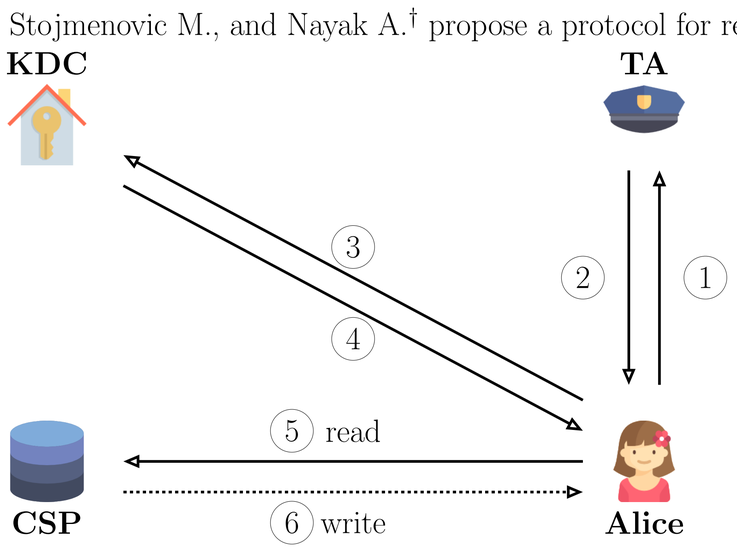
Formal Analyze of a Private Access Control Protocol to a Cloud Storage*

Mouhebeddine Berrima[1], Pascal Lafourcade[2],
Matthieu Giraud[2], and Narjes Ben Rajeb[3].

[1] Université de Monastir, [2] Université Clermont Auvergne, [3] Université Tunis El-Manar.

RSN'12 Protocol Description

Ruj S., Stojmenovic M., and Nayak A.† propose a protocol for reading and writing data stored in the cloud that we call RSN'12.



1. Alice presents her identity to a Trust Authority (TA) ;
2. The TA registers Alice if she is eligible and gives her a token ;
3. Alice presents the token to the Key Distribution Center (KDC) ;
4. The KDC checks the validity of the token using TA's public key, and sends the corresponding keys for signing and decryption to Alice ;
5. Then, Alice can read the files stored on the Cloud Service Provider (CSP) ;
6. If Alice has the right, she can also write files on the CSP.

Security Properties

Confidentiality A secret stored message written by an honest writer is not deducible by an attacker without attribute secret ;

Authentication The signature of a writer is valid only if the attribute secret key comes from KDC, and only if the token to generate the attribute secret key comes from the TA ;

Anonymity An adversary cannot distinguish whether a message comes from Alice or Bob ;

Unlinkability An adversary cannot distinguish the situation in which Alice stores a message m_1 and Bob stores a message m_2 from the situation in which Alice stores m_2 and Bob stores m_1.

Security Analysis

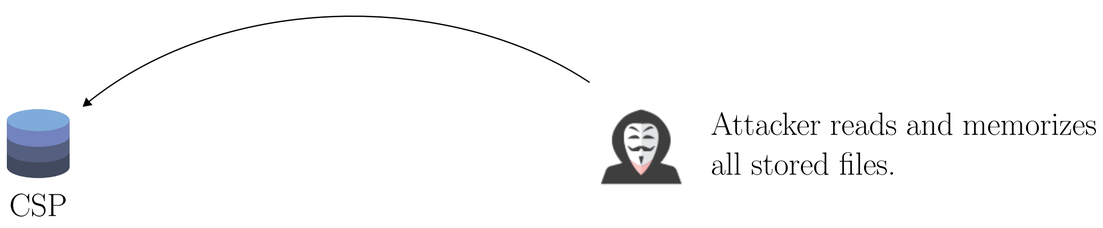
Using ProVerif‡:

Properties	*Validity*
Confidentiality	✓
Authentication	✓
Anonymity	✓
Unlinkability	✗

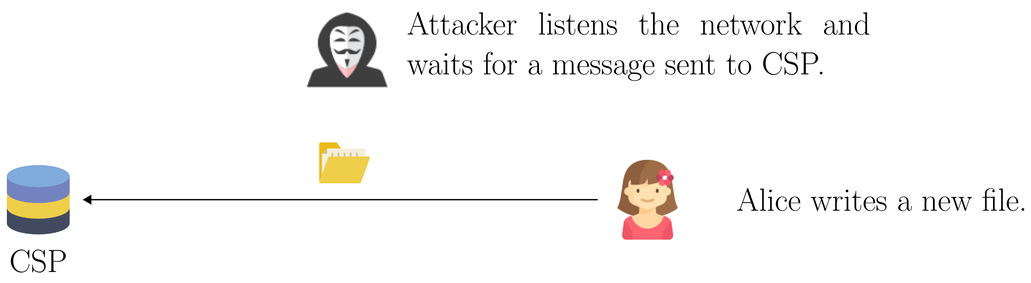
The attacker is a semi-honest reader with valid attribute secret keys, who wants to link the messages to a writer.

Attack on the Unlinkability

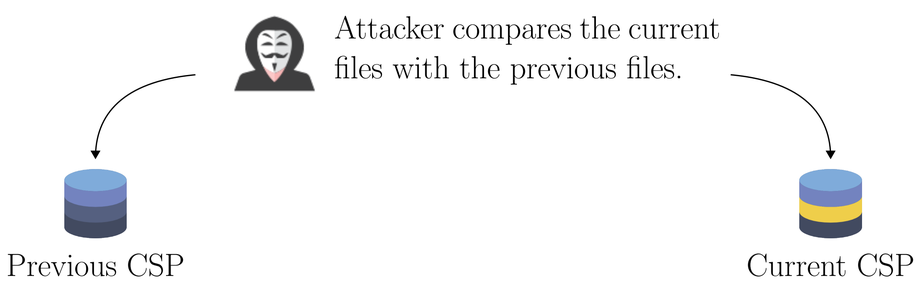
Step 1



Step 2



Step 3



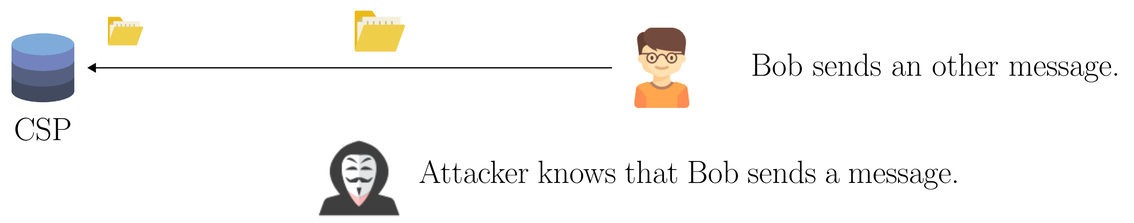
Then, the attacker deduces which file was sent by Alice.

Fixed Protocol

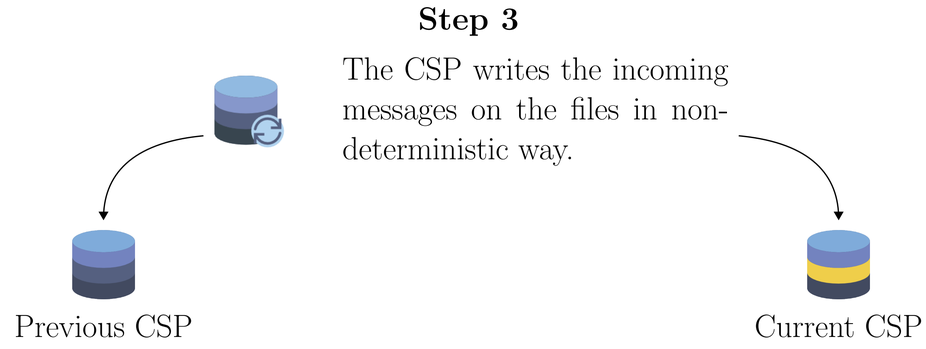
Step 1

The CSP waits for an other writer sends a message before store the Alice's message.

Step 2



Step 3



Then, the attacker cannot link messages and writers.

Acknowledgements

* This research was conducted with the support of the FEDER program of 2014-2020, the region council of Auvergne-Rhône-Alpes, the Indo-French Centre for the Promotion of Advanced Research (IFCPAR) and the Center Franco-Indien Pour La Promotion De La Recherche Avancée (CEFIPRA) through the project DST/CNRS 2015-03 under DST-INRIA-CNRS Targeted Programme.

References

† Ruj, S., Stojmenovic, M., and Nayak, A. (2012). Privacy preserving access control with authentication for securing data in clouds. In Cluster, Cloud and Grid Computing, 12th IEEE/ACM International Symposium on, pages 556–563.

‡ Blanchet, B. and Smyth, B. (2016). Automated reasoning for equivalences in the applied pi calculus with barriers. In CSF'16, pages 310–324.