

Bezpečnost v informačních technologiích (KIV/BIT)

5. Autentizace, autentizační protokoly

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

16. března 2016

1 Autentizace

- pomocí tajemství
 - heslo
 - výzva - odpověď
- pomocí fyzického objektu
- pomocí biometrických informací

2 Autentizační protokoly

Autentizace

Autentizační protokoly

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- autentizace ???
- autorizace ???

Autentizace

- = proces ověření proklamované identity subjektu (druhé strany)
 - = autentikace (z anglického authentication) příp. autentifikace (z franc. authentication).
 - jednotnost odborné terminologie → termíny nedoporučovány
 - autentizace entity (osoby, programu) × autentizace zprávy
 - útočník aktivní → obtížnost autentizace

Pozor: autentizace \neq autorizace

- autorizace = povolení přístupu k souboru, souhlas s provedením operace (např. smazání souboru "data.txt")

Autentizační metody

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

■ ???

Autentizační metody

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační protokoly

- 1 uživatel zná
 - tajemství (např. PIN, heslo či přístupová fráze, soukromý klíč)
 - 2 uživatel vlastní
 - fyzické objekty (platební či ID karta)
 - 3 vlastnosti uživatele (*biometrické* charakteristiky)
 - vrozené charakteristiky daného jedince (otisk prstu, duhovky oka, hlas, DNA, ...)
- výhody × nevýhody
 - max. eliminace nevýhod → vzájemná kombinace metod
 - dvoufaktorová autentizace
 - třífaktorová autentizace

- nejčastější forma - zadání jména a hesla
 - nezobrazovat při zadání (← minimalizace možnosti okopírování)
 - Příklad: Linux/Unix - nezobrazováno nic
 - Windows - * pro každý znak → nevýhoda ???
 - reakce na chybné zadání - neposkytnutí užitečné informace útočníkovi
 - Příklad: způsoby reakce na chybu
- | | |
|----------------|--------------------------|
| ■ jmeno: king | ■ jmeno: king |
| ■ chybné jmeno | ■ heslo: ***** |
| ■ jmeno: | ■ chyba při přihlasování |

Bezpečné heslo

- obtížná zjistitelnost, uhodnutelnost

→ Nevhodná hesla

- vlastní jméno, jméno někoho z rodiny, přítelkyně, manželky, milenky, jméno psa, kočky, apod.
- rodné číslo, datum narození
- číslo domu, adresa, telefonní číslo, SPZ, apod.
- heslo, root, guest, user, 1234, 12345, apod.

Heslo

Deset nejhorších hesel z pohledu bezpečnosti

“Hackerská” studie: prolomení 1M uživatelských účtů na serveru <http://rockyou.com>

Pořadí	Heslo	Počet uživatelů
1.	123456	290 731
2.	12345	79 078
3.	123456789	76 790
4.	Password	61 958
5.	iloveyou	51 622
6.	princess	35 231
7.	rockyou	22 588
8.	1234567	21 726
9.	12345678	20 553
10.	abc123	17 542

Bezpečné heslo

- obtížná zjistitelnost, uhodnutelnost

→ Vhodná hesla

- “nesmyslná” kombinace znaků (tj. písmen, čísel a interpunkce)
 - → obtížná zapamatovatelnost (i pro autora) -
 - tendence zapsání (př. PIN na papírku u plat. karty, otevřený soubor hesla.txt na disku, apod.) = **neakceptovatelné!!!**
 - ← použití mnemotechnické pomůcky (př. posl. 3 písmena na kláv. vpravo odělená čísla, “zašifrovat”, apod.)

Délka hesla

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- délka hesla → doba prolomení hesla
- PIN karty - pouze 4 znaky - dostatečná délka? NE!
- ← zablokování karty po několika chybných pokusech
- s touto vlastností obecně nepočítat
- ares.zcu.cz - také zablokování po několika neúspěšných přihlášeních - **POZOR !!!**
- → eliminace útoku xxx ???
- dostatečná délka ≥ 8 **znaků** (zdůvodnění viz dále)

Použité znaky

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- počet různých znaků v hesle → doba prolomení hesla (s jeho délkou)
- 10 číslic
- 2×26 základních písmen abecedy (a-z, A-Z)
- znaky s diakritikou (á, é, ř, ...)
- interpunkční symboly (. , : ; - ? !, ...)
- speciální znaky (\$, %, &, @, ...)
- počet znaků k dispozici > 80

Rozbor hesla

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Délka hesla Použité znaky		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	10 000 2 minuty	100 000 16 minut	1 000 000 3 hodiny	10 000 000 1 den	100 000 000 11 dní
a-z, 0-9	36 znaků	1679616 5 hodin	60466176 7 dní	2×10^9 8 měsíců	8×10^{10} 25 let	3×10^{12} 900 let
a-z, A-Z, 0-9	62 znaků	14776336 2 dny	916132832 3 měsíce	5×10^{10} 18 let	4×10^{12} 1000 let	2×10^{14} 70 000 let
a-z, A-Z, 0-9; ščáěě...;@#\$%^*?!...	85 znaků	52200625 6 dní	443705312 1 rok	3×10^{11} 120 let	3×10^{13} 10 000 let	3×10^{15} 800 000 let

Autentizace typu výzva - odpověď

Seznam otázek

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- alternativa k systému hesel
- na serveru dostatečně dlouhý seznam otázek a odpovědí
- volba otázek - bez nutnosti zaznamenání uživatelem
- Př:
 - Jméno matky za svobodna?
 - Jméno sestry/bratra?
 - Název střední/vysoké školy?
- přihlášení: náhodný výběr otázky / kontrola odpovědi systémem
- potřeba velkého počtu otázek
- nepříliš praktické

Autentizace typu výzva - odpověď

Algoritmus

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu
pomocí
biometrických
informací

Autentizační
protokoly

- uživatel: volba algoritmu
- Př:
 - $9 \times x$
 - přihášení: zobrazení č. 5
 - uživatel: zadání č. 45 (výsledek algoritmu)
- varianty: různý algoritmus v různou dobu
- terminál má výpočetní výkon (přihlašování pomocí mob. telefonu, PDA, příp. smartcard)
- → použití *kryptografického* protokolu výzva odpověď
 - uživatel A - server sdílení tajného klíče K
 - server: zaslání výzvy N_A (náhodně gen. číslo)
 - uživatel A : zaslání odpovědi $E_K(A, N_A)$

Autentizace pomocí fyzického objektu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- princip: podobně jako klíč od bytu
- dnes většinou karta (např. zákaznická karta do supermarketu, debetní karta, Plzeňská k., JIS, apod.)
- vložení karty do (ke) čtecího zařízení
 - někdy doplnění o zadání hesla (PIN) ← ne-zneužití ztracené karty

Karta s čárovým kódem

- pruhy (příp. mozaika) definované šířky → zakódování znaků
 - jednorozměrný kód
 - dvojrozměrný kód
- možno přečíst pomocí čteček (příp. scannerů)

- př. většina zákaznických karet
- + cena, jednoduchá výroba
- – triviální kopie karty na kopírce



Autentizace pomocí fyzického objektu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Magnetická karta

- magnetický proužek na zadní straně (např debetní karta, karta z pojišťovny, apod.)
- zapsáno cca 150B informace
- PIN na kartě zašifrovaný pomocí soukromého (tajného) klíče (banky)
- další informace např na adr.
http://pandatron.cz/?535&karty_s_magnetickym_pruhem
- + cena, 1 karta cca 3 Kč
- – běžná dostupnost čtecích/zápisových zařízení → kopie karty
- snadné smazání - pouze přiblížení magnetu

Autentizace pomocí fyzického objektu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Čipová karta

- integrován polovodičový čip (mikroprocesor)

- komunikace se čtecím zařízením
- bezpečné uložení citlivých dat

- kontaktní
- bezkontaktní

1 s pamětí (stored value cards)

2 inteligentní (smartcards)

Karty s pamětí

- malé množství paměti (E)PROM (obvykle < 1 KB)
- čtecí/zapisovací zařízení: čtení a zápis do paměti
- př. tel. karty (dříve); pro autentizaci nepoužívány
- zneužití - rel. snadná výroba "věčných" tel. karet

Autentizace pomocí fyzického objektu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Intelligentní čipová karta (smartcard)

- př: 8 bitový CPU, frekvence 4MHz, 16KB ROM, 4KB EEPROM, 1KB RAM
- komunikace pomocí sériové linky 9600 bps
- kryptografický koprocessor, JVM v ROM (někdy)
- rychlý vývoj
- velké množství využití (zdravotní karty, apod.)
- autentizace: protokol **výzva odpověď** - klíč uložen na kartě
- + obtížné zkopírování (nicméně možné)
- – cena, cca 100-1000 Kč

Autentizace pomocí biometrických informací

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

dva kroky:

- zápis uživatele (provede se 1 ×):
 - 1 změření vlastností snímacím zařízením
 - 2 digitalizace
 - 3 uložení *podstatných* vlastností = vzor uživatele
- identifikace:
 - (1) a (2)
 - porovnání se vzory (příp. uživatel: zadání jména → porovnání pouze s jedním vzorem)
- verifikace × identifikace
- + nutná fyzická přítomnost osoby
- – cena technologie
- spolehlivost některých metod – ne vždy funguje tak, jak bychom chtěli

Autentizace pomocí biometrických informací

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Vlastnosti použitých charakteristik

- dostatečná variabilita (ne např. barva vlasů)
- → příznaky - dostatečná *diskriminativnost*
- psychologická akceptovatelnost (snímání obličeje - někde tváře zakryty)
- praktická získatelnost informace (DNA)
- časová neměnnost (stárnutí - obličej, hlas)
- spolehlivost: odolnost vůči podvodům
- dostatečná rychlost: zprac. 2-3 osoby / min je málo

Běžně používané metody

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- otisk prstu
- charakteristiky očí - sítnice, duhovka
- rozpoznání obličeje
- rozpoznání geometrie ruky
- rozpoznání hlasu
- rozpoznání pohybu pera

Otisk prstů

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- jedinečná charakteristika
 - použití tzv. markantů (specifických bodů):
 - zakončení linie, rozvětvení linie, sloučení linií, křížení, bod (ostrov), apod.
 - počet rýh mezi danými markanty
 - rozdělení na sektory: extrakce směru a vzdálenosti rýh
-
- snímače: optické, elektrické, teplotní, ...
 - nejrozšířenější biometrika
 - v praxi často v kombinaci s čtečkou karet



- snímán vzor cév na pozadí oka - jedinečnost
- osvětlení zdrojem světla nízké intenzity, optické zesílení (LED dioda)
- metoda nepříliš rozšířena (viz — níže)
- + přesnost → velká míra bezpečnosti
- — potřeba pohledu přesně do snímače - nepříjemné
- lidé s brýlemi - problém identifikace

Duhovka

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- barva, textura a vzor - jedinečnost
- kvalitní kamera, zdroj infračerveného světla
- informace o orientaci, četnosti a pozici specifických plošek
→ tzv. duhovková mapa
- vytvoření vzoru, porovnání se vzorem
- + bez nutnosti blízkého kontaktu
- přesnost rozpoznání
- – cena



Rozpoznání obličeje

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- snímání kamerou
- uložení charakteristických vlastností (pozice očí, nosu, úst, obočí, příp. uší)
- důraz na automatické určení těchto vlastností
- porovnání se vzorem
- + velký prostor pro oblast vědy
- – nespolehlivost, t.j. chybná funkce systému při řadě událostí
 - změna vzhledu (brýle, vousy, makeup, stárnutí)
 - změna orientace

Rozpoznání geometrie ruky

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- měření délek prstů
- příp. šířka nebo kontura prstů (lepší systémy)
- + jednoduchá technická realizace
- – možnost kopie - např. plastu, apod.
- oteklá ruka, zranění → chybná funkce systému

Rozpoznání hlasu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- vstup signálu: telefon, mikrofon
- nalezení “vhodných” charakteristik osob (mluvčích)
- modelování mluvčích
- v praxi integrace s jinou metodou - např. s rozpoznáním obličeje
- + minimální nároky na HW
- – vyžadována znalost řečových technologií (složitě)
- náchylné na šum - hlučné prostředí
- změny hlasu - nemoc, stárnutí

Rozpoznání pohybu pera při podpisu

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- jedinečnost, nemožnost napodobení na základě znalosti podpisu
- speciální pero → informace o rychlosti, směru a tlaku psaní
- zápis: podpis několikrát (alespoň $5 \times$) → vzor
- autentizace samotná
- + lidé jsou na podepisování zvyklí → oblasti využití (banky, apod.)
- – praktické problémy v technické realizaci (dlouho nevydrží nešetrné zacházení) → malé rozšíření

Autentizace - obecný model

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- Alice: snaha o vytvoření bezpečného spojení s Bobem
 - výměna zpráv s Bobem případně s důvěryhodnou třetí stranou (různé role: certifikační autorita, centrum pro distribuci klíčů, tzv. KDC, atd.)

Předpoklad

- Oskar (aktivní útočník) → odposlech, modifikace, vkládání, příp. mazání zpráv

Cíl

- po dokončení výměny zpráv (=protokolu) zajištěno, že Alice i Bob mají ověřeny identity
 - Alice - opravdu komunikace s Bobem
 - Bob - opravdu komunikace s Alicí
- většinou - zároveň vytvoření klíče pro šifrování jednoho spojení (relace) symetrickým šifrovacím algoritmem (tzv. relační klíč, angl. session key)

Autentizace - základní předpoklady

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- přenos zpráv protokolu otevřenou (nechráněnou) sítí
- → možnost odposlechu, modifikace, vkládání vlastních zpráv, příp. mazání zpráv zasílaných útočníkem
 - obvykle uváděn násl. model; správní účastníci komunikace získávají zprávy výhradně prostřednictvím útočníka (možnost provádění akcí - viz výše - bez zpoždění)
- základní kryptografické algoritmy - bezpečné
- → nemožnost jejich napadení útočníkem \times snaha napadení *kombinace* těchto mechanismů, tedy vlastního protokolu

Subjekty

- A = Alice, B = Bob ... potřeba vzájemné *zabezpečené* komunikace
- O = Oskar ... útočník

Autentizace založená na sdíleném tajném klíči

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Předpoklad

- účastníci komunikace (Alice a Bob) - sdílení tajného klíče K_{AB} (např. osobní předání dříve)

Princip protokolu

- účastník č.1 - zaslání výzvy (challenge) účastníkovi č.2
 - náhodné číslo (někdy označováno jako "nonce") N_i
- druhý účastník - transformace výzvy, zaslání odpovědi
- → označení protokolů: *výzva-odpověď (challenge-response protocols)*

Autentizační protokoly typu challenge-response

jednoduchý příklad

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- 1 $A \rightarrow B: \{A\}$ - info o své identitě
- 2 $B \rightarrow A: \{N_B\}$ - výběr (vygenerování) velkého náhodného čísla (alespoň 128 bit)
- 3 $A \rightarrow B: \{N_B\}_{K_{AB}}$ - zašifrování sdíleným klíčem K_{AB}
 - \rightarrow Bob autentizoval Alici (ne ale obráceně Alice Boba),
 - Oskar mohl zachytit první zprávu a poslat zpět N_B
- 4 $A \rightarrow B: \{N_A\}$ - výběr náhodného čísla N_A
- 5 $B \rightarrow A: \{N_A\}_{K_{AB}}$
 - i Alice ví, že komunikuje s Bobem
 - možnost výběru relačního klíče, zašifrování klíčem K_{AB} a zaslání zpět Bobovi

Autentizační protokoly typu challenge-response

zjednodušení → chybný protokol

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

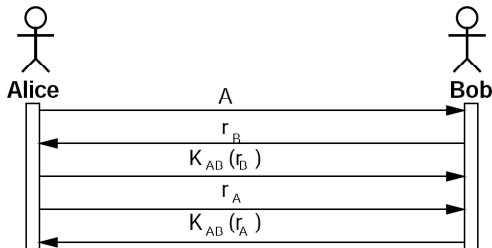
heslo

výzva -
odpověď

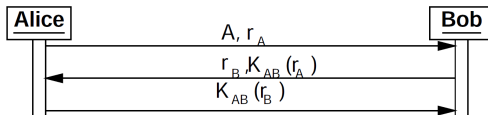
pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly



Zjednodušený protokol (5. zpráv seskupeno pouze do tří)



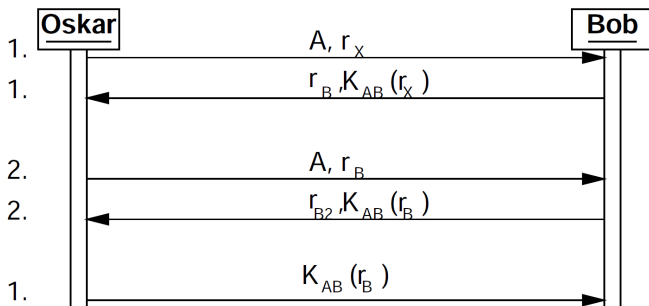
- na 1. pohled OK, ale ..
- umožňuje tzv. reflection attack

Autentizační protokoly typu challenge-response

Útok na zjednodušenou verzi

Předpoklad

- možnost navázání více relací současně s Bobem (např. Bob - banka, více klientů chce provést transakci)



Autentizační protokoly - poznámky

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly



- obtížnot bezchybného návrhu autentizačního protokolu
- používání pouze otestovaných publikovaných metod v praxi
- posílání odpovědi na výzvu $N_X \{X, N_X\}_{K_{XY}}$ (místo $\{N_X\}_{K_{XY}}$, kde $X = \text{id}$ vyzývajícího účastníka) → zamezení reflexivního útoku
 - součástí standardu ISO 9798-2

Authenticated Key Exchange Protocol 2

(AKEP2) [1]

Autentizační protokoly

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- Bellare & Rogaway v roce 1993
- vzájemná autentizace a dohodnutí sdíleného relačního klíče pomocí tří zpráv

Předpoklad

- oba subjekty, které chtějí bezpečně komunikovat, sdílejí od dříve tajné klíče K_1 a K_2
- k dispozici *klíčovaná* jednosměrná hash funkce
 - tzv. Message Authentication Code (MAC) - většinou modifikace jednosměrné hash funkce

Protokol AKEP2

Autentizační protokoly

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď
pomocí
fyzického
objektu
pomocí
biometrických
informací

Autentizační
protokoly

- 1 $A \rightarrow B: \{N_A\}$ - výběr (vygenerování) velkého náhodného čísla N_A ,
poslání
- 2 $B \rightarrow A: M_1 = \{A, B, N_A, N_B\}, \{M1\}_{MAC_{K1}}$ - výběr náhodného
čísla N_B , poslání zprávy
- 3 $A \rightarrow B: M_2 = \{A, N_B\}, \{M2\}_{MAC_{K1}}$ - ověření identit A a B ,
porovnání zaslané a přijaté N_A , ověření $MAC_{K1} \rightarrow$ Bob autentizován,
zaslání zprávy
- 4 B - ověření N_B a $\{M2\}_{MAC_{K1}} \rightarrow$ Alice je opravdová
- 5 $B \& A$ - výpočet relačního klíče $K_{rel} = \{N_B\}_{MAC_{K2}}$ pro komunikaci

Hash vs. šifrovací funkce

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Hash

- ???

Šifrovací funkce

- ???

Hash vs. šifrovací funkce

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství

heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Hash

- **jednocestná** funkce, která z libovolně dlouhého textu vyrobí krátký řetězec konst. délky, tzv. *hash*.
- → není možno zpětně vytvořit původní text

Šifrovací funkce

- ukrytí zprávy
- mám klíč → možnost získání původního textu
- $P = D(E(P, K), K)$

Výhoda

- neplatí restrikce některých států = zákaz používání šifrovacích fcí - zde v protokolu není použita

Nevýhoda

- získání klíče K_2 útočníkem → dešifrování již proběhlé komunikace

Autentizace pomocí třetí strany

Autentizační protokoly

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo
výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

Dříve:

- účastníci komunikace - sdílení tajného klíče
- → pro komunikaci s N stranami potřeba N (párů) klíčů
- → složitost distribuce a správy klíčů

Nyní:

- → zavedení třetí strany, centrum pro správu a distribuci klíčů, tzv. Key Distribution Center (KDC), dále značení S (server)
- každý uživatel pouze jeden klíč, který sdílí se S (např. Alice K_{AS} ; Bob K_{BS})
- autentizace + vytváření rel. klíče pomocí KDC

Autentizace pomocí třetí strany

Nejjednodušší varianta

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační
protokoly

- 1 $A \rightarrow S: A, \{B, K\}_{K_{AS}}$ - vygenerování rel. klíče K , posláni zprávy
 - 2 $S \rightarrow B: \{A, K\}_{K_{BS}}$ - dešifrování, vytvoření a odeslání nové zprávy
- KDC ověření, že první zpráva je od Alice (pomocí klíče)
 - zpráva č. 2 - pouze Bob může dešifrovat
 - = autentizace stran *vedlejším efektem*

Bezpečnostní nedostatky

- 1 A : vytvoření rel. klíče K s Bobem pomocí (1) a (2)
- 2 $A \rightarrow B: \{X\}_K$ - požadavek (např. zaslání peněz)
 - Oskar - odposlech
- 3 $O \rightarrow B: \{X\}_K$ - opětovné zasílání stejného požadavku, tzv. replay attack (přehrávka)

Autentizace pomocí třetí strany

Možnosti obrany

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Autentizace

pomocí
tajemství
heslo

výzva -
odpověď

pomocí
fyzického
objektu

pomocí
biometrických
informací

Autentizační protokoly

- vložení časových razítek do každé zprávy T_A
 - “stará” zpráva → nepoužití
 - problém se synchronizací hodin v síti → platnost razítek (možnost zneužití útočníkem v době platnosti)
- vložení “noncí”
 - potřeba zapamatování všech předchozích noncí; stará nonce → odmítnutí
 - problém se zapamatováním
- adaptace protokolu výzva-odpověď pro více stran - nejlepší



Mihir Bellare and Phillip Rogaway,

“Random oracles are practical: A paradigm for designing
efficient protocols,”

1993, pp. 62–73, ACM Press.