با نام خدا

گزارش پروژه‌ی دوم شبکه‌های کامپیوتری

بهار کاویانی

۹۷۳۱۰۵۱

ترم پاییز ۹۹-۰۰

بخش اول: پرسش‌ها

سوال اول: قالب HEADER بسته‌های پروتکل‌های زیر را با رسم شکل بیان کنید و بگویید وظیفه‌ی هر FILED چیست. (برای پاسخ به این پرسش می توانید از RFCهای 768، 791، 793 و 2473 کمک بگیرید).

- IPv4

شکل سرایند پروتکل IP به صورت زیر است.

Version 4bit	IHL 4bit	Type of Service 8bit	Total Length 16bit	
Identification 16bit			Flags 3bit	Fragment Offset 13bit
Time to Live 8bit	Protocol 8bit		Header Checksum 16bit	
Source Address 32bit				
Destination Address 32bit				
Options				Padding

* Version: این فیلد، ورژن پروتکل IP را مشخص خواهد کرد که در اینجا ورژن ما با توجه به IPv4، ۴ است.
* IHL: مخفف Internet Header Length است. همانطور که در شکل مشخص شده است، هر سطر دارای ۳۲ بیت می‌باشد. فیلد IHL مشخص می‌کند که ما چند سطر در Header داریم. در نتیجه با کمک این فیلد می‌توانیم مشخص کنیم که بخش dataی یک بسته‌ی دریافتی از کجا شروع خواهد شد. شاید از روی شکل به نظر برسد که همواره ۶ سطر داریم اما در حقیقت سطر مربوط به Options متغیر است و بقیه سطرها ثابت هستند. بنابراین کمترین مقدار این فیلد برای headerای که به درستی ایجاد شده، برابر ۵ خواهد بود.
* Type of Service: در پروتکل IP می‌توان به شکلی برای بسته‌ها، اولویت‌دهی انجام داد. مثلا اگر ترافیک ویدیو و وویس داریم که محدوده‌های زمانی روی آن‌ها تاثیرگذار هست و روی کیفیت آن‌ها در مقصد می‌تواند تاثیر زیادی داشته باشد، از این فیلد استفاده می‌کنیم.
* Total length: اندازه‌ی دیتاگرام IPv4 را بر حسب بایت نشان می‌دهد. این اندازه هم شامل بخش header هست و هم data. با توجه به اینکه این بخش 16 بیتی‌ست به پروتکل IP این اجازه را می دهد که datagramهایی تا اندازه‌ی 65535 بایت را بتواند ارسال کند.
* Identification: این فیلد وظیفه‌ی هویت‌دهی به دیتاگرام‌ها یا قطعات بسته را دارد یعنی مشخص می‌کند قطعه متعلق به چه بسته‌ایست تا در مقصد بتوانیم قطعه‌های یک بسته را که قبلا قطعه قطعه شده‌اند، reassemble کنیم.
* Flags: در این بخش ما سه بیت داریم که دوتای آن‌ها پرچم‌هایی کنترلی هستند و بیت اول باید همواره صفر باشد. اولین پرچم کنترلی، Don’t Fragment(DF) نام دارد. هرگاه این پرچم set شود، یعنی به مقصد اعلام شده که این قطعه آخرین قطعه‌ی بسته‌ی اصلی‌ست. دومین پرچم کنترلی، More Fragment(MF) است.

وقتی این پرچم set می‌شود، یعنی هم‌چنان قطعات بیش‌تری از بسته‌ی مربوط به قطعه موجود است که مقصد باید دریافت کند.

* Fragmentation Offset: با کمک این فیلد مشخص می‌کنیم که قطعه‌ی کنونی، چندمین قطعه در بسته‌ی ارسالی است.
* Time to Live(TTL): این فیلد بیش‌ترین زمانی را که یک datagram اجازه دارد در شبکه‌ی اینترنت باقی بماند را نشان می‌دهد. در صورتی که مقدار این فیلد به صفر برسد یعنی احتمالا این قطعه داخل یک حلقه گیر افتاده و نتوانسته به مقصد برسد که اصطلاحا به آن نام "یتیم" و یا "orphan" اطلاق می‌شود. این بسته باید به کلی از شبکه خارج شده و drop شود در غیر این‌صورت منابع را بی‌هدف هدر خواهد داد.
* Protocol: این فیلد بین پروتکل‌های مختلف در سطح لایه‌ی transport تفکیک ایجاد می‌کند.
* Header checksum: مکانیزمی‌است برای چک کردن سرایند که در اصل هدف بررسی آدرس‌های مبدا و مقصد است که در سرایند ذکر می‌شوند. پروتکل IP مکانیزمی برای چک کردن کل data ندارد اما با کمک این فیلد تنها header قطعات را بررسی می‌کند زیرا اهمیت اینکه اطلاعات بین مبدا و مقصد درستی مبادله شوند بسیار بالاست. در غیر اینصورت تعداد ارتباطات و مبادلات اطلاعات اشتباه بالا می‌رود.
* Source Address: آدرس مبدا
* Destination Address: آدرس مقصد

تا اینجا تمام فیلدها اجباری بودند؛ اما از اینجا به بعد فیلدهای اختیاری نیز می‌توانند به header اضافه شوند. البته تعداد این فیلدها نیز محدود است. از آن‌جا که فیلد IHL تنها 4 بیت دارد پس در نهایت اندازه‌ی header ما می‌تواند $2^4 - 1$ سطر داشته باشد. 5 تا از این سطرها که اجباری بودند در نتیجه 10 سطر باق مانده که بتواند به بلوک‌های اختیاری اختصاص داده شود. هر فیلد اختیاری نیز برای آن‌که حتما قانون 32 بیتی بودن سطرها را رعایت کند، در صورت کمتر بودن تعداد بیت ثابت تحت عنوان padding به آن اضافه می‌شود که اندازه‌ی آن 32 بیتی شود.

- IPv6

شکل سرایند پروتکل IPv6 به صورت زیر است.

Version 4bit	Priority / Traffic class 8bit	Flow Label 20bit	
Payload Length 16bit		Next Header 8bit	Hop Limit 8bit
Source Address 128bit			
Destination Address 128bit			
Extension Header Number 1			
Extension Header Number 2			
...			

* Version: این فیلد همانند پروتکل IPv4، ورژن پروتکل IP را مشخص خواهد کرد که در اینجا ورژن ما ۶ است بنابراین مقدار این فیلد برابر 0110 خواهد بود.
* Priority / Traffic class: این بخش مانند فیلد Type of service در IPv4 می‌باشد. یعنی برای بسته‌های ارسالی یک اولویت مشخص می‌کند، در این صورت اگر در مسیر یابی ازدحام صورت گیرد، بسته‌های با اولویت کم‌تر loss خواهند شد اما بسته‌های با اولویت بالا نگهداری می‌شوند تا به مقصد برسند.
* Flow label: این بخش توسط مبدا مقداردهی می‌شود تا بسته‌های مربوط به یک flowی کاری همگی label مشترکی داشته باشند.
* Payload Length: این فیلد اندازه‌ی payload را مشخص می‌کند تا مسیریاب‌ها از روی header بسته بدانند که اندازه‌ی کل بسته چقدر خواهد بود.
* Next Header: گاهی در IPv6 یک سری header افزونه (Extension Header) هم داریم که بلافاصله بعد از header اصلی می‌آید که در این بخش نوع type اولین Extension header مشخص خواهد شد. در برخی مواقع نشان‌دهنده‌ی پروتکل لایه‌ی بالاتر مانند TCP یا UDP است.
* Hop Limit: این فیلد مانند Time to live(TTL) در پروتکل IPv4 می‌باشد که نشاندهنده‌ی حداکثر تعداد گره‌هایی است که بسته می‌تواند از آن‌ها عبور کند. با رد کردن آن تعداد گره، باید بسته‌ی مورد نظر در شبکه از بین برود تا منابع را بی‌هدف مصرف نکند.
* Source address: آدرس مبدا
* Destination address: آدرس مقصد
* Extension Header: ما همانند این بخش را در Option field از IPv4 داشتیم اما دیدیم که توسط فیلد IHL محدود می‌شود و تا تعداد مشخصی می‌توان ویژگی‌های اضافه را به header پروتکل IPv4 بیفزاییم. اما در IPv6 با استفاده از فیلد Next header این محدودیت را از بین برده‌اند.

- UDP

این پروتکل overhead زیادی به بخش data اضافه نمی‌کند. شکل سرایند در این پروتکل به این شکل است:

Source Port 16bit	Destination Port 16bit
Length 16bit	Checksum 16bit

* Source Port: در این فیلد مشخص می‌کنیم که پورت مربوط که فرایند ارسال‌شده چند است. در این صورت ممکن است برای عمل reply به مبدا مورد استفاده قرار گیرد. این یک بخش اختیاری در سرایند پروتکل UDP

است. البته حضور آن اجباری‌ست. منظور از اختیاری بودن، استفاده از آن است. در صورتی که نخواهیم از آن استفاده کنیم تمام 16 بیت آن صفر خواهد بود.

* Destination Port: این بخش برای مشخص کردن متن کامل آدرس مقصد مورد نیاز است.
* Length: این بخش اندازه‌ی کل بسته شامل header و data را به بایت مشخص می‌کند.
* Checksum: این فیلد برای چک کردن بسته‌ی ارسالی‌ست که جمع بیت‌های "شبه سرایند مربوط به اطلاعات سرایند IP "، "سرایند پروتکل UDP " و "دیتا" ست.

- TCP

شکل سرایند پروتکل TCP به صورت زیر است.

<table>
<tr><td colspan="8">Source Port
16bit</td><td colspan="8">Destination Port
16bit</td></tr>
<tr><td colspan="16">Sequence Number
32bit</td></tr>
<tr><td colspan="16">Acknowledgment Number
32bit</td></tr>
<tr><td colspan="4">Data Offset
4bit</td><td colspan="4">Reserved
6bit</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="4">Window
16bit</td></tr>
<tr><td colspan="8">Checksum
16bit</td><td colspan="8">Urgent Pointer
16bit</td></tr>
<tr><td colspan="12">Options</td><td colspan="4">Padding</td></tr>
</table>

* Source Port: شماره‌ی پورت مبدا را نشان می‌دهد.
* Destination Port: شماره‌ی پورت مقصد را نشان می‌دهد.
* Sequence Number: این فیلد شماره‌ی قطعه‌ی ارسالی را در خود نگه می‌دارد تا مقصد در زمان reassemble کردن segmentها بتواند ترتیب آن‌ها را تشخیص دهد.
* Acknowledgment Number: زمانی که segmentی ارسال شد، در این بخش مقدار sequence numberی قرار می‌گیرد که مبدا یا فرستند انتظار داشته آن بسته به مقصد ارسال شده باشد. مقصد با دادن این Ack به فرستند اعلام می‌کند که بسته را دریافت کرده است.
* Data Offset: این فیلد با مقداری که در خود نگه می‌دارد، نشان‌دهنده‌ی این است که بیت‌های مربوط به data از چندمین بلوک شروع می‌شوند و در حقیقت اندازه‌ی header را هم مشخص می‌کند.
* Reserved: این 6 بیت در حال حاضر رزرو شده هستند و باید مقدار 0 داشته باشند. اما ممکن است در آینده برای موضوعات مختلفی مورد استفاده قرار گیرند.
* Control bits: این بخش چندین پرچم کنترلی را در خود دارد که شرح هر کدام در ادامه آمده است:
  * URG: مخفف Urgent Pointer field significant می‌باشد. اگر این پرچم set شده باشد، به این معناست که در این segment ما یک urgent data خواهیم داشت (که فیلد Urgent Pointer محل آن را نشان می‌دهد).

- ACK: اگر set شده باشد یعنی Acknowledgment Number معتبر است.
- PSH: مخفف push است و هر زمان set شده باشد به معنای درخواست push است.
- RST: مخفف Reset the connection
- SYN: مخفف Synchronize sequence numbers است و در زمان‌هایی که set شده، مقدار Sequence Number به عنوان اولین Sequence Number در نظر گرفته می‌شود.
- FIN: مخفف finish و به معنای پایان یافتن connection می‌باشد.

* Window size: این فیلد مقدار اندازه‌ی window را به بایت نشان می‌دهد.
* Checksum: این بخش برای بررسی کردن خطا قرار داده شده.
* Urgent Pointer: این بخش زمانی معتبر است که پرچم URG ست شده باشد. اگر معتبر باشد نشان‌دهنده‌ی محل دیتای Urgent است.

سوال دوم: با جست‌وجو در اینترنت درباره‌ی Transport Layer Security تحقیق کنید، کاربردهای آن را بنویسید و جایگاه آن در مدل لایه‌ای را تشریح کنید.

Transport Layer Security یا به اختصار TLS برای ایجاد امنیت در لایه‌ی Transport می‌باشد. TLS در حقیقت مشتق‌گرفته‌شده از یک پروتکل امنیتی به نام Secure Service Layer یا SSL.

ویژگی‌های این پروتکل به شرح زیر است:

* Encryption یا رمزنگاری: TLS/SSL این قابلیت را برای داده‌های ما فراهم می‌آورد که به صورت رمزشده در بستر اینترنت ارسال شوند.
* Interoperability یا قابلیت همکاری: از آن‌جا که TLS/SSL می‌تواند با هر سیستم‌عامل و یا browser ای کار کند، نشان‌دهنده‌ي قابلیت همکاری آن است.
* Algorithm flexibility: کار کردن با آن با هر مدل الگوریتم Encryption، hashing و ... ساده است.
* Ease of Deployment و
* Ease of Use هم جز دیگر ویژگی‌های TLS/SSL است.

سوال سوم: در مورد IPSec تحقیق کنید.

۱- IPSec چیست؟

مخفف Internet Protocol security است که به مجموعه‌ای از پروتکل‌ها برای ارسال امن بسته‌ها در بستر اینترنت و با پروتکل IP گفته می‌شود. این پروتکل براساس استانداردهای کارگروه مهندسی اینترنت (IETF) ایجاد شده است.

۲- کاربردهای آن را بنویسید.

این مجموعه از پروتکل کمک می‌کند تا دیتاهای ما بتوانند در شبکه‌های عمومی به صورت secure ارسال شوند. یعنی محرمانگی، یکپارچگی و صحت ارتباطات داده را در یک شبکه عمومی تضمین می‌کند.

ویژگی‌های آن عبارتند از:

* محافظت از حمله replay: این ویژگی، یک شماره ترتیبی منحصر به فرد را به هر بسته اختصاص می‌دهد. در صورتی‌که بسته‌ای با شماره ترتیبی تکراری تشخیص داده شود، حذف می‌شود.

* محرمانگی اطلاعات (رمزنگاری)
* یکپارچگی اطلاعات
* احراز منبع و منشاء اطلاعات
* احراز هویت در لایه Network: کد تأیید هویت پیام Hash (HMAC) تأیید می‌کند که بسته‌ها تغییر نکرده‌اند.

۳- مزایا و معایب استفاده از آن را مورد بررسی قرار دهید.

مزایای استفاده از IPSec در ارتباطات، شامل موارد زیر است:

* با هر مدل از دستگاههای اصلی سازگاری دارد.
* به دلیل استفاده از رمزهای متنوع، بهترین امنیت را ارائه می‌دهد.
* هزینه‌های مرتبط با استقرار و مدیریت را با استفاده از یک راه حل ارتباطی ایمن و با کاربرد آسان و با نصب آسان، کاهش می‌دهد.
* پایدار است، به خصوص هنگام تعویض شبکه یا اتصال مجدد پس از قطع شدن اتصال.
* در سطح شبکه عمل می کند بنابراین نیازی به نگرانی در مورد وابستگی برنامه وجود نخواهد داشت.
* در صورتی که بخواهیم آن را در یک شرکت مورد بررسی قرار دهیم این مزیت را دارد که بهره وری کارمندان را افزایش می‌دهد و در هر زمان و هر مکان دسترسی ایمن به منابع شرکت را ممکن می‌سازد.

معایب IPSec :

* می‌توان با استفاده از فایروال‌های محدود کننده آن را مسدود کرد.
* از آن‌جا که داده ها را دو بار کپسوله می‌کند، سریع‌ترین پروتکل نیست و اتصال را کند می‌کند.
* به زمان پردازش و پهنای باند قابل توجهی نیاز دارد.

سوال چهارم: در بسته‌های IPv4 مقدار فیلد Protocol چیست؟ و چه مقادیری می‌تواند داشته باشد؟

این فیلد بین پروتکل‌های مختلف در سطح لایه‌ی transport تفکیک ایجاد می‌کند.

بیش‌ترین مقداری که در این فیلد ممکن است مشاهده شود، مقادیر 17 برای پروتکل UDP و 6 برای پروتکل TCP است.

اما در کل از آنجا که این فیلد ۸ بیتی است مقادیر ۰ تا ۲۵۵ را می‌تواند داشته باشد.