Matthew Johnston
MSc. Computer Science (Networks and Distributed Systems)

Probabilistic Post-Facto Detection of Man-in-the-Middle Attacks on Unauthenticated Diffie-Hellman

Supervisor: Dr Stephen Farrell
2014

This dissertation details a prototype protocol for exposing a man-in-the-middle attacker on Diffie-Hellman key exchanges at a scale where out-of-band verification of matching shared secrets is infeasible. This verification is accomplished by creating a hash value of the shared secrets as seen at each end point and comparing the outputs, where a mismatch in hash values indicates a potential man-in-the-middle. The exchange that each hash value must be able to be identified without divulging the actual identities of the participants.

Two systems for this are created and evaluated, each using a different method of identifying the exchanges in an online database and analysing the results of comparing hash values. One version uses random integers as part of the identifier, where the count of random value choice collision for matching hashes can be compared with the expected count based on the size of the random range. The second has servers create a UUID to record batches of DH exchanges and later compares this local log with the online version, which includes client versions of the exchange.

The random session version works well in the case where a number of participants provide information, offsetting the inaccuracy of the random numbers. While choice of the range and number of exchanges under a particular range is up to a human operator to decide, little modification is required to the underlying protocol.

The UUID version works with fewer participants, though requires more involvement of the human operators and some modifications to the underlying protocol.