

GBData Online Backup

Whitepaper – Data Security

Version 5.x
Jun 2006

Table of Content

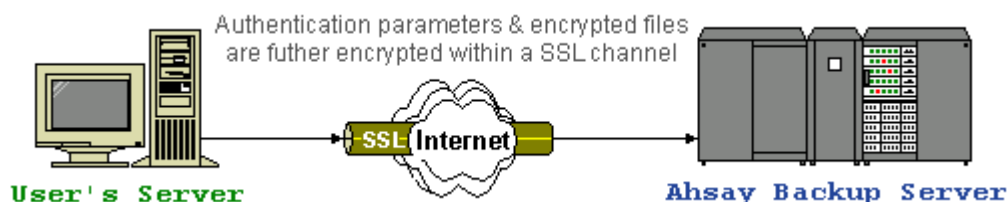
1	Introduction	3
2	GBData Offsite Backup Server – “Secure, Robust and Reliable”	4
2.1	Secure 128-bit SSL communication	4
2.2	Backup data are securely encrypted.....	4
2.3	We don't keep your encrypting key.....	4
2.4	Best encryption algorithm is used.....	4
2.5	Require 8.77×10^{17} years to crack the 128-bit encryption	5
2.6	Restrict access to data by IP addresses.....	5

1 Introduction

This document describes the security measures available in GBData Online Backup software from the user's perspective. It serves as a reference for partners when addressing customers' queries on security.

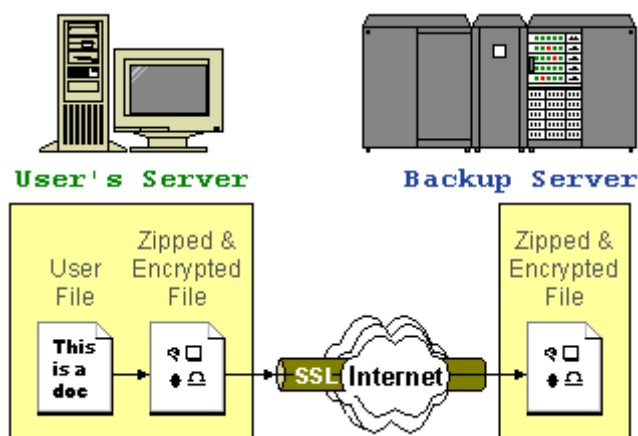
2 GBData Offsite Backup Server – “Secure, Robust and Reliable”

2.1 Secure 128-bit SSL communication



All communications between GBData Backup Server and your computer are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), eavesdroppers have no knowledge of what has been exchanged.

2.2 Backup data are securely encrypted



All of your files are first zipped and encrypted with your defined encrypting key before they are sent to GBData backup server. To all people but you, your files stored on GBData backup server are no more than some garbage files with random content.

2.3 We don't keep your encrypting key

The encryption key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. If this key is lost, all backup files can never be recovered. Therefore, although we have access to all files you stored on our backup server, we have no knowledge of the content of the files you stored.

Reminder : Please make sure you write down you encryption key in a safe place where it will never be forgotten. Otherwise, you will never be able to recover your backup files.

2.4 Best encryption algorithm is used

Currently, the algorithm that we are using to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES)

finalists chosen by National Institute of Standard and Technology (NIST). It subjects to frequent public reviews but no known attack against this algorithm has been reported.

2.5 Require 8.77×10^{17} years to crack the 128-bit encryption

A 128-bit key size has 2^{128} or around 3.4×10^{38} possible combination. Even if you have the world best super computer, ASCI White, SP Power3 375 MHz manufactured by IBM as of November 2000, it would take 8.77×10^{17} years to test all combinations. Assuming your have the super computer, ASCI White, SP Power3 375 MHz has 8192 processors which totals a capability of 12.3 teraflops (trillions of operations/second), available to you. Also it just needs one computer operation to test a possible combination (which is already faster than what it can do). To use brute force attack (checking all combinations) on this encryption algorithm. It would take:

$$\frac{3.4 \times 10^{38}}{12.3 \times 10^{12}} \text{ seconds} \sim 2.76 \times 10^{25} \text{ sec}$$

i.e. 876530835323573935 years or 8.77×10^{17} years

to successfully try all combinations. Let alone ASCI White cannot process as fast as what described here. You can be sure that your data stored on our server is 100% secured.

2.6 Restrict access to data by IP addresses

You can also restrict access to your backup files from the set of IP addresses you defined. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures backup files is not open to all location, even username and password are known.