Abstract

The first part of the thesis is a security analysis of PACE and PACE CAM protocols (Password Authenticated Connection Establishment and Password Authenticated Connection Establishment with Chip Authentication Mapping). These protocols are included in a standard adopted by International Civil Aviation Organization (ICAO). The purpose of these protocols is to aid automation of border control with biometric passports. The security analysis presented here is a follow-up work on 2019 paper "Privacy and security analysis of PACE GM protocol" by Mirosław Kutyłowski and Przemysław Kubiak with draft proofs on security of PACE. In the thesis, full versions are provided as well as they are coupled with security analysis of PACE CAM.

The security analysis is prefaced with a literature review and legal and technical context. An important part of the introduction is a European Union regulation making deployment of PACE obligatory for official personal ID cards issued in the EU. The same regulation also allows for the introduction of extensions of PACE. Two such extensions are presented in the second part of the thesis. This work was published at two major conferences: IFIP Networking 2021 as "Poster: e-ID in Europe - Password Authentication Revisited" and at ESORICS 2021 as "PACE with Mutual Authentication – Towards an Upgraded eID in Europe". Both papers are coauthored by the author of this thesis. These extensions introduce two new functionalities to PACE: Proof of Presence - undeniable cryptographic proof that a successful protocol session has occurred with a given card and Mutual Authentication – strong authentication of both parties participating in the protocol. We discuss security features and design choices for these extensions.

Wrocław, dn. 18.06.2023