

CyberSoft White Papers

POSSIBLE OEM USES OF CYBERSOFT TECHNOLOGY IN THE FIREWALL INDUSTRY. SEPTEMBER 1996

Peter V. Radatti
CyberSoft, Inc.

Copyright © September 1996 by Peter V. Radatti. All Rights Reserved.

The purpose of this document is to provide potential OEM users of CyberSoft technology ideas of how this technology can be combined with their own products to provide new features. These ideas are not limited to the firewall industry. Manufacturers of products other than firewalls can generalize this document to their own needs or feel free to contact us for specific ways in which we can enhance your products.

This document is a list of CyberSoft technology that can be added to firewall systems as feature enhancements. It is not a complete list of CyberSoft product or technology, but represents a surface layer for quick review. Firewalls present a unique opportunity to implement security on a network since they control a choke hold between the outside world and the internal network. As such, anything that is implemented on the firewall has network wide results.

1) Anti-virus (VFind)

Everyone is aware that firewalls are a good place to implement virus scanning. CyberSoft's VFind does this but unlike other virus scanners it is feature rich. It allows the end user to select what platforms to scan for. Today, most firewall implemented virus scanners can only scan for MSDOS viruses. The world is not only MSDOS. For those manufacturers who already have an MSDOS virus scanner in their firewall, we will license those parts that they are missing. VFind is approved for Export

FIREWALL ANTI-VIRUS CAPABILITY

CAPABILITY	NORMAL FIREWALL	FIREWALL WITH VFIND
MSDOS	yes	yes
MACINTOSH	no	yes
AMIGA	no	yes
UNIX	no	yes
MICROSOFT NT	some	yes
MACRO	some	yes
JAVA	no	soon

2) Text Processing (CVDL)

The heart of the VFind anti-virus technology is the CVDL engine. This system allows the creation of pattern models. Any data passing through the system which fits one of the models is flagged. This ability allows the firewall manufacturer to offer email and file scanning for content prior to import or export. Content scanning can allow the customer to enforce pornography policies for textual data as well as insure that critical business information is not exported.

3) Format Conversion (UAD - Universal Atomic Disintegrator)

Many times, files and email entering a site from the Internet are not in a format that can be utilized by the systems on the network. For example, many MSDOS systems can not read uuencoded tar files while some Macintosh systems can read MIME encoded "zip" files. This becomes even more complex for UNIX systems which have a dizzying array of formats. Using UAD, the firewall can decompose the file or email message entering a site into its base components and repackage them in a format compatible with the site. As an example, the system can convert a uuencoded, UNIX compressed, cpio file containing MSDOS zip files into a mime encoded zip file of zip files. UAD off-the-shelf only provides the decomposition and rendering, however, CyberSoft will custom produce the encapsulation technology for a small additional royalty.

4) Type Blocking and Logging (UAD - Universal Atomic Disintegrator)

The UAD product allows you to block files entering a site by file type. Assuming that the customer is an all UNIX and MSDOS site, they could block all executable files from entering their site that were not the specific type of UNIX and MSDOS that they used. (Example: Allow only Sun Microsystems Solaris binaries and MSDOS 16 bit binaries in addition to *.gif and *.txt files) This will cut down on the risks associated with files coming into a site from the outside and discourage employees from using network resources for personal purposes.

UAD can be combined with CIT to provide a cryptographic hash value for every file that enters a site. This includes each individual file contained within a compound file such as "zip" files, even if they are uuencoded, bixhex encoded or mime encoded. This feature allows the firewall to create logs that detail where a file came from, who it went to and when it arrived on the network. Since CIT uses cryptographic hash values and not CRC values, the system administrator can hash any file found on the network, at any time, and determine if it came through the firewall with its special logging feature.

5) System Integrity (CIT - Cryptographic Integrity Tool)

How does your system know if it has been compromised? Does your help desk spend a large amount of time solving end user configuration problems? Using the CIT technology, your product can determine if it was modified in an unapproved way and make automatic corrections. Additionally, your help desk can determine what files were added, deleted or modified in the system since it left the factory and/or was last configured. Not only will this reduce help desk overhead and increase customer satisfaction, but you can advertise that the system is self-maintaining using hardened cryptographic technology. Approved for export.

6) Virtual Integrity Network (CIT)

How does a customer know that the file they received is the file that was sent? Even using a virtual private network does not provide this assurance. Many people rely upon the CRC checking that occurs at the pack level but that checking only deals with the individual packet not the entire file. In addition, the packet data segment can be modified and the CRC value plugged to reflect the change. The virtual private network will keep outsiders from affecting the packet but does nothing for the disgruntled employee or anyone with physical access to the equipment. CIT uses the RSA MD5 algorithm to provide mathematically provable integrity. Your firewall can transmit MD5 hash values prior to the transmission of the file. Once the file is received, it can again be checked and if the values agree, then the file is correct. Transmission of the MD5 hash value needs to be protected in a proprietary way. This means that the customer must have a firewall manufactured by your company at all sites for this feature to work. VFind is approved for export.

In Conclusion

Not all products manufactured by CyberSoft are listed. Custom security products are also available. CyberSoft can supply all products as compiled ready-to-run programs or as libraries that can be linked into your applications. All CyberSoft products are written in K&R Standard C. CyberSoft will consider porting our products to any system required. Aggressive pricing and terms. Ask for Peter V. Radatti when calling about OEM opportunities.

[Back](#)

[Home](#) | [Products](#) | [Support](#) | [Purchase Info](#) | [About Us](#) | [News](#) | [Contact](#)

Questions or comments about this website? Please contact the webmaster. 

© Copyright 2009 CyberSoft, Inc. All rights reserved.



This site certified 508 Compliant