Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 9/2008 **15. září 2008**

9/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1220 registrovaných odběratelů)

Obsah : str.

Příloha: ---

A. Podzimní *Soutěž v luštění 2008*, úvodní informace

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení čtenáři, **15.10.2008** začne tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2008***. Obdobné soutěže pořádal náš e-zin v letech 2000 až 2007.

V prvních letech byly úlohy zaměřeny na klasické šifrové systémy. Od roku 2005 jsem začal doprovázet úkoly doprovodnými komentáři a nápovědami v NEWS. V roce 2006 jsem pak zařadil i vymyšlený doprovodný příběh, který úlohy volně spojoval. Jednalo se o drobné epizody ze života detektiva kapitána Cardy. Příběh vyústil v lov na chameleóna rasy Cryptomelon Pragensis. V loňském roce pak byl použit rozsáhlý doprovodný fiktivní příběh matematika Štěpána Schmidta, který se odehrával v době Marie Terezie. Příběh z 18.století byl zkombinován s fikcí, která popisovala jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře.

Loňské soutěže se zúčastnilo celkem 109 řešitelů. Všechny úlohy vyřešilo nezvykle velké množství soutěžících a to16!

Podle e-mailů, které jsem během soutěže a po ní od vás obdržel, dělají doprovodné texty soutěž pro účastníky atraktivnější, a proto i letos jsem jeden takovýto příběh připravil. Tentokrát se příběh odehrává během druhé světové války. Budete společně s britským důstojníkem Johnem Wellingtonem odhalovat záhadu nového neznámého šifrovacího zařízení a jedné důležité zprávy, která jím byla zašifrována. Ke konečnému cíli budete muset vyřešit řadu lehkých úloh a pomocí nich a simulátoru příslušného šifrátoru důležitou zprávu dešifrovat.

Chcete-li si připomenout starší úlohy a jejich řešení (což se vám může hodit i při hledání správného řešení v letošním roce), můžete je nalézt na domovské stránce našeho e-zinu v sekci věnované soutěžím: http://crypto-world.info/souteze.php .

Přesná pravidla a prvé úlohy soutěže najdete v příštím čísle našeho e-zinu Crypto-World 10/2008, který vyjde 15.10.2008. Všechny informace budou současně dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php .

Soutěž bude určena pouze registrovaným čtenářům našeho e-zinu, do soutěže bude nutné (tak jako v minulých ročnících) se zaregistrovat. Heslo k registraci bude rozesláno čtenářům Crypto-Worldu společně s kódy k jeho stažení.

Soutěžícím přeji pěknou zábavu a úspěšné projití všemi připravenými úskalími!

Ceny a sponzoři letošní souteže

1.cena

Matyáš,V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů, Masarykova univerzita, 2008
(více informací viz recenze v dnešním e-zinu na str. 14-15)
věnuje kolektiv autorů http://www.fi.muni.cz/research/laboratories/labak/
http://www.buslab.org/

P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
http://crypto-world.info/oko/index.php
věnuje autor

Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
http://www.zonerpress.cz/kniha/pro-programatory/linux-profesionalne-programovani-aplikaci
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

SOOM tričko
http://www.soom.cz/index.php?name=box&box=projects/triko/main
věnuje server Soom.cz http://www.soom.cz

2.cena
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
http://crypto-world.info/oko/index.php
věnuje autor

Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
http://www.zonerpress.cz/kniha/pro-programatory/linux-profesionalne-programovani-aplikaci
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

SOOM tričko
http://www.soom.cz/index.php?name=box&box=projects/triko/main
věnuje server Soom.cz http://www.soom.cz

3.cena
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
http://crypto-world.info/oko/index.php
věnuje autor

David Meerman Scott: Nová pravidla marketingu a PR, Zoner Press, 2008
http://www.zonerpress.cz/kniha/pro-webdesignery/nova-pravidla-marketingu-a-pr
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

Ceny pro 3 náhodně vylosované úspěšné řešitele (losuje ze všech řešitelů, kteří splní vyhlášený limit)

1x Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
http://www.zonerpress.cz/kniha/pro-programatory/linux-profesionalne-programovani-aplikaci
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

2x David Meerman Scott: Nová pravidla marketingu a PR, Zoner Press, 2008
http://www.zonerpress.cz/kniha/pro-webdesignery/nova-pravidla-marketingu-a-pr
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

Všem sponzorům děkuji.

B. John Wellington (prolog Soutěže 2008)

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Je rok 1941. Německá armáda obsadila téměř celou Evropu a 22. června brzy ráno německé jednotky bez vypovězení války překročily hranici Sovětského svazu a nyní rychle postupují do nitra SSSR. Do poloviny července obsadili Němci Minsk a poté i Smolensk. 26. září obklíčila německá vojska Kyjev a přilehlé oblasti a zajala přes 650 000 sovětských vojáků.

Jen jeden stát v Evropě – Spojené království - hrdě vzdoruje. Je to právě rok, co se mu podařilo překazit Hitlerův plán Lvoun (operace Seelöwe) na vylodění. Právě také uběhlo smutné výročí prvého mohutného útoku německé Luftwafe na Londýn, který provedla 7. září. Britům se však dařilo sestřelit velké množství německých letadel a Němci díky tomu nezískali dostatečnou převahu ve vzduchu nutnou k uskutečnění pozemní invaze, která byla z tohoto důvodu odložena na neurčito. Málokdo ví, že za britským úspěchem nejsou jen letci, hrdinské činy dalších vojáků, využití radaru, ale také vynikající rozvědná služba a především ***luštitelská služba***.

Tato služba byla založena vládou Spojeného království roku 1939 a sídlí ve venkovském sídle v Bletchley Parku. Toto přísně tajné kryptoanalytické středisko označované *Station X* je umístěno 80 km severozápadně od Londýna. Byli sem povoláni přední matematici, lingvisté a experti v různých oborech (včetně šachistů, hráčů bridge, odborníka na porcelán, kurátora muzejních sbírek apod.), aby zde v utajení po celou válku úspěšně pracovali na luštění šifer zemí Osy a zejména Německa.

Mezi jejich prozatímní největší úspěch patří prolomení jedné z nejrozšířenějších německých šifer produkované přístrojem, který je označován jako *Enigma*. Toto z hlediska ovládání velmi jednoduché zařízení a dle představ Němců velmi bezpečné zařízení, se vyrábí ve velkém množství a patří do výbavy bojových útvarů nejnižší úrovně.

To všechno se na podzim roku 1941 honí hlavou mladému ambicióznímu majorovi radiové služby ***Johnu Wellingtonovi*.** Vzhledem ke svému šlechtickému původu a kontaktům se v roce 1939 dozvěděl o tom, že se sestavuje skupina lidí, kteří budou během války pověření přísně tajným úkolem, který nějak souvisí s luštěním nepřátelských zpráv. Jeho romantická

povaha mu nedala a okamžitě se rozhodl, že se chce také zúčastnit. Jenže přijímací pohovor asi nedopadl tak úplně dobře a John do Bletchley Parku nebyl přijat. Byl však doporučen jako důstojník do jedné z odposlouchávacích stanic, které měly za úkol monitorovat nepřátelský radiový provoz. John tedy místo ve Station X (v Bletchley Parku) skončil v jedné z mnoha *Stations Y*. Konkrétně ve stanici Knockholt jižně od Londýna.

John se však nechtěl spokojit s pouhým velením provozu této stanice, ale snažil se díky svým kontaktům dostat se do Bletchley Parku anebo do rozvědné služby. To se mu sice nepodařilo, ale přesto získala, asi po roce úspěšné služby, jeho stanice v Knockholtu výjimečné postavení. Mimo úkoly spojené s monitoringem nepřátelského provozu a dodáváním zachycených šifrových zpráv do Bletchley Parku byla jeho stanice pověřena spojením s některými rozvědnými skupinami na území Evropy. Důstojník SIS (Secret Intelligence Service), kterého znal pod jménem Hill, za ním osobně dojížděl a pověřoval jej speciálními úkoly.

Bylo tomu tak i na sklonku tohoto září, kdy Hill Johna navštívil a stručně jej seznámil s informacemi potřebnými pro další úkol.

John teď seděl u mohutného stolu ve své kanceláři. Před sebou měl mapu Evropy, ve které měl zapíchány desítky špendlíků s radiovými cíli a zdroji. Popíjel svůj oblíbený čaj a stále myslel na ten dnešní rozhovor. Co se vlastně dozvěděl?

Jeden z osvědčených špionů s přezdívkou Reis – Němec, který měl blízko ke generálnímu štábu, oznámil, že se v blízké době chystá odvysílání velmi důležité zprávy. Nevěděl, co má obsahovat, ale prý bude vysílána někdy po polovině října. Označil však konkrétní berlínské spojení a dodal vysílací plán.

John samozřejmě nechal ihned tuto linku z Berlína monitorovat. Bohužel patřila k těm, v kterých se od června tohoto roku začal místo Enigmy používat nějaký jiný dosud neznámý šifrátor. Bletchley Park zatím nebyl schopen tyto zprávy luštit. Dokonce se nedařilo ani zjistit, jaký šifrátor se používá.

Hill zařídil, že byl německý špión Reis zaúkolován, aby se buď pokusil získat obsah avizované zprávy, nebo (což by ve svém důsledku mohlo být cennější) se pokusil získat další informace k použitému šifrovému zařízení.

Reis se na delší dobu odmlčel. Ozval se až včera a právě kvůli obsahu té poslední depeše ihned Hill za Johnem přijel. Převzal ji a požádal, aby se John této záležitosti speciálně věnoval, neboť nejvyšší velení má zájem jak o zprávu (v minulosti byly informace od Reise vždy velmi cenné), tak samozřejmě o vše, co by mohlo pomoci při odhalení nového šifrátoru.

John teď seděl u stolu a stále si opakoval slova té poslední zvláštní dešifrované depeše a zejména jej znepokojoval závěr zprávy.

Potvrzuji, že zpráva má být velmi důležitá. Nemohu se však dostat k jejímu obsahu. Důstojníci o ní mlčí. Bude vysílána novým šifrátorem SZ. Pokusím se získat jeho popis a technická data. Myslím, že bych se mohl dostat i k jeho aktuálnímu nastavení. Používá se od tohoto června pro spojení na hlavním velení. Mám však problém s heslovými bločky. Pokud mi hesla dojdou a já nebudu moci šifrovat odesílané zprávy dohodnutým způsobem, použiji nějaký jiný, třeba slabý systém. Psát budu jen v náznacích. Informaci o nastavení šifrátoru rozdělím do více zpráv a budu je posílat po částech různými kanály. Věřím, že vše dobře poskládáte. Nemohu postupovat jinak, neboť bych se prozradil.

John si pro sebe v duchu říkal: „Tak tedy příští měsíc budu muset být velmi ostražitý, aby se nám nestalo, že některá z depeší od Reise, obsahující informace o použité šifře, nám unikne. Navíc to vypadá, že nebudou šifrovány dohodnutým agenturním systémem, ale nějakým náhradním způsobem, o němž odesílatel předpokládá, že jej i bez dohodnutého klíče vyluštíme. Pokud se dostaneme k šifrátoru nebo se podaří Reisovi předat nám i plány šifrátoru, budeme pak schopni vyluštit i avizovanou důležitou zprávu a možná se nám podaří prolomit celý šifrátor SZ. To by byl jistě úspěch, který by mu vynesl vysoké ocenění a možná i přiřazení do Bletchley Parku, po kterém tolik toužil.“

John si také dále vzpomněl na Hillova slova: „Pokud se ti podaří tu důležitou zprávu vyluštit, budeme zase blíže vítězství. **To vítězství bude i Tvé vítezství !“.**

C. Autentizace pomocí Zero-Knowledge protokolů

Bc. Jan Hajný, Ústav telekomunikací, FEKT VUT Brno, (xhajny01@stud.feec.vutbr.cz)

Tento článek se zabývá problematikou Zero – Knowledge protokolů, tedy protokolů s nulovou znalostí. Obsahem textu je úvod do této oblasti, důvody vedoucí k vývoji těchto protokolů, analýza možností nasazení při autentizaci klientů v systémech a hlavní rozdíly mezi ZK a klasickými kryptografickými protokoly pro ověření totožnosti.

Klasická autentizace

Cílem autentizace je ověření identity uživatele systému. Hlavním důvodem použití je odepření přístupu k informacím uživatelům, kteří nejsou k takovému přístupu oprávněni. V počítačových systémech je nejčastější autentizace pomocí znalosti tajné informace. Před uvedením uživatele do systému je vygenerováno např. tajné heslo (PIN, fráze atd.), které nadále slouží k ověření identity klienta. Jelikož tajnou informaci zná pouze ověřovatel a klient, předpokládá se, že znalost hesla je pro ověřovatele dostatečný důkaz o pravosti klienta. Příkladem autentizace s použitím klasických autentizačních protokolů může být přístup na zabezpečené webové stránky. Před zobrazením stránky je klient dotázán na uživatelské jméno a heslo, které je pak odesláno zpět serveru k ověření. Známý problém takovéto komunikace je právě přenos hesla přes nebezpečnou oblast – typicky internet. Pokud je heslo odesláno v otevřené formě, je snadno odposlechnutelné. Řešením může být šifrování komunikace mezi klientem a serverem. Toto řešení je v praxi velmi často používané a je základem většiny protokolů. Obměnou může být použití pouze hashe hesla jako prvku k ověření identity.

Hlavním problémem tohoto přístupu je množství tajné informace, které při procesu autentizace odhalujeme. Tajemství ve formě hesla je jediná znalost, která nás odlišuje od jiných uživatelů systému, popř. od možných útočníků. Pokud bude útočník schopen zjistit naše tajemství, nebude pro systém možné odlišit naši identitu od identity útočníka. Tajemství tedy musí zůstat pouze klientovi. Na druhou stranu cílem autentizačního protokolu je odlišit uživatele, musí tedy tajemství používat.

Tímto se dostáváme k problému autentizačních protokolů – tajná informace musí být v protokolech používána, ale na druhou stranu musí zůstat zcela utajena. U běžných protokolů nemáme úplnou kontrolu nad množstvím uniklé informace – pokud použijeme např. přenos šifrovaného hesla, stále útočníkovi dáváme informaci např. o délce hesla (délku zprávy není možné utajit v kryptogramu), popř. možnost odhadnutí hesla pomocí hrubé síly atd.. Je složité přesně definovat, které informace ověřovateli navíc odesíláme. Klient ve své komunikaci při klasické autentizaci tedy většinou odesílá serveru své heslo (v šifrované podobě, či jako hash). Nicméně pro správné ověření server nepotřebuje znát celé heslo klienta, potřebuje získat pouze jediný bit informace – zda je identita klienta pravá, či nikoliv (tedy jestli zná heslo, či nikoliv). Cílem je tedy navrhnout protokol, který by nepřenášel celé tajemství klienta, ale pouze sdělil, zda jej klient zná, či nikoliv.

Důvody vzniku Zero – Knowledge

Hlavním důvodem vzniku protokolů ZK (Zero Knowledge) je právě potřeba kontroly nad množstvím uniklé informace. V předchozím odstavci bylo zmíněno, že takováto kontrola je u stávajících protokolů velmi obtížná, navíc většinou odesílají více informací, než pro jaké byly navrženy. Toto pak může být zneužito útočníkem. Naopak u protokolů typu ZK můžeme dokázat, že odesílají pouze informaci, pro kterou byly navrženy a žádnou další. Není tedy možné (ani po opakovaném běhu protokolu) získat další informace, které by mohly vést k odhalení klientova tajemství. U klasických protokolů často ověřovatel zná tajnou informaci klienta také a ověření proběhne pouze srovnáním. V tomto případě může ověřovatel zneužít této znalosti a vydávat se za klienta, což není zcela jistě cílem protokolu. Tento problém je řešen u ZK protokolů, ověřovatel zde totiž uživatelovo tajemství nezná a stejně jako okolní svět jej z více běhů protokolu nemůže získat.

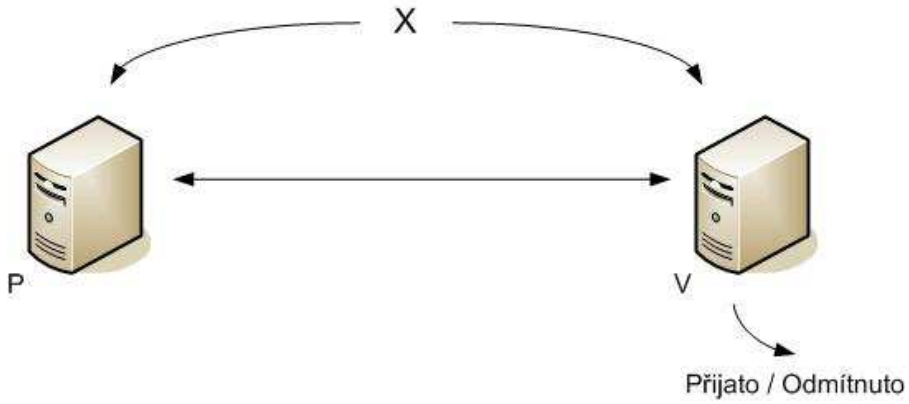
Spojitost s autentizací je tedy zřejmá – můžeme každého klienta v systému nechat zvolit si složitý problém k němuž zná řešení. Potom klient může dokázat znalost takového řešení (což je nyní jeho tajemství) pomocí ZK protokolu bez odhalení informace o tajemství. Autentizace klienta bude úspěšná tehdy, pokud ověřovatel bude pomocí ZK přesvědčen o klientově znalosti tajemství.

Další oblastí, kde můžeme využít ZK protokolů, je samotný důkaz znalosti řešení jakéhokoliv z NP problémů. To je umožněno díky existenci ZK protokolu pro NP úplný problém Hamiltonova cyklu [1]. Toto může být využito např. jako důkaz korektně zvolených vstupů k výpočtu funkce bez jejich vlastního odhalení.

Interaktivní důkazový systém

Před samotnou definicí vlastnosti ZK je nutné zmínit systémy, které tuto vlastnost mohou mít. Jedním z nich je např. interaktivní důkazový systém. Jedná se o dvojici Turingových strojů, které jsou navíc vybaveny komunikační páskou, která jim umožňuje vzájemnou komunikaci. Jeden z těchto strojů je vybaven nekonečnou výpočetní silou, druhý polynomiálně omezen. Tuto dvojici budeme nazývat P a V z anglického Prover a Verifier. P bude tedy klient, který chce být ověřen a vpuštěn do systému. V bude ověřovatel, který chce získat informaci, zda P je skutečně ten, za koho se vydává (zda tedy zná tajemství ve formě řešení problému). Existuje také podobný systém s omezeným strojem P, který má navíc pomocný vstup, který mu dává informaci, kterou potřebuje k řešení problému. Je nutné, aby se P od V odlišoval, pokud by byl stejného typu, nebyl by důvod, aby V s P komunikoval pomocí sdílené pásky a P by nemusel být přítomen.

Struktura a samotný běh systému je znázorněn na Obr. č. 1: Interaktivní důkazový systém:



Obr. č. 1: Interaktivní důkazový systém

Oba stroje získají společný vstup X. Následuje běh a vzájemná interakce na jehož konci je výsledek „Přijato/Odmítnuto“ vycházející od V. Tímto běh systému skončí. Výsledek je tedy, že pár (P, V) přijme X či ho odmítne. V tomto případě může být X výrok, jehož pravdivost vede k odmítnutí nebo přijetí. Pro interaktivní důkazové systémy musí tedy platit dvě základní vlastnosti:

- **Úplnost**: Pokud $X \in L$ (je pravdivé), potom pravděpodobnost, že (P, V) odmítne X je zanedbatelná s délkou X.

- **Spolehlivost**: Pokud $X \notin L$ (není pravdivé), potom pravděpodobnost, že (P*, V) přijme X je zanedbatelná s délkou X, přičemž P* je jakýkoliv klient.

Pokud bychom takovýto systém použili pro ověření identity klienta, jehož tajemství je důkaz pravdivosti výroku, klient by byl do systému vpuštěn téměř vždy, pokud je tvrzení pravdivé (díky úplnosti – klient má důkaz) a téměř nikdy, pokud jeho tvrzení pravdivé není (díky spolehlivosti – klient důkaz nemůže mít).

Tento systém sám o sobě sice poskytuje ověření klienta, nicméně nijak nespecifikuje, které informace budou veřejně odesílány. Z tohoto důvodu není zatím systém nijak zabezpečen proti odhalení tajemství klienta P. Avšak protokoly založené na interaktivních důkazových systémech můžou mít navíc vlastnost Zero Knowledge, tedy nulového úniku informace. Potom můžeme o takových protokolech zkráceně mluvit jako o Zero Knowledge protokolech. Požadavek na utajení všech soukromých informací klienta můžeme specifikovat pomocí požadavku na existenci simulátoru, který bude simulovat veškerý průběh protokolu bez přítomnosti klienta P. Můžeme potom předpokládat, že pokud existuje stroj, který je schopen generovat celý výstup protokolu bez přítomnosti klienta P, není tedy žádné tajemství, známé pouze P, které by bylo v protokolu odhaleno, protože samozřejmě simulátor tajemství nezná.

Definice ZK

Interaktivní důkazový systém (P, V) pro jazyk L může mít vlastnost Zero Knowledge, pokud pro každého polynomiálního ověřovatele V můžeme najít simulátor Mv* běžící v polynomiálním čase, jehož výstup je identicky rozdělený jako výstup dvojice (P, V) pro* $x \in L$.

Tato definice nám říká, že u ZK protokolu je možné najít simulátor, který poběží v polynomiálním čase a který nám bude schopný dát hodnoty neodlišitelné od běhu skutečného protokolu. Tím nám také překvapivě říká, že výstup simulace (tedy i protokolu) nezávisí na tajemství, které zná pouze P, který není přítomen v simulaci. Důvod, proč je simulátor schopen rekonstruovat výstup protokolu i přes neznalost tajemství klienta, je jeho vyšší stupeň volnosti – může generovat zprávy v libovolném pořadí na rozdíl od klienta, který se musí držet protokolu a generovat zprávy v předem daném pořadí.[1]

Další fakt vyplývající z definice je, že simulátor musí být schopen pracovat při komunikaci s jakýmkoliv ověřovatelem V, tedy i nečestným, který se nedrží dohodnutého protokolu. Tato vlastnost nám zajišťuje, že protokol neuvolní tajemství klienta ani v případě, že ověřovatel nebude dodržovat protokol a místo toho bude dělat vše nezbytné k získání tajemství. Pokud simulátor funguje i v této simulaci, nedojde k úniku informace v reálném nasazení.

Pro nadcházející příklad je také důležitá skutečnost, že simulátor musí mít omezenou výpočetní sílu a běžet v polynomiálním čase vzhledem k výroku X.

V uvedené definici je zmíněno, že výstup simulátoru musí mít identické rozdělení jako výstup skutečného protokolu. Potom můžeme nazvat protokol jako PZK – Perfect Zero Knowledge. Pokud jsou si veličiny pouze statisticky blízké (statistická vzdálenost je zanedbatelná), jedná se o SZK – Statistical Zero Knowledge a pro výpočetně nerozlišitelné máme CZK – Computational Zero Knowledge. V následujícím odstavci je uveden příklad protokolu typu PZK.

Příklad PZK protokolu

Protokol založený na isomorfismu grafů, publikovaný v [1], probíhá mezi klientem P a ověřovatelem V následovně:

- Společný vstup pro P i V je G_0 a G_1, což jsou dva grafy o stejném počtu uzlů i hran. Oba grafy jsou tedy přístupné pro P i V. Klient P tvrdí, že zadané grafy jsou isomorfní, tedy že existuje taková permutace π , že platí $G_1 = \pi (G_0)$. P je schopen takovou permutaci vypočítat (díky neomezené výpočetní síle), nebo ji předem zná.

- P zvolí náhodnou permutaci ω a vypočte graf H z G_0. Tento náhodně permutovaný graf odešle ověřovateli.

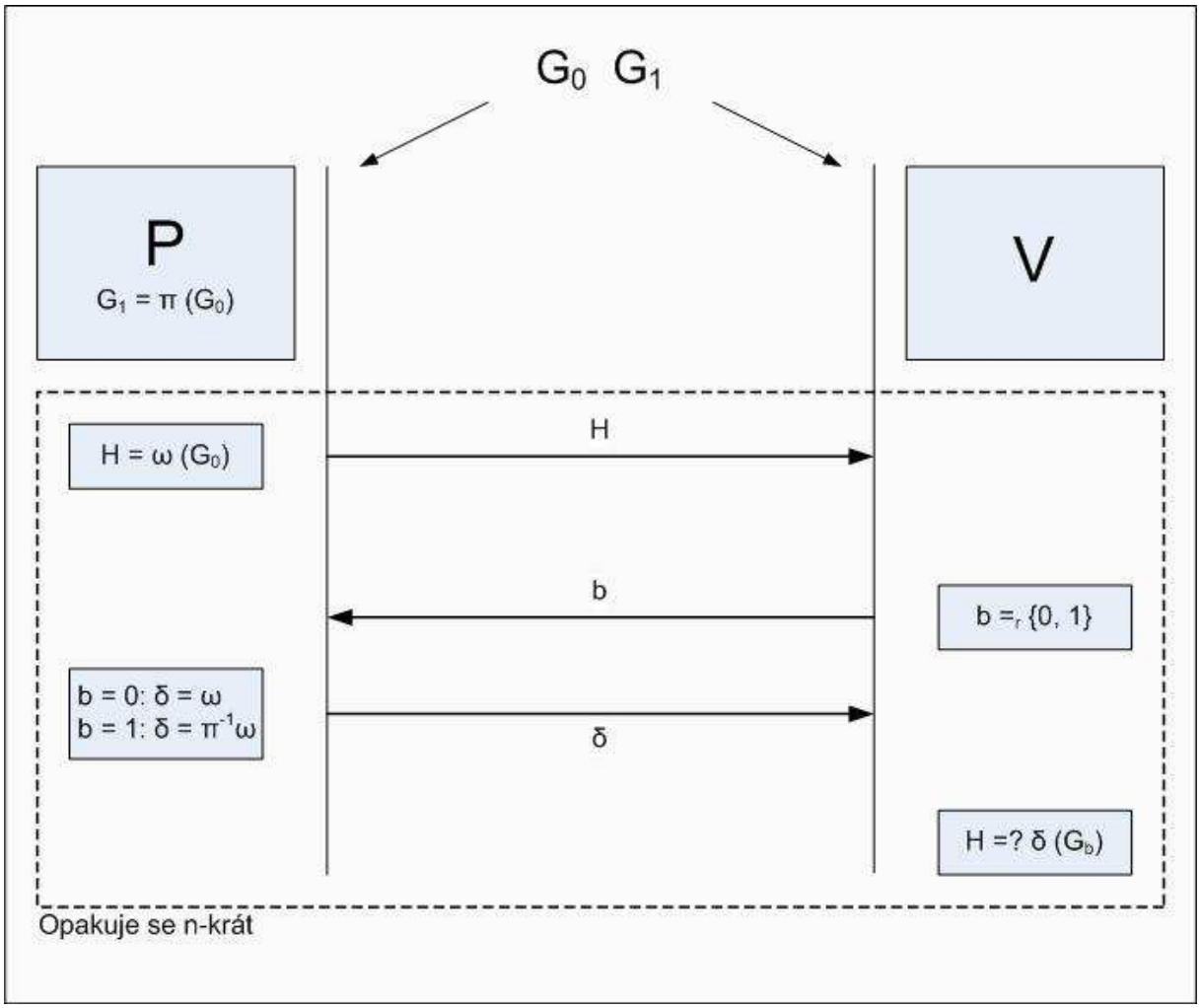
- Ověřovatel V zvolí náhodně bit b a odešle jej zpět P.

- P spočte odpověď na bit b tak, aby byla splněna rovnost $H = \delta (G_b)$ a odešle výslednou permutaci zpět V, který ji ověří.

- Nyní zvolí P novou náhodnou permutaci a odešle nový graf H. Toto se opakuje n-krát,

[1] Ve skutečném běhu protokolu je znalost tajemství vyžadována spolehlivostí.

kde n je bezpečnostní parametr. Pokud je ve všech kolech výsledná permutace přijata, V přijme tvrzení, pokud je zaslána špatná permutace, klient je odmítnut.



Obr.č. 2 – ZK protokol pro isomorfismus grafů

Hlavním cílem protokolu je demonstrovat znalost permutace mezi G_0 a G_1 bez jejího odhalení. Protokol je interaktivní důkazový systém s nulovou znalostí, měl by tedy být úplný, spolehlivý a mít adekvátní simulátor.

Úplnost: *Klient P, který zná permutaci π, by měl být přijat téměř vždy.*
Tato podmínka je splněna, neboť P, který zná permutaci π, je schopen odeslat odpověď v posledním kroku jak na b = 0, tak na b = 1. V prvním případě jednoduše odešle svoji ω, kterou si sám zvolil, v druhém případě odešle $\pi^{-1}\omega$, které také zná. Odpověď tedy bude vždy přijata.

Spolehlivost: *Klient P, který nezná permutaci π, by neměl být přijat s výjimkou zanedbatelné pravděpodobnosti.*
Předpokládejme opak, tedy že klient P sice nezná permutaci π, ale je přijat. V tom případě musel být splněn závěrečný test ve všech případech, tedy jak pro b = 0 tak b = 1. To ovšem znamená, že P je schopen odeslat platnou permutaci jak pro G_0 tak pro G_1, tedy $H = \delta (G_0)$ a $H = \delta' (G_1)$, z čehož vyplývá, že zná $\pi = \delta'^{-1} \delta$, což koliduje s naším předpokladem. Pokud by nebyl schopen odeslat správnou permutaci pro oba stavy b, ale pouze pro 1 ze stavů, byla by

jeho úspěšnost v 1 kole 50 % (pravděpodobnost, že se náhodný bit b od V zrovna trefí do toho, na který P zná odpověď). V n kolech je tato pravděpodobnost již 2^{-n}, což je zanedbatelné.

Existence simulátoru Mv*: *Musí existovat polynomiální simulátor, jehož výstup bude neodlišitelný od skutečného běhu protokolu pro pravdivé tvrzení.* Simulátor funguje v těchto krocích (pro 1 kolo):

1. Mv* zvolí náhodný bit $b' =_R \{0, 1\}$.
2. Mv* zvolí náhodnou permutaci δ a odešle $H = \delta (G_{b'})$ V*.
3. V* zvolí náhodně bit $b =_R \{0, 1\}$ a odešle jej Mv*.
4. Nyní mohou nastat 2 možnosti:
   a) Pokud $b \neq b'$, přesuneme se [2] zpět k bodu 1
   b) Pokud $b = b'$, simulátor pošle na výstup (H', b', δ')

Simulátor běží v očekávaném čase 2n, protože pravděpodobnost shody b a b´ je ½. Tento čas je polynomiální, tedy první podmínka je splněna.

Druhá podmínka je stejné rozdělení výstupu simulátoru Zv* (H', b', δ') a výstupu protokolu (H, b, δ). V protokolu je H zvoleno jako náhodná permutace G_0, u simulátoru jako náhodná permutace G_b. Protože předpokládáme u simulace, že počáteční výrok platí, G_0 je tedy isomorfní s G_1, tedy platí, že náhodná permutace G_1 má stejné rozdělení jako permutace G_0. H a H´ mají tedy identické rozdělení. Dále b a b´ mají také identické rozdělení (jsou totožné) a δ a δ´ jsou již dány testovacím vzorcem, musí být tedy také identicky rozdělené.

Můžeme tedy tvrdit, že daný protokol je interaktivní důkazový systém (splňuje úplnost a spolehlivost) a zároveň má ZK (existuje Mv*). Teoreticky tedy může být použit jako protokol pro ověření uživatele, jehož tajemství (které nikdo jiný nezná), je znalost permutace mezi G_0 a G_1. Samozřejmě se jedná pouze o demonstrativní protokol, jehož nízká efektivita zabraňuje jeho využití v praxi.

Použití ZK protokolů

V předchozím odstavci byl uveden příklad ZK protokolu pro isomorfismus grafů. Jedná se o jednoduchý protokol, na němž je dobře patrná myšlenka ZK protokolů, tedy ověření, zda je klient P schopen vrátit se z jím náhodně modifikované hodnoty k hodnotě původní (zde G_0) ale také zároveň přejít k druhé hodnotě tvrzení (v tomto případě G_1). Pokud zná cestu ze zvolené hodnoty k oběma výchozím hodnotám, můžeme předpokládat, že zná i vztah mezi původními hodnotami (v tomto příkladě G_0 a G_1).

Tento příklad je nicméně velmi neefektivní. Pro každé kolo protokolu je nutné přenášet graf H o n uzlech a dále také výslednou permutaci. Pro ověření totožnosti klienta je pak velikost dat přílišná. ZK protokoly však nemusí být založeny pouze na problému zjištění isomorfie grafů – viz příklady v [4]. Jako nejvíce efektivní se zdají problémy diskrétního

[2] Toto „přetočení“ ověřovatele V* si můžeme dovolit, simulátor může generovat zprávy v libovolném pořadí.

logaritmu, RSA získání kořenů či problém kvadratických reziduí. S protokoly využívající tyto mechanizmy je již možné provádět autentizaci efektivně. Příkladem může být např. implementace ZK pro ověření identity v programu OpenSSH využívající Ohta-Okamoto protokol založený právě na problému získání kořenů [2].

ZK protokoly lze využít také jako stavební prvky pro další, složitější protokoly. Příkladem můžou být například elektronické platební systémy (eCash) [3]. Tyto systémy mohou mít např. zajištěnu bezpečnost pouze v případě, že se klienti chovají podle pravidel protokolu a nijak se od něj neodchylují, to znamená, počítají své vstupní hodnoty do protokolu podle předem daných pravidel. Nyní můžeme ZK použít jako důkaz tvrzení, že jsou námi vložené hodnoty spočteny dle zadaných pravidel (protože každý uskutečnitelný výpočet můžeme brát jako NP tvrzení). Těmito důkazy lze pak převést systém, který byl původně bezpečný pouze pro klienty neodchylující se od protokolu, na systém, který je bezpečný pro jakékoliv klienty.

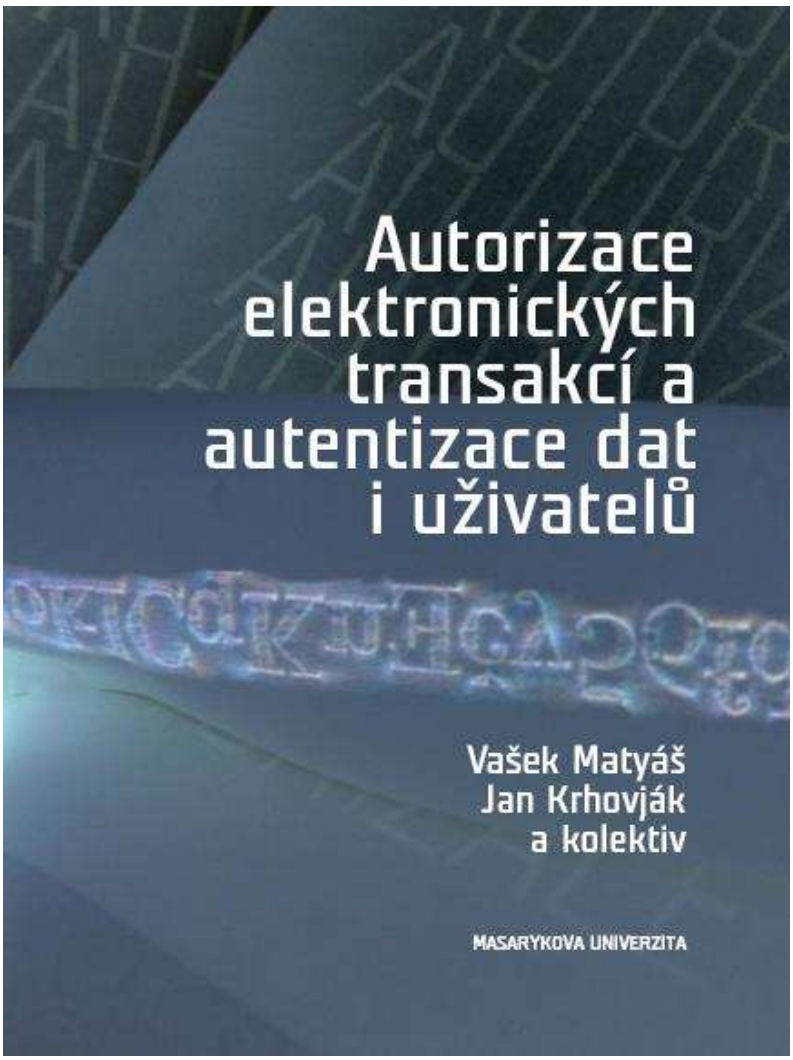
Kvůli efektivnosti přenosu se můžeme také setkat s protokoly, jejichž důkaz bezpečnosti není tak silný, nicméně jsou mnohem efektivnější. Příkladem jsou Σ-protokoly, které jsou velmi podobné ZK, jsou ale bezpečné pouze vůči ověřovateli V, který dodržuje protokol. Využitím dalších konstrukcí nad Σ-protokoly (např. OR-konstrukce) lze ale také získat odolnost vůči V* odchylujícímu se od protokolu.

Závěr

Hlavním cílem tohoto textu bylo seznámit čtenáře s možnostmi autentizace pomocí skupiny protokolů označovaných jako Zero-Knowledge protokoly, tedy protokoly s nulovou znalostí. Výhodou těchto protokolů je možnost kontroly nad množstvím informací, které během svého běhu uvolní. Tato vlastnost je velmi důležitá právě v oblasti ověření identity uživatelů ve veřejném prostředí jako je internet. S použitím těchto protokolů lze dosáhnout stavu, kdy během ověření uživatele nebude uvolněna žádná informace, která by mohla vést k uvolnění uživatelova tajemství. Mimo použití ZK protokolů v autentizaci je zmíněna také oblast důkazů, pro které můžeme ZK použít a zajistit tak vyšší bezpečnost pro komplexnější struktury.

D. Recenze knihy: *Matyáš,V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů*

Vojtěch J. Jákl, MFF UK Praha, (vjj@mff.cuni.cz)



MATYÁŠ Václav (Vašek) - KRHOVJÁK Jan a kol.
Rok vydání: 2008
ISBN: 9788021045569
Počet stran: 128
Vazba: brožovaná
Vydavatelství: Masarykova univerzita
Cena: 220 Kč

Přehled autorů:

MATYÁŠ, Vašek
KRHOVJÁK, Jan
LORENC, Václav
KUMPOŠT, Marek
ŘÍHA, Zdeněk
CVRČEK, Daniel
STAUDEK, Jan
HENDRYCH, Pavel
JANDA, Miroslav
HOLER, Vlastimil
MALINKA, Kamil
ŠVENDA, Petr
STETSKO, Andriy.

Úvodní charakteristika publikace

Tato publikace, známá spíše pod neoficiálním názvem "Elektronické platby", obsahuje téměř kompletní přehled metod a technologií pro autentizaci a autorizaci používaných při elektronických platebních transakcích.

Plus

Známá jména v dlouhém seznamu autorů.
Obsah je dlouhým přehledem lákavých a zajímavých témat z dané problematiky.

Mínus

Výklad každé ze základních částí publikace je podán mírně odlišným způsobem.

Obsah

Už jen přehled a kritická analýza současného stavu (ne)bezpečnosti platebních systémů v úvodní kapitole stojí za přečtení samy o sobě. Ale stejně zajímavé čtení pokračuje i nadále. Přehled základních autentizačních metod a trendů v jejich vývoji ve druhé kapitole obsahuje i fundovaný popis biometrické autentizace a krátkou zmínku o vícefaktorových autentizacích. Následující popis autentizace pomocí certifikátů je speciálně zaměřen právě na platební transakce.
Podobně je orientován i úvod do problematiky bezpečného hardwaru s popisem kryptografických modulů, příslušnými bezpečnostními požadavky a konečně cenným přehledem útoků na bezpečný hardware a to jak logickým, tak i fyzickým, včetně klasifikace útočníků podle jejich schopností a možností a včetně popisu několika vybraných příkladů a hlavních technik útoků.
Celá tato část je napsána velice přehledně a strukturovaně. Bohužel jsou však tu a tam některé složitější termíny a „vzorce“ uváděny spíše jen pro ilustraci, tj. bez potřebného vysvětlení (student, který by se s nimi nesetkal na přednášce, by se je podle toho jen těžko mohl naučit - tj. měl by dokonalý přehled, chybělo by mu však pár konkrétních znalostí).

Hlavní část příručky je podle očekávání věnována vlastní autorizaci platebních transakcí. Po klasifikaci elektronických plateb, způsobů autorizace bankovních operací a systémů pro podporu karetních plateb následuje popis specifikace EMV (Europay-Mastercard-Visa) a příslušných bezpečnostních mechanizmů. Zvláště cenná je analýza bezpečnosti používání čipových karet tohoto typu v praxi. Zde uvedené slabiny tohoto systému a doporučení pro jejich odstranění jsou založeny hlavně na několikaletých zkušenostech z jejich používání ve Velké Británii. Analýza je oboustranná, tj. jak z pohledu bank, tak i z pohledu zákazníka, a je doplněna popisem dnes již klasického *brněnského experimentu*. Zvláštní pozornost je věnována platebním transakcím.

Závěrečná třetina příručky obsahuje čtivý a srozumitelný popis elektronického bankovnictví (internet-banking, tele-banking,…). A opět po popisu základních principů a analýze slabých míst následuje zajímavý přehled možných útoků z pohledu uživatelů. Ten postupně graduje až k popisu více i méně známých způsobů zneužití platebních terminálů.
Samotný popis různých typů útoků by ale byl sám o sobě velice pesimistickým závěrem. Naštěstí je poslední rozsáhlá kapitola věnována velice podrobnému přehledu technik, kterými výrobci karet na známé útoky reagují. Tato část knížky se doopravdy pěkně čte (jako dobře napsaná detektivka, od které se nemůžete odtrhnout). Ale pokud opět použiji jako příklad studenta, který se připravuje na zkoušku, dá mu potom ještě hodně práce vytáhnout si z této části stručný přehled fakt, která by se měl naučit, a strukturovaně si je uspořádat.

Celá příručka obsahuje velké množství fundovaných informací, která takto pohromadě nelze asi nikde jinde nalézt. Zcela jistě tedy poslouží jako základní učebnice pro obor informační bezpečnosti na našich vysokých školách. A zároveň i jako vyhledávaná přehledová příručka pro všechny, kdo se o elektronické platby zajímají.

E. O čem jsme psali v září 2000 – 2007

Crypto-World 9/1999

Crypto-World 9/2000

+ příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

Crypto-World 9/2004

Crypto-World 9/2005

Crypto-World 9/2006

Crypto-World 9/2007

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/