بسم تعالی

شبکه

(استاد مددی)

منبع: شبکه های کامپیوتری - ترجمه دکتر پیرام - دوجلدی آبی رنگ
مهندسی اینترنت - استالینگز

"فهرست مطالب"

محتوای دوره

مفاهیم اولیه

دشواری گذاری انتقال

موضوعات جلسه پوشش درس «جلسه اول»

* رمزنگاری متقارن
* کدهای احراز تمامیت پیام و توابع درهم ساز.
* رمزنگاری کلید عمومی
* زیرساخت کلید عمومی و گواهی هویت.
* مدیریت کلید
* امنیت پست الکترونیک
* امنیت IP
* امنیت web
* احقاق رقمی و پروتکل های هویت شناسی
* دیواره های آتش و سیستم های تشخیص نفوذ

* رمزنگاری متقارن یعنی کلیدهای رمزگشایی و رمزنگاری یکی است.
* رمزنگاری با طول پیام کاری ندارد بلکه درهم ریزی بستی یا بایتی دارد.
* کدگذاری یعنی تشخیص خطا و تصحیح خطا.
* کدینگی خوب است که بیشترین تعداد بیت خطا را تشخیص دهد و بیشترین بیت خطا را تصحیح کند.
* در کامپیوترهای شخصی پیچیدگی محاسباتی تا ۸۰ بیت رمزنگاری شده است.

نامتقارن: کلید رمزگشایی و رمزنگاری متفاوت است و قسمتی Public می شود.

$x^a * x^b = x^{ab}$

encryption رمزنگاری

Decryption رمزگشایی

از ۱۹۷۰ تا ۱۹۹۸ در آمریکا استفاده می‌شد DES (Data Encryption Standard) الگوریتم رمزنگاری

★ روش‌های مدیریت کلید یعنی

★ توابع درهم‌ساز کلیدی ساز.

★ امنیت چیست؟ امنیت (به صورت غیررسمی) عبارت است از حفاظت از ذخیره برای ما ارزشمند است. (شمیر یکی از سه اسرائیلی است که هر رمزی را باز می‌کند)

کشورهای مطرح رمز و رمزنگاری و... کشورهای انگلیس، اسرائیل و امریکا می‌باشند و اروپا

★ شبکه‌های کامپیوتری چیست؟ مجموعه‌ای از کامپیوترهای مستقل است که به‌نوعی با یکدیگر اطلاعات و داده مبادله می‌نمایند.

★ مزیت شبکه‌های LAN چیست؟ ۱- ارتباط مزیکی ساده ۲- ارزان ۳-

★ انواع شبکه‌های محلی را با شکل نام‌برده و مساحت و مدیا که برای توضیح دهید؟

- LAN — بین دو گره که هرگره مثلاً ۲۰ متر باشد
- MAN — بین شهری
- WAN — کشوری یا جهانی

★ سرویس‌های امنیتی:

۱- حفظ جامعیت داده: جهت کامل و بدون تغییر باشد. (integrity)

۲- حفظ محرمانگی داده‌ها: فقط در صورت لو رفتن، داده‌ها طوری رمزنگاری شده و یا رمزنگاری شده باشد که نتوان از آن استفاده کند. (confidentiality)

ب) هویت شناسی (احراز هویت): مکانیزم هایی که پیش از هویت اصلی ارزیابی شده و داده یا شده و جعلی نباشد. (Authentication)

ج): مجوز شناسی: یعنی اینکه کسی که می خواهد داده را بررسی کند می داند که آیا دسترسی دارد یا نه، کلید دارد یا نه.

د): عدم انکار: یعنی مکانیزم تعریف شود که بررسی شده داده بعد از ضبط آن نباشد.

ه): دسترس پذیری: امنیت باید دسترسی را دشوار کند نه غیر ممکن.

★ دو نوع حمله می توانیم داشته باشیم:

۱- حمله فعال: داخلی در بسته های داده ها و یا تغییر محتوا و جعل آن.

۲- حمله غیر فعال: یعنی بیشتر ضبط جمع آوری اطلاعات و یا شنود انجام می دهد.

فعال تغییر دادن، غیر فعال شنود

★: تعریف امنیت اطلاعات چیست؟ امنیت اطلاعات عبارت است از مجموعه ای از ابزارها و فناوری هایی که روز به همراه روش های پذیرفته شده در همکاری با کلیه امنیت دارایی های اطلاعاتی سازمان را تامین می کند.

د: اصول شش گانه کرکهف را توضیح دهید؟ (ج: اسلاید معرفی تاریخی)

س): انواع حملات تحلیل رمزنگاری چیست؟ (ج: اسلاید جلسه ۴)

★ الگوریتم های مورد استفاده در تلفن های همراه A5/1 و A5/2 و AES می باشد.

در حین الگوریتم LTE را با الگوریتم ZUC استفاده می کنند.

س): جانشینی مضاعف، رمزتک الفبایی را توضیح دهید؟

ج: جانشینی مضاعف یعنی استفاده از حروف انگلیسی جهت رمزنگاری بوسیله یک عدد یعنی وقتی حرف کنار هم چیده می شوند طبق عدد رمز اعداد بعدی جایگزین می گردد. مثال:

a b c d e f g h i j k l m n o p q r s

t u v w x y z .

مثلا کلمه Send را با عدد ۴۲۱۴ رمزنگاری کرده اینجا داریم =

S e n d = wgog

۴ ۲ ۱ ۳ بعدی

۴ حرف جلوتر ۲ حرف جلوتر یک حرف جلوتر یک حرف جلوتر

★ رمزهای بلوکی و جریانی در رمزنگاری متقارن انجام می شود.

★ رمزهای قطعه ای «متقارن»
- Block cipher (قطعه ای) قالبی
- Stream cipher (جریانی) دنباله ای

★ قالبی یعنی متن در قالبی هم شکل داده شده و رمزنگاری شده است.

★ دنباله ای یعنی Bit به Bit رمز می شوند.

★ ماشین ساینک :

* سایفر سبک وزن مربوط به استاندارد است که الگوریتمی را ارائه کرده است.

(رمزنگاری سبک وزن برای شبکه های حسگر بی سیم) "سبک وزن light whith"

★ سایفر فوق برای داده ها - مکتوب نوشته بهره از فیلم و اسلام.

★ شبکه پیشرفته فعالیت در همین حوزه می باشد. بیت تدریس غیرحضوری

رمزنگاری نامتقارن

"حله سقم از کتاب استالینگ"

- رمزنگاری کلید عمومی با ۲ هدف:
  - حل مسأله کلید در روش های رمزنگاری متقارن
  - امضای دیجیتال

* مدهای رمزنگاری ۱ اکمال سئوال"

★ تعداد کلیدها اگر n باشد تعداد کلید $\frac{n(n-1)}{2}$ می شود.

★ رمزنگاری کلید عمومی خیلی کند است (۱۰۰۰ برابر کند است).

★ در رمزنگاری کلید عمومی، هر فرد ۲ کلید دارد: ۱- کلید عمومی ۲- کلید اختصاصی

ری ★ ساختار رمزهای فیستل؟

رگ ★ فرآیند خصوصیت رمزنگاری عمومی را بیان کنید؟ مثل PdF

رگ ★ خصوصیات رمزنگاری کلید عمومی: مثل PdF -

الف - متن با توابع ریاضی به جای عملیات جایگزینی و...

ب - استفاده از ۲ کلید

ج - کلیدهای رمزنگاری و رمزگذاری متفاوت اما مرتبط هستند.

→ رسیدن به کلید رمزگشایی از کلید رمزگذاری از لحاظ ریاضی بسیار مشکل و زمانبر.

→ رمزگذاری امری همگانی می‌باشد و لذا نیازی به استراک گذاشتن اطلاعات مرموز ندارد.

→ رمزگشایی از طرف دیگر امری اختصاصی بوده و محرمانگی پیام حفظ می‌شود.

* "Public" یا "پابلیک" یعنی همگانی.

س ـ کلید رمزگشایی چه فرقی با کلید رمزگذاری دارد؟ ص ۱۴ و ص ۱۵ pdf ترم اول

* برای رمزنگاری کلید عمومی کاربردهای زیر را می‌توان در نظر گرفت: ویژه‌ها در اسلام

* تفاوت رمزنگاری سیمتریک و رمزنگاری کلید عمومی. ص ۷ اسلام

* رمزگذاری سیمتریک برای امضا بودن مناسب: ص ۸

* تفاوت رمزنگاری (ملزومات امنیتی) (رمزگذاری با کلید عمومی): ص ۹

* رمزگشایی در اصل یک کلید است که ترکیبی از ۲ کلید می‌باشد که کلید دوم مخفی است.

* جایگزینی یا تکمیل؟ ص ۱۰

* طول کلید عمومی با کلید اختصاصی فرق دارد.

* نقاط ضعف و مزایا

* کاربردهای رمزگذاری کلید عمومی.

۷

* کلیات الگوریتم رمزنگاری RSA .

* علم رمزنگاری ترکیبی از رشته کامپیوتر، ریاضی و فیزیک می باشد.

* علم رمزنگاری خیلی گسترده است

* نمادگذاری RSA .

* پیمانه ای یعنی باقیمانده تقسیم ریاضی $۲۸۶ \overset{۵}{\equiv} ۲$

یعنی ۱۲ تقسیم بر ۵ عدد ۲ را باقیمانده دارد.

* مبانی رمز و ریاضی RSA :

* قراردادها و پیچیدگی RSA .

* تعریف کارا چرا می شکند.

* کتاب رمزنگاری کلید عمومی (دکتر بهزاد) وجود دارد.

* حملات مختلف به RSA . صفحه ۲۱ اسلاید. (کپی)

* راههای مقابله با حملات زمانی به RSA صفحه ۲۲ اسلاید. (می تواند سئوال باشد) صفحه آخر اسلاید

* کتاب امنیت شبکه نوشته تننبام هر چیه دکتر پیدا کرد و مکلین .

* شرکت کادوشه کام آسیا "بهتر است که جهت ردیابی تلفن های همراه کار می کند. BTS

* ردیابی سیگنال موبایل

امنیت شبکه با کمک توابع درهم ساز یک طرفه (جلسه ۱۶)

(کد)

★ تابع درهم ساز کد مربوطه «H(m)» ص۳ "از توابع درهم ساز کد سئوال و آید".

★ امنیت توابع درهم ساز پیچیدگی محاسبه. ص۶

★ چگونه با کمک درهم تحقیق کنیم که پیغام داده: از طریق PDF می توان سرچ کرد (Serche)

① « آسیب ها و ضعف شبکه های اجتماعی » «(در ۱۰ دقیقه)»

② « انواع شبکه های هواوری از نظر فنی »

★ استفاده از رمزنگاری متقارن به جای توابع درهم ساز، ص۲

★ ساختار درونی توابع درهم ساز: ایده ص۸

★ کاربردها مثال با شکل توابع درهم ساز و رمزنگاری متقارن برای احراز هویت؟

« تا پایان این یک سئوال باشد که شکل را بکشید: » ص۱۱ جلسه ۱۶ «کد»

شکل ها بصورت سئوال کد که مربوط به کدام بخش است، جلسه یا ویژگی یا اضافه

★ " " " " برای محرمانگی و تمامیت.

(کد) ★ شکل تابع درهم ساز برای رمزنگاری متقارن برای امضاء؟ ص۱۲ جلسه ۱۶ (کد)

★ توابع درهم ساز چه هستند؟ ص۱۳ ★ شکل صفحه کلید را توضیح دهید؟

(کد)

★ امنیت MD5

★ HMAC ص۱۱

★ امنیت HMAC صف (جلسه پنجم)

★ سلسله مراتب کلیدها

★ مدیریت کلید: سطوح مختلف امنیت برحسب سطوح مختلف، کلیدهای مختلف.

فایل امن شده
امنیت ویروس و ...

★ نوعی زمان تا ۳۰۰ms میلی ثانیه حساس است و در این فاصله می‌توان کلیدها و اطلاعات را بازیابی کرد

لرزش‌های میکروسکوپی را آپدیت کرد ((پردازش صوت Signal Prassesing))

★ کلید نشت هرچی زودتر آپدیت شود امنیت بیشتر است.

★★ کلید جلسه و ثبت کلید اصلی را مقایسه کنید! (می‌تواند تفاوتی از یک سوال باشد)

★ اهمیت طول عمر کلید جلسه صف ۵ درصد

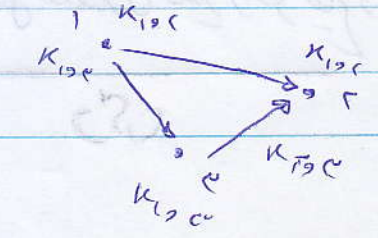
★ درجه امنیت مدیریت کلید (فنی) مهم است. (موضوعی)

★★ مدیریت کلید متکی بر کلید خصوصی است صف ۵ درصد

★ KDC یعنی مرکز توزیع کلید صف (شرح موضوع فوق) (می‌تواند یک سوال باشد)

★★ روش تقطیع به نقطه صف اگر سه کلید داشته باشیم یا زمان زیاد است کلید

$$\frac{n(n-1)}{2} = \frac{3(2-1)}{2} = 3$$



* توضیحات در خصوص شکل مقابل ←

- آلیس با کلید اختصاصی خودش پیام را رمز می‌کند و باباً با کلید عمومی آلیس پیام را باز می‌کند.

- در امضاء با کلید خصوصی رمز می‌شود و با کلید عمومی باز می‌شود.

- توضیح: پیام را با کلید ۵ سازد و با کلید خصوصی رمز می‌شود که فقط با با کلید عمومی می‌تواند رمز را باز کند و از رمزنگاری متقارن به دلیل بالابودن سرعت استفاده می‌شود.

** روش متمرکز توزیع کلید ؛ ص ۸ تا ص ۱۰ نکات مهم و مشترک

(S) * امضاء (جلسه ۶ - ص ۸)

** روش های اطلاع از کلید عمومی ص ۱۱

۱ * اعلان عمومی ص ۱۲

۲ * فهرست راهکار عمومی ص ۱۳

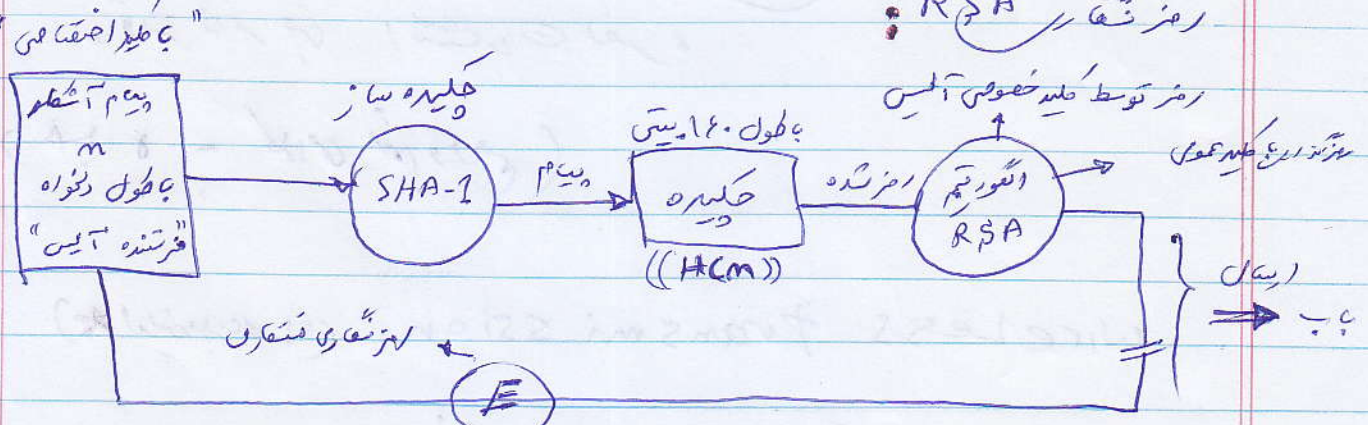
(S)
۳ * مرجع معتبر کلید عمومی "ص ۱۵ سئوال امتحانی" ص ۳ فصل ۳ ((شکل با توضیح))

* در حال اعتماد ، ذخیره اعتماد وجود دارد ((جلسه ششم))
* معمولترین حمله در هویت شناسی : شمارنده ای گذاریم تا Reject شود

امضاء رقمی - ویژگی ص ۴

امضاء رقمی - نیاز مندی ص ۵

* ~~کلید~~ الگوی امضاء دیجیتال با استفاده از SHA-1 (تابع درهم ساز) و رمزنگاری RSA :



روش دوم : با رمزنگاری متقارن (صورت ارسال پیام امن می شود)

* امضاء با کلید اختصاصی رمز می شود ولی کلید پیام با کلید عمومی رمز می شود. (سئوال امتحانی)

* رمزنگاری کلید عمومی اعلام همگانی می شود (برای هر پیام ولی بار امضاء با کلید اختصاصی رمز می شود.

* مدیریت کلید مهمترین بحث امنیت شبکه است - بیشترین حالات سوال امتحان زیاد دارد.
* متصدی کلید عمومی ← مدیریت و توزیع کلید. ص جلسه ۶
** امضاء رقمی - اجزاء و نیازمندی ها - ص جلسه ۶ - مربع های فرستاده شده

جلسه ۴

** انواع هویت شناسی { فردی ص ۳ / سیستم شبکه }

** رمز هویت شناسی ص ۴

** هویت شناسی و کلید عمومی ص ۶

** خطر حمله کننده در هویت شناسی ص ۸ (شاید سوال بیاید)

** انواع حملات تکرار Replay جلسه ۷ (شاید سوال بیاید)

** روش های مقابله با حمله تکرار (جلسه ۷).

* الگوریتم تولید امضاء ؟ ج پیغام و کلید خصوصی فرستنده را به عنوان ورودی گرفته و امضاء را تولید می کند.
* الگوریتم تایید امضاء ؟ ج امضاء و کلید عمومی فرستنده را به عنوان ورودی گرفته و تایید یا امضاء را به عنوان خروجی برمی گرداند.
* کتاب امنیت داده ها آخر فرمول ها خوب است.

« کلمه ذکر شده اشتباه نفرد »

(جلسه ۵ - کلاس نهم و دهم)

(* این جلسه ۹۷) wireless transmission

* در این کلاس استاد بیشتر مفهوم کلی سوال را گفت و نکته

موضوع امتحان بیستم یا قسمتی از آن هست

* اختلال و تداخل را بصورت کامل شرح دهید؟ تداخل فرکانسی که نوع پیشرفته

آن بصورت اختلال فرکانسی عمل می‌باشد یعنی اینکه هر کشوری در حوزه رادیویی

خود فرکانس‌های استانداردی را دارد که در صورت هجوم دشمن در حوزه فرکانسی مثل

امواج ماهواره‌ها و یا رادیوهای بیگانه، سعی می‌کند با صرف انرژی مضاعف

قدرت انرژی مبدأ تولید فرکانس دشمن را شکسته کنترل و یا اختلال امواج ارسال

از آن حوزه جلوگیری کند و به وسیله امنیت نیروی را از مسیر فرکانسی دور نگه دارد

و برعکس یعنی کشورها نیز در بعضی موارد با پخش‌های الکترونیکی سیستم رادیو را مختل می‌کنند.

** کنفرانس در خصوص موضوع فوق و یا Sotelling communication بصورت

موضوع سمینار جهت ارائه در کلاس و لااقل ۲ نمره کلاسی جهت دانشجویان در هفته‌های آتی

قبلاً موضوع در کتاب ... استاد گفته شود.

نمونه سئوال: دیدگاه‌های پارازیت الکترونیک چیست؟ (جلسه اول)

نمونه سئوال: امنیت اطلاعات را توضیح داده و کنترل‌هایی را که بابت امنیت اطلاعات انجام می‌شود

با توضیح دهید؟ (جلسه اول)

نمونه سئوال: شبکه نیازمند در یک سرویس امنیتی را بیان نموده و یکی را به دلخواه تشریح نمایید؟

نمونه سئوال: مفهوم امنیت شبکه‌ای را شامل چیست؟ دسته‌بندی حملات را مشخص و توضیح دهید؟

نمونه سئوال: آنتن‌ها را با ذکر مثال شکل موج‌ها و اشکال آنها چه تعریفی را شامل می‌شود؟

سئوال ★ دسته بندی حملات را مشخص و توضیح دهید؟

سئوال ★ انواع هویت شناسی. { فردی ستیم / سیستم به شبکه

سئوال ★ پروتکل های هویت شناسی. { یک طرفه / دو طرفه

سئوال ★ حملات به پروتکل ها.

★ بحث پروتکل ها خیلی مهم است و می تواند یک طرفه باشد یا دو طرفه باشد و دلیل هم می توان به این پروتکل ها عمل کرده در اصل هویت کاربران نسبت به کارهایی که با آنها انجام می شود در فضای مجازی امکان دستبرد یا حمله دارد.

سئوال ★ اهمیت کدام پروتکل های هویت شناسی کدامند؟

ز) سئوال: احراز هویت چیست؟

ج ★ احراز هویت روش یا مکانیزمی است که براساس آن هر موجودیت مثل کاربر یا شخص بررسی می کند که آیا شریک او در ارتباط یعنی موجودیت طرف مقابل همان است که ادعا می کند و یک اطلاعاتی است که خود را بجای طرف واقعی جا زده است.

★ (احراز هویت در مورد افراد روشی در مورد تشخیص هویت واقعی آنان و اثبات درستی یا نادرستی ادعای آنها در خصوص شخص خودشان است.).

★ ((در دنیای امنیت ارتباطات اینترنتی کاربران قرینه و گیرنده هستند که هر نهایت از افراد حقیقی یا حقوقی با یکدیگر در تعاملند و طبقاً

فرایند اجرای هویت مکانیزمی است که به وسیله آن یک کاربر هویت (یعنی کاربری که ادعا می‌کند) که هویت او را ثابت می‌کند.

* مخفف کلمه هویت سنجی در اینترنت به صورت زیر می‌باشد: AAA / A3

① Authentication — آتانتیکیشن

② Authorization — آتاریزیشن

③ Accounting — اکونتینگ

تعریف ①: مکانیزمی که بر اساس آن یک وسیله هویت حقیقی یا حقوقی کاربر را ثابت می‌کند.

تعریف ②: مکانیزمی که بر اساس آن شخص یا سوژه‌ای که هویت واقعی آن اثبات شده است مجوز چه کارها و عملیاتی را دارند.

تعریف ③: مکانیزمی که بر اساس آن شخص یا سوژه چه مقدار از منابع و سیستم خدمات می‌برد و آیا او را از این سهم خدمات و سهم و صلاحیت آن آگاه کرده است.

مثال: کسی مثل آتی به تو گوید می‌خواهم از خدمات شما استفاده کنم:

① آیا تو واقعاً آرش هستی؟

② آرش چه کارهایی را می‌تواند انجام دهد و انجام چه کارهایی غیرمجاز است.

تعریف نشست : session : به هر مجموعه از عملیاتی که

در یک بازه ی زمانی و با احراز هویت کاربر آغاز می شود و پس طرفین

به تعداد نامشخص با یکدیگر تبادل داده می کنند و در پایان کار با توافق و آگاهی

طرفین خاتمه می یابد، اصطلاحاً نشست گفته می شود

* تعریف نشست رمزنگاری شده چیست؟ : به هر نشستی که در فضای

آن هر پیامی که بین طرفین رد و بدل می شود به روش مورد رمزنگاری شود اصطلاحاً

نشست رمزنگاری شده می گوئیم.

* تعریف کلید نشست؟ « session key » : معمولاً در

ایجاد هر نشست کاربر به یک کلید اصلی نیاز دارد که در نشست کلیه عملیات

الگوریتم ها به آن وابسته است. لذا به محض آنکه طرفین از هویت یکدیگر

مطمئن شدند، فوراً با هم شروع یکدیگر کلیدی تصادفی و یکبار مصرف را تولید و

داده و از آن به بعد (تا پایان نشست) برای رمزنگاری ها و تولید اطلاعات

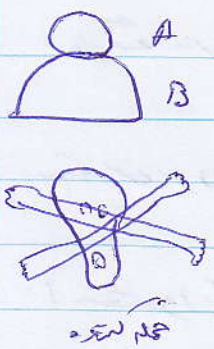
از آن کلید استفاده خواهند کرد. طرفین هیچ کلید نشست را به صورت

انتخاب و ارسال نکنند که هیچ یک از کلیدهای تکراری استفاده نشود.

تذکر: در تمام مکانیزم‌های احراز هویت باید فرض بر این گذاشته شود که یک شخص اخلالگر می‌تواند در هر مرحله از پروتکل خود را به جای یکی از طرفین جا بزند. پس مکانیزم احراز باید بگونه‌ای مستحکم و هوشمندانه عمل کند که جلوی اخلالگر را تا حد امکان بگیرد.

★ احراز هویت براساس چالش و پاسخ؟

(دو طرفه ۵ مرحله‌ای)



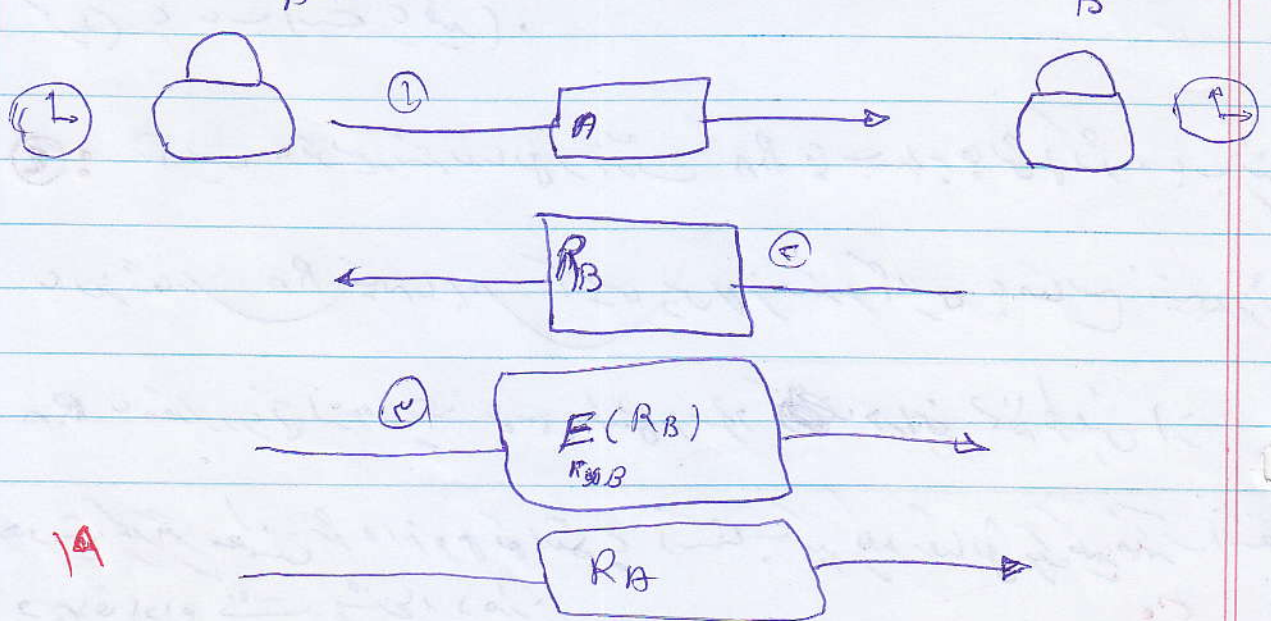
برای باب

① آلیس باید برای شناسه کاربری خود هویت خود را مشخص کند.

- به بیان ساده شناسه کاربری رمز نخواهد شد.

② باب باید از شناسه کاربری آلیس، باید اطلاع داشته باشد تا بتواند برای تشخیص هویت واقعی صدای یک رشته تصادفی مثل R_B تولید و برای آن نام کاربری آلیس را چالش کند.

③ آلیس موظف است R_B را با کلید متقارن مورد توافق رمزنگاری کرده و نتیجه را برای باب بفرستد.



$E_{R_{GA}}(R_B)$

اعمال هویت انجام شد. نشت را کوانت شروع شود.
(لوله کشی)

ادامه ۳: با به خود گیرنده R_B را از $A_{۳}$ جدا کرده و با دریافت پیام $۳_{و}$ تماس میگیریم

سرنشکاری R_{AB} با تماس دریافتی می توانند متوجه شود که آیا پرت پیام واقعاً متعلق

به آن بوده یا خیر. چرا که می توانند R_B را به درستی بفرستد و آن اگر

است مواردی از آنجا که R_B کلاً هویت تماس و ارتباط فضای پرتی مثلاً ۲۵۰

بیت انتقال می شود لذا اعمال آنکه عملکرد (تروری) کلید رشته R_B و نتیجه اطلاعات

اشتراک سیم کرده و هم های آب به تکرار کرده یا نشد در عمل متفاوت است (تا زمانی

با به از هویت واقعی آیین مطمئن شده ولی آیین هنوز نمی داند که آیا دوستان صحیح

کرده با به است یا خیر).

E: آیین با تولید رشته تصادفی و ارسال R_B به به را به چالش می کند. به نیز

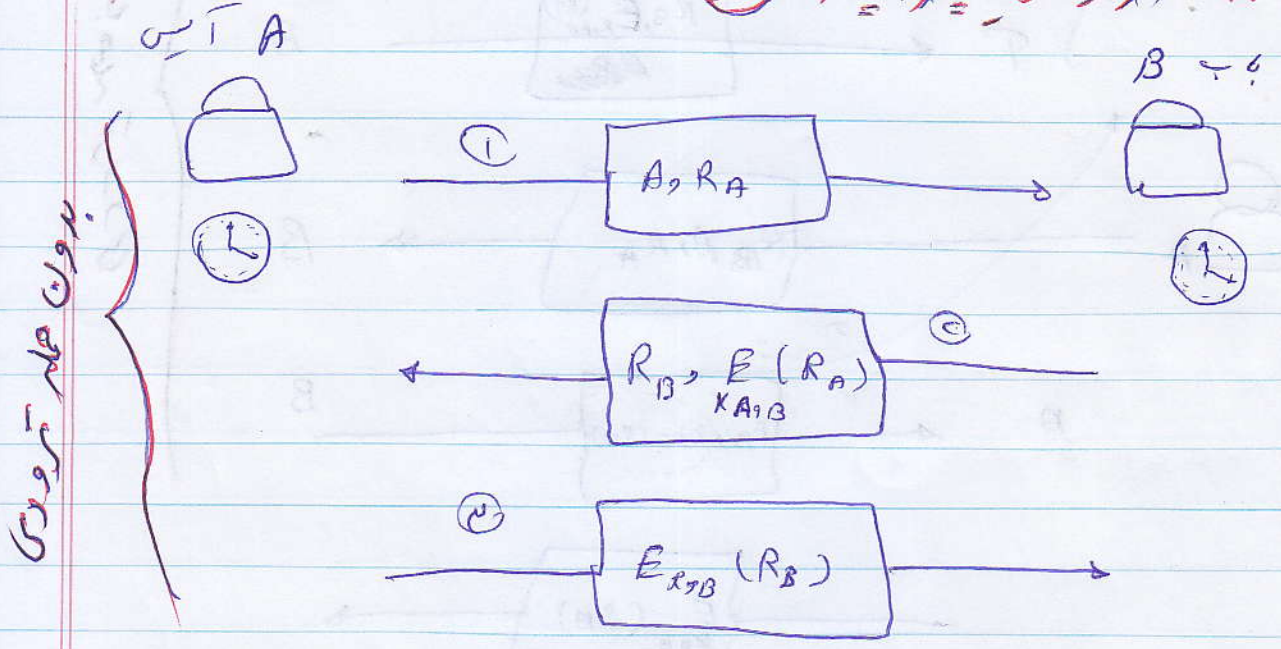
با رمزنگاری R_B نتیجه را برای آیین ارسال می کند و آیین با مقایسه نتیجه از قبل

R_B با مقدار دریافتی از هویت به مطمئن می شود که دارای نسخه کلیش از

هویت یکدیگر مطمئن شده اند و می توانند با انتقاب یک کلید تماس یک کلید مشترک انتقاب

و برای ادام نشت پیشنهاد دهند.

★ احراز هویت یکطرفه ۳ مرحله‌ای (چالش پاسخ ۳ مرحله‌ای) :



★ در آخر نشان میدهیم با این انجام ۳ شناخت احتیاجی نیز نیز و مکانیسم ایجاد می‌شود

فرض کنیم که B باب یک سرویس دهنده است که بطور همزمان با چندین کارمند سرویس

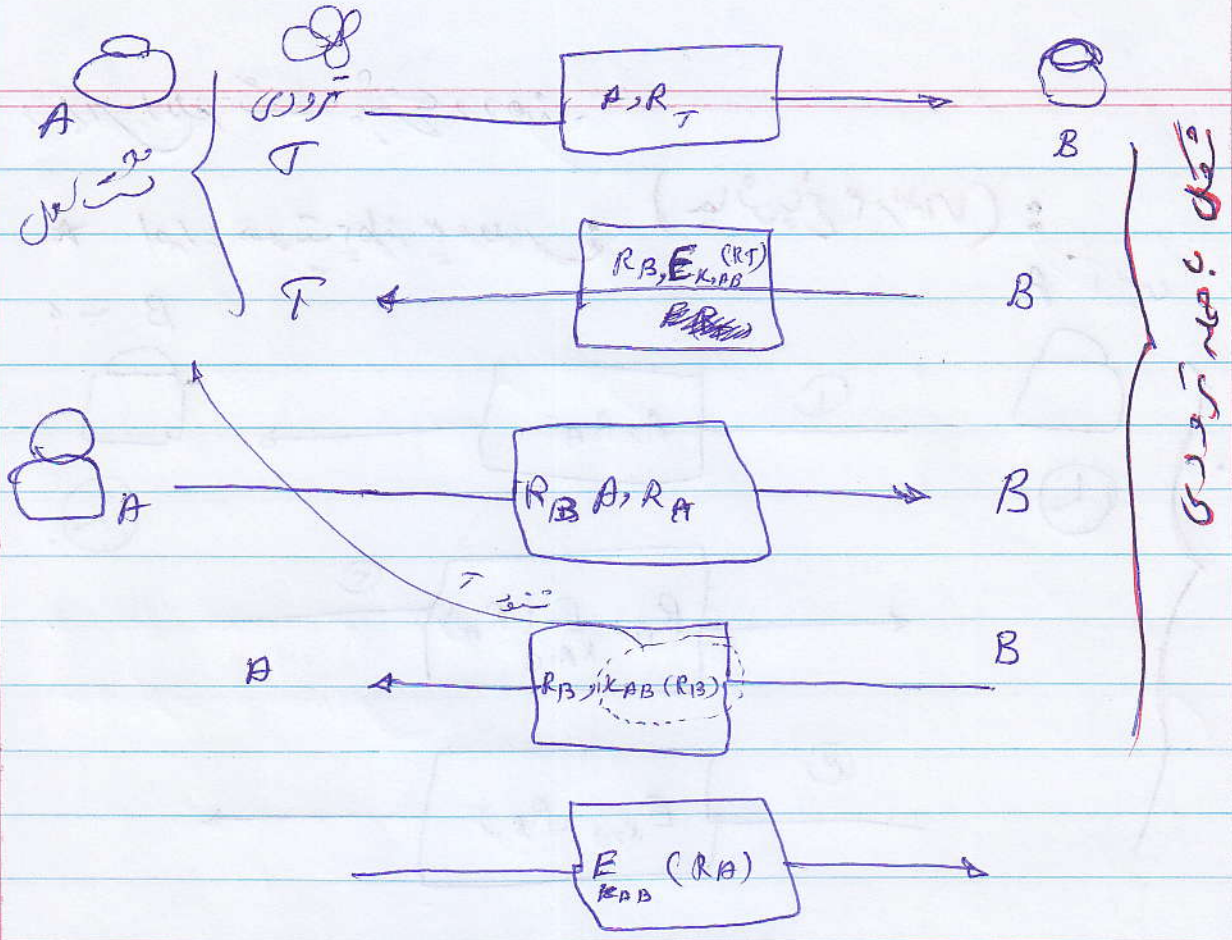
دهنده درخواست دارد ممکن است با چندین مشتری درتعامل باشد که پس از احراز هویت

و دریافت به کارخ سرویس دهد. در بسیاری از سرویس دهنده‌ها این فایلت

این ضرورت اساسی است. حال سناریوی زیر که تردیدی در نفس کند اطلاع نگیر

درآمده هست و خواهد خود را به باب جا زده و از آلیس سرویس بگیرد. لذا حمله‌ای با عنوان حمله باب

"Reflection Attack" را ترتیب دهد:



اشکالات کدوم پروتکل وارد است؟ چه طوری برطرف

پروتکل احراز هویت بیدهام شرودر:

۱): آلیس در اولین گام شناسه کاربری خودش "A" شناسه کاربری سرویس دهنده "B" و رشته تصادفی R_A را برای مرکز توزیع کلید ارسال می‌کند.

۲): مرکز توزیع کلید، ساختمان داده‌ای با ۵ آیتم زیر تولید و با کلید سری آلیس رمز کرده و برای او پس می‌فرستد.

نقش KDS پس از صدور بلیط خاتمه می‌یابد.

۳) : حال آلیس پس از رمزگشایی آیتم هایی که KDS فرستاده، می‌تواند مؤلفه بلیط و کلید نشست K_S را استخراج کند. لذا در پیام سوم با انتخاب رشته چالش بزرگتر R_{AF} آن را با کلید نشست رمز کرده و نتیجه را به همراه بلیط به باب می فرستد.

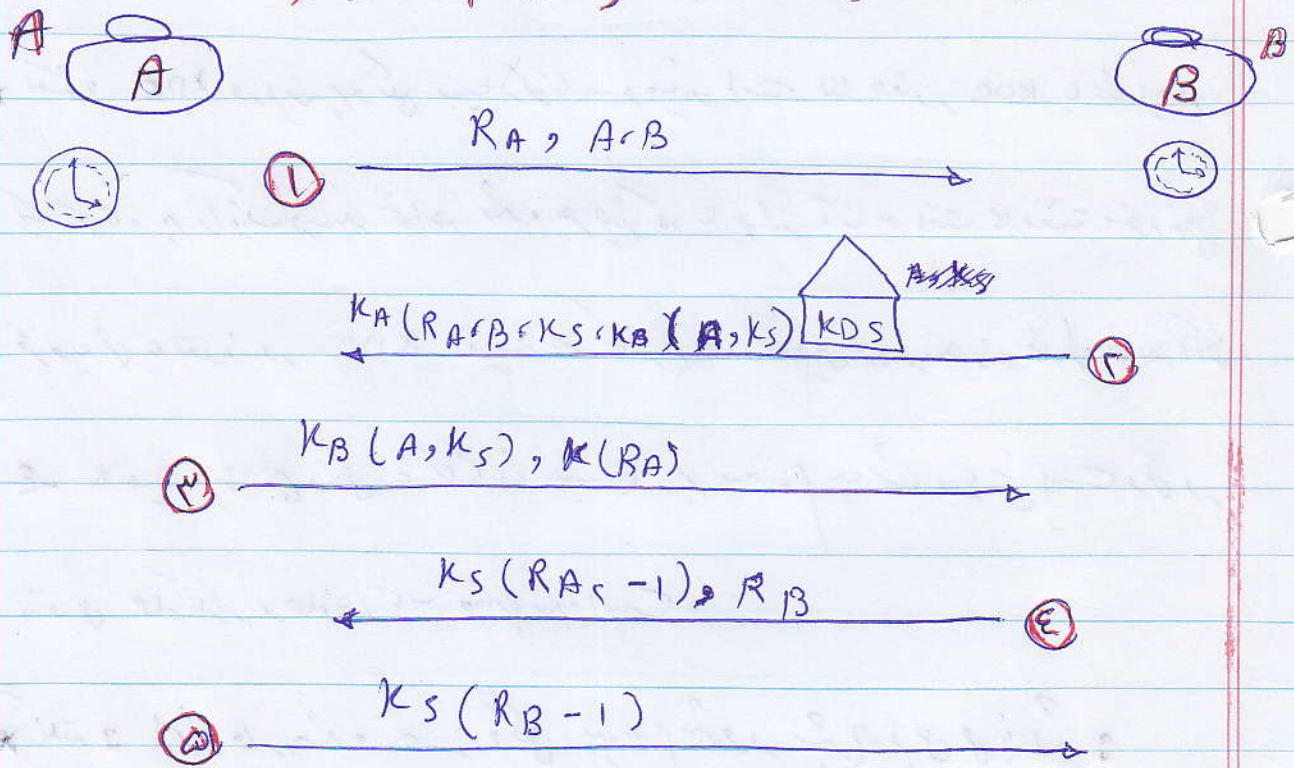
نکته : باب تنها کسی است که می‌تواند بلیط را از رمز خارج کند. بلیط داخل آن که R می‌شد از کلید نشست و هویت بدست آورد.

۴) : برای آنکه باب نیز هویت خود را به آلیس اثبات کند، پیش از رمزگشایی R_A با کلید نشست K_S، یک واحد از آن کم و نتیجه را با رشته‌ای با کلید نشست رمز کرده و به همراه کلید چالش خود R_B به آلیس پس می فرستد.

۵) : آلیس پس از دریافت آیتم های پیام چهارم، ابتداء با کلید نشست، مقدار R_{A_2} را رمزگشایی کرده و آن را پس از امتزاج یک واحد با مقدار ارسالی مقایسه می‌کند تا مطمئن شود پیام دریافتی او دقیقاً با تقاضای او موجود و تکراری نیست. دقت کنید که باب از R_{A_2} یک واحد کم کرده که یک تغییر در R_{A_1} ایجاد کند زیرا $K_S(R_{A_1})$ از پیام

سوم قابل استراف سمع و ارسال مجدد است. حال آلیس با کمک یک واسط کلید مشترک K_S را رمز کرده و برای باب می فرستد تا حضور فعّال او برای باب اثبات شود و باب نیز اطمینان حاصل کند که پیام سوم متعلق به زمان‌های قدیمی نیست.

⇐ شکل پروتکل احراز هویت بیدهام شرودر ⇒



⇐ خواص پروتکل بیدهام شرودر ⇒

نکته مهم: اگر شرودی با فریبکاری در حین ارسال پیام اول (R_A) یا حتی شناسه کاربری باب (B) را تغییر بدهد، آلیس بلافاصله در پیام دوم (رمزشده) از موضوع را کشف خواهد کرد و فطرتاً آنقدر پیام دوم رمزشده شده شرودی نمی‌تواند تغییرات دلخواه را در پیام دوم گونه‌ای ایجاد کند که آلیس گول بخورد.

★ اگر تروری در پیام ارسال شناسه کاربری آلیس یعنی A را تغییر بدهد و شناسه آن را با شناسه کاربری خودش عوض کند و پیام برگشتی با کلید آلیس رمز شده و طبیعتاً آلیس پس از رمزگشایی به درست نیامدن هیچ تطابقی با پیام کلیدی ندارد و از موضوع به راحتی کشف می‌شود. از طرفی مقدار تغییر یافته A درون بلیط هم درج می‌شود و باب این موضوع را خواهد فهمید.

★ تنش KDC در این پروتکل بسیار کوتاه و مفید است لذا حضور KDC باعث ایجاد یک گلوگاه ترافیک در شبکه خواهد شد، هرچند که بعد از آن به دلیت می‌توان سود زیادی متوجه KDC است هکر این سرویس دهنده‌ها را مخاطره خواهد افکند.

۴- ۶ هیت از پروتکل، گمان مبتنی بر مفهوم چالش و پاسخ است ولی در مقابل حمله تکرار و حمله باز تاب مقاوم شده است.

★ نکته: ایرادوارد شده به پروتکل بیدهام شود شرح ذیل می‌باشد:

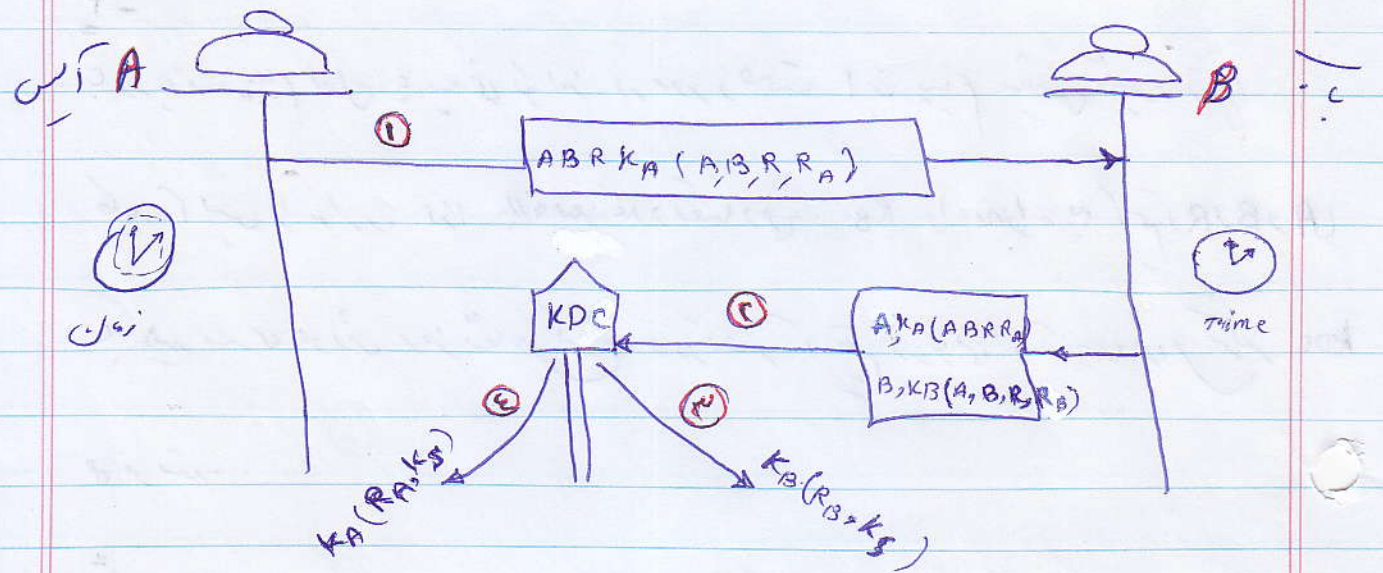
- با توجه به قدرتمند بودن امنیتی پروتکل مورد انتقاد وارد شده به آن اینست که:

★ معمولاً نظر به آنکه کلیدهای نشست K_s کلید مصرف هستند و در هر بار تغییر می‌کنند لذا عموماً افراد و نرم افزارها در نگهداری این کلیدها دقت لازم را نداشته و هرگاه به هر دلیلی تروری بتواند یک کلید نشست قدیمی را از روی ماشین (سیستم) آلیس بدست بیاورد می‌تواند حمله تکرار را از مرحله سوم پروتکل آغاز نماید مشروط به آنکه قبلاً بلیط را استراق سمع کرده باشد، بدیهی است که عدم مراقبت از کلیدها امنیت هر روشی را به خاطره انداخته ولی در اینجا ارزش ذکر کردن آن را دارد که معمولاً روشهای سنت گیرانه‌ای را در مورد کلید رمز اعمال می‌شود ولی در خصوص کلیدهای نشست اینگونه نیست.

امتحان میان ترم - ۹۴/۲/۱۷ پنجشنبه ساعت ۱۰:۱۵ تا ۹:۴۵
تا آخر جلسه هفته بعد

پروتکل احراز هویت «آتوی - ریس ۱»

((جلسه هفتم)) ۱۹ اسفندی



۱- آلیس کار خود را با تولید ۲ عدد تصادفی آغاز می‌کند. R که به عنوان شناسه مشترک بعدی مورد و R_A که در رشته چالش آلیس شناسه گذاری می‌شود.

در اولین پیام آلیس شناسه کاربری خود و شناسه مشترک را به صورت آشکار (A) (R) به همراه یک آیتم رمزنگاری شده چالش با کلید K_{AC} برای باب می‌فرستد. آیتم رمز شده در حقیقت حاوی رمز(R_A و R و B و A) با کلید متقارن آلیس است. از این رو آیتم فقط R_A است که از چشم ترودی مصون می‌ماند.

* توصل به تئوری اطلاعات که در شبکه‌های رمزنگاری کاربرد دارد.

$$Information(A) = -Log P_A \qquad 1010101010 \Rightarrow \frac{1}{2^{10}}$$

$$I(A) = -Log \frac{1}{2} = 1bit$$

طبق این اصل هرچه احتمال وقوع یک پدیده کمتر باشد اطلاعات بیشتری دارد و یک پدیده قابل پیش‌بینی حاوی اطلاعات کمی است و هر چه عضو بیشتر باشد احتمال وقوع کمتر است.

از بین این بلاک آیتم فقط R_A که از چشم ترودی خارج می‌ماند.

۲-

باب دریافت پیام اول باب نمی‌تواند در مورد صحت این پیام تصمیمی بگیرد زیرا کلید آلیس را ندارد. لذا علاوه بر عدد تصادفی R_B را به همراه ۳ آیتم (A و B و R) با کلید سری خودش رمزنگاری کرده و در یک آیتم در بافتی از آلیس برای مرکز KDC می‌فرستد.

۳-

مرکز KDC کلید همه را در اختیار دارد. لذا آیتم مربوط به آلیس را با کلید آلیس و آیتم مربوط به باب را با کلید باب از رمز خارج کرده و در اولین گام مقدار R را از هر دو آیتم استخراج و مقایسه می‌کند تا ثابت شود که این دو پیام دریافتی به یک درگیر تولید شده‌اند. هرگاه هر دو پیام R با هم یکی بودند KDC متقاعد می‌شود که پیام ارسالی از باب در پاسخ به تقاضای کنونی آلیس صادر شده است. در این مرحله KDC برای آلیس و باب یک کلید نشست K_S تولید و آن را به همراه رشته‌هایی از آزمایش‌ها رمزنگاری با کلید متناظر به آنان می‌فرستد.

۴-

پس از دریافت $K_A(R_A, K_S)$ ابتدا آن را از رمز خارج کرده و R_A را

سایت « مرکز خرید اینترنتی digikala.ir »

ارسال رایگان و در سریع‌ترین زمان ممکن به دست شما

با رشته چالش آخر مقایسه می‌کند، همین کار توسط باب با کلید عمومی $K_B(R_B, K_S)$ انجام میگیرد و هرگاه بوب رشته چالش خود را در پیام‌های ارسالی از KDC دید می‌تواند با اطمینان، نشست خود را آغاز کند. از این مرحله به بعد تمامی مکالمات با کلید نشست K_S رمز خواهد شد.

ظرافت‌های امنیتی پروتکل "آت وی رس"

آتوی رایس

۱- از آن‌جا که هیچ کس در بخش جزء KDC کلید سری آلیس را نمی‌داند لذا آلیس و باب با دیدن رشته چالش خود در درون پیامی که از KDC می‌رسد مطمئن خواهند شد که این پیام هرگز تکراری نیست و بدین خواهد توانست از حملات تکرار پیشگیری خواهد کرد.

۲- اگر شخص ثالثی مثل ترودی در آیتم‌هایی که در پیام اول بصورت آشکار ارسال می‌شود تغییری ایجاد کند، این موضوع در KDC کشف خواهد شد زیرا که در این پیام رشته چالش آلیس رمز شده نیز هست و این عدم تطابق به سادگی قابل تشخیص است.

۳- باب تا آلیس در اولین پیامی که برای او ارسال می‌کند در حقیقت برای کلید نشست خود را می‌آزماید، زیرا در صورتی که به هر دلیل کلید نشست خود را به درستی نسبه نکرده باشد پیام ارسالی آن‌ها از سمت خواهد شد.

پروتکل احراز هویت کرب روس KERBEROS

* اصول پایه ای پروتکل کرب روس : «خیلی مهم است»

۱) : هر موجودیت متقاضی سرویس باید هویت خود را اثبات کند.

۲) : هر سرویس دهنده دارای کلمه عبور است و تحت ضوابط خاص سرویس می دهد.

۳) : هر کاربر در اولین مرحله از ورود به سیستم (لاگین Login) هویت خود را اثبات میکند ولی برای سرویس گرفتن از هر سرویس دهنده باید مجوزهای جداگانه ای اخذ کند

* مقاله های اصلی در "کرب روس" عبارتند از:

۱- AS (Authentication server)

هر کاربر در اولین مرحله از ورود به سیستم یعنی فرآیند Login موظف است هویت خود را به این سرویس دهنده اثبات کند.

۲- سرویس دهنده TGS (ticket granting server)

این سرویس دهنده برای دریافت هر نوع سرویس از سرویس دهنده ها در سطح شبکه بلیط صادر میکند.

۳- سرویس دهنده یا سرور (server)

این سرویس دهنده پس از دریافت بلیط، سرویس خاص را به مشتری ارائه میکند. کاربر این سرویس دهنده ها نیاز است.

روال دریافت سرویس در سیستم کربروس

۱- آلیس مانند تمام کاربران دیگر دارای کلید سری است و متقابل سرویس دهنده AS از آن با خبر است. لذا در اولین مرحله از ورود به سیستم، آلیس باید از طریق ایشگاه کاربری خود لاگین کند. این کار با ارسال آشکارشده کاربری آلیس (A) به AS شروع می‌شود.

۲- سرویس دهنده AS دو آیتم K_S و کپی‌پیمایت رمزشده با پیمایت $TGS(A,K_S)$ را برای آلیس تولید کرده و پس از رمزنگاری با کلید سری کاربر آلیس می‌فرستد.

$K_{tgs}(A,K_S)$

$$\{A_S, K_S, K_{tgs}(A,K_S)\} \rightarrow K_A(K_S, K_{tgs}(A,K_S))$$

کلید سری سرویس دهنده TGS (کلید تیکت) — کلید نشست — بلیط (تیکت)

۳- آلیس پیام دریافتی از AS را با کلید سری خود رمزگشایی کرده و کلید نشست و بلیط خود را از (پیام) آن استخراج می‌کند. سپس بلافاصله کلید سری خود را از حافظه پاک می‌کند تا پیش از کسری از ثانیه در حافظه اصلی باقی نماند. حال هزینه ل

که آیس بخواهد از هرکدام از سرویس دهنده‌های شبکه تقاضای سرویس

بدهد با بلیط خود یعنی $K_{TGS}(A, K_B)$ همراه شناسه سرویس دهنده

مقصد تقاضش یعنی B را برای TGS ارسال کند. TGS با توجه به سرویس دهنده B (یا بانک)

در ضمن او با یدی که رفتی و زمان صدور بلیط را به کمک کلید نشست رمزگرده و نتیجه

را به عنوان تیکت سوم ضمیمه کند.

۴- سرویس دهنده TGS ابتدا با کلید متری خود بلیط را رمزگشایی کرده

و از داخل محتویات آن کلید نشست و شناسه آیس را استخراج کند.

سپس با کلید نشست آشکار شده (K_S) رمز شده کلید نشست مورد نظر را رمزگشایی کرده و زمان

صدور بلیط را بدست آورد که مبادا بلیط قدیمی و تکراری باشد. در صورتی که تازگی بلیط

بلیط محرز شود مشخصات آیس مجوز دریافت سرویس درخواستی را داشته و TGS

برای آیس و سرویس دهنده یک کلید نشست K_{AB} تولید و آن را همراه شناسه B با کلید

نشست K_S رمز کرده تا آیس بتواند بدست آید:

$$K_S(B, K_{AB})$$

که این عبارت در حقیقت بلیط آیس برای گرفتن سرویس دهنده B است.

حبس ← ادامه در صفحه بعد

تکته: در این مرحله تیکت در پیام ۳ از آیس ارسال می‌شود تا آیس بتواند با این بلیط از سرویس

دهنده درخواست سرویس کند. برای این کار آیس ابتدا با کلید K_S ۴

$K_S(B, K_{AB})$ را از رمزخارج کرده پس از بررسی درستی نام سرویس دهنده کلید مشترک K_{AB} را از روی آن استخراج می‌کند.»

← سپس A تیکت رمزگشایی به صورت $K_B(A, K_{AB})$ تولید می‌کند که در حقیقت بلیط آیس جهت مراجعه به سرویس دهنده B است. این تیکت (بلیط) را برای آیس ارسال می‌شود تا آیس بتواند با این بلیط از سرویس دهنده درخواست سرویس کند.

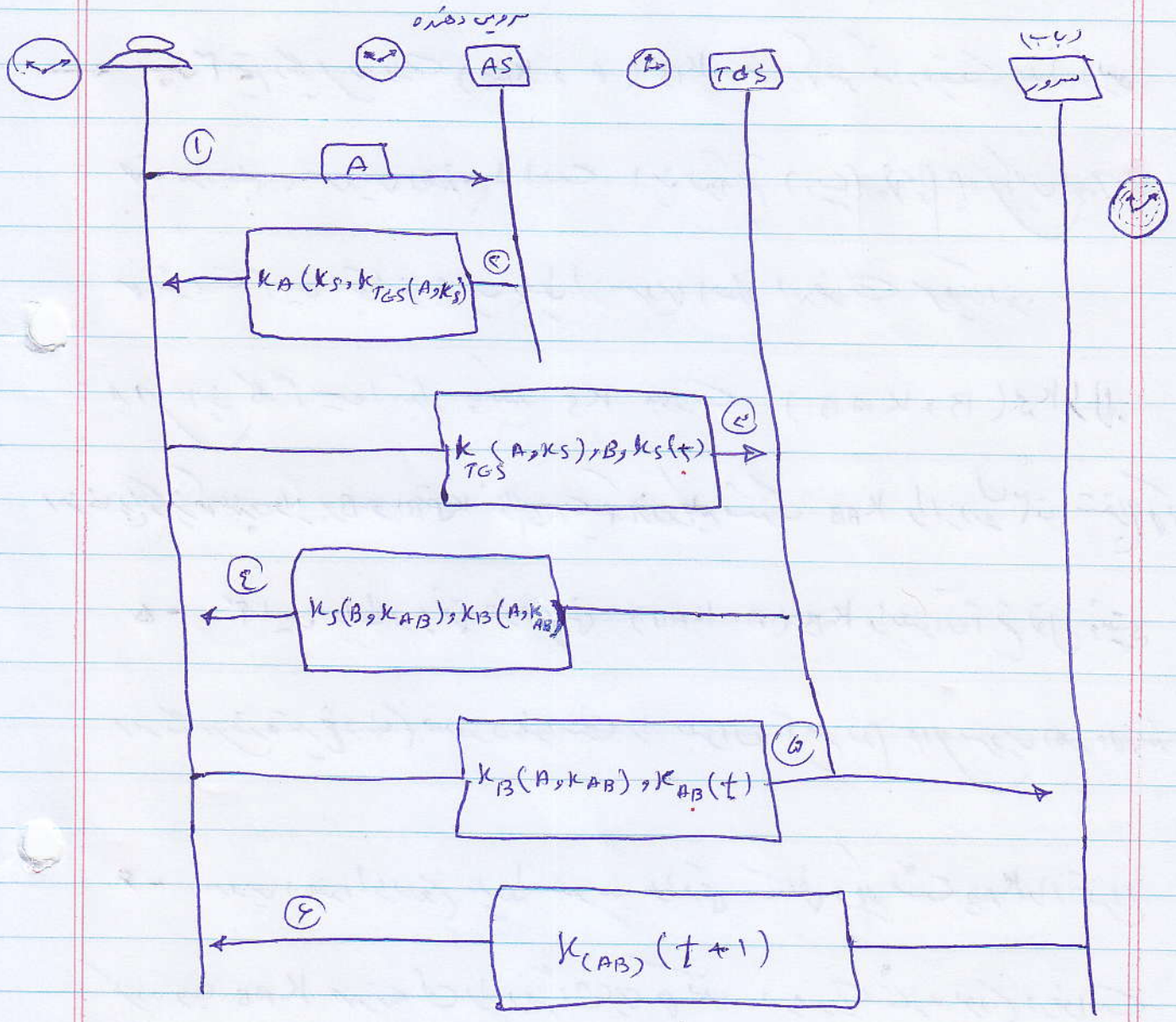
برای این کار آیس ابتدا یک K_S تولید کرده $K_S(B, K_{AB})$ را از رمزخارج کرده و پس از بررسی درستی، نام سرویس دهنده کلید مشترک K_{AB} را از روی آن استخراج می‌کند.

۵- آیس بلیط رمزشده خود یعنی $K_B(A, K_{AB})$ را بعنوان آیتم اول و تیکت رمزنگاری شده تاریخ و زمان صحت درخواست را بعنوان آیتم دوم برای سرویس دهنده می‌فرستد.

۶- سرویس دهنده از روی بلیط هویت و کلید مشترک K_{AB} را استخراج کرده و با K_{AB} مهر زمان را رمزگشایی می‌کند. در صورت تازه بودن درخواست با استفاده از یک ولیدی مهر زمان آن را برای آیس پس می‌فرستد، با این کار هویت سرویس دهنده ثابت می‌شود. چرا که فقط B می‌توانسته بلیط خود را رمزگشایی و از روی آن K_{AB} را استخراج و مهر زمان را بررسی کرده و به آن پاسخ بدهد.

پس از پایان مرحله ششم آلیس و سرویس دهنده تا خواهند بود با کلید مشترک

K_{AB} یک نشست مفشن و رمز نگاری شده برگزار کنند.



آغاز نشست

★ محاظ کردن زمان که بصورت + در ارتباطات وجود دارد برای جلوگیری از حمله تکرار است.

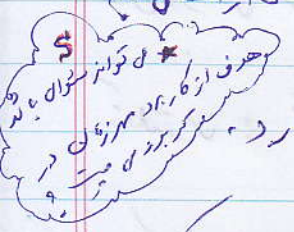
یک نکاتی در مورد کرب روس :

نکته (۱): بلیط ها به نام حمار می شوند بدین معنا که هویت متقاضی بلیط به صراحت در متن بلیط درج می شود. بدین ترتیب امکان آنکه کسی

با عالی‌ترین سطح مجوز، بتواند برای افراد بدون مجوز بلیط تهیه کند منتفی است.

در ضمن اگر شخص ثالث مثل مرورگر کلیدی را اسناق سمع کرد گذشته از آن که قادر به استخراج کلید نشست از درون آن نیست نمی‌تواند آن را با نام خودش به سرویس دهنده بفرستد.

نکته ۲: امکان همه کلدار منتفی است زیرا تقاضاهای ارسالی به سرویس دهنده صرف بلیط و سرویس دهنده زمان دارد.



نکته سوم: فرض کنید شخص ثالث مثل مرورگر پیام سوم را اسناق سمع کند و قبل از آن که اعتبار زمان آن منقضی شود آن را کنار کند در این صورت سرویس دهنده چون آن را با توجه به آن که هنوز زمان اعتبار پیام منقضی نشده بدون اعتنا به تکراری بودن آن پیام چهارم را به مرورگر تحویل خواهد داد. ولی هیچ کلیدی وجود ندارد، زیرا مرورگر کلید k_S را از رمزنگاری عبارت $k_S(B, k_{AB}), k_B(A, k_{AB})$ و طبعاً نخواهد بود آنگاه $k_{AB}(t)$ را پیدا کند.

نکته ۴: در کیب روس گذشته از آن که هیچ کلمه عبوری به صورت آشکار در خط منتقل نمی‌شود شاه کلید پس از چند میلی ثانیه دیگر قابل استفاده نخواهد شد.

نکته ۵: در ساختار کرب روس فقط A_S کاربران را می‌شناسد و کلید آن‌ها را

در اختیار دارد. همچنین TGS با سرویس دهنده ها سروکار دارد و

برای آن بلیط صادر میکند

نکته ۶: سرویس دهنده AS و TGS از دیگاه منطقی از هم جدا هستند

ولی در عمل می توانند بر روی یک ماشین واحد اجرا شوند.

نکته ۷: اگر سرویس های مختلف بر روی یک ماشین واحد ارائه شوند با توجه به آنکه

هرکدام هویت جداگانه ای دارند، برای هرکدام بلیط جداگانه ای صادر خواهد شد.

نکته ۸: هر پروسه بر روی ماشین آلیس که نیازمند سرویسی باشد باید مستقلاً

بلیط تهیه کند. به عبارت دقیق تر TGS بلیطی را برای یک پروسه جهت

دریافت صرفاً یک سرویس خاص ارائه میکند

نکته ۹: با بلیطی که توسط سرویس دهنده AS صادر می شود می توان به دفعات از TGS

تقاضای صدور بلیط از سرویس دهنده های مختلف داشت.

نکته ۱۰: پس از پایان مرحله ششم بین پروسه مشتری و پروسه سرویس دهنده

نشست شکل میگیرد که تا پایان رسمی نشست نیاز به احراز هویت ندارد و از آنجایی که

با کلید نشست رمز شده، نشست امن است.

نکته مهم: رمزنگاری نامتقارن در کنار رمزنگاری متقارن تکمیل کننده سرویس های

امنیتی است.

★ توابع درهمساز را تعریف کنید؟

★ مفهوم شکل چنبره ساز چیست؟

★ رمزنگاری متقارن و رمزنگاری نامتقارن را تعریف کنید؟ نمونه از هرکدام

★ طول کلید ۱۲۸ ۱۹۲ و ۲۵۶ بیت و طول قالب ۱۲۸ بیت

نکته ۱۱: در کربروس بلیط ها برحسب نام کاربری userid و آدرس ماشین از شبکه صادر میشود یعنی حتی اگر از یک ایستگاه کاری work station به ایستگاه کاری دیگری تغییر موقعیت بدهد، قادر به استفاده از بلیط های قبلی خواهد بود و باید از نو تمام مراحل احراز هویت را تکرار کند. بدین ترتیب تغییر میدا و مقصد یک نشست فعال از یک ماشین به ماشین دیگر ممکن نیست

نکته ۱۲: در کربروس سرویس دهنده TGS تقاضای صدور بلیط را از طرف جواز دسترسی ارزش یابی میکند، لذا یک بانک اطلاعاتی خاص سطوح دسترسی کاربران را مشخص کرده است. همین کار در سرویس دهنده های دیگر انجام میشود.

★★ ۱۳: در شبکه یک کربروس امکان استفاده از هر روش رمزنگاری کلید متقارن وجود دارد، در حالی که نسخه های قبلی عملا به DES وابسته بودند ★★ هر کاربری که در خلال مراحل اول و دوم ابتدای احراز هویت و پس به شبکه وارد

می شود بلیط به شکل ($K_{TGS}(A, K_S)$) دریافت می دارد که برای

مدتی معتبر است و او می تواند به کرات از این بلیط بهره بگیرد و با

شروع از مرحله سوم برای دریافت خدمات از هر سرویس دهنده دیگر شبکه

تقاضا بدهد. برای این کار کافی است در پیام سوم نام سرویس دهنده

مورد نظر درج شود. در پاسخ بلیط و خواهد گفت که مربوط به

همان سرویس دهنده است.

** صدور بلیط یک سرویس دهنده برای کاربران بدین معنا نیست که

کاربر می تواند با ارائه بلیط به سرویس دهنده هر سرویس دلخواهی را

دریافت کند، بلکه خود سرویس دهنده هم ممکن است کاربران را وادار

به یک لاگین مجدد کند و دسترسی او به ضوابط خاص فراهم کرده.

ویژگی های جدید کرب روس نسخه پنجم

۱- برای آنکه ستیم کرب روس قابلیت گسترش و ربط شبکه بیشتر از یک را داشته باشد

سعی شده که کل شبکه بصورت سلسله مراتبی در قالب حوزه علمرو تقسیم بندی شود.

هر علمرو برای خودش یک سرویس دهنده As و یک TGS دارد که به کاربران

علمرو خودش را به آنها می دهد و این امکان وجود دارد که مسئول شبکه

قلمروها و سرویس دهنده KDC را به گونه‌ای تنظیم و پیکربندی کند که سرویس دهنده KDC از یک قلمرو اجازه داشته باشد برای همه یا تعدادی از سرویس دهنده‌های قلمرو دیگر، بلیط صادر کند.

گ: امکان این دو اعتماد متقابل بین KDC در دو قلمرو مستلزم چیست؟

مستلزم آن است که بین آنها کلیدی مشترک تعریف شود. در نتیجه هیچ از دو قلمرو های مختلف و تفویض صدور کلید به سرویس دهنده از نوع بخوبی حمایت می شود.

ک: نسخه پنجم در حدود ۲۸۰،۰۰۰ کار آزمایش شده است.

گ: سئوالات میان ترم: انواع حملات و تعریف - رمزهای متقارن و نامتقارن - مفهوم امنیت اطلاعات - تفاوت کدینگ و رمزنگاری - توابع درهم ساز (مفهوم شکل حیات)

بحث‌های قبلی از امنیت خود امّا صنعت بیشتر روی معماری شبکه خواهد بود.

★ معماری شبکه با امنیت شبکه در لایه های TCP/IP :

۱- امنیت در لایه کاربرد

۲- امنیت در لایه انتقال

۳- امنیت در لایه شبکه

۴- امنیت در لایه پیوند داده

۵- امنیت در لایه فیزیکی

۶- داده ها

★ کلیه ی کلیات امنیتی یا تضمین امنیت اطلاعات یعنی ۳، در این لایه ها عمل زیر:

۱) ★ امنیت در لایه فیزیکی: حراست فیزیکی از کانال انتقال، استفاده از تکنیک های FHSS و DSSS در شبکه های بی سیم، کنترل دسترسی های فیزیکی به منابع داده ها.

۲) ★ امنیت در لایه پیوند لایه: رمزنگاری لینک، استفاده از استانداردهای امنیتی WEP، WPA، IEEE ۸۰۲.۱۰۹.

۳) ★ امنیت در لایه انتقال: رمزنگاری کامل یک اتصال، استفاده از SSL و TLS

۴) ★ امنیت در لایه کاربرد: پیاده سازی مکانیزم های امنیتی در سطح برنامه کاربردی SET و PGP

★ مفهوم حمله DOS : حمله اختلال در سرویس دهی یکی از مهمترین حمله ها در شبکه می باشد و باعث از بین رفتن سرویس می شود.

★ مفهوم رمزنگاری لینک: یعنی رمزنگاری لینک یعنی رمزنگاری بر روی بیت های ارسالی بر روی لینک. بدین است که فقط لینک حفاظت می شود.

END to END

رمزنگاری انتها به انتها: هرگاه اطلاعات در سمت چپ سرور تولید شده داده ها رمزنگاری شوند این اطلاعات صرفاً در پروسه زمانی مقصد از بلوک خارج شده و در اپراتور و یا پروسه اصالت مورد استناد قرار گیرد اطلاعات امنیت انتها به انتها ایجاد شده است. همه اطلاعات و حتی هشدارهای امنیتی باید به گونه ای عمل امنیت انتها به انتها تمامی تلاش ها در لایه های زیرین ناکام و ناقص می ماند و نمی توان جزئی اطلاعات بین دو پروسه کاربری هم تبادل کرد.

web ← متن آشکار

برای تامین حداقل امنیت در شبکه های بی سیم

فریم (داده)

بدنه فریم (داده) | CRC

کمیته IEEE

پروتکل بی سیم وب بغرامنیت در سطح شبکه های

رشته تصادفی | RC4

wep (wride Equivelant Priday) سیم

بردار اولیه رشته تصادفی | IV | متن رمز شده

معرفی کرد. هدف از وب محروم نگه داشتن اطلاعات در سطحی معادل با

شبکه های متنی بر سیم مثل اترنت بوده است.

★ در که بیشتر بیت های پر ارزش و بیت های بی ارزش و جود دارد که علامت ۱ یعنی الحاق شدن با...

و یا مثل بیت های ۱۲۸ و ۳۲ در | MSB | LSB | که ۱۲۸ با ۳۲ ۱۶۰

۱۲۸ ۳۲

شبکه در نوع با ۱ | بدنه فریم | CRC | ۱۰۰ bit با ۳۲ bit

۱۰۰ ۳۲

★ مولد تولید شده رشته شبه همگانی در پروتکل وب RC4 و یا شده.

(PRNG)

★ الگوریتم RC4 از متن رمز شده کلید ۱۰۰۰۰۰۰۰ (key و IV) را تولید می کند.

★ در پروتکل web از رمز نگاری کلیدها در access point آکسس پوینت

است. چگونگی تعریف این کلیدها و توزیع آن بین کاربران در استاندارد IEEE

web ← متن آشکار

فریم (داده)

بدنه فریم (داده) | CRC

برای تامین حداقل امنیت در شبکه های بی سیم کمیته IEEE پروتکل بی سیم وب یعنی امنیت در سطح شبکه های

RC4 | رشته تصادفی

بردار اولیه | IV | متن رمز شده

رشته تصادفی

wep(wride Equivelant Privacy

معرفی کرد. هدف از وب محرمانه نگه داشتن اطلاعات در سطحی معادل با

شبکه های مبتنی بر سیم مثل اترنت بوده است.

* در که بیشتر بیت های با ارزش و بیت های با ارزش وجود دارد که علامت ۱ یعنی اتحاد شدن با...

در بیت مثل بیت های ۱۲۸ و ۳۲ در MSB | LSB که ۳۲ با ۱۲۸ یا

۱۶۰ bit یا ۳۲ bit | CRC | بدنه فریم

* مولد تولید شده رشته شبه هنگامی در پروتکل وب RC4 نام دارد. (PRNG)

* الگوریتم RC4 از متن رمز شده کلید ۰۰۰۰۰۰۰۰ (Key) را تولید می کند.

* در پروتکل web از رمزنگاری کلیدها در access spoint آکسس پوینت استفاده می شود. چگونگی تعریف این کلیدها و توزیع آن بین کاربران در استاندارد IEEE

تعریف شده است. لذا ممکن است این کلیدها با سازنده سخت‌افزار به مقادیر مشخص و پیش فرض تعیین شده یا شده و مسئول شبکه موظف است تا آن را تغییر دهد.

بند ۱ - از بدنه فریم که حاوی داده‌های خام است یک کد ۳۲ بیتی کشف خطا (CRC) استخراج و در انتهای داده‌ها اضافه می‌شود.

این کار با استفاده از یک چند جمله‌ای توان ۳۲ بدست می‌آید.

فریم داده ⟸ CRC ⟸ بدنه فریم | CRC

بدنه فریم: متغیر می‌تواند تا ۱۴۷۵ بایت
CRC: ۳۲ بایت
۱ byte + ۳۲ bit = ۱۴۷۵ bit

بند ۲ -
یک دنباله تصادفی دقیقاً هم اندازه با مجموع طول داده و CRC تولید می‌شود. تولید این دنباله تصادفی بر اساس الگوریتم رمزنگاری RC4 انجام می‌شود.

دنباله تصادفی ⟸ RC4 که حداکثر ۱۴۷۵ byte می‌تواند باشد.

★ خود الگوریتم RC4 یک کلید رمزشده و IV دارد.

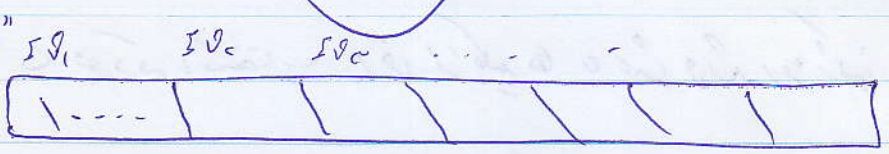
★ بند ۳ - پس از تولید دنباله تصادفی داده‌های مرحله قبل (حاصل CRC) و این دنباله با آن XOR انجام می‌شود تا متن رمزشده بدست بیاید.

بند ۴ - دقت شود که طول IV ۲۴ بیت است.

IV | متن رمزشده

۲۴ bit

نکته: ایده‌ال این است که از هر فریم از یک Cache چند فریم استفاده شود



مشکل کار در web این است که از یک Cache ۲۴ بیتی استفاده می‌کند.

۴) ایرادات وارد بر پروتکل web:

۱- معمولاً افراد هیچگاه زود به زود کلید مشتری خود را عوض نخواهند کرد و ممکن است این کلید ماه‌ها تغییر نکند. با این وجود اگر Cache نیز در فریم‌های مختلف یکسان باشد، امنیت فریم‌های داده از چار حمله و یا تهدیدات مختلف می‌توانند شود.

* همانطور که تغییر Cache برای فریم‌های متوالی در استاندارد توصیه شده ولی اجباری نیست و طبعاً بسیاری از سازندگان سخت‌افزارها برای ساده‌کردن کار خود به این توصیه عمل نکرده‌اند و از همان چون Cache کلاً ۲۴ بیت است با زیاد شدن کارت شبکه Cache از صفر شروع خواهد کرد. لذا نفوذگر می‌تواند به صرف وقت بیشتر و استراق سمع هزاران فریم از یک ایستگاه، فریم‌هایی با Cache های یکسان را دسته‌بندی کرده و آن‌ها را جدا، جدا بشکند. زیرا احتمال کلید برای همه آن‌ها یکسان است.

Cache = ۲۴ bit

$2^{24} = 16777216$ ولی یکی: 2^{24} که توسط کامپیوترها تشخیص داده شده

۲- اشکال دیگر مشهوراً به الگوریتم RC4 وارد می‌کنند، اشکال اصلی RC4 آن بود که انتخاب برخی از کلیدها باعث رمزشکنی داده‌ها بسیار ساده شود. بنابراین انتخاب کلید باید با دقت انجام گیرد تا کلیدهای ضعیف حذف گردند. چنین الزامی هرگز متعارف و منطقی نیست و هیچگاه کلیدهای قوی

★ سازندگان از الگوریتم‌ها حمایت می‌کنند که بصورت یکسان عمل کرده و کلید ضعیف و قوی برای الگوریتم تفاوتی نمی‌کند

و ضعیف را چک نمی‌کند.

«ک»: ضعف RC4 چیست؟

(در پروتکل)

★ یکی از ایرادات وارده به پروتکل WEP آن است که به جای RC4 از پروتکل AES استفاده می‌کرد.

★ یکی از اشکالات وارده به این است که امنیت End to End از برخی راه‌ها تامین نمی‌کند.

۳- ایراد دیگری که به "وب" وارد آمده آن است که هیچگونه تمهیدی توسط برای مدیریت کلیدها اندیشیده نشده و تعریف و توزیع کلیدها بصورت دستی انجام می‌شود.

امنیت در سطح شبکه (لایه شبکه) : IPsec "آیپی سکیوریتی"

* در پروتکل IP هیچگونه سرویس امنیتی برای تضمین بسته های IP ارائه نشده است. وضعیت این موضوع ناشی از اعتقاد زمان بوده است. در دهه 90 شبکه اینترنت آنقدر بزرگ شده بود که نادیده گرفتن آن خود را به شکل یک معضل جدی نشان می داد. لذا یک کمیته ای بنام "IEPT" برای کارهای استاندارد سازی و الگوسازی های مختلف استاندارد سازی ایجاد شد.

IPsec دریک چارچوب کاری وسیع چندین زمینه از خدمات مستقل را در اختیار گذاشته است. که هر زمینه از این خدمات بصورت انتخابی در اختیار کاربران است. قرار بر این شد که پشتیبانی از IPsec در نسخه جدید IP اختیاری و برای نسخه ششم اجباری شود.

* خدمات IPsec را در چهار زمینه کلی دسته بندی کرد:

الف- رمزنگاری بسته های IP (شامل کل بسته یا فقط "پیلود" ("Payload").

ب- تضمین صحت و اصالت پیام ها.

ج- پیشگیری از حملات تکرار.

نکته: در IPsec می‌توان روش امنیتی متقارن و یا کلید توزیع کلید را تغییر داد. بدون آنکه روی سرویس IPsec تغییری لازم باشد.

مهمترین ترتیب اعتبار IPsec به اعتبار الگوریتم رمز یا الگوریتم احراز هویت نگه داشته شده است.

* IPsec یک متدی است که در لایه شبکه کار می‌کند و یکی از خوبی‌های مثبت آن این است که کاربر با هر قابلیت فنی آن درگیر نیست.

* IPsec بر خلاف IP نیاز هست نوعی از ایجاد اتصال در سطح لایه شبکه است.

* مفهوم اتصال امنیتی چیست؟ در ادبیات IPsec به فرآیند ایجاد اتصال و هماهنگی های لازم: اصطلاحاً «سکیوریتی اسوسیشن» "Security Association" یا به اختصار SA و گوشی یا اتصال امنیتی و گویند.

شیوه عملکرد IPsec

الف: حالت انتقال

ب: حالت تونل

الف: هرگاه دو ماشین بخواهند مستقیماً و به واسطه با یکدیگر بسته های IP خود را مبادله کنند، با ایجاد ۲ اتصال امن یا به عبارتی ایجاد دو SA، بسته های IP را پیش از تحویل با یک سرآیند امنیتی موسوم به سرآیند IPsec تازه و فیلدهای مربوط را مقداردهی میکنند. این فیلدها شامل اطلاعاتی نظیر شناسه SA، شماره ترتیب بسته و امضای دیجیتال بسته است. سپس داده های رمزنگاری شده در بسته IPsec قرار میگیرد. پس از تحویل بسته IPsec این بسته مستقیماً دریافت پذیرنده خواهد شد. بدین ترتیب در حالت انتقال هر دو ماشین در شبکه میتوانند بطور مستقیم با یکدیگر تبادل امن داشته باشند.

اشکال کار: در اینجا است که هر دو ماشین در شبکه قبل از مبادله اطلاعات باید بر سر یک الگوریتم توافق کرده باشند.

ب: از این حالت وقتی استفاده میشود که بخواهیم دو شبکه راه دور را از طریق یک زیرساخت عمومی مثل اینترنت به هم متصل کنیم. بسته های IP درون این دو شبکه بصورت معمولی و بدون رمز مبادله میشوند و هیچ یک از روترهای داخل خود را با IPsec درگیر نمیکنند. بسته هایی که برای خروج از شبکه به

دروازه پیش فرض مرزی وارد می شوند به صورت کامل تصرف شده و در قالب یک قطعه اطلاعات خام مرتبط و امضاء می شوند. پس از این قطعه اطلاعات که هیچ محتوای آشکار و مفیدی ندارند پس از اضافه شدن سرآیند IPsec در یک بسته IP جدید قرار می گیرد که آدرس مبدأ آن میدیاب مرزی اول (ابتدای تونل) و آدرس مقصد آن آدرس میدیاب مرزی درست مقابل (انتهای تونل) است. به محض ورود بسته به میدیاب انتهای تونل محتویات بسته از سر خارج شده و پس از بررسی صحت و اصالت به شکل آشکار به بیت مسیر خود را در شبکه داخلی تا رسیدن به ماشین گیرنده ادامه خواهد داد.

نکته ۱): در حالت تونل بسته هایی که در میدیابی دیده می شوند محتوی آدرس مبدأ تونل و آدرس انتهای تونل را در خود دارند و هیچ محتوای بسته هیچ آثاری از تولید کننده و مصرف کننده نوع بسته و اطلاعات موجود در بسته نشان نخواهد داد.

نکته ۱: در حالت تونل شبکه های کد اسم مبدا و مقصد شون همون آدرس مبدا تونل و مقصد تونل است و کاری به آدرس اصلی خود ندارند و مابقی محتوی شبکه هیچ تغییری نکرده و همانطور که مشاهده میکنید تمامی شبکه ها اطلاعات محتوی شبکه شان را خواهند داد. از همین رو بدلیل وجود امضای دیجیتال به ازای هر شبکه امضای هر تکه داده شکاری در محتوی شبکه ها مشترک است. نکته ۲: IPsec در مدل TCP/IP در لایه سوم یا لایه شبکه IP قرار گرفته است. نکته مهم: هر گاه IPsec در حالت تونل یکی از راه حل های زیر را برای شبکه های راه دور از طریق اینترنت به یکدیگر است. به عنوان مثال فرض کنید یک سازمان و شعبات خود را در دنیا شبکه های از طریق اینترنت عمومی به یکدیگر وصل کند. IPsec در حالت تونل می تواند کانال امن و غیر قابل نفوذ بین این شبکه ها بوجود بیاورد.

سئوال: IPsec در دو حالت ذکر شده چه تفاوتی با لایه های OSI دارد؟

IPsec با استفاده از دو سرآیند AH (Authentication header) و ESP (Encapsulating security payload) به هر بسته IP اطلاعات امنیتی را اضافه می کند.

الف) سرآیند AH: هر دستگاه IPsec می تواند با استفاده از سرآیند AH به هر بسته IP فقط صحت و سلامت داده ها و هویت فرستنده بسته را از طریق

تضمین کننده ی محرمانگی اطلاعات هیچ کار خاصی را انجام نمی دهد.

(ج)

* در مورد IPsec چگونه می توان صحت سلامت داده ها را تضمین کرد؟

در بسیاری از کاربردها امکان دستیابی از نوع و محتوای تراکنش های کاربران آگاه باشد اهمیتی ندارد. اما جلوگیری از دستکاری اطلاعات (جلوگیری از حمله کننده ی میانی) حیاتی و اساسی ترین است (حمله کننده MiPla Attae).

در چنین حالتی سرآیند AH بسیار دقیق این نیاز را برآورده می سازد.

ب) سرآیند ESP : چگونه IPsec می تواند محرمانگی را تضمین کند؟

سرآیند ESP با رمزنگاری بخش داده ها و اطلاعات لایه ی بالاتر، محرمانگی را تضمین می کند. تا هیچ اطلاعاتی از شنود در بطن بسته ها مفقود نباشد.

تذکر: می توان IPsec را در یکی از دو حالت تونل و یا انتقال بکار گرفت و حتی می توان آن را در یکی از دو حالت AH (صحت و سلامت) یا ESP (برای احراز صحت در حین رمزنگاری) تنظیم کرد.

بدین نحو ترکیب این دو حالت و دو وضعیت را به وجود می آورد:

(د)

الف: حالت انتقال به همراه سرآیند AH

ب ، حالت انتقال به همراه سرآیند ESP .

ج ، حالت تونل به همراه سرآیند AH .

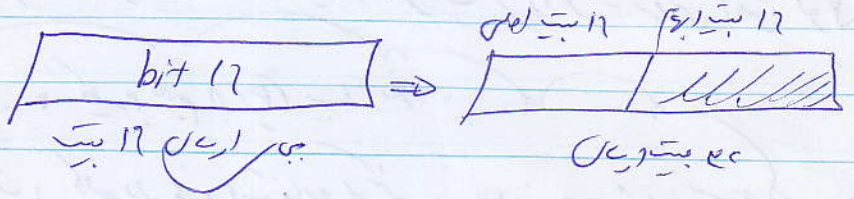
د ، حالت تونل به همراه سرآیند ESP .

IP	AH / ESP	محتویات

(د)

تذکر : از بین ۳ روش فوق ، حالت تونل به همراه سرآیند AH عموماً کاربردی ندارد.

★ تبادل کلید در IPsec : (ادامه سئوال)



(ه) اصول پشت گاه کلید کدام یک از موارد زیر (نمره دارد) امن است و چرا؟

ی) امضای دیجیتال و مزایای آن ؟ از کدام بررسی ها سئوال شده؟

✓ تبادل کلید در IPsec :

در IPsec وقتی دو موجودیت مستقل بخواهند با یکدیگر تبادل امن داشته باشند عموماً سه تعریف ۴ کلید دارد است :

۱- یک کلید برای عملکرد به حالت AH و یک کلید برای حالت ESP ؛ هر یک از این کلید

می‌توانند در زمان شناسایی لطمه‌های خود، از کلید خود ثبت) (که قبلاً به لطمه‌ای که
متقابل رسیده) استفاده کنند. یعنی بیشتر این که از سوی هر یک از طرفین
تولید و در سال پرسوز عمر، کلیدهای مشترک را فراموش شد.

به این ترتیب می‌بینیم که این رویکرد نتوانست به طور کامل به ایجاد دو SA (انتقال امنیتی)
تعریف
و تبادل کلید نیاز خواهیم داشت.

* تذکر: در معماری IPsec کلیدهای متقارن را می‌توان به دو روش زیر تعریف
و توزیع کرد: روش اول: روش دستی: در این روش مسئول شبکه
به ازای هر تک تک سیستم‌ها و افراد کلیدها را تعریف کرده و به روش امن تحویل

مدیریت کلید
- ذخیره: کلید را جایی ذخیره می‌کنیم.
- آپدیت: کلید را تغییر داده و استفاده می‌کنیم. «این مهم‌تر است»

افرادی دهد. (تذکر ۱): بدیهی است که هرگاه تعداد سیستم‌های شبکه
رو به گسترش باشد روش دستی از اثربخشی کامل فاصله خواهد گرفت.

حالت دوم: روش خودکار: در روش خودکار که در زمان تحویل
کلیدهای متقارن از راه‌های مختلف و شکل‌های مختلف تولید و
تحویل می‌شود. (تذکر ۲): روش خودکار برای تولید و تحویل
کلید IPsec استفاده از پروتکل ISAKMP و Oakley استفاده می‌کند.

★ ویژگی شبکه های خصوصی :

در شبکه های خصوصی ارتباط بین شبکه ها از طریق خطوط اختصاصی و تنها اجازه برقراری نشست یا استاندارد سیج داده ها مسئلم ایجاد اشکال فیزیکی در خطوط ارتباطی است و چنین کاری نیز اگرچه ممکن است ولی ساده نیست. لذا شبکه های خصوصی از امنیت بالاتری برخوردارند.

★ شبکه های خصوصی مجازی VPN :

★ شبکه های خصوصی مجازی VPN طوری طراحی شده اند که امکان ایجاد شبکه اختصاصی در بستر اینترنت است.

★ در VPN اگرچه از بستر اینترنت استفاده می شود ولی داده ها قبل از ورود به شبکه رمز می شوند.

★ شبکه های VPN هستند با ایجاد تونل امن بین سیستم های مجاز در هر شبکه سازمانی است. مشروط بر آنکه تمام کانال های ارتباطی از درون شبکه با دنیای خارج قطع شود و هرگونه تبادل و مرجع اطلاعات از طریق این تونل ها انجام بگیرد.

کامپیوترهایی که برای آنها مجوز تعریف شده است می توانند از راه دور به شبکه دسترسی داشته باشند. با VPN می توان تونل های امن بین کامپیوترهای مجاز و سیستم های مجاز شبکه را

ایجاد کرد و پس از احراز هویت، به آن اجازه داد از طریق این کانال امن و رمزنگاری شده به منابع شبکه دسترسی داشته باشد.

نکته: برای ایجاد تونل امن در VPN می‌توان از IPSec استفاده کرد.

نکته مهم: شبکه باید به گونه‌ای پیکربندی شود که کل ترافیک شبکه مجبور به عبور از تونل امن باشد. هرگونه وجود خط ارتباطی ناامن (حتی در صورت تلفن و مودم) کل تأسیسات تونل امن را از بین خواهد برد.

* یکی از سیاست‌های امنیتی، تدوین قواعد سخت‌گیرانه در ارتباط با ترافیک و حذف تمام سوراخ‌ها و خطوط مستقیم تلفن‌ها و سرکشی‌های دوره‌ای به آن‌ها است. یکی از مهم‌ترین نکات در VPN آن است که VPN صرفاً به پروتکل IPSec وابسته نیست، بلکه هر پروتکلی که بتواند مثل IPSec بین دو نقطه یک تونل امن ایجاد کند در برپایی شبکه مفید خواهد بود. به بیان دیگر VPN یک مفهوم است و از IPSec بعنوان یک ابزار استفاده می‌کند. اگر شما بخواهید و بتوانید آن مفهوم را ایجاد کنید، مشکلی نخواهد بود.

نکته: در VPN فرآیند احراز هویت طرفین می‌تواند به روش‌های مختلفی صورت پذیرد.

۱- گواهی‌نامه‌های دیجیتال، کارت‌های هوشمند و کلمات حافظه.

۲- شناسه کاربری و کلمه عبور.

۳- اثر انگشت و ویژگی های شبکیه چشم.

نکته مهم: ضعیف ترین روش احراز هویت در VPN روش مبتنی بر روش ورود شناسه کاربری و کلمه عبور است. (مثل: شناسه کاربری و کلمه عبور را اگر کسی دانسته باشد، می تواند وارد شود.

سخت ترین روش رمزگذاری مبتنی بر اثر انگشت یا ویژگی های چشمی DNA افراد و صورت افراد است.

دیواره آتش Firewall

سیستمی است که بین کاربران یک شبکه محلی و سایر شبکه ها برقرار می کند و نحوه تبادل اطلاعات بین کاربران به منابع شبکه در سطح سطوح، و نحوه ورود اطلاعات را کنترل می کند.

نکته: در حقیقت دیواره آتش محلی است بین اینترنت و بخش شبکه کامپیوتری که شبکه های اسانی تابع از قوانین و حفاظت برداری شده و برای آنها مجوز عبور یا هدف صادر شود.

تذکر: هر نظری که هر یا عملیاتی است و بازرسی و قبت گیری و اعمال خرد کن آن

دیواره آتش هم بعنوان یک فلوگاه می‌تواند فشرده یا لازم نرم‌افزار باشد، تا ضمن
نرم‌افزار، از دام و درخ یک بن‌بست ایجاد شود. (بن‌بست زمانی است که یک
کامپیوتر در حافظه دیواره آتش متصل می‌شود تا طول عمرش تمام شده و بازسازی
اقدام به ایجاد مجدد آن کرده و این کار بصورت متناوب تکرار شود). همین دلیل
دیواره آتش نباید به طراحی صحیح و دقیق دارد تا از حالت Bottle neck
خارج شود. تا ضمن دیواره آتش معمولاً اجتناب ناپذیر است و فقط باید سعی به
گونه‌ای طراحی شود که ... بتوان ایجاد نشود) برای حل مشکل می‌توان از
مبانی تئوری صف استفاده کرد.

★ سیستم کشف اخلالگری (نفوذ) IDS :

سیستم کشف اخلالگری که به اختصار IDS نامیده می‌شود، نرم‌افزاری
است امنی است که با تحلیل ترافیک جاری شبکه و تحلیل فعالیت‌های
فعالیت‌های نفوذگران می‌تواند در صورتی که تشخیص دهد ... یک حمله
به شبکه یا ماشین میزبان صورت گرفته است یا فعالیت‌های نفوذگر ناشی می‌شود.
به شیوه مناسب مسئول شبکه را در جریان می‌گذارد.

تعریف IDS و دیواره آتش

* واکنش IDSها در برابر حملات مشکوک:

هنگامی که یک IDS تشخیص دهد که فعالیت مخرب از اتصال TCP برقرار شده، از طرف دیگر یک کار امکان‌پذیر است و یا به‌ازای به‌کار مشکوک از سیستم در انجام یک مجموعه از عملیات در واکنش به آن فعالیت خواهد کرد. مثلاً ممکن است با ارسال علائم هشدار دهنده، مسئول شبکه را مطلع کند و یا پیغام بسته‌ای یک اتصال TCP شود. در هر صورت مسئول امنیت شبکه ناچار است که دست به کار شده و بررسی تراکنش گذشته بپردازد و علت و نوع حمله را مشخص شده و نتیجه این حمله را تحلیل کند. نتایج تحلیل یک حمله، اکثر اطلاعات حملات شناخته در پایگاه داده IDS ذخیره خواهد شد.

اگر عملیات تحلیل مسئول شبکه متوجه شد که حمله‌ای در کار نیست، احتمالاً زنگ هشدار است یا نه:

الف) یکی از مشکلات طراحی IDS این است که طوری عمل کند و پیکربندی شود که فقط در هنگام حمله واقعی اعلام خطر کند، مثل سیستم‌های دزدگیر ماشین و نه آژیر خطر.