Bezpečnost v informačních technologiích (KIV/BIT)

6. Problém distribuce klíče, transport a dohadování klíče

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

25. března 2015

Obsah

Problém distribuce klíče

- zasílání šifrované zprávy, nutnost klíče pro rozluštění
- předání klíče:
  - osobně (bezpečné, nepraktické a většinou není možné)
  - bezpečný kanál (kurýr, apod.; ne vždy je k dispozici nebo není praktický
    - **př.** banka se stovkami poboček, případně nutnost denních (nebo častějších) změn klíče)
- $\rightarrow$ distribuce klíče často nejslabším článkem mnoha systémů
- ideální:
  - možnost distribuce klíče přímo příslušným komunikačním kanálem (sítí)

Metoda kryptogramů

- Merkle 1974 (publikováno 1978) "Merkle puzzle scheme"
- $A \rightarrow B$:
  - vytvoření velkého počtu kryptogramů (puzzle) tak, aby adresát mohl jeden vyřešit s přiměřeným množstvím operací (hrubou silou)
  - zaslání všech kryptogramů adresátovi
- $B \rightarrow A$
  - volba jednoho kryptogramu náhodně
  - vyřešení hrubou silou (obsaženo **id. kryptogramu + klíč**)
  - zaslání zpět čísla kryptogramu (obě strany teď mají společný klíč)
- $\rightarrow$ možnost šifrované komunikace
- složitá úloha útočníka: potřeba vyřešení **všech** kryptogramů hrubou silou
- vzhledem k dostupným kryptografickým standardům dnes nedostatečné

Metoda kryptogramů - složitost

- $m =$ počet kryptogramů
- $n =$ počet operací pro vyřešení kryptogramu
- $\rightarrow$ složitost pro adresáta: $O(n)$
- $\rightarrow$ složitost pro útočníka: $O(m * n)$
  - $m \approx n \rightarrow$ útočník: $O(n^2) \times$ adresát: $O(n)$
- m a n výběr tak, aby výpočet ještě možný u adresáta $\times$ nemožný pro útočníka

Metoda kryptogramů - příklad

- **Alice**: vytvoření 2^{25} kryptogramů, zašifrování 25 bit. klíčem zprávu:
  - "Kryptogram č. N, klíč zprávy je K"
- **Bob**: náhodný výběr jednoho kryptogramu, rozluštění hrubou silou, zaslání $\rightarrow$ Alice: číslo kryptogramu N + zpráva zašifrovaná klíčem K:
  - $N, C = E_K(P)$
  - potřeba 2^{25} operací na rozluštění kryptogramu
- **Oskar**: potřeba 2^{50} (tj. $n^2 \times n$) operací
- Bob i Oskar stejný výpočetní výkon $\rightarrow$ 10 min $\times$ cca 1 rok

Transport a dohadování klíče

Problém

- Dva uživatelé sítě (Alice a Bob) potřeba bezpečné komunikace
- Jak si spolu vymění tajný klíč a bude zajištěno, že hovoří opravdu s tím, s kým chtějí a ne s útočníkem?

Skupina protokolů

- kombinace autentizace uživatele + výměna klíče pro komunikaci
- (většinou) využití důvěryhodného serveru (**K**ey **D**istribution **C**enter), který sdílí tajný klíč s každým tazatelem o spojení (před začátkem protokolu)
- předchozí přednáška???

Rozdělení bezpečnostních protokolů
(pro autentizaci a transport a dohadování klíče)

- symetrické
  - Wide-Mouth Frog Protocol
  - Needham-Schroeder Protocol
  - Otway-Rees Protocol
  - Kerberos Protocol
- asymetrické
  - Diffie-Hellman (D-H) Protocol
- s nulovou znalostí
  - Protokol založený na obtížnosti hledání Hamiltonových kružnic v grafu

Termíny

- A a B: identifikátory subjektů A (**A**lice) a B (**B**ob), které chtějí komunikovat
- S: důvěryhodný **S**erver (KDC)
- K_{AS}, (K_{BS}): symetrický klíč, znají pouze subjekty: A a S (resp. B a S).
- N_A a N_B: "nonce" (=náhodně generované hodnoty subjekty A a B)
- K_{AB}: symetrický generovaný klíč pro spojení mezi A a B
- I: identifikátor spojení
- T: časové razítko (Timestamp)
- L: doba života (Lifetime)

Útoky na bezpečnostní protokoly

Odposlouchávání:

- komunikace mezi A a B odposlouchávána útočníkem O
- pasivní útok

Podvržení identity:

- útočník O - vytvoření zprávy s falešnou identitou předstírajíc, že je A
- případně O předstírání, že je B, který obdržel zprávu od A
- aktivní $\rightarrow$ větší nebezpečí (násl. také)

Modifikace zprávy:

- útočník O - odposlech zprávy od A, modifikace a přeposlání $\rightarrow B$
- A i B si myslí, že komunikují přímo jeden s druhým

Přerušení komunikace:

- O - zničení (příp. znepřístupnění) přenášené zprávy

Útoky na bezpečnostní protokoly

Útok přehráním (Replay attack):

- zřejme nejběžnější typ útoku na bezpečnostní protokoly
- založen na odposlouchávání a ukládání komunikace
- takto získaná data použita pro podvržení identity útočníka vůči některému ze subjektů
- vzdálený subjekt - žádnou možnost ověřit aktuálnost zprávy
- řešení: vkládání noncí příp. časových razítek do zprávy

Útok ze středu (Man-in-the-middle):

- O mezi komunikujícími subjekty A a B
- navázání komunikace s oběma, vydávání se za jednoho z nich
- využití odposlechnuté komunikace
  - pro A se O jeví jako B a naopak

Wide-Mouth Frog Protocol

- návrh: Michael Burrows v r. 1989 [1]
- zřejmě nejjednodušší
- zajištění *autentizace* subjektů a *distribuce* klíče pro společnou komunikaci
- *tvůrcem klíče - jeden ze subjektů*
- distribuce klíče přes důvěryhodný server
- *klíče s omezenou dobou platnosti*

Wide-Mouth Frog Protocol

1. $A \rightarrow S$: $A, \{T_A, B, K_{AB}\}_{K_{AS}}$:
   - Alice vytvoří zprávu (vloženo časové razítko, id Boba a náhodně vygenerovaný klíč spojení K_{AB}), zašifruje sdíleným klíčem se severem, přidá své id a pošle na server
2. $S \rightarrow B$: $\{T_S, A, K_{AB}\}_{K_{BS}}$:
   - Server rozluští, vloží nové časové razítko a id Alice, zašifruje klíčem sdíleným s Bobem a pošle Bobovi
   - Bob rozluští svým klíčem, získá id Alice a relační klíč, komunikace může začít

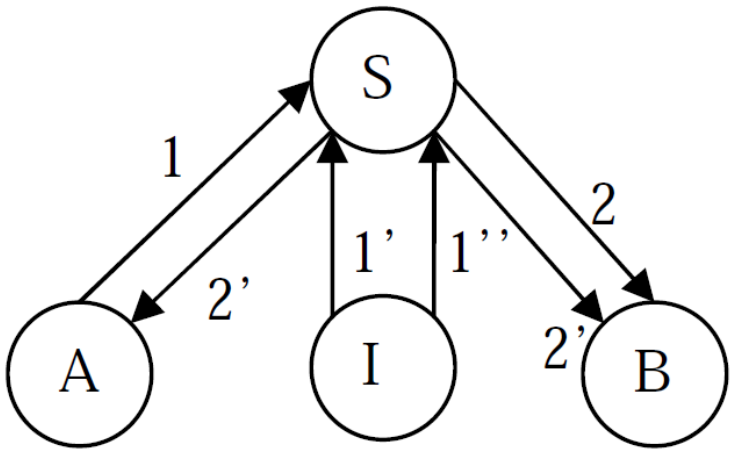
Problémy

- nutnost použití globálních synchronizačních hodin
- KDC k dispozici všechny klíče $\rightarrow$ možnost prozrazení
- **hodnota relačního klíče je zcela na navazovateli spojení (Alice)** $\leftrightarrow$ dostatečná spolehlivost

Wide-Mouth Frog Protocol - útok

- Gavin Lowe (1997) [2]

1. $A \rightarrow S$: $A, \{T_A, B, K_{AB}\}_{K_{AS}}$
2. $S \rightarrow B$: $\{T_S, A, K_{AB}\}_{K_{BS}}$
1. $O_B \rightarrow S$: $B, \{T_S, A, K_{AB}\}_{K_{BS}}$
2. $S \rightarrow A$: $\{T'_S, B, K_{AB}\}_{K_{AS}}$
1. $O_A \rightarrow S$: $A, \{T'_S, B, K_{AB}\}_{K_{AS}}$
2. $S \rightarrow B$: $\{T''_S, A, K_{AB}\}_{K_{BS}}$



- Oskar: odposlech komunikace
- možnost přeposílání přijatých zpráv (vydávajíc se za Alici nebo Boba)
- server prodlužuje platnost čas. razítka T

Needham-Schroederův symetrický protokol [3]

- 1978 - Roger Needham a Michael Schroeder
- pro poskytnutí klíčů +
- vzájemná autentizaci subjektů pomocí důvěryhodného serveru (KDC=Key Distribution Center)
- zajímavý zejména z historických důvodů → základem mnoha autentizačních protokolů a protokolů pro distribuci klíčů
- × není bezpečný → nedoporučuje se pro praktické použití

Needham-Schroederův symetrický protokol - popis

1. $A \rightarrow S$: $\{A, B, N_A\}$: Alice chce komunikovat s Bobem, pošle na server svůj a Bobův id + vygenerovanou nonci
2. $S \rightarrow A$: $\{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$: server S vygeneruje klíč spojení mezi Alicí a Bobem K_{AB} a pošle zpět kopii zašifrovanou klíčem K_{BS} pro Boba, celá zpráva je pro Alici zašifrována klíčem K_{AS}
3. $A \rightarrow B$: $\{K_{AB}, A\}_{K_{BS}}$:
   - Alice rozšifruje, zkontroluje nonci N_A - zda je její zpráva nebo replay
   - dále zkontroluje $B \rightarrow$ zjistí, zda Oskar (útočník) zprávu (1) nezachytil a nenahradil v ní B vlastní identitou (KDC by tak vyrobilo "tiket" pro Oskara)
   - OK $\rightarrow$ pošle tiket s klíčem relace Bobovi (zašifrováno klíčem K_{BS})
4. $B \rightarrow A$: $\{N_B\}_{K_{AB}}$: Bob pošle svojí nonci zašifrovanou relačním klíčem K_{AB}.
5. $A \rightarrow B$: $\{N_B - 1\}_{K_{AB}}$: Alice pošle zpět $N_B - 1$, čímž Bob ověří, že komunikuje s Alicí a že nejde o podvrh

Needham-Schroederův symetrický protokol - útok

- slabost: zjištění starého relačního klíče K_{AB} Oskarem $\rightarrow$ možnost vytvoření nové relace s Bobem přehráním zprávy (3), tzv. "replay útok":
  3. $O \rightarrow B$: $\{K_{AB}, A\}_{K_{BS}}$: Oskar pošle Bobovi relační klíč + id. Alice
  4. $B \rightarrow A$: $\{N_B\}_{K_{AB}}$: Bob zjistí K_{AB}, vytvoří nonci N_B a pošle ji Alici zašifrovanou relačním klíčem
  5. $O \rightarrow B$: $\{N_B - 1\}_{K_{AB}}$: Oskar zachytí a rozluští zprávu a pošle Bobovi upravenou nonci
  6. Bob zkontroluje, že je nonce OK a věří, že mluví s Alicí
- $\rightarrow$ opraveno v r. 1987 $\rightarrow$ Otway-Reesův protokol - viz dále
- základem protokolu Kerberos

Otway-Reesův protokol

- symetrický protokol

1. $A \rightarrow B$: $I, A, B, \{N_A, I, A, B\}_{K_{AS}}$
2. $B \rightarrow S$: $I, A, B, \{N_A, I, A, B\}_{K_{AS}}, \{N_B, I, A, B\}_{K_{BS}}$
3. $S \rightarrow B$: $I, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
4. $B \rightarrow A$: $I, \{N_A, K_{AB}\}_{K_{AS}}$

- Nutno, aby identifikátor relace I a obě nonce N_A i N_B nebyly v průběhu navazování spojení změněny.

Otway-Reesův protokol - útok

- John Clark and Jeremy Jacob [4]

1. $A \rightarrow B, \mathbf{O}$: $I, A, B, \{N_A, I, A, B\}_{K_{AS}}$
2. $B \rightarrow S$: $I, A, B, \{N_A, I, A, B\}_{K_{AS}}, \{N_B, I, A, B\}_{K_{BS}}$
3. $S \rightarrow B$: $I, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
4. $\mathbf{O} \rightarrow A$: $I, \{N_A, I, A, B\}_{K_{AS}}$

- Oskar zachytí zprávu (1), v kroku (4) pošle zprávu odvozenou ze zachycené zprávy
- hodnoty I, A a $B \rightarrow$ nový klíč K_{AB}

Protokol Kerberos

- varianta Needham-Schroedenova protokolu, doplnění časových razítek (doporučení Denningové a Sacca [5])
- použití v mnoha reálných systémech, např. Orion
- předpoklad, že všechny časy jsou synchronizovány s KDC

Protokol Kerberos - princip

Značení (připomenutí)

- T: časové razítko (Timestamp)
- L: doba života (Lifetime)

Princip

1. $A \rightarrow S$: $\{A, B\}$
2. $S \rightarrow A$: $\{T, L, K_{AB}, B\}_{K_{AS}}, \{T, L, K_{AB}, A\}_{K_{BS}}$
3. $A \rightarrow B$: $\{A, T\}_{K_{AB}}, \{T, L, K_{AB}, A\}_{K_{BS}}$
4. $B \rightarrow A$: $\{T + 1\}_{K_{AB}}$

- (3) Alice, zkontrolovat, zda $B = B$
- (4) Bob, zkontrolovat, zda jsou obě A ve zprávě shodné

Diffie-Hellman (D-H) Protocol

- zveřejnění: 1976 - Whitfield Diffie a Martin Hellman
- první autor: Malcolm Williamson z tajné vládní instituce Government Communications HeadQuatrters z V. Británie - několik let dříve
  - utajení až do r. 1977 - dále už nemělo vliv
- vytvoření **šifrovaného spojení** mezi komunikujícími stranami přes nazabezpečený kanál bez předchozí dohody šifrovacího klíče
- + útočník odposlouchávající komunikaci - nezachycení klíče (← zkonstruován všemi účastníky komunikace a nikdy není poslán v otevřené formě)
- − bezbrannost proti útoku "Man in the middle"

Diffie-Hellman (D-H) Protocol

1. A, B: dohoda dvou velkých prvočísel p a α:
   - $(p-1)/2$ - prvočíslo
   - $2 \leq \alpha \leq p-2$
   - p a α nemusí být tajná $\rightarrow$ možnost volby a zaslání druhé straně otevř. kanálem
2. $A \rightarrow B$: volba x (náhodné tajné číslo), zaslání $\alpha^x \, mod \, p$
   - $1 \leq x \leq p-2$
3. $B \rightarrow A$: volba y (náhodné tajné číslo), zaslání $\alpha^y \, mod \, p$
   - $1 \leq y \leq p-2$
4. A: příjem $\alpha^y \, mod \, p$; výpočet tajného klíče $k = (\alpha^y)^x \, mod \, p$
5. B: příjem $\alpha^x \, mod \, p$; výpočet tajného klíče $k = (\alpha^x)^y \, mod \, p$

Diffie-Hellman (D-H) Protocol - bezpečnost

- útočník O - odposlech:
  - (1) znalost p a α
  - (2) znalost $\alpha^x \, mod \, p$
  - (3) znalost $\alpha^y \, mod \, p$
- pro výpočet tajného klíče $(\alpha^y)^x \, mod \, p$ potřeba x a y
- určení x z $\alpha^x \, mod \, p$ - **velmi obtížný problém**
  - příp. y z $\alpha^y \, mod \, p$

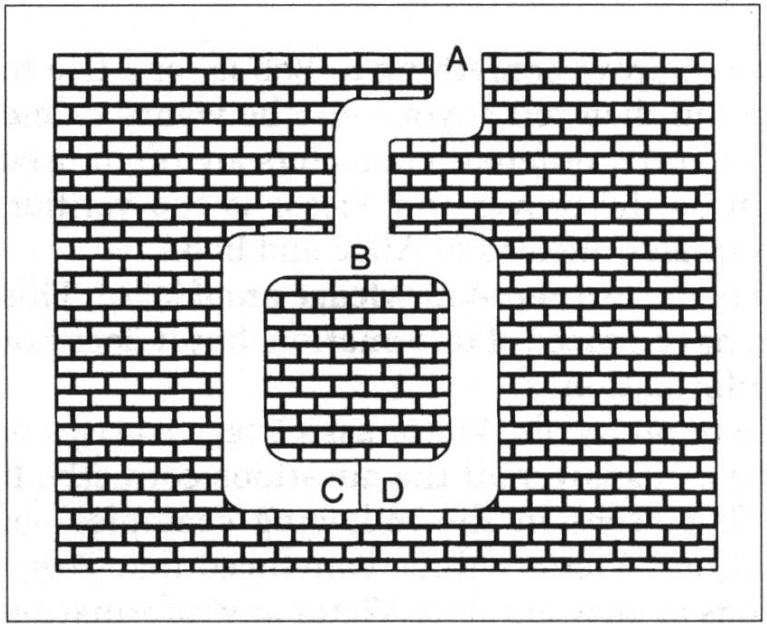
D-H Protocol - útok "Man-in-the-middle"

- $O \rightarrow B$: přijetí zprávy (2)
  - nahrazení $\alpha^x \rightarrow \alpha^{x'}$
- $O \rightarrow A$: přijetí zprávy (3)
  - nahrazení $\alpha^y \rightarrow \alpha^{y'}$
- skončení protokolu:
  - $A \leftrightarrow O$: klíč $\alpha^{xy'}$
  - $B \leftrightarrow O$: klíč $\alpha^{x'y}$
- A, B: komunikace prostřednictvím O

Protokoly s nulovou znalostí
Zero Knowledge (ZK) Identification Protocols

- symetrické protokoly, požadavek sdíleného tajného klíče s KDC
- problém: vyzrazení klíče třetí straně, ta se potom může vydávat za nás (Alici, či Boba)
- $\rightarrow$ návrh protokolů s nulovou znalostí, Zero Knowledge (ZK) Identification Protocols
- bez šifrování, sekvenčních čísel ani časových razítek
- Demonstrace znalosti nějakého tajemství, aniž by ho ověřovatel mohl zjistit a předat dalším

Ukázka na příběhu o jeskyni
jednoduchý příklad [6]



- Jen ten, kdo zná tajné heslo umí otevřít dveře mezi místy C a D
- Alice zná tajné heslo. Chce tuto znalost prokázat Bobovi bez vyzrazení tajného hesla. Jak provést?

Ukázka na příběhu o jeskyni - jednoduchý příklad - řešení

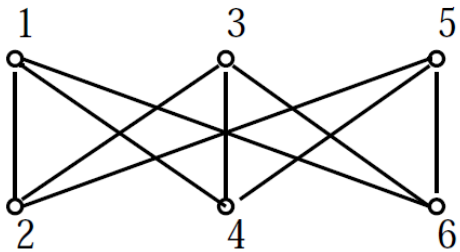
1. Bob: u bodu A
2. Alice: jde do jeskyně, zastavení u bodu C nebo D
3. Bob: po té, co Alice zmizí v jeskyni, jde k bodu B
4. Bob: zavolá na Alici:
   - vrať se levou cestou
   - (případně) vrať se pravou cestou
5. Alice: vyhoví. Použití tajného hesla, pokud je potřeba.
6. opakování kroků (1-5) n krát

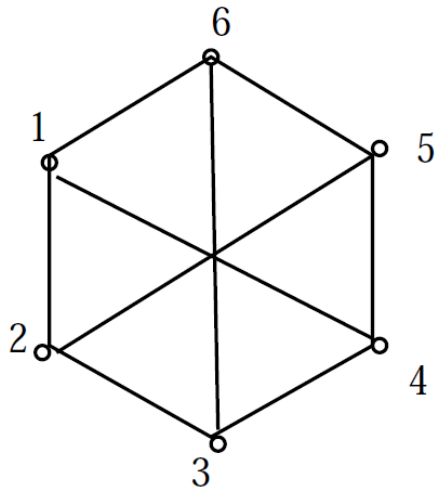
- nemožnost přesvědčení třetí strany o pravosti důkazu
- jde opravdu o protokol s nulovou znalostí
- pravděpodobnost, že Alice švindluje je $\frac{1}{2^n}$, kde $n =$ počet iterací

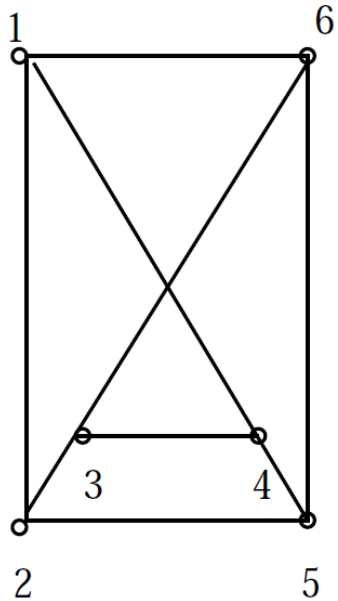
Protokol založený na obtížnosti hledání Hamiltonových kružnic v grafu [7]

Zero Knowledge (ZK) Identification Protocols

- Hamiltonova kružnice = neorientovaná uzavřená cesta, která prochází každým vrcholem grafu právě jednou
- hledání H. kružnic v grafu - velmi složité
- rozhodnutí, zda jsou dva grafy G a H jsou izomorfní - také velmi složité (viz násl. grafy)?







Protokol založený na obtížnosti hledání Hamiltonovských kružnic v grafu

Zero Knowledge (ZK) Identification Protocols

- Alice: tvorba grafu G s Hamiltonovskou kružnicí, předání grafu G $\rightarrow$ Bob
- Bob: znalost pouze G (neznalost H. kružnice)
- Alice: snaha autentizace pomocí znalosti H. kružnice bez jejího prozrazení

Jak? (řešení zjednodušeno)

1. Alice: vytvoření grafu H - izomorfní k G pomocí náhodné permutace, graf H $\rightarrow$ Bob
2. Bob: žádost o důkaz:
   - důkaz, že H je izomorfní ke G
   - ukázání Hemiltonovy kružnice
3. Alice: zaslání požadované odpovědi
4. jdi na krok (1); (po n iteracích je pravděpodobnost, že Alice podvádí $(\frac{1}{2})^n$)

 Michael Burrows, Martin Abadi, and Roger Needham, "A logic of authentication," *ACM Transaction on Computer Systems*, vol. 8, pp. 18–36, February 1990.

 Gavin Lowe, "A family of attacks upon authentication protocols," Tech. Rep., University of Leicester, 1997.

 R. Needham and M. Schroeder, "Using encryption for authentification in large networks of computers," *Communications of the ACM*, vol. 12, no. 21, December 1978.

 John Clark and Jeremy Jacob,

"A survey of authentication protocol literature: Version 1.0," 1997.

D. Denning and G. Sacco,
"Timestamps in key distributed protocols,"
Communication of the ACM, vol. 8, no. 24, pp. 533–535, 1981.

J J Quisquater, L C Guillou, M Annick, and T A Berson,
How to explain zero-knowledge protocols to your children, vol. 435, pp. 628–631,
Springer-Verlag, 1990.

M. Blum,
"How to prove a theorem so no one else can claim it,"
in *Proceedings of the International Congress of Mathematicians*, Berkeley, California, 1986, pp. 1444–1451.