شروع	یکشنبه، 25 اردیبهشت 1401، 3:45 عصر
وضعیت	پایان‌یافته
پایان	یکشنبه، 25 اردیبهشت 1401، 4:10 عصر
زمان صرف شده	24 دقیقه 59 ثانیه
جمع نمره	20.60 از 22.50
نمره	**9.16** از 10.00 (92٪)

سؤال 1

درست

نمره 1.50 از 1.50

..... یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار میدهد. در ..... هر دو سمت، در فرایند تولید کلید مشارکت میکنند.

a. Key Transport - Key Agreement

b. Key Agreement - Key Transport ✔

پاسخ شما صحیح می باشد

پاسخ درست « Key Agreement - Key Transport» است.

سؤال 2

کامل

نمره 4.00 از 4.00

در مورد هر یک از روش های "**طبقه بندی ترافیک بر مبنای محتوا**" و "**طبقه بندی ترافیک آماری**" بصورت مختصر و مفید شرح دهید.

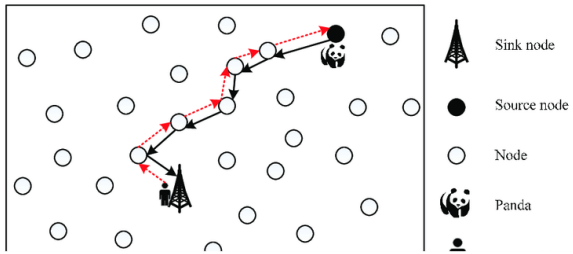
دیدگاه:

سؤال 3

درست

نمره 2.00 از 2.00

شکل زیر به مساله Panda-Hunter اشاره دارد، برطبق این مساله تعداد زیادی حسگر، در منطقه‌ای به منظورتشخیص وجودپانداها قرارداده شده است، هرزمان که وجود پاندایی توسط حسگر تشخیص داده شود، سیگنالی به مرکز جمع‌آوری داده ارسال می‌گردد. در این میان شکارچی وجود دارد که قصد دارد توسط اطلاعات ارسالی از حسگرها به محل پاندا پی ببرد و با رسیدن سیگنال به مرکز شکارچی می‌تواند نحوه رفتار حرکت پانداها و اتفاقاتی که رخ داده است را دریابد. (لازم به ذکر است که حسگرها توسط پروتکل‌های مسیریابی چندگامه، داده خود را به دست مرکزجمع آوری می رسانند.) **با توجه به اطلاعات گفته شده، در رابطه با این مساله کدام مفهوم در شبکه از اهمیت بالایی برخوردار است و دسته‌بندی مربوط به آن را بنویسد. همچنین بیان کنید که شکارچی از طریق چه نوع حمله‌ای می‌تواند به اطلاعات حسگرها دست پیدا کند؟** (پاسخ را با خط فاصله از هم جدا نمایید مانند x-y و در کادر پایین بنویسید.)



پاسخ: ✗

پاسخ درست: حریم خصوصی زمانی و آماری - شنود

دیدگاه:

سؤال 4

درست

نمره 3.00 از 3.00

برای هر یک از سوالات زیر، نزدیک ترین پاسخ مناسب به آن را انتخاب کنید:

مسئولیت اعتبارسنجی گواهینامه ها بر عهده کدام است؟	VA ✔
در این روش ویژگی های آماری سربسته مورد بررسی قرار میگیرد.	SPI ✔
سلسله مراتب چند سطحی از اعتماد.	زنجیره گواهینامه ✔
جمله <<گواهی‌نامه توسط چندین مرجع صدور گواهی‌نامه امضا می‌گردد.>> چه مفهومی را نشان می‌دهد؟	cross signing ✔
کدام‌یک از پارامترهای فیلد گواهی نامه نیست؟	اصلاح کننده سریال ✔
گواهی‌نامه‌های صادر شده شامل چه اطلاعاتی می‌باشد؟	کلید عمومی- هویت فرد ✔

پاسخ شما صحیح می باشد

پاسخ درست:
مسئولیت اعتبارسنجی گواهینامه ها بر عهده کدام است؟ → VA, در این روش ویژگی های آماری سربسته مورد بررسی قرار میگیرد. → SPI,
سلسله مراتب چند سطحی از اعتماد. → زنجیره گواهینامه,
جمله <<گواهی‌نامه توسط چندین مرجع صدور گواهی‌نامه امضا می‌گردد.>> چه مفهومی را نشان می‌دهد؟ → cross signing,
کدام‌یک از پارامترهای فیلد گواهی نامه نیست؟ → اصلاح کننده سریال,
گواهی‌نامه‌های صادر شده شامل چه اطلاعاتی می‌باشد؟ → کلید عمومی- هویت فرد

سؤال 5

پاسخ نیمه درست

نمره 1.60 از 2.00

کدام گزینه جزو وظایف PKI است؟

یک یا چند گزینه را انتخاب کنید:

1. **مدیریت کلید عمومی بکار رفته در شبکه**
2. **مدیریت شناسه‌ها**
3. **ابطال گواهینامه‌ها**
4. **توزیع گواهینامه‌ها**
5. **مدیریت گواهینامه‌ها**

پاسخ شما تا حدودی صحیح است

شما به درستی 4 گزینه را انتخاب کرده‌اید

پاسخ درست عبارت است از: **مدیریت کلید عمومی بکار رفته در شبکه**,

مدیریت شناسه‌ها,

توزیع گواهینامه‌ها,

ابطال گواهینامه‌ها,

مدیریت گواهینامه‌ها

سؤال 6

پاسخ نیمه درست

نمره 2.50 از 4.00

صحیح یا **غلط** بودن هر یک از گزاره های زیر را مشخص کنید:

در شبکه‌های تلفن همراه فعلی، احراز اصالت بین سیم‌کارت و هسته شبکه صورت می پذیرد.	صحیح	✓
در PKI صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد.	غلط	✓
روش‌های SPI در لایه شبکه به بررسی آماری header بسته‌های می پردازد.	صحیح	✗
در یک گواهی‌نامه می‌توان شناسه الگوریتم یک امضا را دریافت.	صحیح	✓
روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد.	صحیح	✗
تنها راه برای اطمینان بخشی از صحت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است.	غلط	✓
در طبقه‌بندی ترافیک بر مبنای DPI، محتوای سربسته لایه انتقال مورد بازرسی قرار می‌گیرد.	غلط	✗
در شبکه‌های تلفن‌همراه ارتباط از گوشی فرستنده تا گوشی گیرنده به طور مستقیم رمز است.	صحیح	✗

پاسخ شما تا حدودی صحیح است

شما به درستی 4 گزینه را انتخاب کرده‌اید

پاسخ درست:

در شبکه‌های تلفن همراه فعلی، احراز اصالت بین سیم‌کارت و هسته شبکه صورت می پذیرد. → صحیح,

در PKI صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد. → غلط,

روش‌های SPI در لایه شبکه به بررسی آماری header بسته‌های می پردازد. → غلط,

در یک گواهی‌نامه می‌توان شناسه الگوریتم یک امضا را دریافت. → صحیح,

روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد. → غلط,
تنها راه برای اطمینان بخشی از صحت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است. → غلط,
در طبقه‌بندی ترافیک بر مبنای DPI، محتوای سربسته لایه انتقال مورد بازرسی قرار می‌گیرد. → صحیح,
در شبکه‌های تلفن‌همراه ارتباط از گوشی فرستنده تا گوشی گیرنده به طور مستقیم رمز است. → غلط

دیدگاه:

سؤال 7

درست

نمره 6.00 از 6.00

کدام مورد صحیح است و کدان غلط؟

مدیریت فرایند احرازاصالت در شبکه‌های نسل چهار برعهده MME است.	غلط ✗
در شبکه‌های نسل دو یکپارچگی و محرمانگی پیام بین ME و BTS حفظ می شود.	صحیح ✗
نهاد مدیریتی MSC/SGSN در شبکه‌های نسل دو و سه برای شروع فرایند احراز اصالت نیاز به IMSI دارد.	صحیح ✓
در شبکه‌های نسل سه حمله‌گر با تغییر الگوریتم‌های رمزنگاری مورد پشتیبانی کاربر، می تواند او را شنود کند.	صحیح ✗
بردارهای احراز اصالت به منظور احراز اصالت کاربر در اختیار RAN قرار می‌گیرد.	صحیح ✗
در شبکه‌های نسل سه و چهار، تضمین یکپارچگی برای سطح داده وجود ندارد.	غلط ✗

پاسخ شما صحیح می باشد

پاسخ درست:

مدیریت فرایند احرازاصالت در شبکه‌های نسل چهار برعهده MME است. → صحیح,

در شبکه‌های نسل دو یکپارچگی و محرمانگی پیام بین ME و BTS حفظ می شود. → غلط,

نهاد مدیریتی MSC/SGSN در شبکه‌های نسل دو و سه برای شروع فرایند احراز اصالت نیاز به IMSI دارد. → صحیح,

در شبکه‌های نسل سه حمله‌گر با تغییر الگوریتم‌های رمزنگاری مورد پشتیبانی کاربر، می تواند او را شنود کند. → غلط,

بردارهای احراز اصالت به منظور احراز اصالت کاربر در اختیار RAN قرار می‌گیرد. → غلط,

در شبکه‌های نسل سه و چهار، تضمین یکپارچگی برای سطح داده وجود ندارد. → صحیح

دیدگاه: