CopiaFacts Security Issues

Copia International, Ltd
1220 Iroquois Drive, Suite 180, Naperville, IL 60563, USA
Phone: (630) 388-6900 Fax: (630) 778-8848

Web: www.copia.com E-Mail: copia@copia.com

First Edition: June 2002

Introduction

The software of the CopiaFacts product line is secure by design. However the fact that the software controls resources which connect to the outside world using telephone lines and networking may give rise to concern about security issues. The purpose of this document is to address such concerns and explain how the design of the product limits the possibility of a breach of security.

A CopiaFacts system normally consists of one or more computers running the server engine programs, and zero or more client computers which can initiate fax or e-mail transmissions from the server engine. The server engine can also receive incoming telephone calls and either interact with the caller by voice messages and DTMF tones, or receive an incoming fax, or both. Outbound calls can also be made to receive incoming faxes (polling), and voice calls can be made either to leave voice messages or to begin an interactive session with the person called.

The CopiaFacts server engine normally runs as an automatically-started user application, but there is also an option (from release 7.1) to start it as a Windows service. In either case a login and password will be needed to identify a user and control access to network and/or local file resources.

Application Structure

Only one program in the CopiaFacts suite controls hardware capable of communicating with the outside world. This is COPIAFACTS.EXE, which consists of a main program with a number of dynamically linked libraries (DLLs), some of which communicate with hardware-vendor supplied application programming interfaces (APIs) which control voice and fax boards. In earlier releases, this program was named FAXFACTS.EXE. One of the DLLs of the COPIAFACTS program also controls outbound e-mail operations, via standard Windows API calls. No other Copia-written program has the ability to communicate outside the network on which the application is running.

It is possible to configure COPIAFACTS so that it avoids opening and controlling all of the available channels on a particular voice or fax board. In this case another program running on the same machine could control some of the channels. Equally if the COPIAFACTS program is not running at all, other applications could control the boards. The board manufacturer's driver installation is likely to include sample, test, and diagnostic programs which exercise every capability of the board.

Serial-Port Modems

CopiaFacts does not support serial-port modems either for faxing or any other purpose. Some of our configuration screens still refer to serial port modems and an experimental interface was written some years ago, but this interface does not work with the current release and has never been included in the delivery.

In sending e-mail, the Windows API functions called by CopiaFacts might initiate a modem dial-up connection to the Internet, depending on how Windows is configured either on the machine running COPIAFACTS or on a machine acting as a network gateway. In practice, no customers using CopiaFacts e-mail features are likely to configure their systems in this way.

Voice and Fax Hardware

CopiaFacts supports various voice and fax boards manufactured by Brooktrout, Commetrex, and Intel (Dialogic/Gammalink). These boards either connect direct to a telephone line or connect through a separate telephony interface board supplied by the same manufacturer. CopiaFacts interfaces with these boards through the manufacturer's API and drivers. All boards manage multiple telephone channels, and some boards support both voice and fax.

For voice applications, the channel carries an audio signal which is played from a disk file or recorded to a disk file, usually VOX or WAV format. The file contents must represent an audio waveform capable of being transmitted by the telephony circuit, and it is not posible to transfer an arbitrary data file by this means. Voice applications can also generate tones for transmission and can detect and recognize specific tones such as DTMF tones produced by the keys on a telephone.

Voice applications open an audio channel as soon as the telephony connection is made, with no protocol needed to synchronize any devices at each end of the line. By contrast, a fax application sends and receives specific tones at the start of each call to enable the devices to recognize that a fax transmission is to follow, and then exchange capability data to agree the parameters for the call. This procedure always follows the ITU Recommendation T.30. The tones and signals are different from those used by a data modem and none of the boards supported by CopiaFacts can synchronize with or work with a data modem.

Some of the boards supported by CopiaFacts may share base hardware with the same manufacturer's other boards which do perform data transmission. However the two types of board have different firmware which is not field upgradable, and the two uses require completely different APIs. A board controlled by CopiaFacts therefore has no ability to respond to or connect with a data call from a modem or other device capable of transmitting data.

Fax Transmission and Reception

The purpose of fax transmission is to send a facsimile of a document. To do this an original document is scanned (or computer-generated) to produce 'bitmap' where the white and dark pixels (picture cells) of the image are represent as a stream of 1 and 0 bits. Color faxing operates on the same principle, but uses more than one bit to represent each pixel. Before transmission, the bitstream is compressed using (for bi-level images) procedures defined in ITU recommendations T.4 and T.6.

Document files prepared for fax transmission by CopiaFacts must contain an image block already compressed (either T.4 or T.6) ready for transmission. Such an image block is almost always placed in a standard tagged image file format (TIFF). Tagged items in this file specify parameters such as the dimensions and resolution of the image, which are used to set up the transmission parameters. TIFF files can also contain user-defined tags containing any arbitrary data, but there is no means for CopiaFacts to transmit data from such tags.

It is theoretically possible to treat an arbitrary file as a raw bitmap which if viewed as a image would show as a page of apparently random black dots. Such an arbitrary bitstream could be encoded T.4 or T.6 and transmitted as a fax. This technique is the basis of various encryption and steganography systems which use fax standards to transmit data. Although CopiaFacts has no capability to create such a file, it could transmit one created elsewhere because it would be indistinguishable from a normal faxable TIFF file containing a complex document image.

CopiaFacts is capable of transmitting any faxable TIFF file for which the CopiaFacts programs have read access. It is normally configured, however, so that documents to be transmitted by fax reside in specific folders.

All fax documents received by CopiaFacts are stored as T.4 or T.6 encoded images in a TIFF file. The only other tags created in such a file are those needed to describe the image. No other file format can be created for an incoming fax document by the CopiaFacts software. The folder(s) into which documents are received are pre-defined in the CopiaFacts configuration and cannot be specified by the sender of the fax, although CopiaFacts can be set up to allow a remote caller using IVR, or DNIS, to specify into which of the pre-configured folders the fax to be transmitted to CopiaFacts is to be placed.

There are options to print received documents on a nominated printer; to forward them to an e-mail recipient either in TIFF format or converted to PDF; or to store them as fax files and forward them on request. CopiaFacts has no capability to extract any hidden information from the received block of image data, but could be configured to run another program after receipt of the fax transmission which could perform an arbitrary operation on the received file.

ASCII File Transfer

Almost all the fax boards supported by CopiaFacts have the ability to accept a listable ASCII file and transmit it as a fax. This is done by using built-in or user-specified font file to rasterize the text and create page-images on the fly which are then transmitted. A user authorized to transmit faxes could therefore initiate the transfer of information in any ASCII file for which the CopiaFacts programs have read access. The recipient of a fax originating from an ASCII file in this way would be able to view the file as a document image, but would only be able to recover the ASCII text by using optical character recognition (OCR) techniques.

Binary File Transfer

ITU Recommendations T.4 and T.30 provide for transfer of data files using a modified version of the fax protocols (ITU T.434). Very few standard fax machines have the capability to send or receive data files but it is available on some fax boards, including some of those supported by CopiaFacts. The Binary File Transfer (BFT) capability is signaled by a setting in the data exchanged to negotiate the transmission parameters at the start of a fax call.

Brooktrout and Gammalink are the only boards supported by CopiaFacts which allow BFT. CopiaFacts calls none of the special Brooktrout API functions which are needed to send or receive this format. Although CopiaFacts does not support BFT on Gammalink fax boards, nor expect to receive such files, the Gammalink settings utility does allow the capability to receive such files to be enabled in the Gammalink registry settings. When enabled, the received path and filename would be pre-specified.

Denial of Service

It is of course possible to place sufficient incoming calls to block all available CopiaFacts telephone lines. It is also possible to devise mis-coded T.4 or T.6 data which when received as a fax results in the creation of a document file with a very large number of pages, which could disable or block a printer configured to print incoming faxes. Copia is not aware of any other pattern of usage which can predictably cause the CopiaFacts program to fail.

E-Mail

CopiaFacts has no capability to receive e-mail. It does have the ability to send e-mail when so configured. Typically this is either used directly, for e-mail broadcasting, or to notify other system events or status. In the latter category is included the forwarding by e-mail of incoming fax documents. Such documents can either be forwarded as TIFF files (as they were created on receipt) or converted to Adobe PDF format on the fly before e-mail transmission.

There are two methods of transmitting e-mails. For very small volumes, or for occasional notifications, CopiaFacts can appear as a simple MAPI client, using a pre-specified login, and use MAPI to transmit the messages. Such usage is subject to the permissions and restrictions configured for the MAPI user.

Most CopiaFacts e-mail operations use SMTP protocol. CopiaFacts uses the domain name server (DNS) configured in Windows for the node, to look up available mail exchange (MX) records for the target domain. A connection is then attempted to a mail transfer agent (MTA) specified by the MX record, and the e-mail is transmitted using SMTP. There is also an option to specify that certain domains are to be served by a single specific mail forwarder. This is occasionally needed when a very slow target domain is encountered, and the user can obtain permission from an ISP to use them for forwarding mail. An ISP login and password can be held by CopiaFacts for use in this way.

Any restrictions required on the usage of DNS or SMTP would normally be applied externally to CopiaFacts, either through the use of a firewall or by other methods. CopiaFacts will attempt any e-mail transmission for which a valid e-mail address has been provided, and with any specified attachments for which the CopiaFacts programs have read access.

Privacy

The account which is running the COPIAFACTS program normally requires access to an entire directory tree which contains queues, documents to be transmitted, documents received, and all control and configuration files. In some cases it may also be a requirement for this account to have administrator status to allow full use of the fax board drivers. This user account therefore can see all transmitted and received files.

A client user generating outbound faxes and e-mails, or receiving incoming faxes, can be restricted to see only a personal subset of the directory tree, normally a single subdirectory of the USERJOBS folder, which contains incoming and outgoing documents. Currently, setting up permissions on these user folders is the responsibility of the system administrator and Copia do not provide a utility for this purpose. The control files which determine the structure, contents and usage of the subfolders can be located in a higher-level folders to which client users do not have access.

The main queue folders, containing control files which will initiate outbound fax and e-mail transmissions, have to be visible to all users so that files can be written there from client software. These files currently contain the target fax or e-mail number, the subject of an e-mail, and the contents of a cover sheet memo if applicable, but not the actual document files which are stored in the personal folder. The COPIAFACTS program already has the capability to retrieve this personal information from a separate file in the users own folder under USERJOBS, and the next major release of the CopiaFacts client software will create two separate files which can be used in this way without leaving recipient and memo information in a common folder.

Null Session Share Access

Some fax board software, notably that from Gammalink, requires access to transmitted and received fax files and folders from driver-level code which has no actively logged-in user (i.e. a null session). When this data resides on a fileserver, it must do so in a share which is named on the NullSessionShares registry key. Naming a share in this way causes Windows to allow access to the share by any driver-level code. To avoid compromising security in this way, release 7.1 of CopiaFacts will implement an option to copy files from the network drive to a local temporary folder, in application-level code, before initiating a Gammalink transmission, and to receive files into a local temporary folder before moving them in application-level code to the correct network destination. Users of earlier releases will be able to remove the sharename (default COPIA) from the NullSessionShares key after upgrading.

Virus-infected Documents

The CopiaFacts 'Document Converter' feature handles requests to fax out items such as Word Documents, Excel Spreadsheets, etc., by preconverting documents to TIFF format. Such documents may originate either inside the company using CopiaFacts, or can also be extracted for faxing from an Outlook mailbox using the CopiaFacts X/Mail feature. These features are optional components, not included in the basic software. The conversions are done by a standalone program which can run on a different machine from those controlling the fax boards, but which still requires access to the queue and document storage folders.

The conversions are done using an Office or Acrobat or other automation object. If these applications have virus-checking and other security features turned off, there is a risk that opening a document containing a virus could infect the system. On the other hand leaving virus-checker enabled would prevent the automatic, unattended conversion of documents.

System Administration

Many CopiaFacts installations run successfully in a closed machine room with routine administration carried out by means of a remote control package such as Symantec's pcAnywhere or VNC. CopiaFacts includes no security features which reflect this mode of operation, and it is the users' responsibility to secure the operation of the remote control software.

Administration Authorization

The CopiaFacts licence control system includes an option to allow certain administrative functions to be password-protected. For example the setting-up of new users could be restricted to specific users only. Although these mechanisms exist they have not yet been implemented in the CopiaFacts administration programs. This work is planned for a future release, and for the present the authorization must be controlled, if necessary, by limiting access to specific administration programs.

Audit Trail

CopiaFacts keeps a comprehensive system log which includes details of all incoming and outgoing calls and outgoing e-mails. A new log file is started each day and users are responsible for how long this information is retained. In addition, each outgoing transaction has a control file (.FS file) which is normally retained for some time after the event to allow reporting and audit. For incoming faxes a control file (.MCF file) is also generated for each transaction. These control files record all available information about the transaction, including for outbound items a record of each transmission attempt. Programs are included to view and report on the system log file, but since it is in standard DBF format most users load it into Excel for viewing and/or analysis.