امنیت تجارت الکترونیک

فصل سیزدهم:
امنیت لایه انتقال

تهیه و تنظیم: دکتر آرش حبیبی لشکری
منبع: کتاب "اصول امنیت برای تجارت الکترونیکی"

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

- ابزار TCP Wrapper
- امنیت لایه انتقال (TLS)
- دروازه های مداری و Socks
- پروتکل مدیریت کلید و انجمن امنیتی‌اینترنت (ISAKMP)

امنیت لایه انتقال

ابزار TCP Wrapper

ابزار TCP Wrapperمعرفی شده توسط Wietse venema، ابزاری برای نظارت و کنترل هر دو ترافیک شبکه مبتنی بر TCP و UDPاست.

این ابزار نیازمند هیچ تغییری در سیستم‌عامل یا نرم‌افزار سرویس‌دهنده نمی‌باشد.

در اصل TCP Wrapper چون تصمیماتش را بر اساس آدرس‌های IPمی‌گیرد، کنترل دسترسی ضعیفی را نیز فراهم می‌کند.
در اصل، ویرایش اصلی این ابزار برای کمک به پیگیری یک رمزشکن، که مکررا به یک سیستم کامپیوتری در دانشگاه تکنولوژی Einhoven در هلند حمله می‌کرد، نوشته شده است.

لذا، برای اهداف واقعه نگاری بسیار مفید است.

شرح کامل نحوه عملکرد این ابزار در یونیکس

دروازه های مداری و Socks

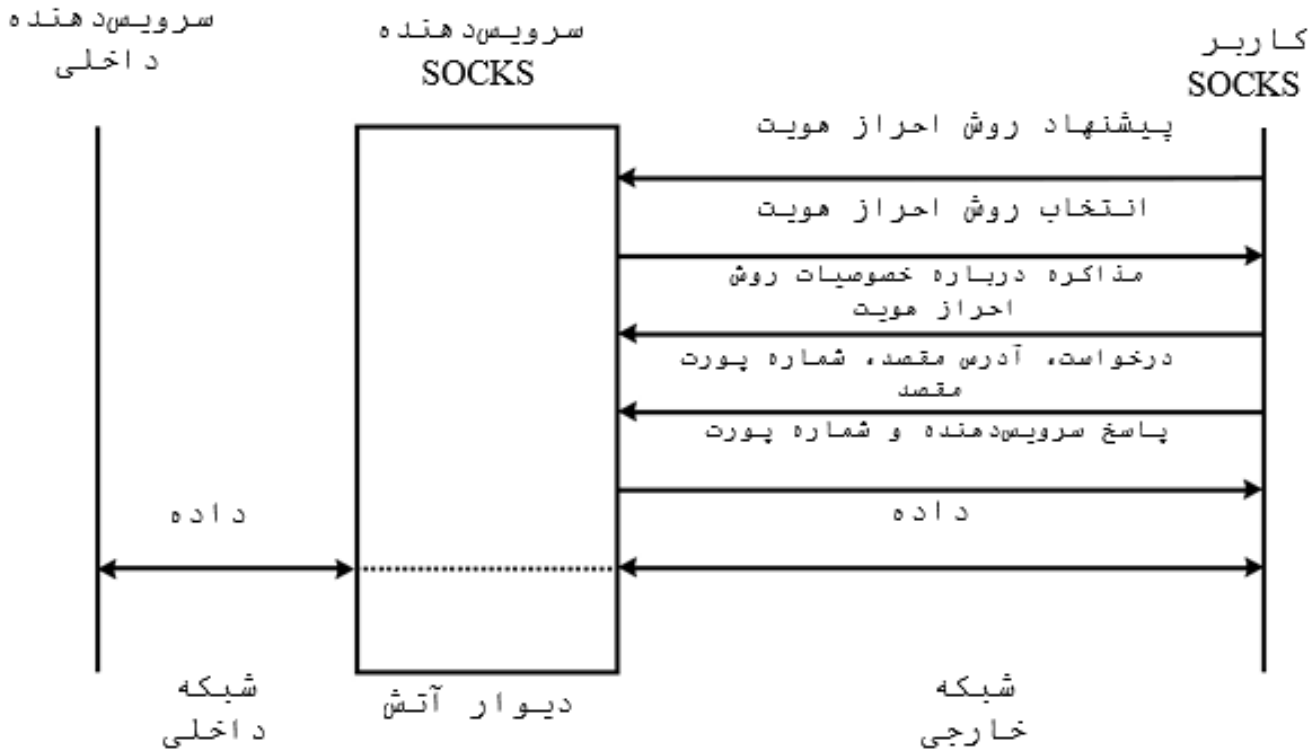
دروازه‌های مداری تقویت کننده‌های لایه انتقال هستند

یک دروازه مداری داده را از طرق زیر انتقال می‌دهد:

- یک ارتباط بین میزبان داخلی و دروازه امنیت؛
- یک ارتباط بین دروازه و میزبان خارجی؛
- و بالعکس. دروازه‌های مداری معمولا به عنوان یک مکانیزم دیوارآتش پیاده سازی می‌شوند.

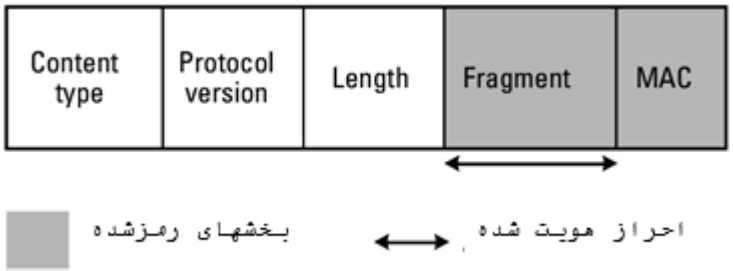
SOCKS ویرایش 4، پروتکلی است که پیمایش دیوارآتش ناامنی را برای برنامه‌های کاربردی سرویس-گیرنده – سرویس دهنده مبتنی بر TCP فراهم می‌کند.
SOCKS ویرایش 5، برنامه‌های کاربردی برپایه - UDP را به خوبی یک چارچوب احراز هویت نیز پشتیبانی می‌کند (و یک طرح آدرس‌دهی گسترده شده، که در اینجا قابل ملاحظه نخواهد بود).
این پروتکل بین لایه انتقال و لایه کاربردی عمل می‌کند

Socks


سرویس‌د هنده
د اخلی
سرویس‌د هنده
SOCKS
کاربر
SOCKS
پیشنهاد روش احراز هویت
انتخاب روش احراز هویت
مذاکره درباره خصوصیات روش
احراز هویت
درخواست، آدرس مقصد، شماره پورت
مقصد
پاسخ سرویس‌دهنده و شماره پورت
داده
داده
شبکه
د اخلی
دیوار آتش
شبکه
خارجی

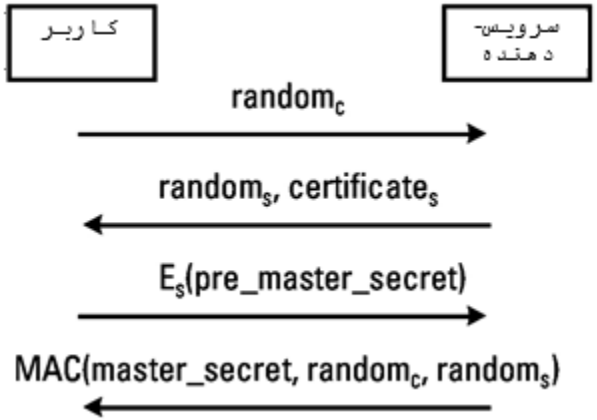
امنیت لایه انتقال (TLS)

لایه‌های TLS



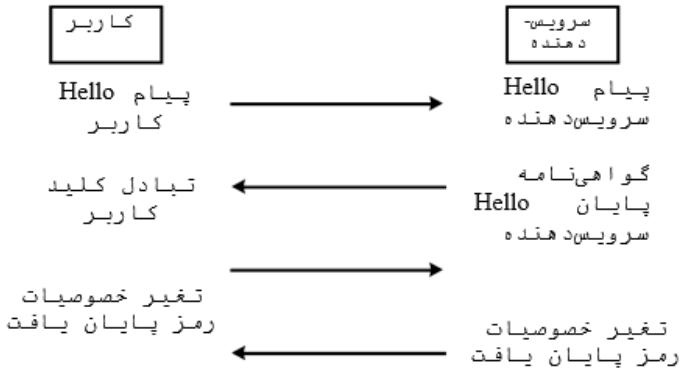
قالب رکورد TLS

امنیت لایه انتقال (TLS)



مراحل دستدهی TLS با احرازهویت کاربر

master_secret = prf (pre_master_ secret, randomC ,randoms)



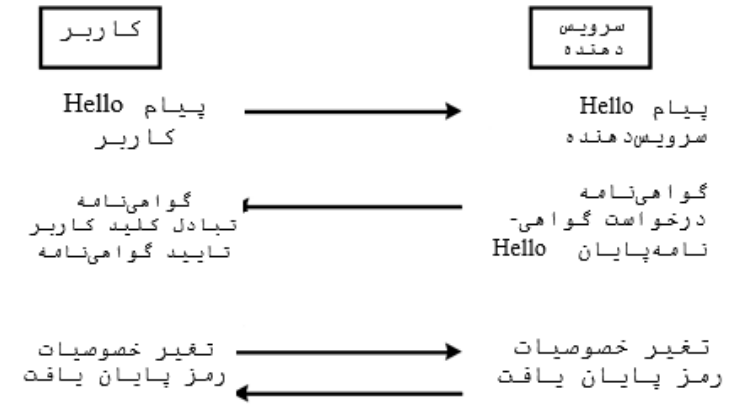
مراحل دستدهی TLS با احرازهویت سرویس‌دهنده

prf (master_ secret, MD5(handshake_messages),SHA-1(handshake _messages))

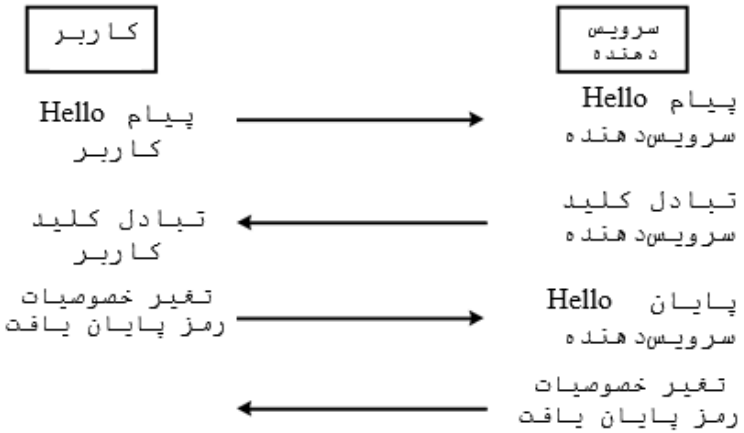
با محرمانگی:
TLS_RSA_EXPORT_WITH_RC4_40_MD5
بدون محرمانگی
TLS_RSA_WITH_NULL_MD5

امنیت لایه انتقال (TLS)

مراحل دستدهی TLS با احرازهویت دوطرفه



ایجاد یک نشست TLS گمنام با توافقنامه کلید



احرازهویت ساده و لایه امنیت (SASL)

SASL مکانیزمی برای افزودن قابلیت احرازهویت و محرمانگی به پروتکل‌های اتصال‌گرا می‌باشد.

بعلاوه، SASL می‌تواند یک لایه امنیتی - برای یکپارچگی و حریم خصوصی- بین پروتکل و اتصال متناظر وارد نماید.

لایه امنیتی به محض اینکه مبادله احرازهویت سرویس‌دهنده - سرویس‌گیرنده تمام می‌شود، فعال می‌شود.

وقتی لایه امنیتی تحت تاثیر باشد، تمام پیام‌های پروتکلی توسط لایه امنیتی قبل از اینکه منتقل شوند، پردازش می‌شوند (رمزنگاری می‌شوند).

شرح عملکرد SASL

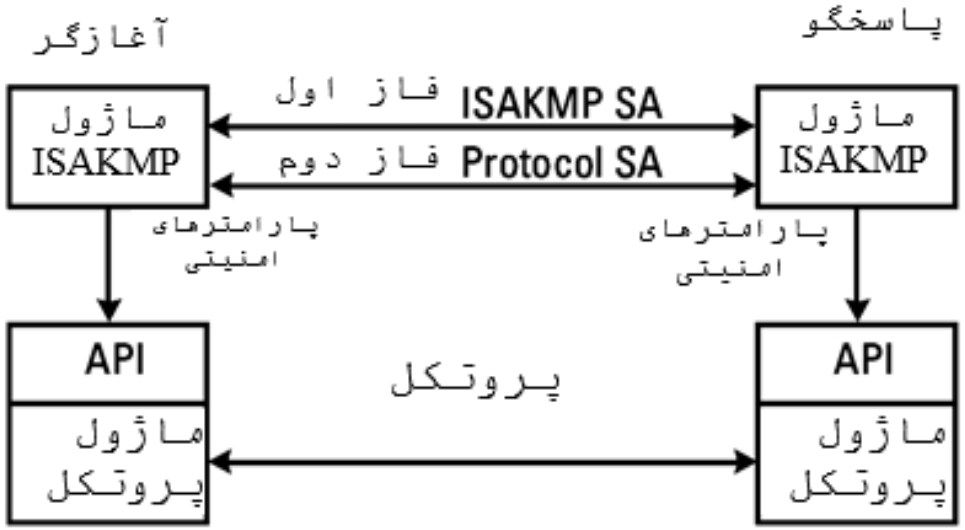
پروتکل مدیریت کلید و انجمن امنیتی‌اینترنت (ISAKMP)

در زمان ایجاد کلیدها برای SAها، سه رویکرد قابل اتخاذ است:

رویکرد host-oriented keying

رویکرد user-oriented keying

رویکرد سوم این است که میزبان‌های ارتباطی یک کلید نشست جدید برای این ارتباط ایجاد کنند.



گفتگوهای ISAKMP

نمونه ساختار یک پیام ISAKMP

Initiator Cookie				
Responder Cookie (none)				
Next Payload=1 (SA)	MjVer	MnVer	Exchange Type=2	Flags
Message ID				
Length				
Next Payload=0	RESERVED	Payload Length		
Domain of Interpretation=1 (IPSEC DOI)				
Situation=0x01 (SIT_IDENTITY_ONLY)				
Next Payload=0	RESERVED	Payload Length		
Proposal #1	Protocol–Id=1 (PROTO_ISAKMP)	SPI size=0	#Transforms=2	
Security Parameter Index (none)				
Next Payload=3	RESERVED	Payload Length		
Transform #1	Transform–Id=1 (KEY_IKE)	RESERVED2		
Attribute Type=1 (Encryption alg.)	Attribute Length			
Attribute Value=DES–CBC				
(other preferred attributes)				
Next Payload=0	RESERVED	Payload Length		
Transform #2	Transform–Id=1 (KEY_IKE)	RESERVED2		
Attribute Type=1 (Encryption Alg.)	Attribute Length			
Attribute value=3DES–CBC				
(other preferred attributes)				

خلاصه: ابزار **TCP Wrapper**، امنیت لایه انتقال **(TLS)**، دروازه های مداری و **Socks**، پروتکل مدیریت کلید و انجمن امنیتی‌اینترنت **(ISAKMP)**

جلسه بعدی: امنیت لایه کاربردی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.