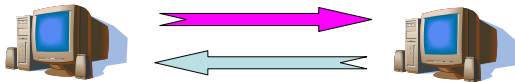


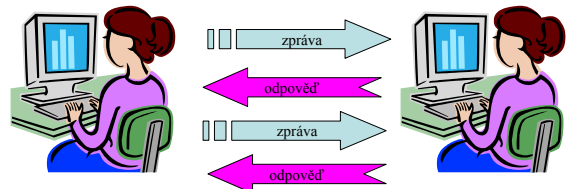
PV157 – Autentizace a řízení přístupu

Autentizační protokoly



Protokol

- Protokol je několikastranný algoritmus definovaný posloupností kroků, které specifikují akce prováděné dvěma a více stranami, pro dosažení určitého cíle



Kryptografické protokoly

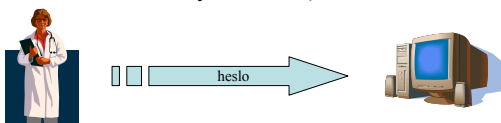
- **Autentizační protokol** – zajistí jedné straně určitou míru jistoty o identitě jiné strany (té, se kterou komunikuje)
- **Protokol pro ustavení klíče** (key establishment protocol) – ustaví sdílené tajemství (typicky klíč)
- **Autentizovaný protokol pro ustavení klíče** (authenticated key establishment protocol) – ustaví sdílené tajemství se stranou, jejíž identita byla potvrzena

Autentizační protokoly

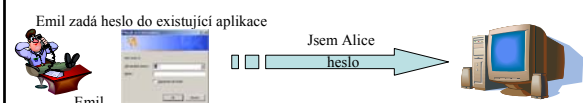
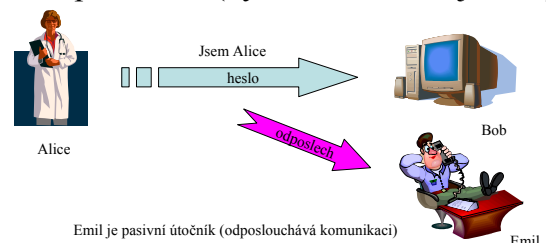
- Během protokolu autentizujeme:
 - Pouze jednu ze stran
 - Obě strany
 - Kontinuální autentizace
- Kdo koho autentizuje
 - Alice vyzývá Boba, aby se autentizoval
 - Bob se autentizuje rovnou sám bez výzvy

Autentizace heslem

- Alice se autentizuje Bobovi tak, že mu pošle své heslo
- Heslo je možné odposlechnout
- Bob po úspěšné Alicině autentizaci zná Alicino heslo a může se (např. vůči Cyrilovi) autentizovat jako Alice (pokud Alice používá stejné heslo pro autentizace vůči různým stranám)

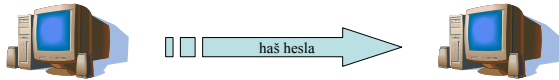


Útok impersonací (vydáváním se za jiného)

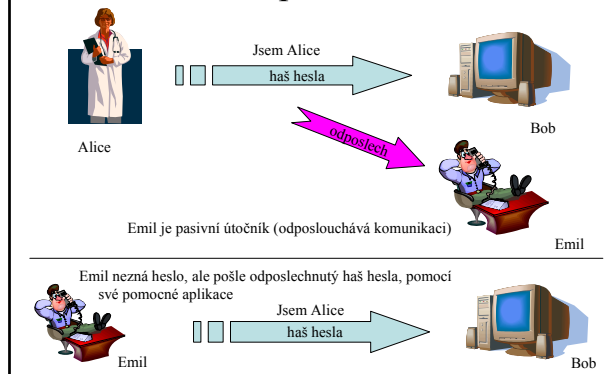


Hašované heslo

- Při autentizaci se neposílá heslo samotné, ale pouze haš hesla
- Kdo odposlechne haš nezíská automaticky heslo
- Haš však lze použít pro podvodnou autentizaci



Útok přehráním

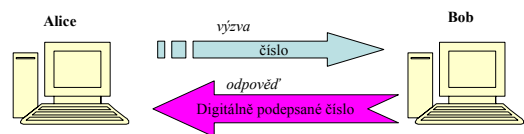


Další útoky na protokoly

- Zmíněné útoky impersonací a přehráním
- Úplný výčet je nesnadný, ale zmínit je třeba
 - útoky **prolínáním** (interleaving) – kombinujeme zprávy z více průběhů – obvykle, ale ne nutně jen, stejného protokolu – ať již ukončených, nebo právě probíhajících
 - **slovníkové** útoky – na protokoly využívající hesla, diskutováno později u autentizace uživatelů
 - útoky **využitím známého klíče** (known-key) – obvykle u protokolů pro ustanovení klíče, kde se klíč ustanoví na základě staršího/ch (útočníkovi známého/ch) klíče/ů

Protokoly výzva-odpověď

- Protokoly typu výzva-odpověď (challenge-response)
 - Odposlechem výzvy i odpovědi útočník moc nezíská
 - Bob se může přesvědčit o identitě Alice, bez získání jejího tajemství



Časově proměnné parametry

- **Náhodná čísla** (random numbers) – čísla, která jsou nepredikovatelná (v tomto kontextu zahrnujeme pod náhodná čísla i čísla pseudonáhodná). Použitím náhodných čísel zajišťujeme jedinečnost a „aktuálnost/čerstvost“. Získat skutečně náhodná čísla je netriviální (vyžaduje speciální HW zařízení). V praxi obvykle používáme pseudonáhodná čísla (které na základě tajného stavu - semínka (seed) generují sekvence čísel). Značíme **r**.
- **Sekvence** (sequence numbers) – monotonně rostoucí posloupnost čísel (obě strany musí dlouhodobě uchovávat informaci o poslední hodnotě). Jednoznačně identifikují zprávy a umožňují detekovat útoky přehráním předchozí komunikace. Značíme **n**.
- **Časová razítka** (timestamps) – obě strany musí synchronizovat a zabezpečit hodiny. Zajišťují jedinečnost a časovou přesnost. Značíme **t**.

Protokoly výzva-odpověď

- Založené na symetrických technikách
 - Symetrické šifrování
 - Jednosměrná funkce s klíčem
 - Generátory passcode
- Založené na asymetrických technikách
 - Dešifrování
 - Digitální podpis

Symetrické techniky

- Založené na symetrickém šifrování (Alice a Bob sdílí tajný symetrický klíč **K**)
- Standard ISO/IEC 9798-2
- Jednostranná autentizace (časové razítko)
 - $A \rightarrow B: E_K(t_A, "B")$
- Možné útoky
 - Útok přehráním: odposlechnu $E_K(t_A, "B")$ a pošlu jej rychle znovu (v době platnosti t_A)
 - Změna hodin: odposlechnu $E_K(t_A, "B")$, později změním hodiny B tak, aby odpovídaly času t_A a znovu pošlu $E_K(t_A, "B")$

Symetrické techniky

- Jednostranná autentizace (náhodné číslo)
 - $A \leftarrow B: r_B$
 - $A \rightarrow B: E_K(r_B, "B")$
- Možné útoky
 - Útočník odposlouchává a ukládá $[r_B, E_K(r_B, "B")]$, pokud se challenge r_B opakuje, pak je schopen poslat správný response. Případně se může aktivně snažit ovlivnit vytváření náhodných r_B (např. ovlivněním vstupu generátoru náhodných čísel Boba).
- Oboustranná autentizace (náhodná čísla)
 - $A \leftarrow B: r_B$
 - $A \rightarrow B: E_K(r_A, r_B, "B")$
 - $A \leftarrow B: E_K(r_B, r_A)$

Symetrické techniky

- Založené na klíčovaných jednosměrných funkcích (Alice a Bob sdílí tajný symetrický klíč **K**)
- Standard ISO/IEC 9798-4, protokoly SKID
- Oboustranná autentizace
 - $A \leftarrow B: r_B$
 - $A \rightarrow B: r_A, h_K(r_A, r_B, "B")$
 - $A \leftarrow B: h_K(r_B, r_A, "A")$
 - h_K je MAC algoritmus

Symetrické techniky

- Generátory passcode – hand-held (PDA, kapesní počítače) pro bezpečné uložení dlouhodobých klíčů doplněné zadáním PINu uživatele
- Subjekty A, B sdílí tajný klíč s_A a tajný PIN p_A
 - $A \leftarrow B: r_B$
 - subjekt A zadá do generátoru přijatou výzvu r_B a vloží svůj PIN
 - $A \rightarrow B: f(r_B, s_A, p_A)$



Asymetrické techniky

- Založené na dešifrování soukromým klíčem
- Jednostranná autentizace
 - $A \leftarrow B: h(r), "B", P_A(r, "B")$
 - $A \rightarrow B: r$
- h – hašovací funkce
- $h(r)$ slouží k prokázání znalosti r bez jeho odhalení

Asymetrické techniky

- Založené na digitálním podpisu
- Standard ISO/IEC 9798-3
- Jednostranná autentizace (časové razítko)
 - $A \rightarrow B: cert_A, t_A, "B", S_A(t_A, "B")$
- Možné útoky
 - Útok přehráním: odposlechnu $S_A(t_A, "B")$ a pošlu jej rychle znovu (v době platnosti t_A)
 - Změna hodin: odposlechnu $S_A(t_A, "B")$, později změním hodiny B tak, aby odpovídaly času t_A a znovu pošlu $S_A(t_A, "B")$

Asymetrické techniky

- Jednostranná autentizace (náhodné číslo)
 - $A \leftarrow B: r_B$
 - $A \rightarrow B: cert_A, r_A, "B", S_A(r_A, r_B, "B")$
 - r_A zde zabraňuje útokům s vybraným textem
- Možné útoky
 - Obdobné útoky na náhodné r_B jako v případě symetrických technik
- Oboustranná autentizace (náhodná čísla)
 - $A \leftarrow B: r_B$
 - $A \rightarrow B: cert_A, r_A, "B", S_A(r_A, r_B, "B")$
 - $A \leftarrow B: cert_B, "A", S_B(r_B, r_A, "A")$

Protokoly pro mgmt klíčů

- Účel
 - Přenos klíče
 - Ustavení klíče
 - Aktualizace klíče (strany sdílí dlouhodobý klíč **K**)
 - Zároveň i autentizace jedné nebo obou stran
- Počet stran
 - Protokol pro dvě strany
 - Protokol s důvěryhodnou třetí stranou

Symetrické techniky přenosu klíče

- Aktualizace klíče založená na symetrické šifře (Alice a Bob sdílí tajný klíč **K**)
 - Přenos klíče (1 zpráva, časové razítko)
 - $A \rightarrow B: E_K(r_A, t_A, "B")$
 - Přenos klíče (výzva-odpověď, náhodné nebo sekvenční číslo)
 - $A \leftarrow B: n_B$
 - $A \rightarrow B: E_K(r_A, n_B, "B")$

Symetrické techniky přenosu klíče

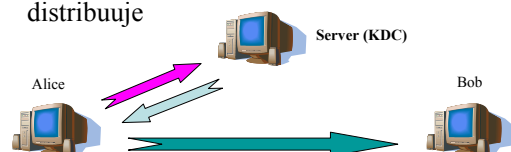
- Přenos klíče odvozením
 - $A \rightarrow B: r_A$
 - Nový klíč $W = E_K(r_A)$
- Aktualizace klíče se vzájemnou autentizací
 - AKEP2 (Authenticated Key Exchange Protocol 2)
 - $A \rightarrow B: r_A$
 - $A \leftarrow B: ("B", "A", r_A, r_B), h_K("B", "A", r_A, r_B)$
 - $A \rightarrow B: ("A", r_B), h_K("A", r_B)$
 - Nový klíč $W = h'_K(r_B)$
 - h_K je MAC algoritmus, h' je MAC algoritmus (odlišný od h), obě strany sdílí K , z K je odvozen K'

Symetrické techniky přenosu klíče

- Přenos klíče bez předchozího sdíleného tajemství
 - Shamirův protokol bez klíčů (Shamir's no-key protocol)
 - Komutativní symetrická šifra E
 - Každá strana má svůj symetrický klíč K_A, K_B
 - $A \rightarrow B: E_{K_A}(X)$
 - $A \leftarrow B: E_{K_B}(E_{K_A}(X))$
 - $A \rightarrow B: E_{K_B}(X)$
 - Nyní obě strany sdílí X ; byly nutné 3 zprávy

Kerberos

- **KDC** (key distribution center) – server sdílí klíč s každým klientem; (klienti však mezi sebou klíče nesdílí); distribuuje klíče, které generuje.
- **KTC** (key translation center) – server negeneruje klíče sám; klíč dodá jedna ze stran; server klíč distribuuje



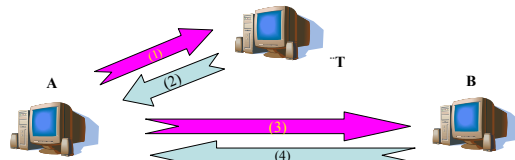
Kerberos

- Vznikl při projektu Athena na MIT
- Symetrická šifra E
- 2 strany (A, B) a důvěryhodný autentizační server (značíme T)
- Cíl:
 - autentizace subjektu A vůči B
 - ustavení klíče k (zvolí T)
 - případně distribuce tajemství sdíleného A a B
- Každá strana sdílí tajemství se serverem K_{AT}, K_{BT}



Kerberos

- Zjednodušená verze protokolu
 - L – doba platnosti („lifetime“)
 - Def.: $\text{ticket}_B = E_{K_{BT}}(k, \text{“A”}, L)$, $\text{auth} = E_k(\text{“A”}, T_A)$
 - (1) $A \rightarrow T: \text{“A”}, \text{“B”}, n_A$
 - (2) $A \leftarrow T: \text{ticket}_B, E_{K_{AT}}(k, n_A, L, \text{“B”})$
 - (3) $A \rightarrow B: \text{ticket}_B, \text{auth}$
 - (4) $A \leftarrow B: E_k(T_A)$



Asymetrické techniky přenosu klíče

- Zašifrování podepsaných klíčů
 - $A \rightarrow B: P_B(S_A(\text{“B”}, k, t_A))$
 - (volitelné) časové razítko t_A zároveň autentizuje A vůči B
- Separátní šifrování a podpis
 - $A \rightarrow B: P_B(k, t_A), S_A(\text{“B”}, k, t_A)$
 - Pouze v případě, kdy z podpisu nelze získat podepsaná data
- Podepsání zašifrovaných klíčů
 - $A \rightarrow B: t_A, P_B(\text{“A”}, k), S_A(\text{“B”}, t_A, P_B(\text{“A”}, k))$

Asymetrické techniky přenosu klíče

- X.509 obousměrná autentizace s přenosem klíče
- Def.: $D_A = (t_A, r_A, \text{“B”}, P_B(k_1))$
 $D_B = (t_B, r_B, \text{“A”}, P_A(k_2))$
- Protokol
 - $A \rightarrow B: \text{cert}_A, D_A, S_A(D_A)$
 - $A \leftarrow B: \text{cert}_B, D_B, S_B(D_B)$

Asymetrické techniky ustavení klíče

- Diffie-Hellman protokol pro ustavení sdíleného tajemství
 - Společné prvočíslo p, generátor α v Z_p
 - A volí tajné x, B volí tajné y
 - $A \rightarrow B: \alpha^x \text{ mod } p$
 - $A \leftarrow B: \alpha^y \text{ mod } p$
 - A a B sdílí $K = \alpha^{xy} \text{ mod } p$

Otázky?

Vitány!!!

Příští přednáška 20. 10. 2004 v 18:00
Polosemestrální písemka 3. 11. 2004 v 18:00

matyas@fi.muni.cz
 zriha@fi.muni.cz