Secure Multi-Party Schemes for Intelligent Connected Infrastructures

Streszczenie

W niniejszej pracy analizowano wybrane aspekty bezpieczeństwa protokołów kryptograficznych mających zastosowanie w rozproszonych systemach teleinformatycznych, takich jak infrastruktura systemów transportowych. W systemach tych węzły - pojazdy oraz stacje drogowe - komunikują się za pomocą technologii krótkiego zasięgu oraz technologii komórkowych. Kryptograficzne protokoły komunikacyjne w węzłach wykonywane są na urządzeniach o ograniczonych zasobach obliczeniowymi z potencjalnie wadliwą pseudolosowością. Dlatego w badaniach uwzględniano wpływ wycieków losowości na bezpieczeństwo wykonywanych protokołów wielostronnych. Badania mają charakter teoretyczny i praktyczny: od strony teoretycznej analizowano i wzmacniano bezpieczeństwo wybranych schematów podpisów, protokołów uwierzytelniania i anonimowej wymiany komunikatów w środowiskach wielowęzłowych; od strony praktycznej badano wykonalność i wydajność proponowanych rozwiązań kryptograficznych za pomocą implementacji testowch dla wybranych urządzeń niskoenergetycznych. Formalne aspekty badań obejmują redefiniecję modeli bezpieczeństwa z uwzględnieniem adwersarzy majacych dostęp do wartości losowych, oraz analizę bezpieczeństwa w zaproponowanych modelach. Oprogramowanie testowe obejmuje wykorzystanie efektywnej biblioteki dla krzywych eliptycznych, implementujacej asymetryczne odwzorowania dwuliniowe, z funkcjonalnym interfejsem programistycznym wykonanym głównie w języku Python. W tym kontekście praca łączy elementy analizy teoretycznej z potencjalnym wdrożeniem przemysłowym i może być traktowana jak studium wykonalności zaproponowanych protokołów kryptograficznych odpornych na wycieki losowości, w wybranych węzłach infrastruktury sieci pojazdów.

Wyniki badań obejmują pięć publikacji, oznaczonych od PI do PV, w których zaproponowano wzmocnione protokoły kryptograficzne dla scenariuszy transportowych. W publikacjach PI, PII i PV analizowano pewne znane z litertury protokoły podatne na ataki z wyciekiem losowości. Dodatkowo w pracy PV przeprowadzono kryptanalizę oryginalnego protokołu, nie wymagającą wycieku losowości. W pracach tych zaproponowano ulepszenia oryginalnych protokołów oparte na technikach: przeniesienia obliczeń z kluczami tajnymi do wykładnika, podziału kluczy tajnych na składowe, oraz mechanizmach odświeżania składowych. Techniki te zostały wykorzystane w artykułach PI, PII, PIII oraz PV. W artykule PIV zaproponowano protokół zapewniający anonimowość wymiany komunikatów w środowisku wielostronnym, odporny na ataki wykorzystujące wiązania adresów infrastruktury telekomunikacyjnej. Protokół ten łączy właściwości podpisów pierścieniowych z technikami reszyfracji. Oprócz omówienia wyników z publikacji PI - PV, w rozprawie przedstawiono również rozszerzoną analizę bezpieczeństwa dla schematu z publikacji PI. Analizę wydajności wszystkich opracowanych protokołów, przeprowadzono na sprzęcie laboratoryjnym udostepnionym przez agencje Szwedzkiej Administracji Transportu.