Department of Computer Science
Faculty of Fundamental Problems of Technology
Wroclaw University of Technology

Anonymous Authentication Using Electronic Identity Documents

by

Kamil Kluczniak

A thesis submitted in partial fulfillment for the degree of Doctor of Philosophy

in the

Institute of Computer Science
Polish Academy of Sciences (IPI PAN)

Supervisor: Prof. Mirosław Kutyłowski
Co-supervisor: Dr Łukasz Krzywiecki

November 2015

Abstract

In this dissertation we consider the concept of domain signatures. This concept was recently proposed by BSI, German Federal Office for Information Security. The goal is to provide an efficient technique to sign data with regards to domain pseudonyms. The key privacy feature of domain signatures is that a user's identity within a domain is hidden behind a pseudonym and it is infeasible to link the pseudonyms of the same user in different domains. Despite of the anonymity of domain signatures, it is also required that each user in the system is certified by a relevant authority.

Domain signature is a relatively new concept and we may observe the lack of a firm background of formal definitions. Despite of some previous papers on this topic, it seems that by far no satisfactory definitions and security models have been given. To justify this claim, we give an exhaustive review on previous notions and constructions, pointing out some issues and mistakes. Then we introduce three different definitions for domain signatures which capture different cases. We propose efficient domain signature schemes which we prove secure in these models.

In the first part of the dissertation we introduce a definition for domain signatures in which domains may appear ad-hoc. This means that a user may derive domain pseudonyms and compute signatures only from his secret key and a domain specific string. We also design an efficient domain signature scheme and prove its security in our model.

In the next part of the dissertation we concern domains which are no longer virtual, but are related to an infrastructure, which provides some domain specific public keys. The idea captures the case investigated in the previous work, however, our definition seems to capture the specifics of domain signatures more closely. Then, we introduce a construction for this case which does not require on the signer's side to do "heavy" arithmetic operations, and thus it may be implemented on resource constrained devices. Therefore, our construction is more suitable for implementation on smart cards, which makes it especially useful for applications such as electronic identity documents. Then we also prove formal security of our construction in the proposed model.

In the next part of the dissertation we introduce a model for the dynamic/adaptive case where domains may appear in an ad-hoc manner. Also in this case, our definition seems to overcome some issues present in previous work, especially in case of defining the privacy properties for domain signatures. We introduce an efficient construction and prove its security in the underlying model.

All our domain signature schemes fix some problems which were present in the previous work, and in some cases even outperform them in terms of efficiency.

Streszczenie

W niniejszej rozprawie rozważamy koncepcje podpisów domenowych. Koncepcja ta została zaproponowana ostatnio przez BSI, Niemiecką Federalną Instytucję ds. Bezpieczeństwa Technik Informacyjnych. Celem podpisów domenowych jest dostarczenie efektywnej techniki podpisywania danych odnosząc się do pseudonimów domenowych. Kluczową cechą w zakresie prywatności jest to, że tożsamość użytkownika w domenie jest ukryta za pseudonimem, oraz że niemożliwe jest skorelowanie pseudonimów tego samego użytkownika w różnych domenach. Pomimo anonimowości w podpisach domenowych, wymagamy również aby każdy użytkownik w systemie był certyfikowany przez właściwy organ.

Podpis domenowy jest stosunkowo nową koncepcją i można zaobserwować brak solidnej podstawy w postaci formalnej definicji modelu. Pomimo że podpisy domenowe były już badane w poprzedniej literaturze, wydaje się, że obecne wyniki są w tej kwestii niezadowalające. Aby uzasadnić to stwierdzenie analizujemy dotychczasowe wyniki wskazując na pewne problemy i usterki. Później wprowadzamy trzy różne definicje podpisów domenowych, opisujące różne przypadki. Podajemy konstrukcje protokołów dla tych przypadków oraz udowadniamy pożądane własności bezpieczeństwa w zaproponowanych modelach.

W pierwszej części rozprawy podajemy definicje dla podpisów domenowych w których domeny mogą pojawiać się ad-hoc. Oznacza to, że użytkownik może obliczać domenowe pseudonimy i składać podpisy tylko za pomocą swego tajnego klucza i pewnego ciągu identyfikującego domenę. Podajemy również wydajny schemat podpisu, którego własności udowadniamy w naszym modelu.

W kolejnej części rozprawy rozważamy domeny, które nie są wirtualnymi bytami, ale są związane z infrastrukturą, która jest odpowiedzialna za dostarczenie publicznych parametrów domeny. Podejście to obejmuje koncepcje które były badane w dotychczasowej literaturze, natomiast nasza definicja wydaje się bliżej ujmować specyfikę podpisów domenowych. Następnie wprowadzamy schemat podpisu, który nie wymaga po stronie podpisującego wykonywania czasochłonnych arytmetycznych obliczeń, a zatem nasza konstrukcja może być realizowana na urządzeniach z ograniczonymi zasobami. Stąd nasz podpis bardziej nadaje się do wdrożenia na kartach inteligentnych, co sprawia, że rozwiązanie jest szczególnie użyteczne w aplikacjach takich jak elektroniczne dokumenty tożsamości. Również i tu poddajemy nasz podpis formalnej analizie bezpieczeństwa w zaproponowanym modelu.

W kolejnej części rozprawy wprowadzamy model dla dynamicznego/adaptywnego przypadku, w którym domeny pojawiają się ad-hoc. Również w tym przypadku, nasza

definicja wydaje się przezwyciężać niektóre problemy występujące w poprzednich schematach, zwłaszcza w przypadku definiowania właściwości prywatności podpisów domenowych. Również i tutaj podajemy konstrukcje efektywnego schematu podpisu oraz udowadniamy jego bezpieczeństwo w naszym modelu.

Wszystkie nasze schematy podpisów domenowych rozwiązują problemy, które występowały w poprzednich rozwiązaniach. W niektórych przypadkach nasze podpisy są bardziej efektywne pod względem obliczeniowym od istniejących.