

Unauthorized disclosure



- ➡ Use keys-encrypting keys to protect long-term keys
- ➡ Use secure data erasure to overwrite memory after key use. Scan memory for key patterns and repeat.
- ➡ Separation of duties such that collusion is required to compromise the system
- ➡ Secure shred keys on paper, fine-crush hardware containing keys, secure data erasure on disk
- ➡ Consider different keys for different use to minimize impact of unauthorized disclosure

Loss

➡ Key escrow and secret-sharing protocols