Lab 3 :: Key Exchange and Breaking DES

Luke Anderson *luke@lukeanderson.com.au*

28 & 31 March 2017

1 Breaking DES

The key space of DES is 2^{56}. If a secret key k was selected purely at random from the keyspace, an adversary would have to attempt 2^{55} possible keys (half the key space) before encountering the correct key.

1.1 Questions

Imagine you were performing a chosen-plaintext attack on DES. Is there a property of DES that would allow you to reduce your work by a factor of 2 (i.e. to 2^{54})?[1]

DESX is an improvement on the strength of normal DES by adding two extra keys, $DESX(m) = k_3 \oplus E_{k1}(m \oplus k_2)$. Imagine we created DES$\frac{X}{2}$ (or DES Half X) by instead computing $E(m) = k_3 \oplus E_{k1}(m)$. How would you go about breaking this cypher, assuming you have two plaintext-cyphertext pairs. Thus, how much stronger is DES$\frac{X}{2}$ compared to normal DES? Why does the whitening key added to DESX (i.e. $m \oplus k_2$) prevent the the attack we used on DES$\frac{X}{2}$?

2 Merkle's Puzzles

Merkle's Puzzles is a conceptually simple public-key cryptosystem. Alice, wanting to speak securely to Bob, generates m boxes and sends them to Bob. Each box is encrypted using an easily broken cypher (for some definition of "easily") and contains the box number b_i and a stronger shared secret k.

[1] If you're stuck, see Chapter 7.4.3 of the *Handbook of Applied Cryptography*

Bob selects a box at random, breaks it, and sends the previously secret box number b_i back to Alice. Alice and Bob now have a shared secret k.

To retrieve their shared secret, Bob only needs to open a single box. Our eavesdropping attacker Eve however would statistically need to open $\frac{m}{2}$ boxes before finding box b_i.

Attached to this lab is the source code for a minimal Merkle Puzzle system. For each of the puzzles, a key and the box number are encrypted using a simple DES cypher. Note the speed at which a large number of puzzles may be generated and how slow it can be to break each of these boxes. The latter can be seen by increasing or decreasing the key complexity.

2.1 Questions

In the minimal Merkle Puzzle system example above, a symmetric cypher (DES) is used to “secure” the puzzle. Can a puzzle be secured using a Hash-based Message Authentication Codes (HMAC)? If so, how so? If not, why not?

We have only considered an eavesdropping attacker Eve so far. Mallory, as oposed to Eve, can modify messages and even create her own. Does Merkle's Puzzles by itself defend against Mallory in any way? Why not?

3 Diffie-Hellman key exchange

Ensure you understand the steps for the Diffie-Hellman key exchange, particularly which variables become public and which remain private. A reduced version is given below but refer to Wikipedia[2] or the *Handbook of Applied Cryptography* for more details.

$A \rightarrow B : \alpha,\ p,\ \alpha^a \bmod p$
$B \rightarrow A : \alpha^b \bmod p$
Shared secret $s = (\alpha^a \bmod p)^b \bmod p = (\alpha^b \bmod p)^a \bmod p$
Shared key $= hash(s)$

[2] See http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange