Review of group 9 report on Privacy Enhanced Access Control

Applied Cryptography

November 30, 2015

Troels Thomsen 152165
Rasmus Haarslev 152175
Vilius Maskovas 107154
Justas Mikalajunas 107083

1 Outcome

The report successfully compared two established systems (IdeMix and U-Prove) implementing privacy enhanced access control enabling the reader to make an informed decision on whether to use either system for the user's own use case, and which system would fit best for the use case of avoiding grading bias on DTU campusnet assignments hand-ins.

2 Scope

While the report explains the two systems well and how they could be implemented on campusnet to avoid grading bias, the report does not contain any new system or technology of the authors' own invention. While this was not strictly a requirement for the presented solution, we would have liked to see some level of ingenuity in the solution. The report even mentions that *"A more simple token based system based on protocols like Kerberos [18] could have been developed, but since we found no studies with experience using such an approach, we have not considered it further."* and in our view it could have been very interesting to see an attempt at solving the problem in this way instead of analysing existing systems.

3 Protocols

The paper does not go into detail about the specification of the two protocols. Hence, it is only implicitly stated that they assume the protocols are secure. As there has been no explicit analysis of the protocols, we can assume that the paper does not take into account that they may not be secure. What is more, it does not include any assumptions about the quality of the low level implementation. This allows us to assume that the implementation contains errors. If the protocols are not secure in the specification, or the implementation, then the conclusion of the paper is false.

4 Summary

The overall report is thorough and well written. It does solve the initial problem in its own defined scope well. Some assumptions were not explicitly stated, but it can be argued that they were implicitly assumed. As mentioned in the analysis above, it would have been interesting to see some new ideas generated, but the report solves the problem.