Secure Backup/Restore

Introduction

This document outlines the design decisions and assumptions made for the provided backup and restore functions written in Bash.

Functions

- **validate_backup_parameters** Validates the number and format of arguments provided for the backup function.
- **backup**: Performs the backup operation, including:

  Validating source and destination directories.

  Creating a timestamped subdirectory for the backup.

  Finding modified files within the source directory based on the specified number of days.

  Creating temporary directories to hold modified files for individual subdirectories.

  Creating tar archives of modified files within each subdirectory.

  Encrypting the tar archives with the provided encryption key.

  Creating a single tar archive containing all the encrypted archives.

  Compressing and encrypting the final archive.

  Transferring the encrypted archive to a remote server.

  Cleaning up temporary directories.

- **validate_restore_parameters**: Validates the number and format of arguments provided for the restore function.
- **copy_files_to_restore_dir**: Copies all files from the backup directory to the restore directory.
- **perform_restore**: Decrypts and extracts files from the backup directory:

  Decrypts individual encrypted files within the backup directory.

Extracts the contents of decrypted tar archives.

Recursively processes newly extracted files for decryption and extraction.

Design Decisions

- **File Selection** The backup function only backs up files modified within the specified number of days. Unmodified files are skipped.
- **Temporary Directories** Temporary directories are used to hold modified files before creating tar archives for individual subdirectories. This ensures that only modified files are included in the archives.
- **Encryption** Encryption is applied to individual tar archives after creation. The decryption key is required for restoring the data.
- **Remote Backup** The backup function can optionally transfer the final encrypted archive to a remote server using scp.
- **Restore Process** The restore function decrypts individual files within the backup directory and then extracts the contents of decrypted tar archives. It recursively processes newly extracted files for further decryption and extraction.

Assumptions

- The script has access to the gpg command-line tool for encryption and decryption.
- The script has permission to read and write files in the specified source and destination directories.
- File paths provided as arguments are absolute paths.
- A public/private key pair is used for SSH authentication. The private key is stored securely on the backup server, and the corresponding public key is added to the authorized_keys file on the remote server. document