Secure File Transfers in Heterogeneous Environments

Thomas Burg

Product Manager

comForte GmbH,

Germany

While FTP is a well-established standard for transferring files, it lacks any security features to protect the integrity or confidentiality of the data transferred. This article looks at replacements for the FTP file transfer protocol. The first half looks at the technologies involved while the second half looks at some solutions available for the NonStop platform.

Introduction

File transfer may well be one of the oldest applications within the computing domain. In the early stages, "files" were only transferred between various types of media (punch cards, magnetic tapes, floppy disks) and the computer. As soon as computers got connected with each other, the requirement to transfer files between different computers arose.

A bit later, file transfer was only possible between computers of the same type using proprietary protocols and networks. With the advance of standards in networking, standards for file transfers developed. The first wave of standards dealt with transferring files over direct modem connections and included variants such as ZMODEM or Kermit.

The rapid adoption of TCP/IP network as networking standard has resulted in establishing the "FTP over TCP/IP" protocol[1] as the *de facto* standard for file transfer, which is still in predominant use today. With FTP running on nearly every type of computer it seemed like the topic of file transfer was dealt with once and for all.

Unfortunately, the computing and networking world of today is a much more hostile environment as it was twenty years ago when the FTP standard was established. More and more business is done in complex IT environments with a complex networking infrastructure and criminals have realized the potential for cyber crime. What started as "hacking for intellectual satisfaction" has been turning more and more into a big business of reaping money from companies or individuals who do not protect themselves properly.[2] While the FTP standard fares very well in terms of availability it does not offer any protection against cyber attacks such as password sniffing or spying for confidential data, which is why different protocols have been built to replace FTP.

The trend to replace the FTP protocol with more secure ones is strongly driven by new regulations enforcing minimal security standards such as the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA).

Thomas Burg has nearly 20 years of NonStop experience. Building upon his strong background in systems programming and networking, he is now focusing on the fascinating topic of computer security. Within comForte, Thomas is responsible for security products and services. He can be reached at T.Burg@comforte.com.

The Challenges of Replacing FTP

While it is becoming common knowledge that FTP should be replaced with something better for security reasons, picking the "something better" is not an easy task: As of today no single standard has emerged which is as predominant and well-accepted as FTP (whenever a standard is as predominant as FTP, this tends to drive cost down as multiple vendors will be competing with compatible solutions).

Picking the right solution will depend on many factors, as a "file transfer" from or to a NonStop system can occur in many different environments:

- The transfer can be initiated either on the NonStop system (in which case it is the client) or on the remote system (NonStop system as server)

[1] The FTP standard is described in the RFC 959 available at http://www.ietf.org/rfc/rfc959.txt

[2] See http://www.securityfocus.com/news/11209 for an article on how modern cyber attacks evade detection by anti-virus software. Citing from there: "The attackers are well motivated--no longer by fame, but by money", said Amit Yoran, former director of the National Cyber Security Division of the U.S. Department of Homeland Security and now an independent consultant. "Several years ago, the high-visibility activity seemed to be ego driven--criminal to be sure, but less motivated by theft fraud and other sorts of criminal advantage. In today's environment there is a well-established and thriving criminal element that works in the cyber domain."

- The transfer can be initiated automatically (batch) or in an interactive fashion (user-driven)
- The file transfer can be internal only (such as an upload of a source or object file) or it can implement data distribution to an external entity
- The file being transferred can be structured or unstructured
- For either an internal or an external file transfer scenario, you may be in control of all systems involved—which would make picking a solution easier. Or you could be forced to find a solution which is compliant with the "XYZ" product on a system you have no control over.

All these factors have to be weighed in when picking a replacement for FTP. In the next section we will look at different solutions competing for the replacement of FTP.

Secure FTP Solutions

As mentioned in the introduction, no single protocol has emerged to replace FTP. Various products implementing different protocols result to a complex market space. Before looking at some solutions available on the market, we will shed some light on technical and protocol choices when replacing FTP.

Protocols for secure file transfer. "The nice thing about standards is that there are so many of them to choose from."[3] There are two different types of secure file transfer protocols which are in widespread use:

- There is an enhancement to standard FTP[4] which uses the same FTP commands (and protocol) over secure sockets, i.e., over SSL/TLS. This is known under the names of FTPS, FTP-over-SSL, FTP-TLS or FTP-SSL. This protocol has been adopted by various Windows-based FTP clients very early on. As of today, FTP- -SSL is in very wide adoption in the market space, as there are numerous commercial and/or free implementations for all major platforms. It is also supported by several 6530 terminal emulation vendors.
- There is also another protocol, unfortunately named SFTP (and therefore falsely implying a relationship with the FTP protocol) which also provides secure file transfer. This protocol is implemented using SSH (Secure SHell), a suite of secure network connectivity tools and is not related to the FTP protocol at all. SSH[5] and SFTP are popular especially in the Unix world.

The following table compares the two protocols SSL and SSH on which the two file transfer protocols above are based.

Protocol	History	Authentication	Other
FTP-SSL	SSL was created by Netscape in 1995 to secure Internet traffic FTP-SSL was first drafted as standard in 2001	Uses PKI to authenticate the SSL session. Logon to FTP session with username and password	Sits "on top" of FTP standard Popular in Windows world early on
SFTP	SSH was created by a Finnish student to secure Unix shell access in 1995 Support for file transfer was added a little later	Either through Public/Private Key pairs or through username and passwords	Not related to FTP standard at all Popular in Unix world early on Openssh in wide use in Unix world

Files can also be transferred by using the http(s) protocol, by e-mail and of course, there are many proprietary protocols for (secure) file transfer. A future-proof solution should at least optionally support one of the two standards mentioned above for optimal compatibility with other solutions.

Potentials for FTP Improvements. Every file-transfer product will do one thing: It will transfer files. So does FTP, which is freely available on just about every computer these days—thus a file transfer product will have to offer at least one feature which goes beyond the simple capabilities of FTP. Potentials for improvement of FTP abound:

- Security of the file transfers: As mentioned before, the FTP protocol does not offer any security features except for the user authentication via username and password. Better solutions support strong authentication and protect the integrity and the privacy of the file being transferred. Ideally, the security of the file transfers should be based on standard protocols as mentioned in the prior section rather than on a "homegrown" protocol[6]
- Guaranteed delivery: If a file transfer fails halfway through the process, some products will restart the file transfer and guarantee delivery that way
- Auditing and Management tools
- Automatic post-processing of the transferred file on the remote system. This could mean transferring a file from a NonStop system to another system, converting it to a PDF file and sending it as an e-mail
- Support of higher-level protocols: The Electronic Data Interchange (EDI) protocol is the data format used by the vast majority of electronic commerce transactions in the world. Some products for file transfer are focusing around higher-level protocol such as EDI.

Protocol-driven Solutions.

With all the potential features described in the prior section, it is clear that different products can vary widely in their scope. In this section, we will categorize products and then look at some exemplary implementations available for the NonStop platform.

Protocol-driven solutions are solutions which simply implement the protocols for secure file transfers mentioned in Section Protocols for secure file transfer. By doing so, they interoperate with other solutions implementing the

[3] This famous phrase was coined by Andrew S. Tanenbaum in his book "computer networks" back in 1981 – however it is valid until today – possibly even more so.

[4] The enhancement to FTP is being proposed as an RFC, see http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html for details. Putting "draft-murray" into Google will bring you both the aforementioned page and the latest version of the proposed RFC.

[5] SSH is a rich set of protocols and standardized in a multitude of RFC's.

[6] Note that a "protocol" for secure file transfer is more than just picking a "cipher suite" such as 3DES or AES: A protocol combines different cipher suites to solve complex issues such as key generation and prevention of man-in-the-middle-attacks. That why simply specifying a well-known cipher-suite such as 3DES does not suffice to make a file-transfer solution bullet-proof.

same standards on different platforms. They are typically easy to set up and will make your NonStop system compatible with internal or external systems which support the same protocols.

We will be looking at two protocol-driven solutions by comForte[7] in the following.

SecurFTP/SSL: Transparently adding SSL to FTP file transfer. SecurFTP/SSL was launched in early 2003 and thus has been one of the first solutions for secure file transfer on the NonStop platform. It uses a "proxy-based" approach as shown in the following diagram:

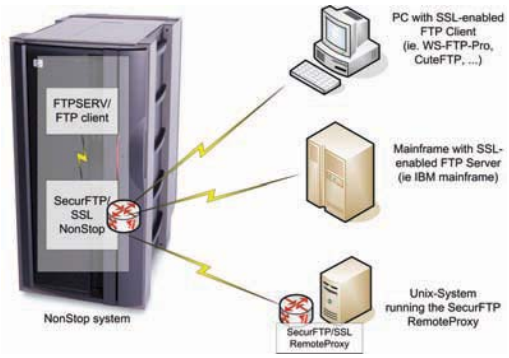

Figure 1

If the FTP solution on the remote system already supports FTP-SSL, no comForte software is required on the remote system. If the FTP solution on the remote system does not support FTP-SSL, the RemoteProxy component will add SSL support on the remote system making it a multi-platform solution.

The proxy approach leaves the FTP or FTPSERV component in place on the NonStop platform. This way existing solutions for file transfers in batch environments which have integrated these components into TACL macros, Netbatch or similar environments won't have to be modified at all. A simple configuration change will "activate" SecurFTP/SSL and thus transparently secure the file transfers.

An optional add-on to SecurFTP/SSL will enhance the control of the remote users that FTPSERV offers: it contains its own user database which is independent of Guardian users and allows for fine-grained access control ("user guest can only download from this subvolume"—with guest not even existing as Guardian user or alias) and auditing.

SecurFTP/SSH: File transfer using SFTP over SSH for the NonStop platform. When SecurFTP/SSL was launched in 2002 the focus in the NonStop world was transferring files between the NonStop platform and Windows PC. Back then, the SSH protocol was not widely adopted in the Windows world so implementing the SSL protocol first was a natural choice for comForte.

With more and more customers asking for secure file transfer to Unix systems (without having to install the RemoteProxy component as in Figure 1), comForte has created a second "flavor" of SecurFTP implementing the "SFTP over SSH" standard. SecurFTP/SSH has been built from scratch for the NonStop platform and supports running with or without OSS.

SecurFTP/SSH is available for the NonStop platform only and will interoperate smoothly with the various implementations for other platforms. Other than in 2002, today many PC-based file transfer solutions (i.e., WS-FTP-Pro) will now support SSH-based file transfers as well.

As SecurFTP/SSH fully replaced FTPSERV and the FTP client on the NonStop platform, existing batch infrastructures using TACL macros or the like will have to be changed.

Choosing a protocol-driven solution. Picking a protocol-driven solution can be a bit tricky: There are (at least) two standards for secure file transfer, so you will have to take a careful look at the platforms you want to exchange files with as well as your current environment for file transfers. In a heterogeneous environment, you may well end up having to implement both protocols.

Enhanced File Transfer Solutions

Enhanced File Transfer Solutions go beyond offering file transfer by implementing more of the features mentioned in section Potentials for FTP Improvements. There are many players in that market, some offering cross-platform solutions, some offering solutions built specifically for the NonStop platform. Again, we will be looking at some exemplary solutions in the following.

TeleFTP. TIC Software's TeleFTP product[8] is a NonStop System-based FTP Client that automates the transmission of Spooler reports and files. TeleFTP also provides:

- Conversion of data into document formats such as PDF, HTML and ZIP prior to data transmission
- XML-based configuration file and Desktop GUI for ease of administration
- API for applications to invoke FTP transmission programmatically
- ALIAS database for grouping remote FTP destinations.

The integration of SecurFTP/SSL provides the enhanced security to TeleFTP in protecting the transformed documents during its transmission to remote FTP servers.

MessageWay: Expanded B2B functionality. MessageWay[9] is a greatly-enhanced file transfer product that integrates SecurFTP/ssl into its operation. Offering all of the Potentials for FTP Improvements mentioned above, MessageWay also adds many additional features to provide

[7] See http://www.comforte.com/securftp

[8] See http://www.ticsoftware.com/index.cfm?page=teleftp

[9] See http://www.messageway.com/

expanded B2B functionality. A few of these are:

- Support for additional communications protocols to augment SecurFTP/ssl communications, including protected FTP data access
- Dynamic routing to automatically steer data to its destination based on inspection of data type, content, and other criteria
- Any-to-any translation subsystem that can output multiple data formats in one pass for flexible application integration
- Operates on Linux, Unix, and Windows as well as NonStop; supports multiple SQL databases, e.g., MySQL; Oracle, for flexibility.

DataExpress. DMBGroup Inc.[10] offers DataExpress as the definitive file transfer, management and scheduling solution for companies who need to route, format, and secure business-critical information in an automated fashion over public and private networks. The product is available in two versions, one specifically for the NonStop platform (DXNS) and one for Windows and UNIX platforms (DXOP).

DataExpress customers continue to depend on the product in their mission critical applications to manage, move, and report on their data flow over a wide spectrum of protocols. DataExpress connects to all legacy and Internet transmission protocols, including bisync, async, Connect:Direct, FTP/S, HTTP/S and BulkData Gateway at the Federal Reserve. SecurFTP/SSL integrates seamlessly with the DataExpress application, providing secure file transfers over SSL using FTP

For the past 20 years DataExpress has been implemented in a variety of industries including banking, financial services, and insurance.

Summary

The seemingly simple task of "replacing FTP with something secure" opens up a whole world of competing technologies and products. Before deciding on your future solution, make sure to look at your requirements in detail.

After having determined your requirements, you should know whether to aim for a simple, "protocol-driven" solution or if you need a richer solution supporting more features such as the "enhanced file transfer" solutions described earlier.

There is a rich variety of solutions available for the NonStop platform, so the choices are all yours.

[10] See http://www.dataexpress.com/