C.P.A. Secure Technologies -Secure by Design

The C.P.A. Secure servers, C.P.A. Secure clients, and FIPS 140-2 validated C.P.A. Secure cryptographic software technologies have been designed from the beginning to provide secure, end-to-end encrypted exchange and storage of sensitive data using a wide variety of popular public standards and protocols. They are not FTP products with grafted-on security features, nor are they proprietary file transfer programs with open standards support added on.

The design of the C.P.A. Secure technologies and their support for HTTPS-based communications enables them to be deployed in a modern network architecture, without resorting to "pass-through proxies", proprietary VPNs, odd firewall rules, or other methods that employ non-standard network entities. Together, C.P.A. Secure technologies can be used to provide a complete enterprise-level secure data transfer, processing, and storage solution.

This paper uses a series of commonly accepted security 'best practices' to help illustrate how C.P.A. Secure technologies are secure by design. These are drawn from the June 2004 "Engineering Principles for Information Technology Security" report written by the US National Institute of Standards and Technology (NIST).

NIST is responsible for developing standards and guidelines that provide adequate information security for US Federal government agencies. As part of this, NIST has developed a series of Federal Information Processing Standards known as FIPS (FIPS 140 covers cryptographic modules, with FIPS 140-2 being the most recent, and stringent, version of this standard). NIST, together with the Canadian government's Communications Security Establishment, manages the Cryptographic Module Validation Program (CMVP) that tests products for FIPS compliance.

NIST's Engineering Principles publication covers cryptography, software engineering and network design, with a focus on achieving defense in depth through the use of "system-level security principles" in the "design, development, and operation" of IT systems. NIST Special Publication 800 27A "Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A" can be found online at:
http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

"Treat security as an integral part of the overall system design."

When implementing C.P.A. Secure our engineers took a paranoid perspective regarding the Internet and the operating systems and associated programs our products would utilize. To this end we adopted a defense-in-depth architecture. Below are some examples, as implemented in our C.P.A. Secure data transfer and storage technologies.

- The security of the files handled by C.P.A. Secure does not depend on the security, or lack thereof, of the OS that it runs on.

- By design C.P.A. Secure is not able to push files, which means it cannot be used to push malware into trusted networks if it is ever compromised.

- "Least privilege" authorization is implemented for tight administrative control over what users can and cannot do.

● C.P.A. Secure's virtual user interface helps implement 'least privilege' by providing tight administrative control over what users can and cannot see, including command options, files, folders, logs and user information.

● C.P.A. Secure uses a separate file and folder/directory naming convention than that used by the underlying OS (another benefit of the virtual interface).

● Exclusive use of FIPS 140 validated encryption for transport and storage.

● All files received by C.P.A. Secure are stored using its built-in AES encryption, so they cannot be read, and executables cannot be run, by untrusted parties.

These examples, and others, are explained in greater detail later in this paper.

C.P.A. Secure provides a secure exchange-point that Web browsers as well as third-party secure file transfer clients can upload to, download from, and store data on. C.P.A. Secure supports HTTPS, FTPS and SFTP based encrypted data transfers, and includes built-in FIPS 140-2 validated cryptography to provide its unique 256-bit AES encrypted data storage. These capabilities enable C.P.A. Secure to provide secure end-to-end encrypted data transfer, without the need to use third-party encryption programs.

"Ensure that developers are trained in how to develop secure software."
Our C.P.A. Secure developers have one or more current security certifications from the respected SANS (SysAdmin, Audit, Network, Security) Institute. SANS <www.sans.org> provides information security training and certification on a global basis and runs the Internet Storm Center, the Internet's "early warning system." In addition, C.P.A. Secure technologies have been built and are maintained by developers with strong technical and security training and experience. All of them hold at least a four year degree in engineering or computer science, and have on average ten years of post-collegiate development experience.

"Assume that external systems are insecure."
C.P.A. Secure technologies were created to run on Windows servers, so from the beginning C.P.A. Secure technology was designed so its security was not dependent on that of the underlying operating system (OS). To this end our engineers developed (and FIPS 140-2 validated) our cryptography platform, as well as our file transfer 'plumbing' and secure setting storage. By not leaving data 'in the clear' on disk or in memory, and by strongly encrypting data when storing it, C.P.A. Secure is designed to survive an intrusion against the OS. One result is that C.P.A. Secure technologies were not affected by the release of CodeRed and related malware.

"Protect information while being processed, in transit, and in storage."
Most secure file transfer products focus, almost exclusively, on protecting data in transit. Unfortunately, files are usually much more vulnerable when stored on a publicly accessible secure file transfer servers than while in transit, even over the Internet.

Unlike C.P.A. Secure, when other secure transfer clients encrypts and sends a file to a secure file transfer server, the server receives, decrypts and stores the file. If the file was unencrypted at the time it was encrypted for transmission, then that will be stored unencrypted on the server. This means the file can be read by anyone who gains access to the server.

C.P.A. Secure technology eliminates this storage vulnerability by automatically re-encrypting each file it receives, before writing them to disk. This approach also eliminates the need to use PGP or other third-party file encryption programs (and the associated headaches that come with distributing such programs and managing their encryption keys).

To secure files in transit, C.P.A. Secure and the Windows-based C.P.A. Secure clients use Microsoft's FIPS 140-1 validated SSL encryption libraries.

To secure files in storage, C.P.A. Secure uses the 256-bit AES encryption and the SHA-1 libraries in its built-in FIPS 140-2 validated cryptographic module.

To secure files when processing them between transfer and storage encryption, C.P.A. Secure uses the smallest possible buffers in order to prevent the exposure of large chunks of sensitive information in memory.

"Protect against all likely classes of attacks; Implement least privilege."

C.P.A. Secure systems are designed to protect against Web, FTP and SSH attacks from Internet users, as well as against MySQL and Windows networking attacks from internal users and rogue administrators on the local console. Careful data scrubbing is a key component in how C.P.A. Secure servers defend themselves against Internet attacks, but the principle of least privilege is equally important to their defense capabilities.

Least privilege means giving users the smallest, most restricted set of permissions necessary to accomplish any particular task. At the operating system level, least privilege is enforced by OS security policy and NTFS permissions. Least privilege is controlled at the application level by a tight system of user and group privileges, which are organized into security profiles for easy administration. The following are a just few of many examples of how C.P.A. Secure implements the principle of least privilege.

● By default, no one can configure or access a C.P.A. Secure server except our administrators.

● By default, C.P.A. Secure users are locked to specific home folders; additional access must be explicitly granted by a C.P.A. Secure administrator (and details of this change are automatically logged).

● By default, C.P.A. Secure Group Administrators have no permission to edit or run any tasks; this permission must be explicitly granted.

C.P.A. Secure Wizard is a free ActiveX control that provides Microsoft's Internet Explorer Web browser with a number of useful features, including an easy-to-use GUI interface to select and transfer multiple files and the ability to circumvent Internet Explorer's built-in file size and time-out limitations. C.P.A. Secure Wizard also provides the ability to do SHA-1 file integrity checks (an integral part of providing file non-repudiation) as well as automated file compression and the automatic resumption of interrupted file transfers.

"Where possible, base security on open standards for portability and interoperability."

The following examples demonstrate how C.P.A. Secure technologies have been built from the beginning based on open standards.

● C.P.A. Secure cryptography uses the AES, SHA-1 and SSL encryption standards.

● C.P.A. Secure file transfer services are built on industry standard HTTP over SSL (HTTPS), FTP over SSL (FTPS) and SSH (SFTP), each of which is governed internationally by various "RFC" documents.

● C.P.A. Secure supports standard X.509 certificates.

"Strive for operational ease of use."

Data can be securely exchanged with C.P.A. Secure servers over encrypted connections using a wide variety of third-party SSL and SSH-based secure FTP clients, as well as with the Internet Explorer, Mozilla, Netscape, Opera and Safari Web browsers (with or without Java and ActiveX-based C.P.A. Secure file transfer Wizards). These provide GUI and command line solutions for manual and automated/scheduled transfers for virtually every computing environment.

In addition to encrypted transfers, all C.P.A. Secure clients provide the following capabilities when used with C.P.A. Secure storage servers.

● SHA-1 file integrity checking (part of providing file non-repudiation)

● File Compression (which can provide faster transfers)

● Resumption of interrupted transfers (saves time when sending large files)

"Implement layered security."

Rather than trusting in the security of the underlying OS, C.P.A. Secure relies on its own privilege system and FIPS 140-2 validated cryptography to protect files and settings from unauthorized view and use.

This means that, even if a hacker gains Windows Administrative privileges**,** they cannot reset C.P.A. Secure user passwords because the C.P.A. Secure userbase is its own separate system. This also means that, even if a hacker can "buffer overflow" or otherwise hack into the C.P.A. Secure application, they still need to come up with the right encryption keys to get access to C.P.A. Secure data. And this is not easy because every file on a C.P.A. Secure server is encrypted with its own key, those keys are encrypted, and no blanket permissions are awarded to Windows users.

In addition, C.P.A. Secure's virtual file system obscures the identity of the underlying file structure. Some examples of this are its substitution of random IDs in place of file names, and its use of random folder IDs in place of actual folder names.

"Design and implement audit mechanisms to detect unauthorized use and to support incident investigations."

C.P.A. Secure technologies actively record file transfers, user and folder maintenance, setting changes, sign-ons, secure message posts and other actions. Interesting events (such as username locked out for too many password attempts) can trigger email notices to authorized parties.

Rather than write out log entries to long text files, C.P.A. Secure audit records are written to an easy-to-access ODBC database.

Online audit record screening is built into C.P.A. Secure. Offline audit reports can easily be built using any number of scheduling tools. Audit records can also be archived for permanent off-server storage.