

Cryptography

Conclusions

Kc Udonsi

Compression vs Encoding vs Encryption

- ➔ Compression is a potentially reversible operation to reduce the size of data. It may leverage an encoding which uses less bits to store data. It should not be used to secure data by itself. E.g zip, tar, zip, gzip etc
- ➔ Encoding is the reversible representation of data e.g base64, UTF-8, UTF-16 etc
- ➔ Encryption is the concealing of data using a cryptographic algorithm and a secret value (the “Key”)

Security through Obscurity

- ➔ Not advised for cryptographic algorithms but ...
- ➔ Can be deployed (intelligently) in addition to other security measures to further mitigate a threat
- ➔ Non-linear key space (some keys are more secure than others) + secret algorithms can be used to weaken encryption for unauthorized users of a cryptographic system

Common implementation pitfalls

- ➔ DO NOT re-invent the wheel “Roll your own cryptography”
- ➔ USE well maintained cryptography libraries and adhere to any and all documentation warnings
- ➔ DO NOT use known weak/broken cryptographic algorithms
- ➔ USE cryptographically secure randomness for the generation of nonces, IV etc
- ➔ DO NOT re-use nonces, IV etc. Cryptographic algorithms rely on some principles to be effective. DO NOT compromise the principles
- ➔ DO NOT hard-code cryptographic keys
- ➔ ENSURE the encryption strength in use is sufficient for the data protected
- ➔ Exercise caution when using time as a variable for cryptographic computation