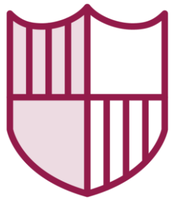
Reviewing Key Countermeasures

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Defending Cryptographic Attacks



Secure cryptographic keys

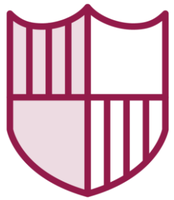
Utilize IDS to monitor access and key exchanges

Encrypt keys with passphrases and passwords

Don’t embed keys inside of the source code or binaries

Defending Cryptographic Attacks

Do not allow the transfer of private keys for certificate signing



Symmetric algorithms should utilize a key size of 168 bits or 256 bits

Ensure message authentication is implemented for the encryption of symmetric-key protocols

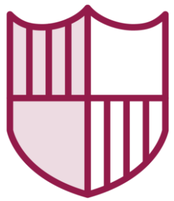
Utilize a key size of 1536 bits or 2048 bits for asymmetric algorithms

Defending Cryptographic Attacks

Consider a key size of 168 or 256 bits for hash algorithms

Utilize recommended tools and products

Limit the number of operations per key



All hash functions should utilize the largest bit length possible

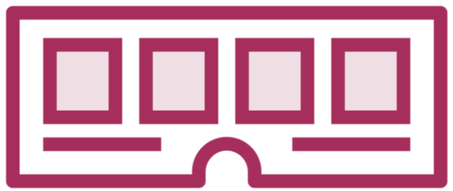
Key Stretching

A technique used in cryptography to make a password, passphrase, or other secret data more resistant to dictionary attacks by adding computational work.

Key stretching reduces the effectiveness of brute-force attacks

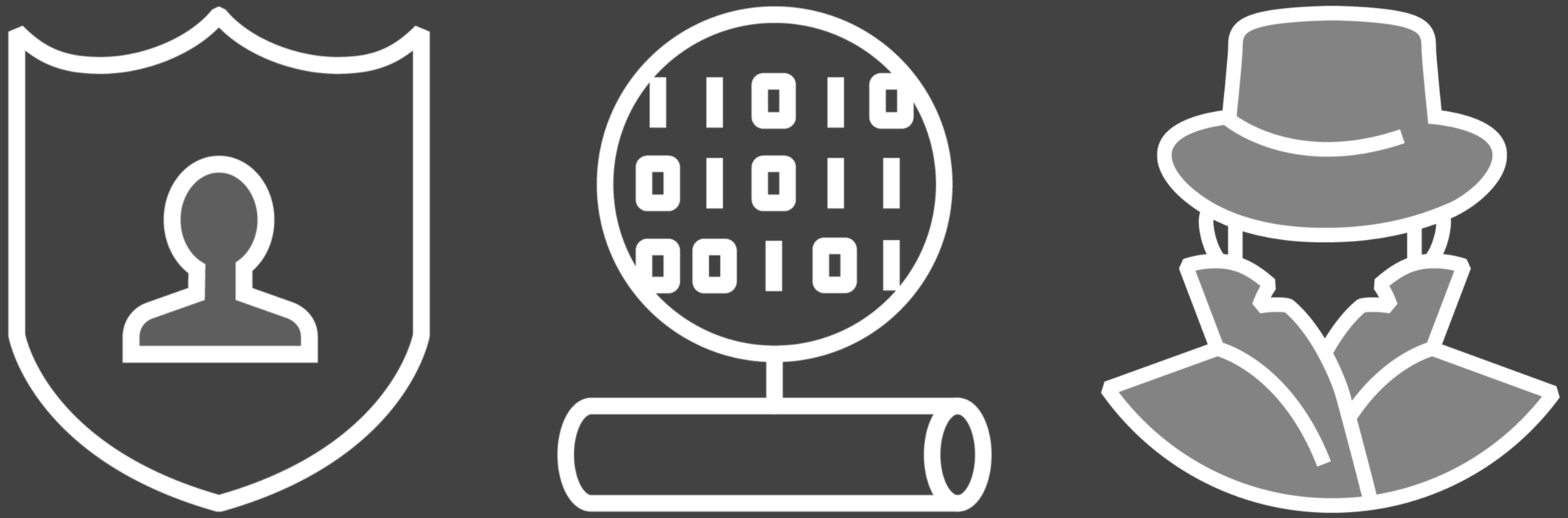
Considerations

The time it takes to stretch the key



The amount of memory required

The level of security provided

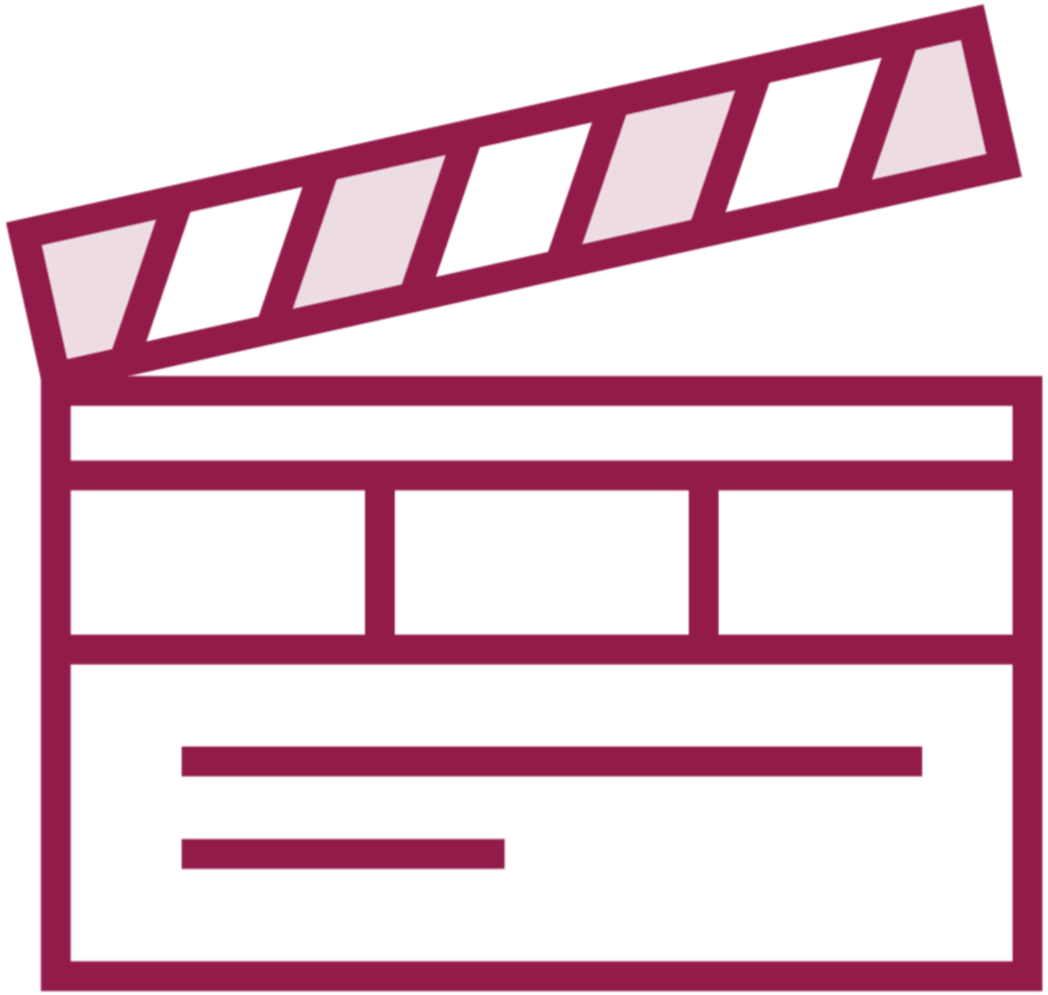


A security professional's job isn't to stop attackers, it's to slow them down or discourage them.

Learning Check

Learning Check

- Use passphrases and passwords
- Don’t store keys in binaries
- Highest bit count possible
- Key stretching
- Slow them down!



Ethical Hacking Series