Meet-in-the-Middle Attack

Return to Glossary

Meet-in-the-Middle Attack is a known-plaintext attack that can greatly reduce the number of brute-force permutations required to decrypt text that has been encrypted by more than one key. Such an attack makes it much easier for an intruder to gain access to data.

A meet-in-the-middle attack targets block cipher cryptographic functions. The intruder applies brute-force techniques to both the plaintext, which is ordinary text before it is encrypted, and the ciphertext, or encrypted text that has been transformed from plaintext, of a block cipher.

The intruder then attempts to encrypt the plaintext according to various keys to achieve an intermediate ciphertext, or text that has only been encrypted by one key. Simultaneously, the intruder attempts to decrypt the ciphertext according to various keys, seeking a block of intermediate ciphertext that is the same as the one created by encrypting the plaintext. If there is a match of intermediate ciphertext, it is highly probable that the key used to encrypt the plaintext and the key used to decrypt the ciphertext are the two encryption keys used for the block cipher.

The name for this exploit comes from the method: Because the intruder tries to break the two-part encryption method from both sides simultaneously, a successful effort enables the intruder to “meet in the middle” of the block cipher.

Source: https://internetofthingsagenda.techtarget.com/definition/meet-in-the-middle-attack