امنیت تجارت الکترونیک

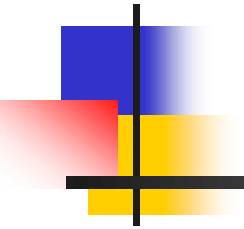
فصل یازدهم:
امنیت لایه دسترسی شبکه

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

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست

- حالت انتقال غیرهمزمان (ATM)
- شبکه خصوصی مجازی ATM
- پروتکل نقطه - به - نقطه (PPP)
- پروتکل احرازهویت توسعه پذیر (EAP)
- پروتکل رمزعبور یک بار-مصرف (OTP)
- پروتکل کنترل رمزنگاری (ECP)
- پروتکل‌ایجاد تونل در لایه دوم (L2TP)



امنیت لایه دسترسی شبکه

مقدمه

این فصل به بحث در مورد مسائل امنیتی مرتبط با لایه دسترسی شبکه در مدل اینترنت می‌پردازد.

به دلیل پیشرفتهای تکنولوژی شبکه محلی یا LAN، و تا حدودی به دلیل ادغام تکنولوژی‌های شبکه (از قبیل شبکه تلفن و اینترنت)، همانطور که انتظار می‌رود، دراین لایه تنها پروتکل‌های انتها- به- انتهای "ساده" بکار نمی‌رود.

لایه دسترسی شبکه در مدل اینترنت تقریبا مطابق است با لایه‌های پیوند داده و فیزیکی در مدل منبع OSI.

شرح دولایه زیرین و نحوه عملکرد آنها:

لایه فیزیکی و لایه پیوند داده

نقش پروتکل انتها – به – انتها:

مکانیزم امنیتی موجود و مشکل آن،

راه حل پیشنهادی ساده و راه حل پیشنهادی پیشرفته

حالت انتقال غیرهمزمان (ATM)

یک تکنولوژی سوئیچینگ بازپخش- سلولی برای دسترسی‌های پهنای باند مسکونی و ارتباطات WAN از طریق زیرساختهای عمومی

اتصال‌گرا است، یعنی از مسیرهای ثابت که به اتصال کانال مجازی (VCC) معروفند، در شبکه استفاده میکند

پشتیبانی از انتشار چندپخشی، یا همان ارتباطات نقطه - به - چند نقطه (از قبیل کنفرانس تصویری)

شرح ساختار یک سلول ATM، سربارها و شناسه ها

سرویسهای امنیتی ATM

- احراز هویت موجودیت
- احراز هویت داده
- محرمانگی داده
- یکپارچگی داده
- تبادل کلید
- تبادل URL و گواهی
- کنترل دسترسی

احراز هویت

از آنجاییکه ATM اتصال‌گرا است، احراز هویت موجودیت، در طی ایجاد ارتباط اجرا می‌شود.

ارتباط امن بین دو SA را به اصطلاح مشارکت امنیتی می‌نامند.

مشخصات امنیتی ATM معرف دو پروتکل است: یکی دست‌دادن دوطرفه و دیگری سه‌طرفه

پارامترها در پروتکل دست‌دهی سه‌طرفه

پیام ها	پارامترها
موجودیت شرکت‌کننده	X
تولید یک Nonce توسط X	R_x
خصوصیات مذاکره	$SecNeg_x$
گواهی‌نامه X.509 شرکت کننده X	$Cert_x$
رمزگذاری داده با کلیدعمومی X یا کلید متقارن	$Enc_{K_x}(Data)$
محاسبه امضاء دیجیتالی X برپایه داده هش شده	$Sig_{K_x}(h(Data))$
برای حمل ایمن کلیدهای X بکار می‌رود.	$ConfPar_x$

دست‌دهی سه‌طرفه برای ATM

جریان	دست‌دهی ساده	احراز هویت	تبادل کلید	تبادل گواهی‌نامه
1: $A \rightarrow B$	$A, \{B\}, R_a, SecNeg_a$			$Cert_a$
2: $B \rightarrow A$	$A, B, SecNeg_b$	$R_a, R_b, Sig_{K_b}(h(A, B, R_a, R_b, SecNeg_a, SecNeg_b))$	$Enc_{K_a}(ConfPar_b), Sig_{K_b}(h(..., ConfPar_b))$	$Cert_b$

محرمانگی، کنترل دسترسی

محرمانگی نیز در لایه ATM اعمال شده است که از محتوای سلول ATM محافظت می‌کند.

محتوی با کلید نشست، رمزگذاری می‌شود

بالا بودن سرعت رمزگذاری بسیار حائز اهمیت است

رمزنگاری نرم‌افزار نمی‌تواند این نیازمندی را برآورده نماید، پس فقط از دستگاه‌های سخت-افزاری خاصی استفاده می‌شوند

مشکل بالقوه رمزنگاری سلول و راه حل پیشنهادی

شرح احرازهویت و یکپارچگی سطح کنترل

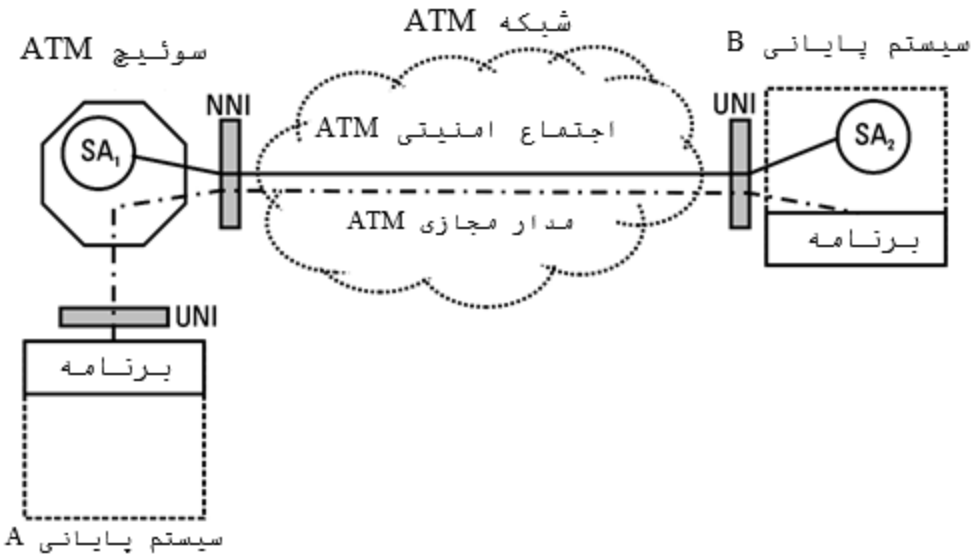
شرح امنیت چندپخشی

تبادل پیام امنیتی ATM

شبکه خصوصی مجازی ATM

ATM کارکرد امنیتی غنی دارد که اجازه ساخت پیکربندی‌های امنیتی گوناگون را بوجود می‌آورد:

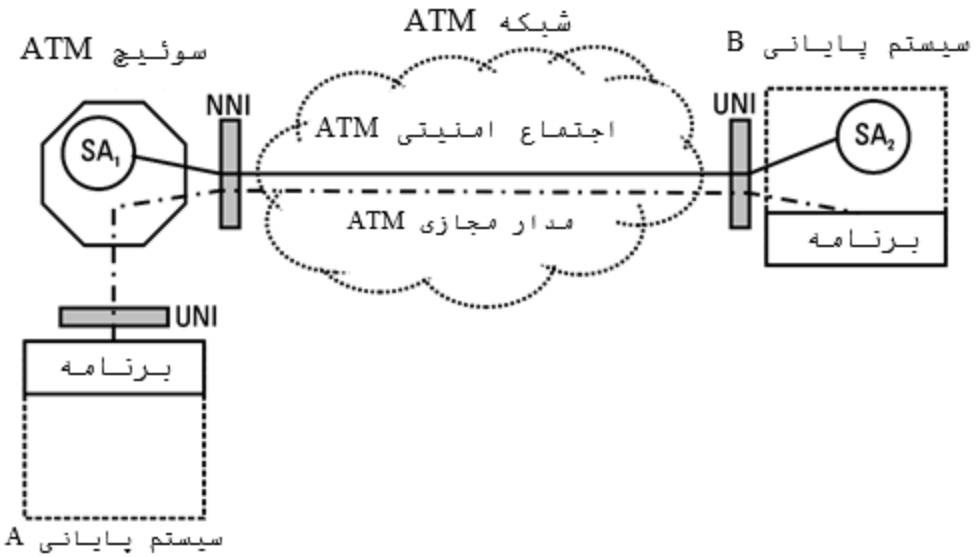
- واسط شبکه کاربر (UNI) بین یک سیستم کاربری (از قبیل‌ایستگاه‌های کاری کاربران) و یک سوییچ ATM
- واسط شبکه شبکه (NNI) بین دو سوییچ ATM در یک شبکه ATMکه شامل چندین سوییچ ATM



شبکه خصوصی مجازی ATM

ATM کارکرد امنیتی غنی دارد که اجازه ساخت پیکربندی‌های امنیتی گوناگون را بوجود می‌آورد:

- واسط شبکه کاربر (UNI) بین یک سیستم کاربری (از قبیل‌ایستگاه‌های کاری کاربران) و یک سوییچ ATM
- واسط شبکه شبکه (NNI) بین دو سوییچ ATM در یک شبکه ATMکه شامل چندین سوییچ ATM



پروتکل نقطه -به -نقطه (PPP)

پروتکل نقطه – به - نقطه (PPP)، یک پروتکل لایه- پیوند - داده که برای انتقال دیتاگرام‌های چندین پروتکل روی اتصال‌های سریالی استفاده می‌شود

با PPP یک کاربر می‌تواند، بار نمونه، با استفاده از یک ارتباط تلفنی در سوئیچینگ مداری به یک ISP متصل شود. یک پیکربندی معمولی شامل:

- یک کامپیوتر است که نرم افزار PPP را اجرا کرده و یک مودم تلفنی با پورت سریال به آن متصل است.
- سرویس‌گیرنده معمولا شامل یک نرم افزار شماره‌گیر است که ارتباط تلفنی را ایجاد می‌نماید

این پروتکل از کپسوله‌سازی برای تسهیم همزمان پروتکل‌های لایه- شبکه متفاوت روی یک اتصال استفاده نموده و شامل فازهای زیر است:

- اتصال مرده
- ایجاد اتصال
- احراز هویت
- پروتکل لایه شبکه
- پایان اتصال

پروتکل احرازهویت رمزعبور (PAP)

پروتکل احرازهویت رمز عبور (PAP c023) یک پروتکل دست‌دادن دو طرفه است که احرازهویت ضعیفی ارائه می‌کند

آشکارترین ضعف امنیتی PAP این است که رمزعبورها به صورت رمزنگاری نشده ارسال می‌شوند:

- اگر یک استراق سمع کننده یک رمزعبور معتبر بدست آورد، به راحتی می‌تواند یک حمله بازپخش ترتیب دهد.
- امکان حملات جستجوی فراگیر رمزعبور نیز وجود دارد زیراایجاد اتصال از نوع بدون حالت یا stateless است، بنابراین طرف احرازهویت کننده نمی‌تواند تعداد تلاشهای ناموفق احرازهویت را شمارش کند.

این پروتکل هیچ حفاظتی از فریم‌های ارسالی در پروتکل لایه شبکه که فاز احرازهویت را دنبال می‌کنند، ارائه نمی‌کند

پروتکل CHAP

پروتکل CHAP (CHAP c223) امنیت رمزعبور بهتری نسبت به PAP ارائه می‌دهد. CHAP بعد ازایجاد اتصال اولیه اجرا شده و شاید هر زمانی بعد از آن تکرار شود

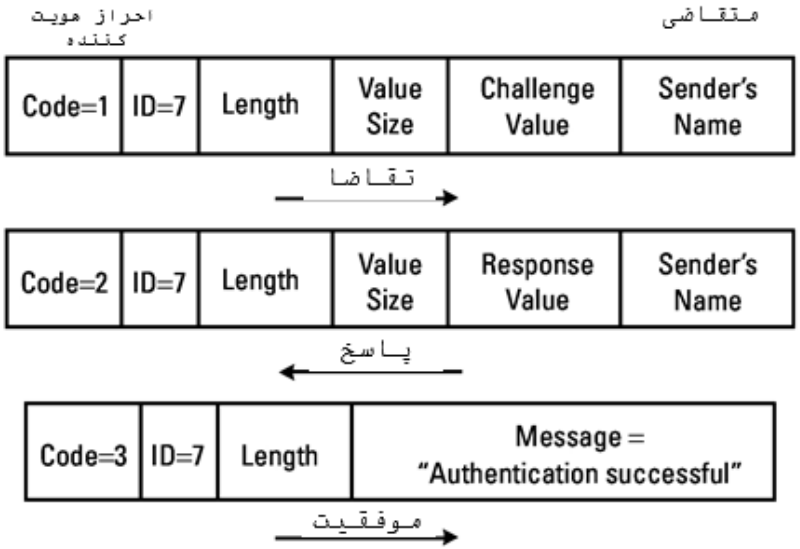
یک دست‌دادن سه‌طرفه است که درخواست‌کننده را احراز هویت می کند

یکی از پارامترهای مذاکره (گزینه‌های پیکربندی) باید انتخاب تابع درهم‌ساز یکطرفه برای استفاده باشد. در حال حاضر فقط MD5 قابل استفاده است

دراصل CHAP یک پروتکل چالش- پاسخ است

برخی منابع منحصر به فرد برای شماره‌های سحرآمیز عبارتند از:

- شماره‌های سریال ماشین
- آدرس‌های سخت افزاری شبکه دیگر
- ساعتهای زمان-روز
- اندازه گیری‌های دقیق زمانهای ورودی وقایع فیزیکی، از قبیل پذیرش بسته در شبکه‌های متصل دیگر، زمان پاسخ سرویس-دهنده، یا سرعت تایپ کردن یک کاربر انسانی.



پروتکل احرازهویت توسعه پذیر (EAP)

پروتکل احرازهویت توسعه پذیر PPP یا همان EAP پروتکلی عمومی‌برای احرازهویتPPP است که CHAP را به خوبی سایر مکانیزم‌های احرازهویت پشتیبانی می‌کند

وقتی EAP استفاده می‌شود، ، مانند مورد CHAP، هیچ مکانیزم احرازهویت مشخصی توسط LCP انتخاب نمی‌شود.

قالب بسته EAP در شکل زیر شان داده شده است. معنی کد، شناسه (ID)، و فیلد طول شبیه همان مواردی هستند که برای CHAP در بخش قبل توضیح دادیم. فیلد کد می‌تواند به معنی یک بسته درخواست، پاسخ، موفقیت یا شکست باشد.

مکانیزم احرازهویت با مقدار فیلد نوع مشخص می‌شود:

کد	شناسه	طول	نوع	داده

نوع=3 برای چالش MD5 (مشابه با CHAP)

نوع=4 برای رمزعبور یک بار-مصرف

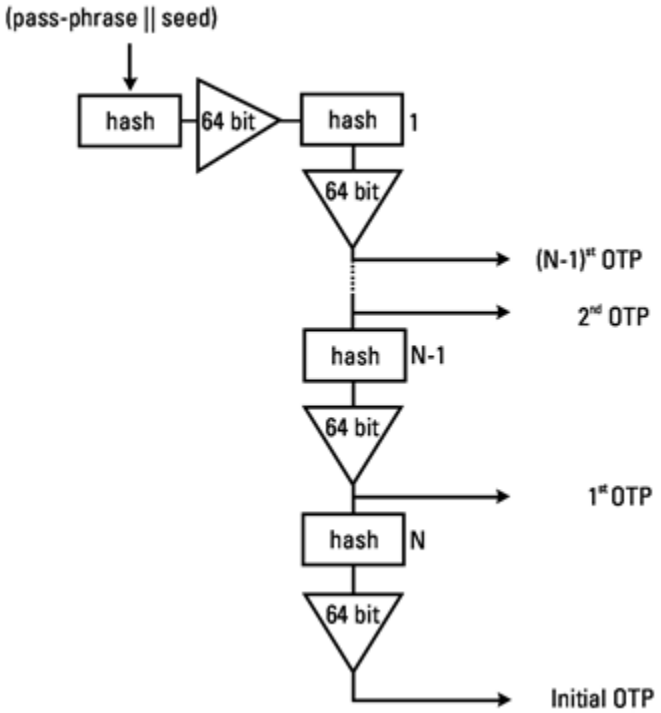
نوع=5 برای کارت نشانه عمومی

نوع= ناشناخته برای EAP-TLS (آزمایشی، RFC 2716)

پروتکل رمزعبور یک بار-مصرف (OTP)

یک مکانیزم مبتنی بر رمزعبور بوده که برای حفاظت از حمله‌های بازپخش طراحی شده است

مانند CHAP، از توابع درهم‌ساز یک طرفه و چالش استفاده می‌کند (MD5 اجباری است، MD4 و SHA-1انتخابی هستند).



به طور خاص پروتکل OTP از زنجیره توابع درهم‌ساز به نحوی که در پرداختهای خرد PayWord استفاده می‌شود، بهره می‌گیرد.

این دو مقدار، گذر-واژه و دانه، همانطور که در شکل روبرو نشان داده شده است، به عنوان ورودی برای تولید رمزعبور استفاده می‌شود.

پروتکل کنترل رمزنگاری (ECP)

پروتکلی است که از محرمانگی دیتاگرام‌های حمل شده در یک PPP محافظت می‌کند

یک بسته ECP در فیلد اطلاعات پروتکل PPP کپسوله می‌شود

ECP نمی‌تواند قبل ازاینکه PPP به فاز پروتکل لایه شبکه برسد آغاز شود (بعد از فاز احرازهویت):

نوع=0 به معنی الگوریتم رمزنگاری اختصاصی می‌باشد؛

نوع=1، ویرایش قدیمی‌از رمزنگاری ECP DES، منسوخ شده است

نوع=3 به معنی DES (DESE-bis, RFC 2419)؛

نوع=2 به معنی Triple-DES (3DES, RFC 2420).

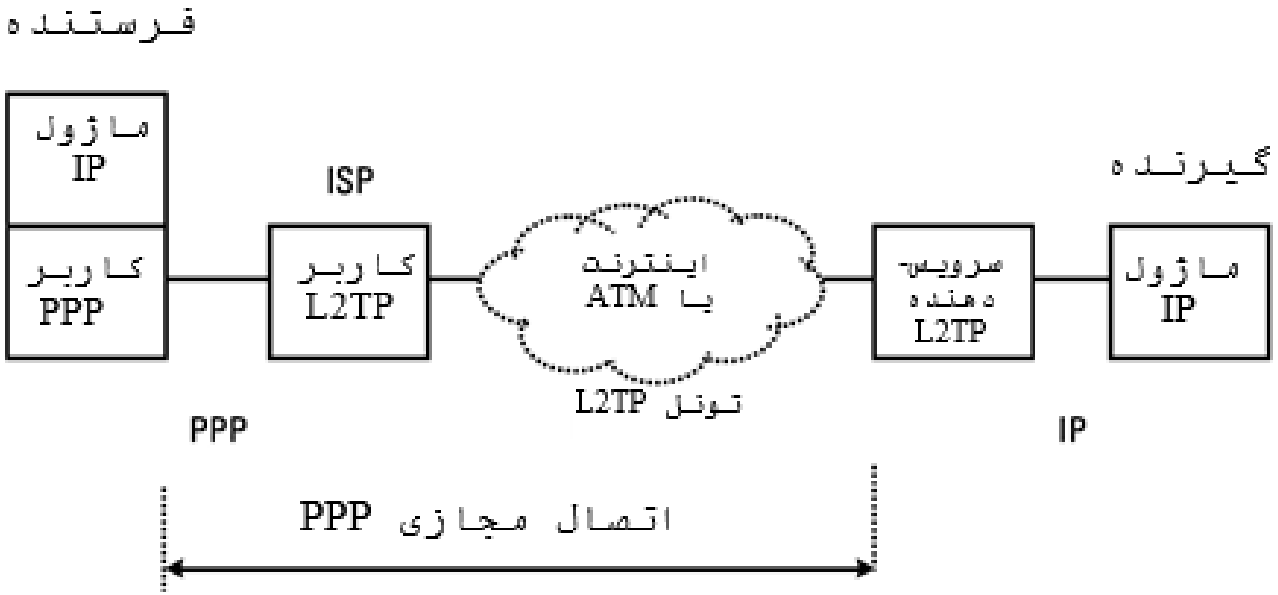
پروتکل‌ایجاد تونل در لایه دوم (L2TP)

پروتکل‌ایجاد تونل در لایه دوم (L2TP) پروتکلی است که ترافیک PPP را روی شبکه‌های گوناگونی تونل می‌زند

ویرایش اول، PPTPدارای معایب امنیتی زیادی بود که در ویرایش دوم برطرف شدند.

در زمان کپسوله کردن یک دیتاگرام PPP، پروتکل L2TP سربار خود را به دیتاگرام PPP اضافه می‌کند.

سربار L2TP شامل، شناسه تونل برای ارتباط کنترلی، و شناسه نشست برای نشست داخل تونل است.



خلاصه: حالت انتقال غیرهمزمان (ATM)، شبکه خصوصی مجازی ATM، پروتکل نقطه -به -نقطه (PPP)، پروتکل احرازهویت توسعه پذیر (EAP)، پروتکل رمزعبور یک بار-مصرف (OTP)، پروتکل کنترل رمزنگاری (ECP)، پروتکلایجاد تونل در لایه دوم (L2TP)

جلسه بعدی: امنیت لایه اینترنت

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