SECURE AUTHENTICATION IN PRIVACY PROTECTION SYSTEMS

Lukáš Malina
Master Degree Programme (2), FEEC BUT
E-mail: xmalin15@stud.feec.vutbr.cz

Supervised by: Jan Hajný
E-mail: hajny@feec.vutbr.cz

ABSTRACT

Anonymous authentication is a mean of authorizing a user without identification. The technology provides privacy of the user and yet preserves the security of the system. Generally, Anonymous Authentication Systems (AAS) have application as electronic cash, electronic vote, group signatures etc. This paper presents an improvement to AAS, which is being developed at the FEEC BUT, and suggests how to improve the authentication phase. Specifically we propose the deployment of Perfect Zero Knowledge Protocol (PZKP), which provides greater security.

1. ÚVOD

V dnešní době se stává hlavním médiem Internet, který nabízí řadu služeb, z nichž některé z různých důvodů požadují po uživateli prokázaní oprávněnosti k přístupu. Identifikace a autentizace entit či osob z pohledu znalosti informace je pro digitální svět nejčastější a používají se tři způsoby (použití login/heslo, proces výzva-odpověď a koncept nulové znalosti). Díky různým útokům jsou první dva způsoby považovány za méně bezpečné. Nabízí se tak třetí způsob, který při vhodném použití poskytuje anonymitu uživatelům a zabraňuje neoprávněnému stopování či sledování chování uživatelů.

Systémy anonymní autentizace (**AAS**) mají za úkol chránit soukromí uživatele a přitom mu poskytnout bezpečný přístup ke službám (data, přístup a jiné aktiva), které smí uživatel oprávněně používat. Důležitou částí AAS často bývá **protokol nulové znalosti** (**ZKP**) [2], kde žadatel má za úkol přesvědčit ověřovatele o znalosti tajemství díky správnému reagování na úkoly či prokázaní matematické dovednosti bez uvolnění informací vedoucí k odhalení svého tajemství. Ověřovatel si jeho reakce uchovává a za jistých podmínek může odhalit identitu nečestných žadatelů. Ověřovatel však nemusí být vždy čestný a může uchované data zneužít, ZKP označíme jako Honest Verifier Zero Knowledge (**HVZK**). V návrhu představíme tzv. **perfektní protokol nulové znalosti** (**PZKP**), kde již nespoléháme na to, že ověřovatel je čestný, čímž se zvýší bezpečnost z pohledu žadatele.

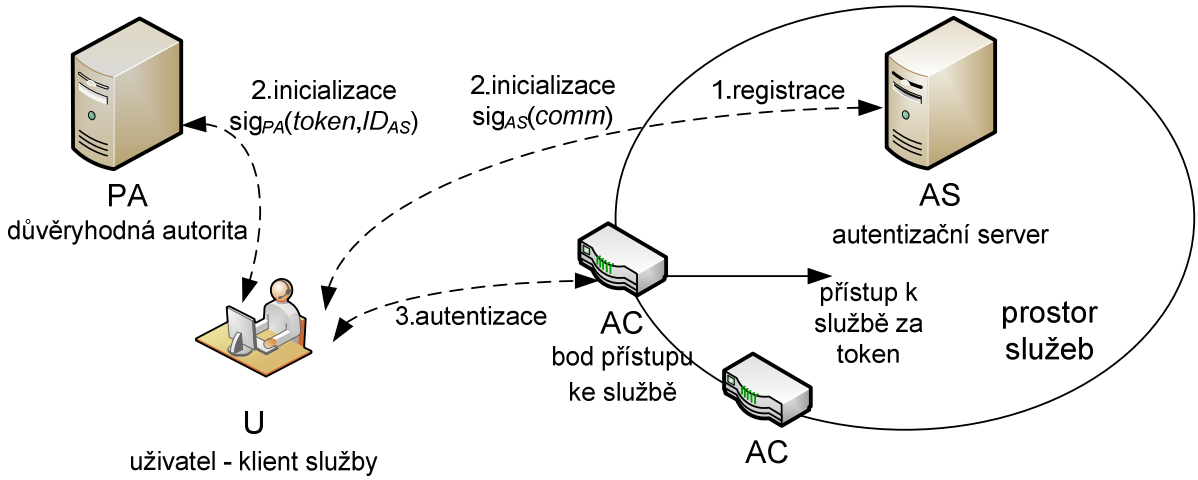
2. ANONYMNÍ AUTENTIZAČNÍ SYSTÉM

Obecně systémy AAS mohou najít uplatnění např. ve skupinových el. podpisech, elektronických platbách, různých přístupových systémech či v elektronických volbách, kde je

anonymita volícího nutností. Systémy AAS jsou konstruovány z několika bezpečnostních protokolů, ZKP, slepých podpisových schémat, závazků a jiných primitiv, vycházejících především z asymetrické kryptografie. Na fakultě FEKT VUT v Brně je vyvíjen systém Anonymous Authentication with Spread Revelation (**AASR**), který využívá problému diskrétního logaritmu (PDL) a autentizaci na bázi HVZK. Je postaven na poskytování *tokenu* sloužícího k přístupu k digitální službě. *Token* je elektronicky podepsaná digitální informace a lze ho využít pouze jednou. Při jeho řádném použití nevyzrazuje žádná data vedoucí k identifikaci jeho majitele a v rámci jisté pravděpodobnosti ho nelze padělat.

2.1. KONSTRUKCE SYSTÉMU AASR

Obrázek 1 zobrazuje strany v systému AASR: uživatel (U), autentizační server (AS), ověřovatel-přístupový bod (AC) a veřejná důvěryhodná autorita (PA). Systém před udělením přístupu pracuje ve třech fázích. Nejprve proběhne **registrace**, kde se U fyzicky zaregistruje u AS a uloží se jeho *IDu* s veřejným klíčem. Poté probíhá **inicializace** (tolikrát, kolik si uživatel zaplatí tokenů), výsledkem U získá od AS podepsaný závazek *comm* obsahující tajný klíč *w*. Vytvoří si *token* a pošle PA, která kontroluje platnost podpisu od AS, konstrukci *tokenu* a vrací U již použitelný podepsaný *token* s ID_{AS}. Pokud chce U využít chráněných služeb, musí proběhnout **autentizace** pomocí *tokenu*, která je podrobněji popsána v 2.2.



Obrázek 1: Schéma konstrukce AASR.

2.2. AUTENTIZACE S ČESTNÝM OVĚŘOVATELEM

Tato fáze používá ∑-protokol, konkrétně Schnorrův protokol pro autentizaci ZKP, více v [3]. Uživatel prokazuje znalost tajemství *w* tím, že správně odpoví pomocí *z* na výzvu *e* a AC ukládá hodnoty pro AS. Pokud nečestný U zneužije *token*, AS spolu s PA odhalí *w* vedoucí k *IDu* a jeho postihu. Zde však předpokládáme zcela čestného ověřovatele AC, kterému klient musí důvěřovat. Výhodou je efektivita (použitelné na smartcard). Následující návrh však přináší větší bezpečnost, kdy již uživatel nemusí důvěřovat ověřovateli AC, který zejména v nedůvěryhodném prostředí nemusí být vždy čestný.

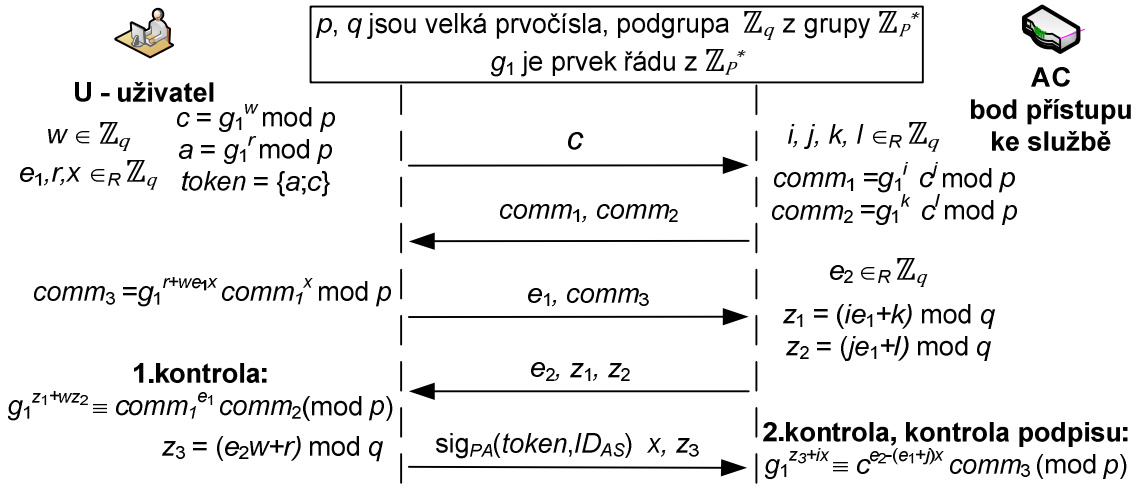
3. NÁVRH AUTENTIZACE S OVĚŘOVÁNÍM PŘÍSTUPOVÉHO BODU

Návrh s ověřováním přístupového bodu AC zanáší do fáze autentizace větší bezpečnost, jde o protokol PZKP, který vychází ze schématu v [1]. Kromě uživatele se zde prokazuje i

ověřovatel, kdy U může při špatné odezvě od AC protokol zastavit. Nicméně větší bezpečnost sebou přináší dva kroky navíc v komunikaci a více výpočetních operací.

3.1. SCHÉMA AUTENTIZACE S OBECNÝM OVĚŘOVATELEM

Komunikaci opět otevírá U, kdy pošle c. Místo náhodné výzvy odpoví AC dvěma závazky $comm_1$ a $comm_2$, ve kterých jsou svázány a skryty jeho identifikátory, které získá od AS při konstrukci systému. Uživatel použije $comm_1$ pro vytvoření vlastního závazku $comm_3$ a spolu s náhodnou výzvou e_1 zašle prvky k AC, který odpoví na výzvu e_1 reakcí z_1, z_2 a přidává výzvu e_2. Uživatel nejprve zkontroluje reakce z_1 a z_2, pokud odpovídá 1.kontrola, pak odpoví podepsaným *tokenem* s ID_{AS}, vlastní reakcí z_3 a náhodným exponentem x, díky nimž AC autentizuje uživatele (2.kontrola, kontrola podpisu). Matematický popis viz obrázek 2.



Obrázek 2: Návrh bezpečnější autentizace PZKP v AASR.

4. ZÁVĚR

Článek v úvodu představuje anonymní autentizaci a její výhody. Jako praktický příklad je uveden systém AASR a jeho konstrukce, kde je blíže popsána fáze autentizace pomocí ZKP. Jako návrh zvýšení bezpečnosti je předložena nová fáze autentizace využívající PZKP, která ověřuje uživatele a prověřuje korektní chování ověřovatele. Přínosem návrhu je, že klient již dále nemusí důvěřovat ověřovateli. Je vhodné návrh implementovat do nedůvěryhodného prostředí (Internet) a v důvěryhodném prostředí (uzavřené sítě, přístup přes smartcard) lze ponechat méně výpočetně náročnou autentizaci ZKP.

LITERATURA

[1] CRAMER, R., DAMGARD, I., MACKENZIE, P.: Efficient zero-knowledge proofs of knowledge without intractability assumptions. In *Public Key Cryptography* (2000), Springer, pp. 354–373.

[2] MICALI, S. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof symtems. *Journal of the ACM 38* (1991), 691-729.

[3] SCHNORR, C.: Efficient signature generation by smart cards. *Journal of Cryptology* (1991).