Merkle's Puzzles
The first of many

Sivert Johan Solem
Department of Telematics
sivertso@stud.ntnu.no
May 4, 2014

Introduction

Communicating. It's one of the base needs of society, and it has been for millenia. For an almost equal amount of time, people have wished to communicate without others being able to eavesdrop. From this was born cryptography. In the beginning, cryptography relied on secrets shared over secure channels, codebooks surrounded by diverse security measures, and the complete failure of a system once the secret has been discovered by a malicious third party.

Until the middle of 1970, that is. That was when public-key cryptography was in it's infancy, and when Ralph C. Merkle published his article Secure Communications Over Insecure Channels [3]. In this essay, we will examine the system described by Merkle, and comment on the changes in cryptography after the paper's release.

The Key Exchange system

Merkle's puzzles are one of the first described systems that allows for secure communication and authentication services over insecure channels. Systems such as these have the additional benefit that if communication has been compromised, it is relatively easy to change the keys and thereby secure the communications again.

Merkle's system works as follows; Alice wants to communicate securely with Bob. The channel they can communicate on is insecure, so they need to secure it. To secure the channel, they will need to agree on a key. Alice then creates many keys and encrypts all of them separately, together with a key ID and a constant. The keys are not very securely encrypted, so that when she transfers all the chiphertexts to Bob, he can select one at random and brute-force it in a relatively short amount of time. When he has decrypted one of the chiphertexts, he sends the key ID back to Alice, and all following communication will be encrypted with the referenced key. These chiphertexts are what is known as Merkle's puzzles.

Notice how both the chiphertexts and the selected key ID has been transmitted plaintext. This means that a malicious party, Eve, in theory knows all she needs to know to eavesdrop on Alice and Bob. The problem for Eve is that the puzzles are not in order, so knowing the key ID does not tell her which puzzle to solve, though she will recognize the correct one when she finds it. Assuming there are m puzzles and each puzzle takes $O(n)$ time to solve, Eve will on average need to solve $m/2$ puzzles to break the cipher. This results in the whole problem being of size $O(n^2)$, assuming $n \sim m$.

Authentication

Authentication is also a feature of the puzzles, though it requires a trusted third party having a lookup between users and their set of puzzles. This assumes that only Alice knows the answer to all of Alice's puzzles, and is therefore the only user that can reply to communications encrypted with the key from a randomly chosen puzzle. The verification is then checking the puzzle set Alice sent Bob against the set marked Alice at the Trusted Third Party. If they are identical, Bob knows that Alice is who she reports to be. Likewise, for Alice to verify that she is talking to Bob, they perform the same procedure with Bob's puzzles. After ended comminucations, it may be advised to remove the used puzzles from the puzzle sets.

In this authentication scheme, it is important that users change out their puzzles regularly, and probably with a seperate authentication scheme against the authentication provider. With such an authentication server, it is reasonable to assume that Eve has aquired the puzzles to her intended marks as soon as she can. If the puzzles are not changed, Eve may be able to solve enough of them to succesfully impersonate the owner.

Legacy

When people look to early key exchange protocols, the Diffie-Hellman key exchange protocol is the one that is usually referenced. With good reason, as well, since their paper was published first.[1, 1976] Merkle did start his work, and would have been published first, if the Commun. ACM had not rejected his paper on the grounds that it was simply not how cryptography was done, and there were no references to established literature. [2] Despite Merkle's paper being published after Diffie and Hellman's, Hellman has on several occasions credited Merkle with the concept of public-key cryptography, and he refers to the Diffie-Hellman protocol as the Diffie-Hellman-Merkle key exchange protocol.[5]

In 1997 it was revealed that Merkle was not the first father of public-key cryptography, as the British GCHQ had the idea of public-key cryptography already in 1969, and developed it into a functioning system in 1972.[4]

Systems based around the concept of public-key cryptography are now prevalent in the cryptographic community, though symmetric cryptography is generally faster. The result is that high-throughput services use a public-key encryption to exchange keys for use in the symmetric encryption of the data.

References

1. W. Diffie and M.E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

2. Ralph C. Merkle. Publishing a new idea.

3. Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, April 1978.

4. Simon Singh. Unsung Heroes of Cryptography.

5. Jeffery R. Yost. An interview with Martin Hellman, November 2004.