CrashPlan PROe Security

CrashPlan PROe is a continuous, multi-destination solution engineered to back up mission-critical data whenever and wherever it is created. Because mobile laptops often are connected to unsecured networks, a very high standard of security is required to ensure privacy. CrashPlan PROe's multi-layered approach to security was engineered to meet this high standard and exceeds industry best practices, while balancing an enterprise's need for convenience and flexibility.

Security Context

To understand the security of CrashPlan PROe, it helps to have a high-level familiarity within the context of how CrashPlan PROe works:

1. CrashPlan PROe backup begins with the client recognizing file modifications made by the user in real time. Files are analyzed quietly in the background to identify what is unique about the change. Unique information is broken into blocks, then compressed and encrypted symmetrically using a local archive key.
2. The encrypted information flows through a secure communications channel to multiple destinations as specified by an administrator.
3. Data remains in its encrypted state on disk, at the destination. Decryption occurs only when authorized personnel supply the password or archive key to restore the data.
4. CrashPlan PROe restore begins when the user or administrator selects files to restore. Encrypted blocks are received by the client, decrypted using the local archive key, decompressed and written out locally to disk to complete the file recovery process.

Technology

CrashPlan PROe executes within the confines of a secure Java virtual machine. All cryptographic functions rely on the industry standard Cryptographic Extensions (JCE)[1] provided therein. There are numerous security benefits to this architecture, including:

Type safe execution
Only secure, type safe byte code is executed, providing protection against buffer overflows and similar mistakes traditionally exploited by attackers.

Open model
Rather than relying exclusively on "security through obscurity," the cornerstones of our security frameworks are available via open-source for peer review.

Comprehensive security framework
The JCE has been widely reviewed and deployed in countless enterprise applications.

Solution Highlights

- Secure, 448-bit Blowfish file encryption
- AES 128-bit, TLS-based communications encryption
- LDAP and Shibboleth SSO authentication server support
- Flexible key escrow policy
- Secure, globally unique identifiers
- Audit-able, logged restores
- Automated data retention policies and life-cycles
- Tamper-proof backup archives
- Centralized administration and event logging
- Flexible policy management and enforcement
- Proxy support

Account Security

CrashPlan PROe can leverage your existing LDAP or Shibboleth server for user authentication. User account states can be updated in real time (pushed) or delayed (pulled), depending on the authentication system used. With this model, CrashPlan PROe does not store user login information in its database.

Roles

In CrashPlan PROe, a user account may be authorized with the roles below, listed from those with the least to those with the most permissions:

Desktop User
Permission to back up to a CrashPlan PROe Server (default).

PROe User
Permission to access the CrashPlan PROe admin console. Access is restricted to the users' computers and their data (default).

Org Manager
Read-only access to all users in their respective organization and all child organizations.

Org Admin
Read/write access to all users in their respective organization and all child organizations.

All Org Manager
Read-only access to all users in all organizations.

All Org Admin
Read/write access to all users in all organizations.

Admin Restore Limited
Permission to perform a limited size restore for all devices the admin has permission to view.

Admin Restore
Provides permission for user to restore data on behalf of other users within the organizations the admin has permission to view.

Push Restore
Permission for the admin to initiate a restore to any device the admin has permission to view.

Server Administrator
Permission to edit all system information not reserved exclusively for the SYSADMIN. Read/write access to all users, all organizations, all children and all servers.

SYSADMIN
Read/write access to all users, all organizations, all children and all servers.

In addition, admins with full SYSADMIN permission can create and assign custom roles.

Internal Accounts

Accounts can be created by end users without IT intervention, provided the user knows the following information:

Registration Key (aka Organization ID)
A unique and secure, 64-bit, globally unique identifier (GUID) containing 16 letters and/or numbers, which is cryptographically secured to prevent a brute force, dictionary-style attack to join the environment.

CrashPlan PROe Server hostname
The resolvable hostname to the IP address of the CrashPlan PROe Server.

Accounts created via this method are limited to Desktop User and PROe User roles. These roles have no administrative or managerial permissions.

External Accounts

CrashPlan PROe can leverage your existing LDAP or Shibboleth server for user authentication. User account states can be updated in real time (pushed) or delayed (pulled), depending on the authentication system used. With this model, CrashPlan PROe does not store user login information in its database.

Account Lifecycle

Accounts can move from one state to another. Account states include:

Active
Account may interact with their data and computer(s).

Deauthorized
The user is logged out of the deauthorized client installation. Users may reactivate themselves.

Blocked
Account is considered temporarily inactive and blocked from all login activity. Users may not reactivate themselves.

Deactivated
Inactive status. Account is no longer considered in use and users may not reactivate themselves.

From a security point of view, these states can be transitioned and subsequently trigger pre-defined data retention polices. For example, if an employee's status becomes inactive, CrashPlan PROe no longer accepts backups from this user, until the user is reactivated. The data is held for 30 days, after which it is deleted.

Data Security

Files and their respective metadata are 448-bit Blowfish encrypted using the Archive Key on the source computer. This has several benefits:

- Data may be stored at unsecured or untrusted destinations, such as a third-party cloud provider, with no risk of their contents being discovered.
- Because all metadata is encrypted, there are no hints available as to what data was encrypted and stored.

Encrypted data is securely transmitted and stored in a proprietary, virtual disk-type structure optimized for security, reliability and performance on the CrashPlan PROe server.

Data is MD5 checksummed at multiple points during the backup process. Additionally, data is checksummed after encryption at the source to provide to destinations the ability to detect corruption or tampering without having encryption keys for the original data.

Archive Key Creation

An archive key must be present on a system before the first backup occurs. Typically, keys are created at the time of installation using either the random key generation feature in CrashPlan or a custom key provided by the IT department.

Keys are created using a secure, random number generated from Oracle's Java Cryptography Extensions framework. This framework is an audited, open-source implementation, proven to exceed industry standard practices.

Archive Key Storage on Client

In order to support unattended backups, it is necessary to store the archive key in plaintext on the local file system.

To ensure the archive key is given the highest possible security relative to the data being backed up, the archive key's file permissions are set to read-only for the user who installed the CrashPlan PROe client. Typically, the client is installed with an administrative account and will only allow read-only access to the key by that administrator.

We highly recommend using a full-disk encryption technology such as BitLocker on Windows, File Vault on Mac OSX or a third-party solution to protect your data as well as the CrashPlan archive key.

Archive Key Management

There are three methods of managing archive keys in CrashPlan PROe:

448-Bit Encryption
Uses the account password to encrypt the archive key.

448-Bit Encryption + Password
Uses an additional password to encrypt the archive key.

448-Bit Encryption with Custom 448-Bit Key
A user-provided, 448-bit archive key (PROe Client only).

448-Bit Encryption

In this mode, the account password is used to encrypt the archive key.

Note, the account password is NOT used to encrypt backup data. The account password may be changed at any time.

448-Bit Encryption Archive Key Escrow
For the 448-bit encryption protection mode, the archive key is escrowed on the CrashPlan PROe Server.

448-Bit Encryption + Password

If additional client security is required, the user may elect to symmetrically encrypt their archive key with a user-provided archive key password. This facilitates key escrowing while preventing administrators from accessing protected data. However, if the archive key password is lost, no one can restore from the backup archive.

Due to the potential for unrecoverable data, CrashPlan PROe gives the administrator the option to disable this feature.

448-Bit Encryption with Custom 448-Bit Key

In this model, the user provides a 448-bit archive key. To ensure security in untrusted, hostile storage environments that are not under direct IT control, the key is not escrowed under this mode. This approach requires you to manually manage your own keys but provides assurance that there is no way a third party can retrieve your data. This is the most secure yet least convenient policy.

Due to the potential for unrecoverable data, CrashPlan PROe gives the administrator the option to disable this feature.

Communications Security

Communications between PROe Client and PROe Server are encrypted with a unique, computer- and session-specific AES 128-bit key. As part of the client deployment process, IT staff will be able to provide the hostname, port and a RSA 2048-bit public key for the CrashPlan PROe Server. We have excluded the certificate negotiation facilities in our implementation of TLS and are not vulnerable to a compromised Certificate Authority or attacks against the certificate exchange process. Also, if the PROe Server or Client detects corruption, replay or man-in-the-middle attacks, the session is terminated and will need to be restarted from the beginning. The PROe Client supports network environments that require network traffic to route through a proxy server.

The specific steps and technologies for establishing the connection are outlined as follows:

1. **Establish TCP Connection**
   A single TCP connection to a single port, typically port 443, is used for all communication.
2. **Establish Communication Session**
   Session key negotiation, as defined by the TLS specification, is used to establish a unique,128-bit key for both the client and server.
3. **Client Version Verification**
   PROe Clients must meet minimum version requirements to ensure data integrity before validation of identities is allowed by PROe Server.
4. **Identity Verification**
   The computer and user identities are verified at the application level before any additional operations are permitted.
5. **Establish Application Session**
   User and computer have passed all tests, so session is promoted to an application session allowing for backup and restore.

Client Version Verification

Once the communication session has been secured, additional steps are taken to verify the application security layer. PROe Client provides additional information about itself to PROe Server, including:

Version
What is the PROe Client version running?

OS
On which OS and VM environment is the Client running?

IP Address
What is the IP Address of the PROe Client?

TimeZone
In which timezone is the computer located?

The PROe Client must present additional information about itself before an application login attempt will be accepted. The PROe Server logs the information received and verifies the integrity. Invalid data results in a disconnect. Valid data results in a "proceed" message to PROe Client.

Computer Identity Verification

At this point, the PROe Client and PROe Server are still considered "untrusted" and have no rights beyond additional verification. The first step is for the client to present its unique, 64-bit identity to the untrusted PROe Server.

The PROe Server verifies if this identity is:

Valid
Is this a valid identity?

Active
Is this identity allowed to connect?

Unique
Is this identity already connected within the enterprise?

If any of the above is false, the client is immediately

disconnected.

If the identity is valid, the PROe Server acknowledges it by sending back its own unique, 64-bit identity to the PROe Client.

User Identity Verification

Having received the go-ahead, PROe Client now has a secure communication channel over which to communicate. Note, no actual permission to back up (or do anything else) has yet been granted. PROe Client requests account creation/login using the following information:

RegistrationKey
Cryptographically secure, unique identifier for requesting area to back up to

Username
Identity of user

Password
Secure hash and salt of user's password, or actual password if LDAP is enabled in client

GUID
Globally unique identifier of computer

Deferred Request
Request to defer login for this computer (server must OK)

Configuration Version
Version of the client configuration PROe Client is using

Note, the account password is never transmitted to the CrashPlan PROe Server in plain text. On the client, the account

password is salted with a 64-bit random number and hashed multiple times using SHA-1. This hash value is transmitted to the CrashPlan PROe Server and used to validate the user's identity.

PROe Server receives above information and validates the contents. If all information is correct, permissions are assigned to connection based on user's defined roles. New users only have the right to back up (store) data. Validation is complete and consistent based on PROe Server configuration, including:

Registration Key
Is this registration key valid? Known? If not, disconnect.

LDAP
If registration key provided is backed by LDAP services, identity management is deferred to identity management server in real time.

SSO
If registration key provided is backed by Shibboleth SSO services, identity management is deferred to identity management server in real time.

GUID
Is user trying to create an account with a GUID assigned to another user? That would be impossible, disconnect.

User State
Is this user considered valid and "active" in the organization? Or have rights been rescinded?

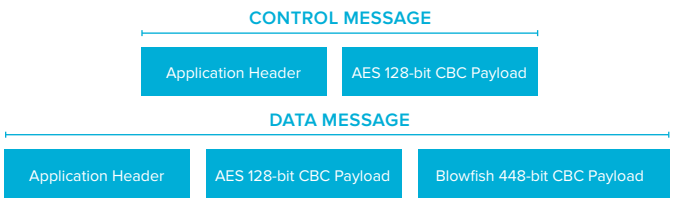
Computer State
Is this computer still considered "active" and able to back up? If not, take prescribed action (i.e. permanently disconnect PROe Client).

Deferred Request
Does this registration key permit invalid login? If not, disconnect.

If all criteria are validated, including the optional dependency on a third-party identity management system, permission is granted to the PROe Client to back up and restore. Note, at this time, no additional permissions are granted. The application enforces that their data "sandbox" is unique to that specific user. Ultimately, after all checks have passed, the client merely has the right to store encrypted backup data at the destination.

Control vs. Data Communications

Control messages, which communicate information such as verification or status, are constructed of a six-byte application header and an AES 128-bit encrypted payload as specified by the TLS protocol. Data messages, which deliver the 448-bit Blowfish encrypted file data, are constructed of a six-byte application header, AES 128-bit encrypted metadata and the Blowfish encrypted file data.



Establish Application Session

Now that client authenticity, user identity and machine identity have been established, the session is allowed access to the backup and configuration layer.

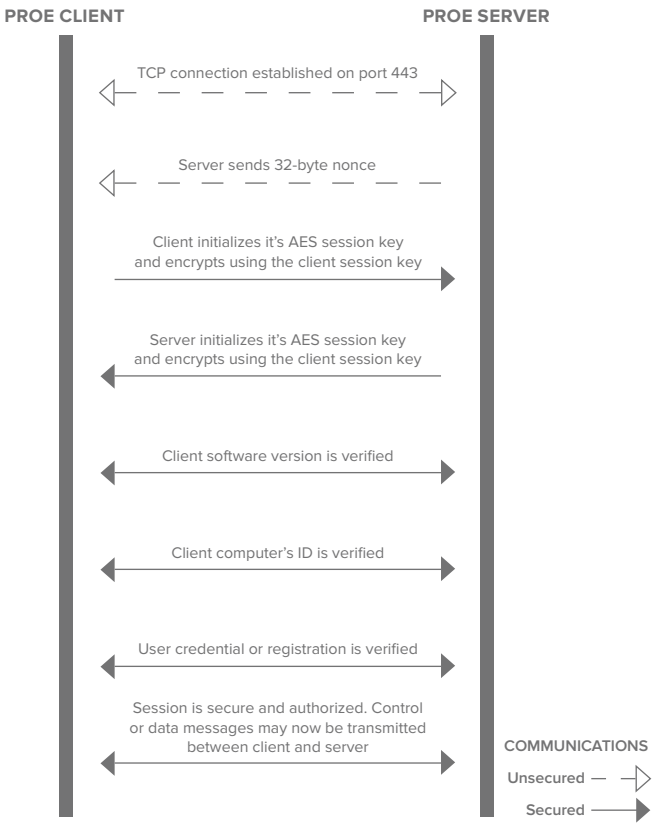
The client configuration version is inspected and validated. If the client is "behind" on administrative configuration and/or controls, those controls are pushed down to the client and enforced locally. The configuration includes various runtime operation settings including:

Client UI Settings
All elements of the desktop UI have fine-grain controls permitting the setting and/or locking of various settings.

Destinations
Both permitted and required destinations. This provides administrative controls over what is backed up and to where.

The application session layer remains persistent and connected for the duration of the session. The advantage of this approach is additional configuration and/or statistics are able to be moved in real time, independent of the backup layer.

Secure Communications Sequence Diagram



Web Security

CrashPlan PROe provides a web administration interface to manage backup for all PROe Clients. Users may also be allowed to restore their files via the web interface. The web interface can be configured to require HTTPS for all communication.

HTTP Session Creation
Session IDs are generated using a secure random number class and hashed with a secure hashing algorithm.

HTTP Session Communication
Session IDs are sent in the header of the HTTPS GET request.

HTTP Session Use
Sessions identify end user for duration of session to avoid having to repeatedly authenticate for each request. Each request is validated against the current active session.

HTTP Session Expiration
Sessions expire after 30 minutes of no activity.

HTTP Input Validation
All data input into CrashPlan PROe forms is validated and scrubbed of any HTML tags (including SCRIPT) to prevent XSS, XSRF attacks. Additionally, any data passing through to database is merged with previously compiled SQL statements to prevent SQL injection attacks.

Database Security

CrashPlan PROe contains an embedded database to facilitate configuration storage, usage reporting and identity management. The database is not accessible via a network socket and is only available to the CrashPlan PROe application. Encrypted copies of the database are dumped automatically to available storage points. Encrypted data keys are only present in data stream if key escrowing policy is in effect (refer to encryption key security).

CODE42 **CORPORATE HEADQUARTERS** 1 MAIN STREET SE #400 / MINNEAPOLIS, MN 55414 / 612.333.424 / WWW.CRASHPLANPROE.COM/CONTACT / WWW.CODE42.COM