تمرین 3 امنیت.

«به نام خدا»

امیرمحمد پیرحسینلو
۹۵۳۱۰۱۴

---

(۱) اگر $ticket_{tgs}$ لو بود، attacker می‌تواند ID_c و ID_{tgs} که به‌صورت plaintext است را به‌راحتی به دست آورد پس در مرحله‌ی 3 که ($c \rightarrow tgs \quad ID_c | ID_v | ticket_{tgs}$) است خود را جای کلاینت واقعی جازده و به سرورهای مختلف به دست آورد. اما باید در workstation کلاینت واقعی حضور یابد تا ip (network address) او را داشته باشد. همچنین lifetime نباید کوتاه باشد.

---

(۲) برای آن است که کلاینت بارها و بارها پسورد خود را وارد نکند. همچنین پسورد تا نرود. (زیرا قبلاً در قالب plain text ارسال می‌کرد.)

$$\text{session key} \rightarrow E(K_c, ticket_{tgs})$$

$$ticket_{tgs} = E(K_{tgs}, (ID_c | AD_c | ID_{tgs} | TS_1 | Lifetime1))$$

---

(۳) الف) شخص O، ID خود را می‌فرستد، شخص U با کلید عمومی O یک عدد رندوم را رمزنگاری کرده و برای او می‌فرستد. در صورتی که پیام واقعاً به O رسیده باشد، O آن را رمزگشایی کرده و عدد رندوم را به دست آورد. پس عدد رندوم (R_2) را برای U می‌فرستد. اگر عدد دریافتی توسط U همان عدد رندوم تولید شده توسط U باشد، O احراز هویت می‌شود در غیر این صورت نمی‌شود.

ایراد ط: شخص A می‌تواند بین O و U قرار گیرد و عملیات روبه‌رو رخ دهد.

replay attack

$O \rightarrow A \quad ID_o$

$A \rightarrow U \quad ID_a$

$U \rightarrow A \quad E(PU_a, R_2)$

$A \rightarrow O \quad E(PU_o, R_1)$

$O \rightarrow A \quad R_1$

$A \rightarrow U \quad R_2$

---

(۳) ب) از این طریق O، احراز هویت می‌شود برای U. شخص O مقدار R_1 را با کلید خصوصی رمزنگاری برای U می‌فرستد. U هم با کلید عمومی شخص O، آن را به دست می‌آورد و مطمئن می‌شود که O، R_1 را به‌درستی دریافت کرده است.

مشکل: شخص سوم مثل C پیام‌ها را از O می‌گیرد (خود را جای U جازده و احراز هویت با O انجام می‌دهد) سپس آن‌ها را به U می‌فرستد و از U نیز پیام می‌گیرد و به O می‌فرستد. مشکل اصلی استفاده از کلید عمومی/خصوصی هم برای authentication و هم برای encryption است.

(4) راه کار: استفاده از پروتکل kerberos با تغییرات زیر:

① C → AS $ID_c | ID_{tgs}$

② AS → C $E(k_c, ticket_{tgs} | X)$ ← اضافه می‌شود

کلاینت با دریافت داده چون k_c را دارد (همان password خودش) و X و $ticket_{tgs}$ را به دست می‌آورد.

③ C → TGS $ID_c | ID_v | ticket_{tgs} | E(X | Y)$

X و Y به دست می‌آورد.

X بین TGS و AS رد و بدل شده است.

پس k_{tgs} و Y را به دست می‌آورد.

④ TGS → C $ticket_v$

Y هم بین سرور و k_{tgs} می‌تواند مبادله شود. (از طریق $ticket_v$)

⑤ C → V $ID_c | ticket_v$

⑥ C → V داده: $E(Y, داده)$

$$ticket_{tgs} = E(k_{tgs}, (ID_c | AD_c | ID_{tgs} | TS_1 | lifetime1 | X))$$

$$ticket_v = E(k_v, (ID_c | AD_c | ID_v | TS_2 | lifetime2 | Y))$$

---

(5) الف) A می‌داند که k'_{AB} با B به صورت امن share شده است زیرا عدد رندوم او در خط دوم مبادله پیام به صورت رمز شده توسط کلیدی که تنها او و B می‌دانند به او بازگشته است.

B می‌داند که k'_{AB} با A به صورت امن share شده است زیرا N_A با k'_{AB} رمز شده است و تنها به وسیله کسی که k'_{AB} را می‌داند باز می‌شود که فقط A, B آن را می‌دانند.

ب) A می‌داند که k'_{AB} تازه است (جدید است) زیرا همراه با N_A بازگشته است و پیام 2 بعد پیام 1 آمده است. B می‌داند k'_{AB} جدید است زیرا خود او آن را ساخته است.