Christopher Morgan

CS465: Security

Sep 25, 2013

Diffie-Hellman

1. **Describe the Diffie-Hellman protocol.**

The Diffie-Hellman protocol is a sequence of steps that allow two individuals to establish a shared key (call it K) for private communication over an insecure medium. No passive eves dropper will be able to obtain the key or derive it. It works by having two parties (call them Alice and Bob):

1. Select a pair of numbers (call them p and g). P is a large prime number and g is a primitive root mod p.
2. Have both Alice and Bob generate private keys for themselves (call Alice’s a and Bob’s b). a and b are both large prime numbers.
3. Have both Alice and Bob generate public keys to share with each other (call Alice’s A and Bob’s B). This is done with the following equations:
   1. A = (mod p)
   2. B = (mod p)
4. Alice and Bob exchange A and B.
5. Now both Alice and Bob generate their shared secret key (called K).
   1. Alice does the following: K = (mod p)
   2. Bob does the following: K = (mod p)
6. Alice and Bob now have a shared secret key to use for encryption.
7. **Show how Mallory can conduct a man-in-the-middle attack when Alice and Bob conduct the DH protocol from question #1.**

Mallory conducts a man-in-the-middle attack by setting up two private keys one with Alice (call it Ka) and one with Bob (call it Kb). She then lets Alice and Bob believe they are just talking to each other. The exchange would happen something like the following:

1. Alice and Bob would follow the steps described in #1 up to step 3.
2. Mallory would intercept the exchange of p and g. She would then follow step 2 from problem #1 to generate two private keys intended for Alice and Bob (call them ma and mb).
3. Mallory would then generate two public keys intended for both Alice and Bob (call them Ma and Mb). She would do something like the following:
   1. Ma = (mod p)
   2. Mb = (mod p)
4. Mallory would then exchange public keys with both Alice and Bob. Bob would receive Mb. Alice would receive Ma. Mallory would receive A and B as described in problem #1.
5. Mallory, Alice, and Bob would then generate their shared keys.
   1. Alice, Ka = (mod p)
   2. Bob, Kb = (mod p)
   3. Mallory to Alice, Ka = (mod p)
   4. Mallory to Bob, Kb = (mod p)
6. Alice and Bob now have a secret key that they think is for each other, when really Mallory is sitting in the middle sharing a key with each one of them. This allows Mallory to fool Alice and Bob into thinking they are talking securely but they really are only securely talking to her.
7. **What is the recommended key size for p?**

512 bit prime

http://mathworld.wolfram.com/Diffie-HellmanProtocol.html

1024 bit prime

<http://crypto.stackexchange.com/questions/1963/how-large-should-a-diffie-hellman-p-be>

1. **Why is the recommended size for p for DH so much larger than the recommended key size for AES?**

The reason is because the size of the key for AES is not the sole point that makes it secure. AES performs key extensions, swaps columns, and other such denaturing activities in order to encrypt data. The key is a single ingredient to get the bit mixing going. A small key in AES just simply makes the key easier to guess.

However, with DH its entire security relies on the fact that given A = (mod p) you cannot regenerate ‘?’. Therefore, if p is small or g the entire security of DH fails. In other words, the security of DH comes from P and g being large enough that it is computationally infeasible to compute ‘?’. P must be large so that all the possibilities for ‘?’ are impossible to compute. It is for this reason that DH relies on the large size of p, where as AES doesn’t directly.