Streszczenie rozprawy doktorskiej

Pierwszą częścią rozprawy doktorskiej jest analiza bezpieczeństwa protokołów PACE (Password Authenticated Connection Establishment) oraz PACE CAM (PACE with Chip Authentication Mapping). Protokoły te zawarte są w standardzie przyjętym przez International Civil Aviation Organization (ICAO). Ich celem jest automatyzacja procesu kontroli granicznej z użyciem paszportów biometrycznych. Analiza bezpieczeństwa przedstawiona w rozprawie to rozwinięcie pracy z 2019 roku "Privacy and Security Analysis of PACE GM Protocol" autorstwa prof. Mirosława Kutyłowskiego i dra Przemysława Kubiaka z zarysami dowodów bezpieczeństwa dla podstawowych własności protokołu PACE. W niniejszej rozprawie, przedstawiamy pełne wersje dowodów wraz z argumentacją dla protokołu PACE CAM.

Część analizy bezpieczeństwa jest poprzedzona wstępem zarysowującym kontekst prawny, technologiczny oraz zawierającym przegląd literaturowy. Istotną częścią wprowadzenia są rozporządzenia Unii Europejskiej, które obligują państwa członkowskie do implementowania protokołu PACE w warstwie elektronicznej oficjalnych dokumentów tożsamości oraz pozwalają na rozszerzenia funkcjonalności tych protokołów. Dwa takie rozszerzenia są przedstawione w drugiej części rozprawy. Są to wyniki opublikowane na dwóch czołowych konferencjach, a autor rozprawy jest jednym ze współautorów. Pierwsza praca ukazała się na konferencji IFIP Networking 2021: "Poster: eID in Europe - Password Authentication Revisited", zaś druga "PACE with Mutual Authentication – Towards an Upgraded eID in Europe" na konferencji ESORICS 2021. Rozszerzenia to, odpowiednio, PACE PoP (Proof of Presence) - rozszerzający podstawowy protokół o funkcjonalność niezaprzeczalnego dowodu że udana sesja protokołu miała miejsce z udziałem okreslonej karty oraz PACE MA (Mutual Authentication) - rozszerzająca protokół o możliwość silnego kryptograficznego uwierzytelnienia obu stron uczestniczących w protokole. W rozprawie omawiamy własności bezpieczeństwa i decyzje projektowe dla tych protokołów.

Wrocław, 19.06.2023