Governments of Canada, the United Kingdom, Norway, and Russia. He is chief scientist at SPYRUS.

Ron LaPedis, CISSP-ISSAP, ISSMP, MBCP, MBCI

Mr. LaPedis spent 25 years with Hewlett Packard becoming a business continuity and security specialist, consulting with key customers and partners. At SanDisk, he launched a dual factor authentication solution with VeriSign and RSA and a managed a virtual application solution with RSA and Citrix. He is named on one storage patent and two virtualization applications. He is director of product management and marketing at SPYRUS.

For more information about SPYRUS products, visit *www.spyrus.com* or contact us by email or phone.

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
(408) 392-9131 phone
(408) 392-0319 fax
info@SPYRUS.com

East Coast Office
732-329-6006 phone
732-329-6211 fax

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000
Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au
info@SPYRUS.com.au

Document number 412-000001-02

Microsoft GOLD CERTIFIED Partner