Encryption

Encryption is one of the steps to take when designing a system with Defence in depth. Here we go over what you need to be concerned about and different implementations to consider.

Threat Model

Threat modelling is hard. The most widely-applicable framework that I have stumbled across is to frame up your model with respect to the following scopes, from lowest to highest:

- Neighborhood Hacker
- Corporate Surveillance
- Nation-State Espionage

Consider at which level you would like to defend against when considering the options available to you.

Responsibility Levels

There are three levels of responsibility for any hosted service:

- Physical/Infrastructure
- Service Provider/OS Admin
- Application admin/consumer

Physical/Infrastructure

Digital Ocean:

- Local Droplet Storage: https://www.digitalocean.com/community/questions/droplet-native-storage-is-it-encrypted-similarly-to-block-storage-volumes?answer=54705
- Block Storage: https://docs.digitalocean.com/products/volumes/

Service Provider/OS Admin

- Enabled:
  - HTTPS: https://blog.securityevaluators.com/does-https-protect-your-privacy-9e8903f576d3
- Planned:
  - LUKS: https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
  - Encrypted Tarballs: https://www.tecmint.com/encrypt-decrypt-files-tar-openssl-linux/

Application Admin/Consumer

Built-In Nextcloud Functionality: https://nextcloud.com/blog/encryption-in-nextcloud/

- Server-Side Storage Encryption:
  - https://nextcloud.com/encryption/
  - https://docs.nextcloud.com/server/latest/user_manual/en/files/encrypting_files.html
  - A note on local storage:
    A server-wide key stores a server password in the Nextcloud data directory and uses it to decrypt the server key in the users' data directory, which in turn is used to decrypt data.

    When using per-user keys, the key in the data directory is per user and encrypted with the user password. We take great care to ensure keys never enter storage but keys will be kept in memory on the Nextcloud server for the duration of user login sessions to facilitate decryption and encryption of data.

    Per-user keys only offer additional protection over a server-wide key in the case of physical theft of the Nextcloud server and storage or a security breach of the sever *provided the user(s) do NOT log in for the duration of the breach*.
- End-to-End File-level Encryption:
  - https://nextcloud.com/endtoend/
  - https://github.com/nextcloud/end_to_end_encryption
  - https://www.techrepublic.com/article/how-to-enable-end-to-end-encryption-for-the-nextcloud-app/

Revision #7
Created 10 May 2021 17:28:00 by andrewcz
Updated 15 June 2021 03:58:09 by andrewcz