A Hybrid Encryption Technique Supporting Expressive Policies

Stefan G. Weber
Center for Advanced Security Research Darmstadt (CASED)
Mornewegstrasse 32, 64293 Darmstadt, Germany
stefan.weber@cased.de

We sketch a novel hybrid encryption technique that supports expressive policies. It is hybrid, as it combines ciphertext-policy attribute-based encryption (CP-ABE) [BSW07] with location-based encryption (LBE) [SD03] on the level of symmetric keys. It enables encryption under expressive policies, since it can efficiently handle attributes with continuous values, like location.

We use the following notation: $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$. Hereby, $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Finally, $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$. Decryption succeeds if R's attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. It employs a *location lock mapping* $f_{LL}(L^{(P_1,P_2})$, according to the following principle: first, GPS coordinates P_1, P_2 are concatenated. Second, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a 128 bit string (assuming 128 bit symmetric keys), the location lock value. Our *hybrid encryption scheme* works as follows: first, a random session key Key_S is generated. Second, the message is symmetrically encrypted under Key_S, producing ciphertext CT_1. Third, Key_S is XORed with the location lock value, generating a hybrid key Key_H. Fourth, the output is concatenated with an encoding of the location area. Fifth, the resulting string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2. CT_1 concatenated with CT_2 form the ciphertext CT. Then, CT is transferred to a receiver R. The *scheme for hydrid decryption* works as follows: first, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. Second, on successful decryption, the location area $s_{LL^{(P_1,P_2)}}$ is extracted. Third, R's current GPS position P_R is verified to be inside the location area by means of a tamper-resistant GPS receiver. On success, the location lock value can be computed. It is then XORed with the recovered Key_H, in order to reconstruct Key_S. Finally, Key_S is used to symmetrically decrypt CT_1 to M.

We are currently working on applications of this technique in the areas of *end-to-end secure attribute-based messaging* [Web09, BPW10, WRM10, WKRM11] and *identity and access management* [WMRM10].

References

[BSW07] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (SP '07). pp. 321–334. IEEE CS (2007)

[SD03] Scott, L., Denning, D.E.: A Location Based Encryption Technique and Some of Its Applications. In: ION National Technical Meeting 2003. pp. 730–740 (2003)

[Web09] Weber, S.G.: Securing First Response Coordination with Dynamic Attribute-Based Encryption. In: Conference on Privacy, Security and Trust (PST 2009) / (CONGRESS 2009), pp. 58-69. IEEE CS (2009)

[WRM10] Weber, S.G., Ries, S., Mühlhäuser, M.: Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging. Telecooperation Report No. TR-13, ISSN 1864-0516 (2010)

[WMRM10] Weber, S.G., Martucci, L.A., Ries, S., Mühlhäuser, M.: Towards Trustworthy Identity and Access Management for the Future Internet. In: The 4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS 2010)

[BPW10] Brucker, A.D., Petritsch, H., Weber, S.G.: Attribute-Based Encryption with Break-Glass. In: Workshop on Information Security Theory and Practice (WISTP 2010). Springer (2010)

[WKRM11] Weber, S.G., Kalev, Y., Ries, S., Mühlhäuser, M.: MundoMessage: Enabling Trustworthy Ubiquitous Emergency Communication. In: ACM International Conference on Ubiquitous Information Management and Communication 2011 (ACM ICUIMC 2011). ACM Press (2011)