A. Wussler

OpenPGP Email Forwarding Via Diverted ECDH Key Exchanges

IETF 114
2022-07-29

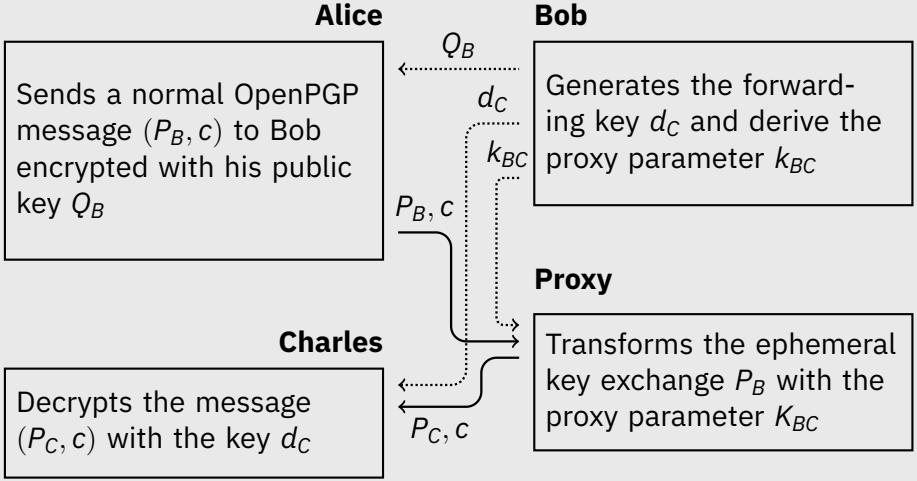
Outline

- Automatic e-mail forwarding
- Diverting the secret
- OpenPGP implementation
- Threat model
- Conclusions, Q&A

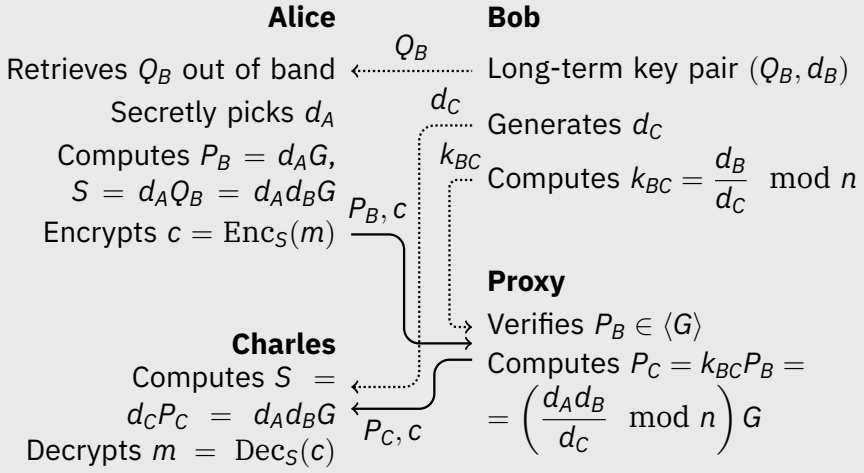
Automatic E-Mail Forwarding

- Proxy re-encryption: Ciphertext transformation so that it can be decrypted by a different party than was originally intended.
- Transformation is carried out without access to decryption secrets, plaintexts, or interactive communication with secret-key holders[5].
- Used in ElGamal-encrypted mailing list[6], proposed for use in redirection[3, 1, 2].
- We propose it for automatic OpenPGP email forwarding using ECDH.

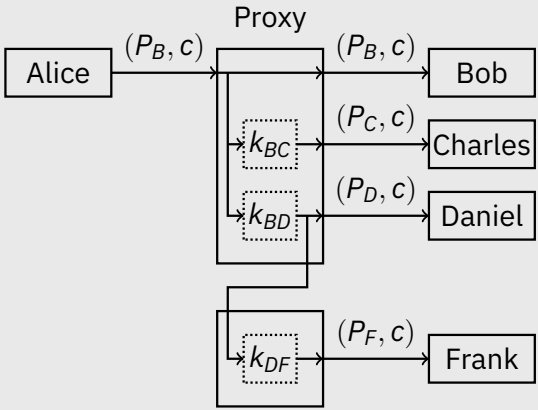
Diverting the secret (I)



Diverting the secret (II)



Forwarding schema



OpenPGP implementation

Alice	It is transparent to the sender, that might not support the feature and should not know a forwarding happens.
Bob	It requires only a one-time set-up from the original recipient, that does not require to be online.
Server	The server, has only one curve multiplication to perform in constant time.
Charles	**Requires a modifications when deriving the symmetric key from the ephemeral secret[7] using a modified version of the KDF for the forwarded recipient.**

It has been implemented in OpenPGP.js and GopenPGP.

OpenPGP changes

In the computation of the shared secret the following KDF is used[7]:

```
MB = Hash( 00 || 00 || 00 || 01 || ZB || Param );
```

- The recipient key fingerprint is used as channel binding information.
- Channel binding information is recommended[4] for security.
- Charles's implementation needs to know the original recipient fingerprint when decrypting:
  - Adding the fingerprint to the PKESK. This makes the messages distinguishable.
  - Adding the fingerprint to the forwardee key. This ensures the key can only be used for forwarded messages and is accepted once when the forwarding is set up.

Threat model

We assume the original recipient (Bob) is always honest, since his objective is to protect his key and his e-mails.

- If any set of forwarded parties colludes (and is able to submit messages to the proxy) they are still left with an instance of the ECDH.
- If the proxy and any forwarded party collude it is possible to recover Bob's private key:

$$d_i k_i = d_i d_i^{-1} d_B = d_B \mod n.$$

  This is partially mitigated from OpenPGP's key usage flags.

A simulation proof is included in the paper.

Conclusions

- The protocol is compatible on the sending side with all ECC-enabled OpenPGP implementations.
- The protocol is non-interactive, Bob can generate all parameters without any further exchange.
- It is possible to deploy this for a single provider for internal forwarding, with a high practical impact.
- The trust is distributed: the secret key is shared between the server and the forwarded party, both can’t recover the key alone.
- We considered the use of Curve25519 because it is practical to implement in constant time, fast, and well-regarded in the community.

References

Full paper can be accessed at: `https://www.wussler.it/ECDHForwarding.pdf`

[1] Aono, Y., Boyen, X., Phong, L.T., Wang, L.: Key-private proxy re-encryption under lwe. In: Proceedings of the 14th International Conference on Progress in Cryptology INDOCRYPT 2013 - Volume 8250. pp. 1–18. Springer-Verlag, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-319-03515-4_1

[2] Ateniese, G., Benson, K., Hohenberger, S.: Key-private proxy re-encryption. In: Fischlin, M. (ed.) Topics in Cryptology – CT-RSA 2009. pp. 279–294. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

[3] Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. **9**(1), 1–30 (Feb 2006). https://doi.org/10.1145/1127345.1127346, `https://doi.org/10.1145/1127345.1127346`

[4] Barker, E., Chen, L., Roginsky, A., Vassilev, A., Davis, R.: Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Tech. rep., NIST (April 2018), `https://doi.org/10.6028/NIST.SP.800-56Ar3`

[5] Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding. Lecture Notes in Computer Science, vol. 1403, pp. 127–144. Springer (1998). https://doi.org/10.1007/BFb0054122

[6] Khurana, H., Heo, J., Pant, M.: From proxy encryption primitives to a deployable secure-mailing-list solution. In: Ning, P., Qing, S., Li, N. (eds.) Information and Communications Security. pp. 260–281. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)

[7] Koch, W., Wouters, P., Huigens, D., Winter, J., Yutaka, N.: Openpgp message format. RFC draft-ietf-openpgp-crypto-refresh-06, RFC Editor (Jun 2022), `https://datatracker.ietf.org/doc/draft-ietf-openpgp-crypto-refresh/06/`

Q & A