دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

آزمایشگاه امنیت داده و شبکه
http://dnsl.ce.sharif.edu

درس ۹: کربروس

محمد صادق دوستی

فهرست

پروژه آتنا (Project Athena)

- **آتنا:** ایزدبانوی نگهبان شهر آتن
- **پروژه آتنا:** پروژه‌ای مشترک بین MIT، DEC و IBM

- **هدف:** ایجاد محیطی برای محاسبات توزیع شده.
- آغاز ۱۹۸۳، پایان تحقیق و توسعه ۱۹۹۱.
- هنوز (۲۰۱۵) هم به فعالیت ادامه می‌دهد.
- **بودجه:** ۵۰ میلیون دلار
- **محصولات اصلی:** Kerberos، سیستم X Window، پیام‌رسان Zephyr

کربروس (Kerberos یا Cerberus)

- **کربروس (Κέρβερος)**: بر گرفته از اسطوره یونانی

☜ نام سگی سه‌سر که محافظ دروازه‌های عالم مردگان بود؛ نمی‌گذاشت زندگان مزاحم ارواح شده و ارواح از عالم مردگان خارج شوند.

تاریخچه کربروس – ۱

- مبتنی بر پروتکل تصدیق هویت نیدهام–شـرودر (۱۹۷۸) و اصـلاح شده آن توسط دنینگ و ساکو (۱۹۸۱).
  - ☜ کلید متقارن؛ استفاده از KDC؛ به کارگیری برچسب زمانی.
- نسخه ۱ الی ۳ کربروس در MIT به صورت داخلی.
- نسخه ۴ در سال ۱۹۹۰ به طور رسمی منتشر شد.
  - ☜ استفاده از DES برای رمزنگاری
  - ☜ دارای محدودیتها و اشکالات امنیتی فراوان

تاریخچه کربروس – ۲

- نسخه ۵ در ۱۹۹۳ به طور رسمی منتشر شد (RFC 1510).
- تا سال ۲۰۰۰، رمزنگاری در آمریکا «سلاح» محسوب می‌شد.
  - انتشار کد کربروس به خارج از آمریکا جرم بود.
  - دانشگاه KTH سوئد با الهام از مستندات نسخه ۴، نسخه‌ای از کربروس را با عنوان eBones منتشر ساخت.
- استاندارد ۵ کربروس (RFC 1510) در سال ۲۰۰۵ تحت عنوان RFC 4120 اصلاح شد.

تاریخچه کربروس – ۳

- سایر اصلاحات کربروس در ۲۰۰۵:
  - به کارگیری روشهای متنوع رمزنگاری و صحت (RFC 3961)
  - به کارگیری AES (RFC 3962)
- در سال ۲۰۰۷، MIT کنسرسیوم کربروس را تشکیل داد.
  - شامل شرکتهایی چون اراکل، اپل، گوگل، و مایکروسافت
  - نهادهای دانشگاهی نظیر KTH، استنفورد و MIT
- مایکروسافت با توجه به استفاده از کربروس در Active Directory، چندین بهبود عمده در آن داده است.

تاریخچه کربروس – ۴

- بهبودهای مایکروسافت:
  - به روز رسانی GSS-API در RFC 4121
  - مذاکره الگوریتمهای رمز در RFC 4537
  - امکان استفاده از زیرساخت کلید عمومی در کربروس (PKIINIT) در RFC 4556
  - OCSP برای PKINIT در RFC 4557
  - الگوریتمهای RC4-HMAC برای کربروس در RFC 4757
  - رمزنگاری خم بیضوی برای PKINIT در RFC 5349

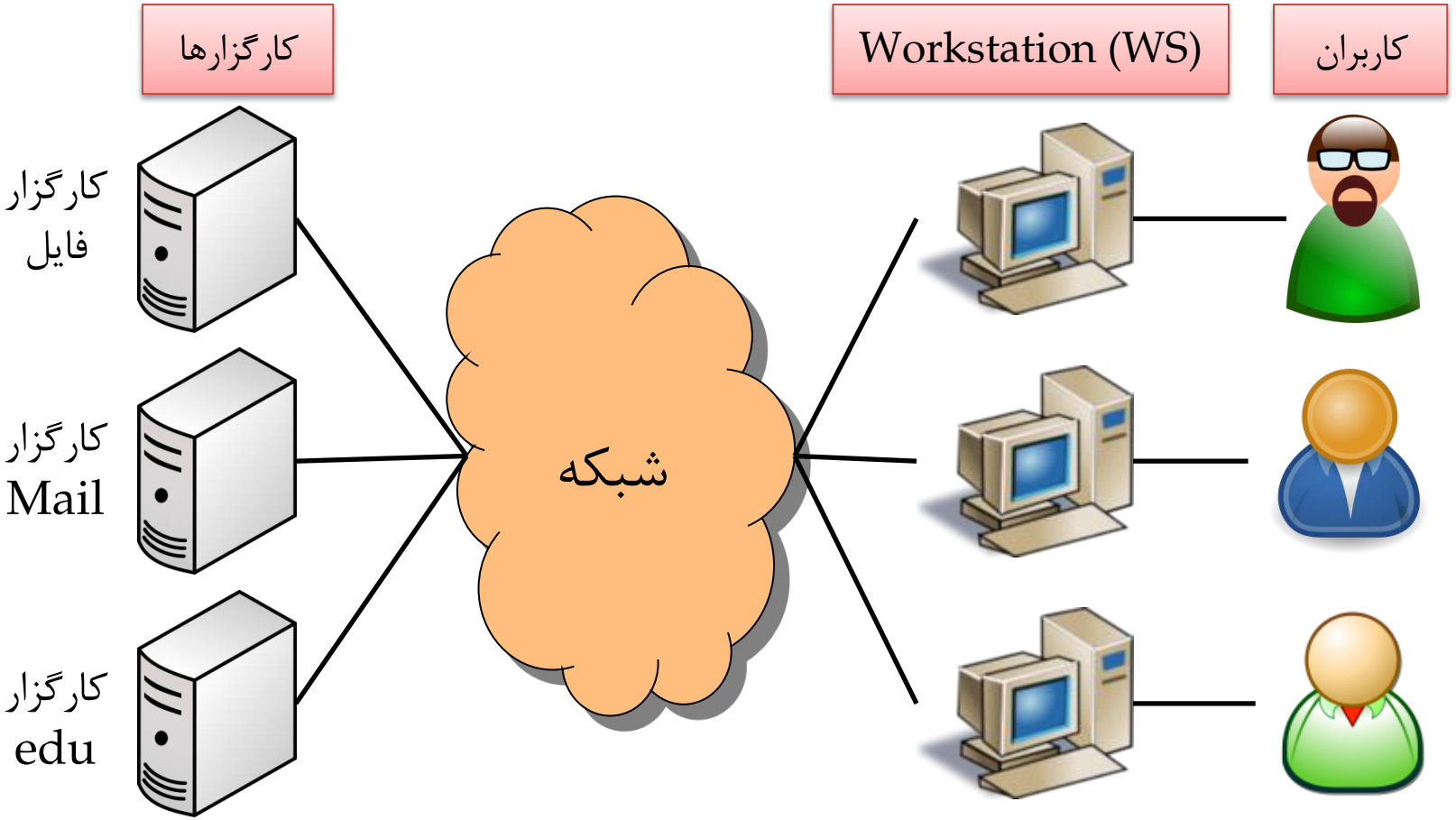
تاریخچه کربروس – ۵

- سایر بهبودهای مایکروسافت:
  - قیود جدید برای نامها در RFC 6111
  - پشتیبانی از گمنامی در RFC 6112
  - پیش-تصدیق هویت در RFC 6113
  - استاندارد سازی نامگذاری در RFC 6806
- امروزه سه پیاده‌سازی عمده از کربروس وجود دارد: MIT، هایمدال (Heimdal) و مایکروسافت (Active Directory)

فهرست

- تاریخچه
- **کربروس در سطح بالا**
- جزئیات کربروس ۵
- قلمروهای کربروس
- کربروس در امروز

تصدیق هویت در یک سیستم توزیع شده



سه روش تصدیق هویت در یک سیستم توزیع شده

۱. **اعتماد کامل به WSها:** هر WS، هویت کاربران خود را تصدیق می‌کند. هر کارگزار، بر اساس ID تصدیق شده کاربر، خدمت ارائه می‌دهد.

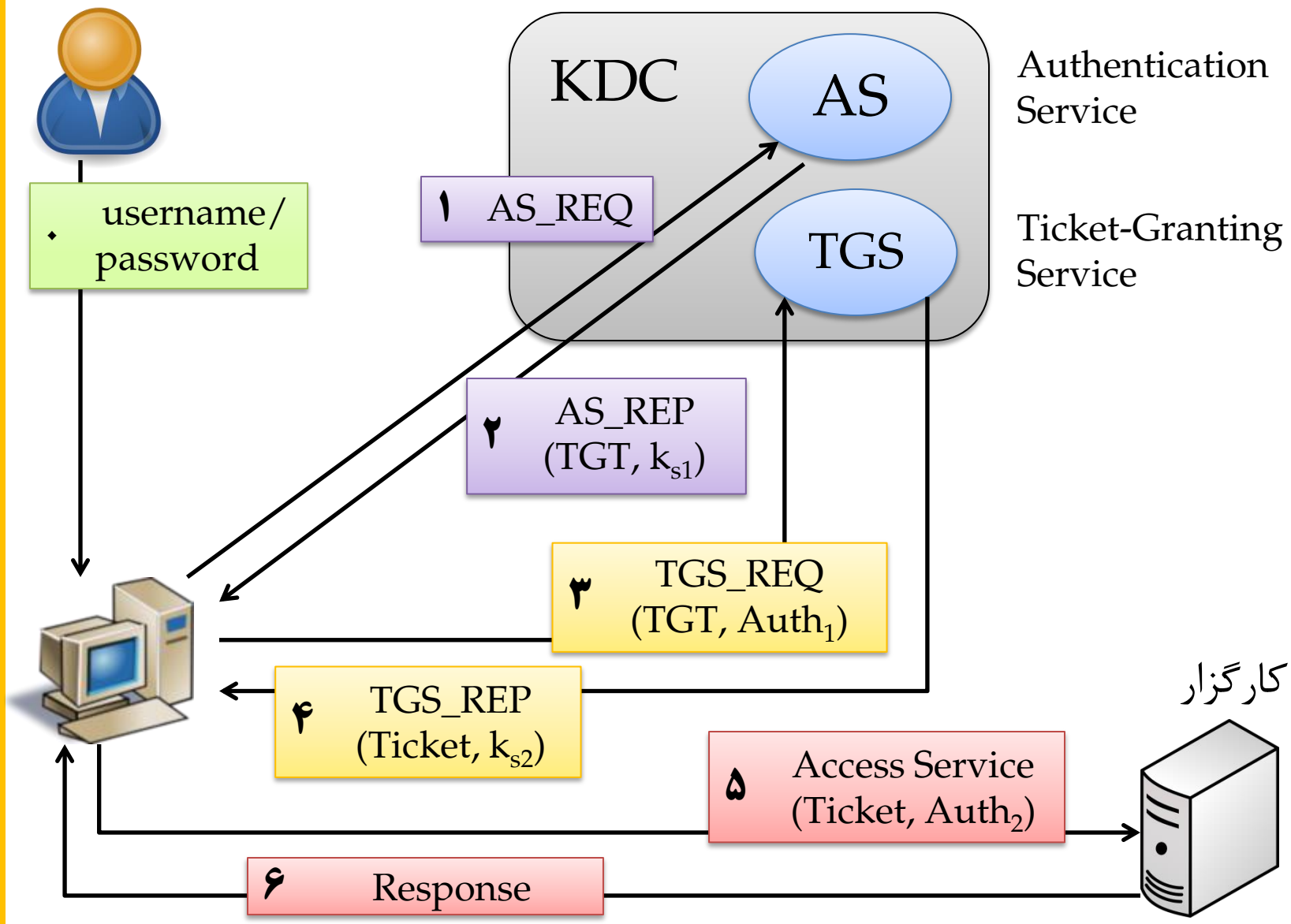
۲. **اعتماد متوسط به WSها:** هر WS خود را برای کارگزار، تصدیق هویت می‌کند. پس از آن کارگزار به تصدیق هویت کاربران توسط WSها اعتماد دارد.

۳. **کمترین اعتماد به WSها:** هرکاربر ID خود را برای سرویس، و هر سرویس ID خود را برای کاربر تصدیق نماید. WSها صرفاً نقش اجرای پروتکلها را دارند.

اهداف طراحی کربروس

- کربروس روش سوم را که امن‌تر و مناسب محیطهای بزرگ است برگزید.
- سایر اهداف:
  - **امنیت**؛ در برابر حملات فعال و منفعل
  - **اتکاپذیری**؛ نبود تک‌نقطه خرابی در سیستم
  - **شفافیت**؛ کاربر غیر از وارد نمودن نام کاربری/گذرواژه برای بار نخست، دیگر درگیر تصدیق هویت نشود. (SSO اولیه!)
  - **گسترش‌پذیری**؛ سیستم باید بتواند تعداد زیادی کاربر و کارگزار را پشتیبانی نماید.

موجودیتهای کربروس ۵ و تعامل در سطح بالا



سلسله مراتب کلیدها در کربروس ۵

- **گذرواژه:** کلید طولانی مدت به روش مشخصی (مـثلاً درهـم‌سـازی) از روی گذرواژه کاربر ساخته شده و در یـک انبـاره مرکـزی نـزد KDC نگهداری می‌شود.
  - ☜ در طول نشست، فقط یک مرتبه ورود نام کاربری / گذرواژه (SSO).
  - ☜ باید در اسرع وقت از حافظه WS پاک شود.
- **بلیت اعطای بلیت (TGT) و k_{s1}:** عمر آن برابر عمر نشست است. در طی نشست فقط یک مرتبه نیاز به دریافت آن است.
- **بلیت (اعطای سرویس) و k_{s2}:** عمر آن برابر عمـر نشسـت اسـت. در طی نشست، به ازای هر سرویس، فقط یک مرتبـه نیـاز بـه دریافـت آن است.

هدف از بلیت‌ها و کلیدهای نشست

- هر بلیت حاوی اطلاعاتی است که به دارنده آن اجازه می‌دهد طی دوره زمانی مشخص، به خدمت مورد نظر دست یابد.
  - **بلیت اعطای بلیت:** دسترسی به خدمت دریافت بلیت
  - **بلیت اعطای سرویس:** دسترسی به سرویس مورد نظر
- بلیت‌ها به صورت **آشکار** در اختیار WS قرار می‌گیرند، و WS بلیت‌ها را به صورت **آشکار** به TGS یا کارگزار می‌دهد.
- برای جلوگیری از **تکرار**، کلیدهای نشست مورد استفاده قرار می‌گیرند.
  - WS به همراه بلیت، Authenticatorای را ارائه می‌کند که با کلید نشست ساخته شده و حاوی برچسب زمانی است.

اعتماد در کربروس

- کاربران به WSها اعتماد دارند.
  - به همین دلیل گذرواژه خود را به WS می‌دهند.
  - با این حال WS باید بلافاصله پس از دریافت TGT و k_{s1}، گذرواژه را از حافظه‌اش پاک نماید.
- همه به KDC اعتماد دارند.

فهرست

- تاریخچه
- کربروس در سطح بالا
- **جزئیات کربروس ۵**
- قلمروهای کربروس
- کربروس در امروز

جزئیات کربروس ۵

- در ادامه مهمترین بخش‌های پیامهای کربروس ۵ را می‌بینیم.
- عمداً از برخی از جزئیات صرفنظر کرده‌ایم تا فهم پیامها ساده‌تر باشد.
- نمادگذاری:
  - W: ایستگاه کاری (Workstation)
  - U: کاربر، S: کارگزار
  - K_U: کلید طولانی مدت کاربر با KDC (بر اساس گذرواژه)
  - K_{TGS}: کلید طولانی مدت TGS
  - K_S: کلید طولانی مدت کارگزار با KDC

دو پیام نخست: دریافت TGT و کلید نشست ۱

- W→AS: $ID_U \parallel ID_{TGS} \parallel TIMES \parallel n_W$
- AS→W: $ID_U \parallel TGT \parallel$

$$\{k_{s1} \parallel TIMES \parallel n_W \parallel ID_{TGS}\}K_U$$

- TIMES: زمان آغاز و پایان اعتبار TGT

$$TGT = \{k_{s1} \parallel ID_U \parallel ADDR_W \parallel TIMES\}K_{TGS}$$

که در آن، $ADDR_W$ آدرس شبکه (معمولاً IP) ایستگاه کاری است.

دو پیام دوم: دریافت بلیت و کلید نشست ۲

- **W→TGS:** $ID_S \parallel TIMES \parallel n'_W \parallel TGT \parallel Auth_1$
- **TGS→W:** $ID_U \parallel TICKET_S \parallel$

$$\{k_{s2} \parallel TIMES \parallel n'_W \parallel ID_S\}k_{s1}$$

$$TGT = \{k_{s1} \parallel ID_U \parallel ADDR_W \parallel TIMES\}K_{TGS}$$

$$TICKET_S = \{k_{s2} \parallel ID_U \parallel ADDR_W \parallel TIMES\}K_S$$

$$Auth_1 = \{ID_U \parallel t_W\}k_{s1}$$

دو پیام سوم: تصدیق هویت دو طرفه با کارگزار

- W→S: $TICKET_S \parallel Auth_2$
- S→W: $\{t'_W \parallel Subkey \parallel Seq\#\}k_{s2}$

$$TICKET_S = \{k_{s2} \parallel ID_U \parallel ADDR_W \parallel TIMES\}K_S$$

$$Auth_2 = \{ID_U \parallel t'_W \parallel Subkey \parallel Seq\#\}k_{s2}$$

- در پیامهای بالا، W و S روی یک زیر کلید (Subkey) برای فقط یک مرتبه خدمت توافق می‌کنند.

فهرست

- تاریخچه
- کربروس در سطح بالا
- جزئیات کربروس ۵
- **قلمروهای کربروس**
- کربروس در امروز

مفهوم قلمرو (Realm)

- به تعدادی «کاربر و سرویس» (Principal) که همگی در حیطه کنترل یک KDC کربروس هستند، قلمرو آن KDC گفته می‌شوند.
- معمولاً هر قلمرو خودمختار بوده و تحت نظارت یک راهبر (Administrator) قرار دارد.
- گاه ممکن است کاربر یک قلمرو بخواهد از کارگزار قلمرو دیگر خدمت بگیرد.
- برای این منظور باید روابط اعتماد مشخصی تعریف شود.

☜ **کاربرد:** خدمات بین دو سازمان، دو شرکت، دو دانشگاه، و ...

راهکار کربروس ۴

- در کربروس ۴، برای خدمت‌دهی بین قلمروها، لازم است هر دو KDC با هم کلید مشترک داشته باشند.
- WS ابتدا برای AS خود تصدیق هویت شده و TGT می‌گیرد.
- WS با ارائه TGT به TGS خود، یک بلیت برای دسترسی به TGT قلمرو دیگر می‌گیرد.
- WS بلیت گام قبل را به TGS قلمرو دیگر داده و بلیتی برای دسترسی به کارگزار قلمرو دیگر می‌گیرد.
- WS بلیت گام قبل را به کارگزار قلمرو دیگر داده و خدمت می‌گیرد.

ایراد راهکار کربروس ۴، و راهکار کربروس ۵

- اگر N قلمرو داشته باشیم، راهکار کربروس ۴ به $O(N^2)$ کلید بین KDCها نیاز دارد.
  - ☜ عدم گسترش‌پذیری
- در کربروس ۵، تمام پیامها حاوی اطلاعات قلمرو هستند.
  - ☜ WS در ابتدا قلمرو خود و ID_{TGS} را به AS می‌گوید.
  - ☜ AS قلمرو TGS را به WS گفته و قلمرو WS را در TGT می‌گنجاند.
  - ☜ TGS قلمرو S را به WS گفته و قلمرو WS را در بلیت می‌گنجاند.

راهکار کربروس ۵ (ادامه)

- علاوه بر تغییرات فوق، کربروس ۵ در هر پیام تعدادی پرچم (Flag) را تنظیم می‌کند.
- یکی از پرچمهای مهم، پرچم FORWARDED است.
  - بلیتی که این پرچم روی آن تنظیم شده باشد، می‌تواند با نشانی شبکه‌ای متفاوتی صادر شود.
  - مفید برای وقتی که شبکه ساختار سلسله مراتبی (درختی) دارد.
  - به جای اشتراک کلید بین هر دو KDC، می‌توان در ساختار درختی شبکه بین هر دو گره (KDCهای مجاور در درخت) کلید به اشتراک گذاشت.
  - کافی است بلیت در مسیر بین WS و S روی درخت FORWARD شود.

فهرست

- تاریخچه
- کربروس در سطح بالا
- جزئیات کربروس ۵
- قلمروهای کربروس
- **کربروس در امروز**

خروجی اجرای کربروس ۵ (اکتیو دایرکتوری) در Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	WS	KDC	KRB5	222	AS-REQ
2	0.006	KDC	WS	KRB5	217	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
3	0.008	WS	KDC	KRB5	284	AS-REQ
4	0.029	KDC	WS	KRB5	583	AS-REP
5	0.032	WS	KDC	KRB5	634	TGS-REQ
6	0.050	KDC	WS	KRB5	628	TGS-REP

```
> Frame 1: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: WS (192.168.1.2), Dst: KDC (192.168.1.3)
> User Datagram Protocol, Src Port: 1225 (1225), Dst Port: 88 (88)
> Kerberos
```

```
0000  00 00 00 01 00 06 00 d0  59 37 b6 d3 f8 78 08 00   ........ Y7...x..
0010  45 00 00 ce 2b 84 00 00  80 11 8b 45 c0 a8 01 02   E...+... ...E....
0020  c0 a8 01 03 04 c9 00 58  00 ba a0 06 6a 81 af 30   .......X ....j..0
0030  81 ac a1 03 02 01 05 a2  03 02 01 0a a4 81 9f 30   ........ .......0
0040  81 9c a0 07 03 05 00 40  80 00 10 a1 17 30 15 a0   .......@ .....0..
0050  03 02 01 01 a1 0e 30 0c  1b 0a 65 72 6f 64 72 69   ......0. ..erodri
0060  67 75 65 7a a2 0d 1b 0b  45 58 41 4d 50 4c 45 2e   guez.... EXAMPLE.
0070  43 4f 4d a3 20 30 1e a0  03 02 01 02 a1 17 30 15   COM. 0.. ......0.
0080  1b 06 6b 72 62 74 67 74  1b 0b 45 58 41 4d 50 4c   ..krbtgt ..EXAMPL
0090  45 2e 43 4f 4d a5 11 18  0f 32 30 33 37 30 39 31   E.COM... .2037091
00a0  33 30 32 34 38 30 35 5a  a6 11 18 0f 32 30 33 37   3024805Z ....2037
00b0  30 39 31 33 30 32 34 38  30 35 5a a7 06 02 04 78   09130248 05Z....x
00c0  c6 48 38 a8 19 30 17 02  01 17 02 02 ff 7b 02 01   .H8..0.. .....{..
00d0  80 02 01 03 02 01 01 02  01 18 02 02 ff 79         ........ .....y
```

نکات مهم – ۱

- KDC در پاسخ به نخستین AS-REQ، خطای PREAUTH-REQUIRED را ارائه داده است.

☜ پیش-تصدیق هویت (Pre-Authentication) یکی از بهبودهای مایکروسافت بر کربروس است (RFC 6113)

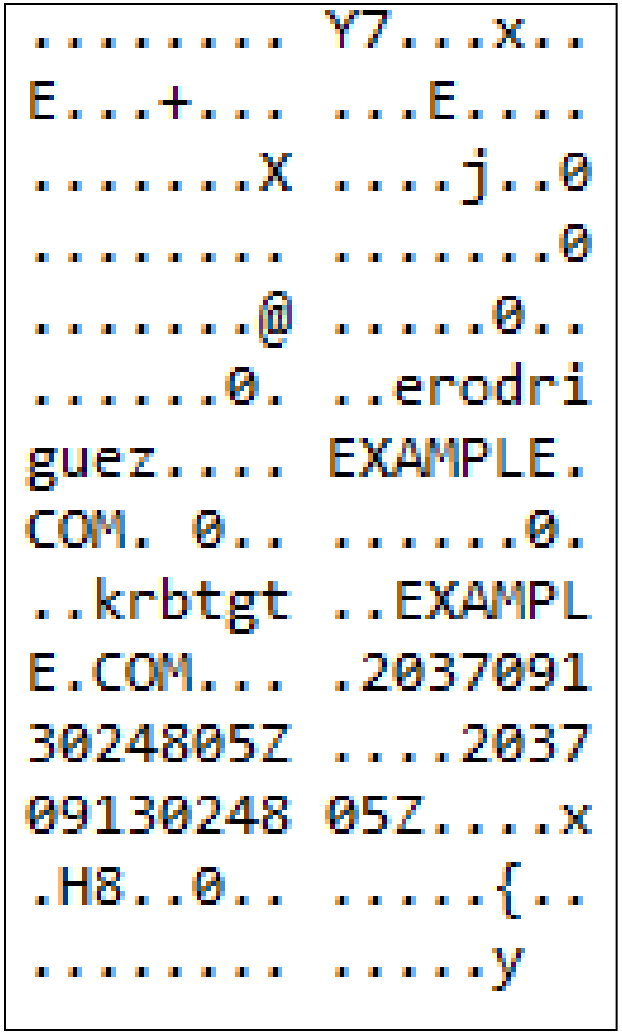
☜ AS به WS بلیت TGT را نمی‌دهد، مگر آنکه WS ابتدا ثابت کند که کلید K_U را دارد ← افزایش امنیت

نکات مهم – ۲

- کربروس از UDP پورت ۸۸ استفاده می‌کند.
- در حال حاضر امکان به کارگیری TCP پورت ۸۸ نیز وجود دارد.
- حتی در RFC 6251 امکان بهره‌گیری از کربروس بر بستر SSL/TLS نیز تعریف شده است.

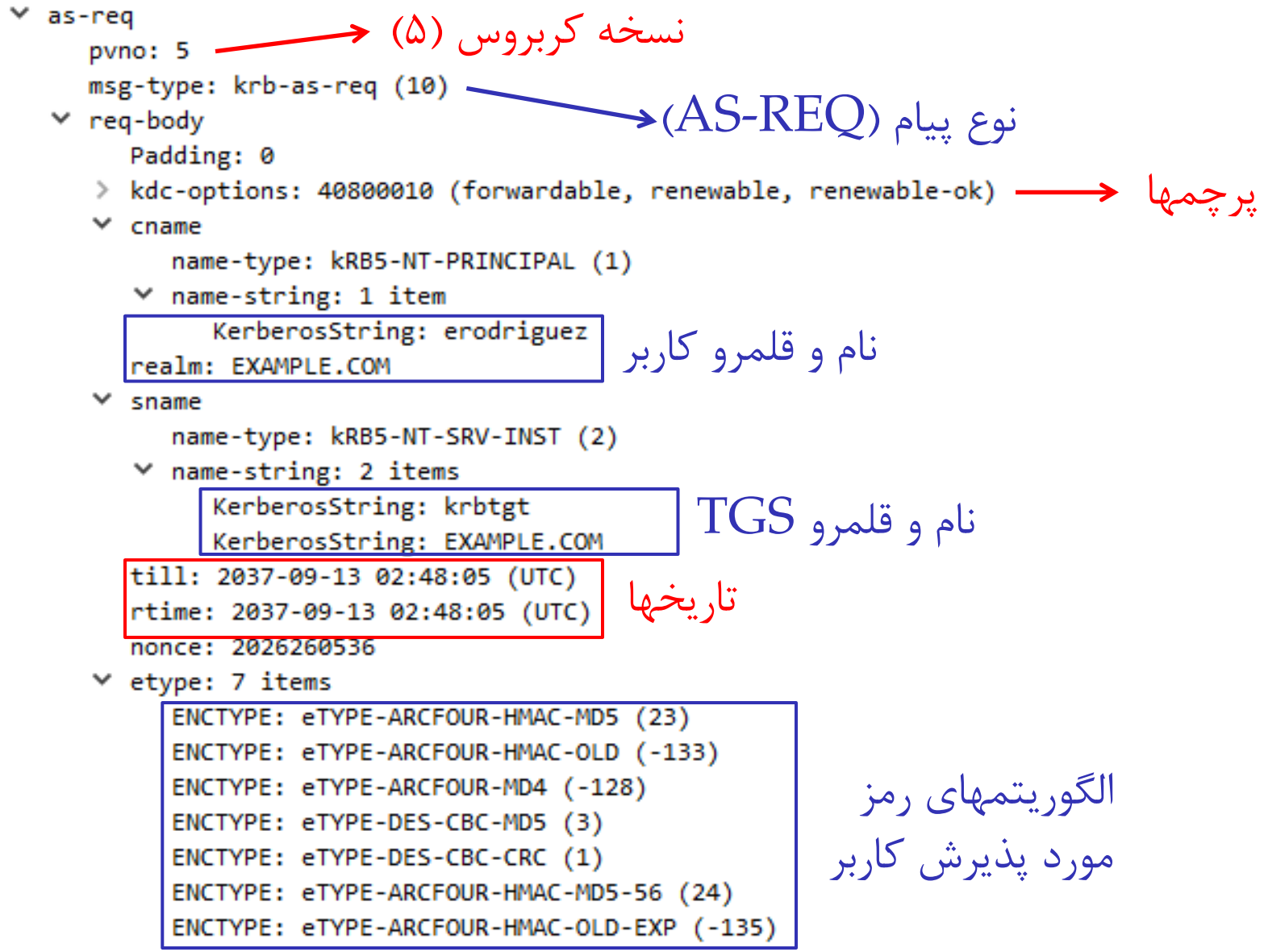
نکات مهم – ۳

- برخی از پیامها به صورت آشکار قابل مشاهده هستند:



- نام کاربر: erodriguez
- نام قلمرو: EXAMPLE.COM
- واژه krbtgt
- تاریخها (20370913...)

تفسیر Wireshark از پیامهای کربروس – ۱



تفسیر Wireshark از پیامهای کربروس – ۲

- **تمرین:** خطای PREAUTH-REQUIRED

```
krb-error
    pvno: 5
    msg-type: krb-error (30)
    stime: 2005-02-27 00:55:08 (UTC)
    susec: 0
    error-code: eRR-PREAUTH-REQUIRED (25)
    realm: EXAMPLE.COM
  sname
      name-type: kRB5-NT-PRINCIPAL (1)
    name-string: 2 items
        KerberosString: krbtgt
        KerberosString: EXAMPLE.COM
    e-text: Additional pre-authentication required
  e-data: 301f3009a103020102a20204003012a10302010ba20b0409...
    PA-DATA PA-ENC-TIMESTAMP
      padata-type: kRB5-PADATA-ENC-TIMESTAMP (2)
        padata-value: <MISSING>
    PA-DATA PA-ENCTYPE-INFO
      padata-type: kRB5-PADATA-ETYPE-INFO (11)
        padata-value: 30073005a003020103
          ETYPE-INFO-ENTRY
            etype: eTYPE-DES-CBC-MD5 (3)
```

تفسیر Wireshark از پیامهای کربروس – ۳

❑ AS-REQ به همراه PREAUTH

```
▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  ▼ padata: 1 item
    ▼ PA-DATA PA-ENC-TIMESTAMP
      ▼ padata-type: kRB5-PADATA-ENC-TIMESTAMP (2)
        ▼ padata-value: 3041a003020103a23a04389af39164ea9a4463038fbfb502...
            etype: eTYPE-DES-CBC-MD5 (3)
            cipher: 9af39164ea9a4463038fbfb502a438460b7799eed050f9c7...
  ▼ req-body
      Padding: 0
    > kdc-options: 40800010 (forwardable, renewable, renewable-ok)
    ▼ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▼ name-string: 1 item
          KerberosString: erodriguez
      realm: EXAMPLE.COM
    ▼ sname
        name-type: kRB5-NT-SRV-INST (2)
      ▼ name-string: 2 items
          KerberosString: krbtgt
          KerberosString: EXAMPLE.COM
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 2026260536
    ▼ etype: 1 item
        ENCTYPE: eTYPE-DES-CBC-MD5 (3)
```

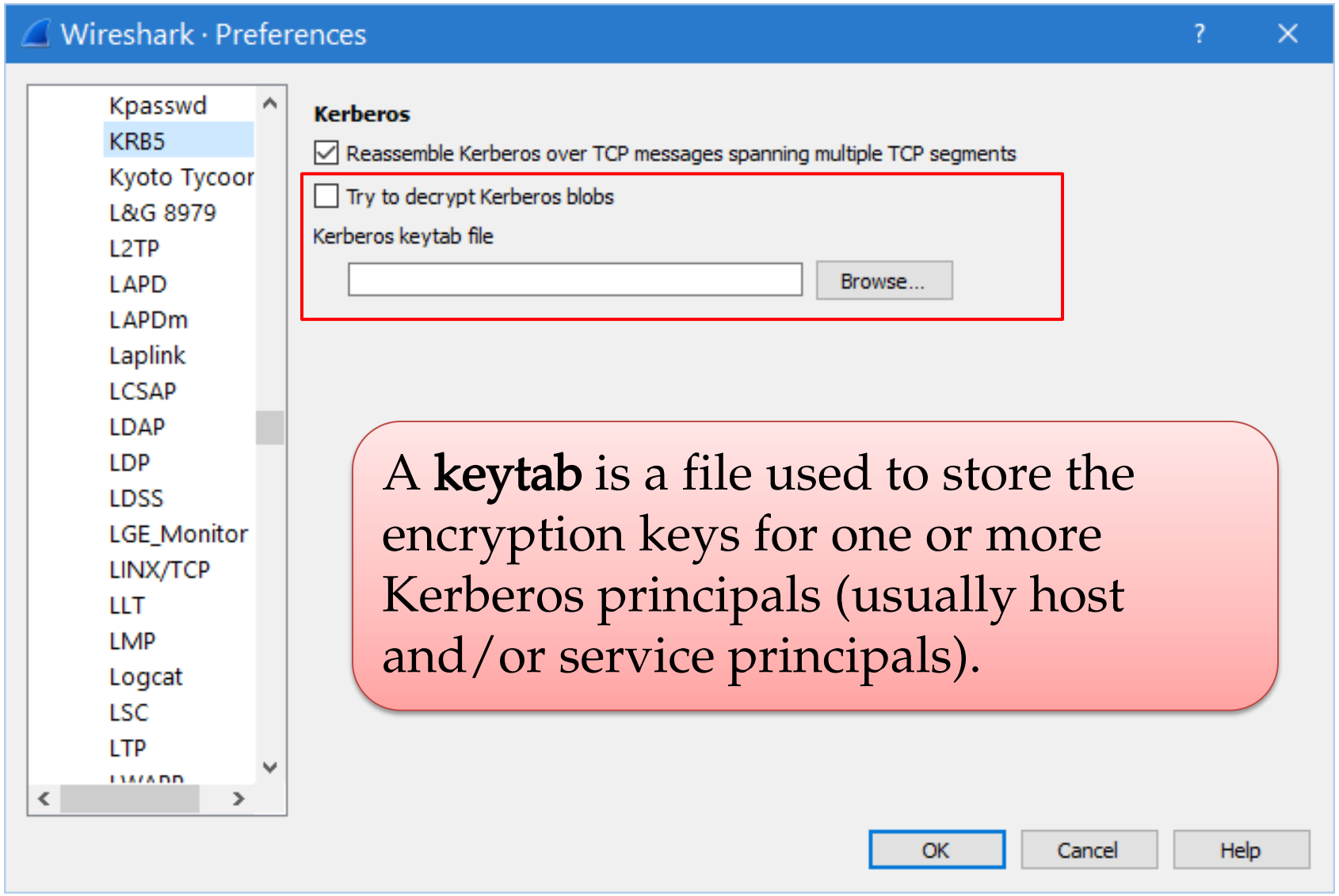
داده رمز و تصدیق هویت شده

تفسیر Wireshark از پیامهای کربروس – ۴

```
as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    crealm: EXAMPLE.COM
    cname
        name-type: kRB5-NT-PRINCIPAL (1)
        name-string: 1 item
            KerberosString: erodriguez
    ticket
        tkt-vno: 5
        realm: EXAMPLE.COM
        sname
            name-type: kRB5-NT-SRV-INST (2)
            name-string: 2 items
                KerberosString: krbtgt
                KerberosString: EXAMPLE.COM
        enc-part
            etype: eTYPE-DES-CBC-MD5 (3)
            cipher: ac40de43f0b35a90dd4e73499b5e49a477f7df1bc9ec75b4...
    enc-part
        etype: eTYPE-DES-CBC-MD5 (3)
        cipher: 3a27d16a33e888966cba3a94ee1986630b4cfff48c0dcec7...
```

بلیت (شامل بخش آشکار و رمز شده)

رمزگشایی پیامهای کربروس به کمک فایل keytab



A **keytab** is a file used to store the encryption keys for one or more Kerberos principals (usually host and/or service principals).

برنامه‌های Kerberized

- یکی از روشهای پیاده‌سازی SSO در سازمانها، توسعه برنامه‌های Kerberized است.

☜ برنامه‌هایی که قادرند با بلیتهای کربروس کار کنند و بر اساس این بلیتها به کاربران خدمت دهند.

- APIهای متنوعی برای Kerberize نمودن برنامه‌ها وجود دارد.

- مرورگرها نیز می‌توانند با بلیتهای کربروس کار کنند.

☜ مناسب برای کاربردهای مبتنی بر وب.