Ahsay Online Backup

Whitepaper – Data Security

Version 5.x
Jun 2006

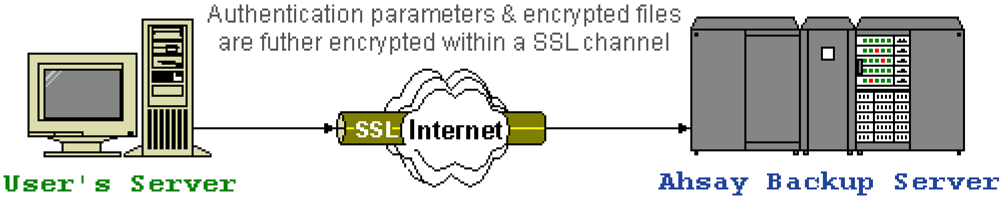
Table of Content

1 Introduction

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

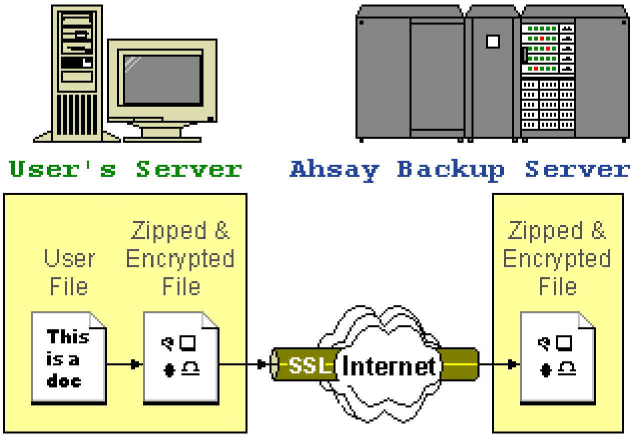
2 Ahsay Offsite Backup Server – "Secure, Robust and Reliable"

2.1 Secure 128-bit SSL communication


Authentication parameters & encrypted files are futher encrypted within a SSL channel
SSL
Internet
User's Server
Ahsay Backup Server

All communications between Ahsay 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 Ahsay backup server. To all people but you, your files stored on Ahsay backup server are no more than some garbage files with random content.

2.3 Encrypting key are well protected

The encrypting 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. Thus, even the system administrators will not be able to decrypt and view the content of your files stored on the backup server without your permission. This unfortunately means if the encrypting key is lost, you will never be able to recover your backup files.

Technical Details

The encrypting key for the different backup sets are stored the config.sys file, which is encoded by a proprietary algorithm:

(Windows)	C:\Documents and Settings\administrator\.obm\config\config.sys
(Linux)	~/.obm/config/config.sys
(Mac OS X)	~/.obm/config/config.sys

If client software cannot locate the config.sys (due to accidental deletion or logon to a new machine with the same account), it will prompt the user to re-enter the encrypting key for the backup set and then store it in the local config.sys.

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 x 10^{17} years to crack the 128-bit encryption

A 128-bit key size has 2^{128} or around 3.4 x 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 x 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:

3.4 x 1038
-------------- seconds ~ 2.76 x 10^{25}sec
12.3 x 1012

i.e. 876530835323573935 years or 8.77 x 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 are not open to all location, even username and password are known.