Dissent: Accountable Anonymous Group Messaging

Erratum 2

Andrew Wiedemann, Doug von Kohorn, Henry Corrigan-Gibbs, Bryan Ford

Introduction

Dissent [2] is a protocol for sender-anonymous group-wise broadcast, which builds on an anonymous data collection protocol by Brickell and Shmatikov [1]. Since publication of Dissent, we previously discovered an attack on the underlying Brickell-Shmatikov protocol utilized by Dissent described in an erratum [3]. However, there is an additional attack, the "file descriptor replay," which directly targets Dissent and not its underlying protocols. The file descriptor replay attack is easier to perpetrate than the attack on Brickell-Shmatikov and the attacker remains anonymous. The attack may be prevented by requiring group members to generate fresh primary encryption/decryption keypairs before every protocol round. Protecting Dissent from the file descriptor replay also provides protection from the previously described attack. For other applications utilizing the Brickell-Shmatikov protocol, consult the first erratum [3] for related security information.

File Descriptor Replay

This is an attack against Dissent's [2] file descriptors.

After at least one protocol round has been successfully completed, an adversary can misbehave in subsequent protocol rounds so as to break the anonymity of the messages sent in the first (successfully completed) round. The adversary can be located anywhere in the ordering of the participants. Mounting the attack requires that: (1) all participants reuse their primary (long-term) encryption keypairs over many protocol rounds, and (2) the attackers participate in at least two such protocol rounds with the same participants.

Attack Summary

For every round of Dissent, all participating members must generate a file descriptor containing an encrypted seed and unencrypted hash value for every member in the clique. Each member i chooses a random seed s_{ij} for each member j, and for each $j \neq i$, generates L_i pseudo-random bits from s_{ij} to obtain ciphertext C_{ij}:

$$C_{ij} = \mathrm{PRNG}\{L_i, s_{ij}\} \ (j \neq i)$$

Member i now XORs her message m_i with each C_{ij} for $j \neq i$ to obtain ciphertext C_{ii}:

$$C_{ii} = C_{i1} \oplus \ldots \oplus C_{i(i-1)} \oplus m_i \oplus C_{i(i+1)} \oplus \ldots \oplus C_{iN} \ \ (j = i)$$

Member i then computes hashes $H_{ij} = \mathrm{HASH}\{C_{ij}\}$, encrypts each seed s_{ij} with j's public key to form $S_{ij} = \{s_{ij}\}_{yj}$, and collects the H_{ij} and S_{ij} for each j into vectors. It is important to note that the file descriptor which member i created has exactly one mismatched seed-hash pair; namely the seed-hash values for i.

$$C_{ii} \neq \mathrm{PRNG}\{L_i, s_{ii}\}$$

Therefore, if an attacker replays a file descriptor from a previous honest round the creator of the file descriptor will not be able to generate C_{ii}. Because member *i* will not be able to broadcast a valid C_{ii} such that HASH{C_{ii}} = H_{ii}, the member *i* who initially generated the initial file descriptor will be revealed.

Implications for Dissent

This attack is particularly dangerous for the Dissent protocol because the misbehaving node does not require any escalated privileges (such as ring location) and remains anonymous during the attack. The attacker can perpetrate this from any ring location because the act only requires that he submits a particular file descriptor. The attacker is able to remain anonymous because of the anonymity provided by the Brickell-Shmatikov protocol.

Prevention

Group members can prevent this attack by generating new primary encryption keypairs for every round of the protocol. By using unique keypairs for every round, no member will be able to decrypt their designated seed to produce a valid ciphertext for file descriptors replayed from previous rounds. This will also prevent the category of replay attacks described in the initial erratum.

References

[1] Justin Brickell and Vitaly Shmatikov. Efficient anonymity-preserving data collection. In 12th KDD, August 2006.

[2] Henry Corrigan-Gibbs and Bryan Ford. Dissent: accountable anonymous group messaging. In CCS, pages 340 350, October 2010.

[3] Henry Corrigan-Gibbs and Bryan Ford. Dissent: Erratum.