Secure Key Management

Storage, Destruction

Kc Udonsi

ATTEMPT CRYPTANALYSIS; INVEST $$$$$$$
COMPROMISE ENCRYPTION KEYS; INVEST $$
imgflip.com

Threats to Cryptographic Keys

All your keys are belongs to me

- ➡ Weak/Insecure generation
- ➡ Attack on transmission
- ➡ Unauthorized disclosure
- ➡ Loss

Weak / Insecure key generation

- The security of cryptographic algorithms rests in the key. Weak keys => Easy cryptanalysis on key space
- Sometimes, not using all keys in the key space may result in weakness
- Poor key choices e.g use of mutations of dictionary strings
- Weak/non-cryptographically safe randomization for key generation

Attack on transmission

- No error detection during transmission. May lead to garbled or partially decrypted cipher text. Violation of availability
- Malicious key swap. Malicious keys used for encryption. Violation of confidentiality. Man-in-the-middle attacks

Unauthorized disclosure

- Improper storage of long-term keys e.g SSH private keys with weak access permissions, keys on disk unencrypted, keys in memory unencrypted

- Bribery; insider threat

- Improper destruction; key can be reconstructed

- Improper implementation; transmitting keys in plaintext

Loss

- ➡ No backup mechanisms in place
- ➡ Single point of failure

Good Key Hygiene

Weak / Insecure key generation

- Where applicable, all keys in the key space should be equally likely and provide the strong encryption

- Use cryptographically safe mechanisms to create random values when needed.

- Consider using cryptographically secure PRNGs to generate keys from an easy to remember but obscure (hard to guess) seed.

- Poor key choices e.g use of mutations of dictionary strings

Attack on transmission

- ➡ Good key transmission algorithms include some form of error detection
- ➡ Nonces, certificate authorities and web of Trust can be leveraged to ensure integrity and ownership of transmitted keys

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