Random APIs

More documentation to come.

Platform-Specific Default Random

The implementation of the default random generator varies by platform. The implementation on each platform must be thread-safe and automatically seeded, and should be cryptographically secure to the extent possible. Currently supported platforms have the following implementation details:

- Apple platforms use `arc4random_buf(3)`.
- Linux, FreeBSD, and other UNIX-like platforms use `getrandom(2)` when available; otherwise, they read from `/dev/urandom`.
- Fuchsia platforms use `getentropy(3)`.
- Windows platforms use `BCryptGenRandom`.