امنیت تجارت الکترونیک

فصل ششم:
امنیت تراکنش پرداخت

تهیه و تنظیم:
دکتر آرش حبیبی لشکری

اولین نسخه: دی 1394
بروزرسانی: مهر 1395

فهرست:

- گمنامی کاربر و عدم توانایی ردیابی مکانی
- گمنامی پرداخت کننده
  - نام مستعار
- عدم قابلیت ردیابی
  - تابع درهم سازی تصادفی در iKP
  - تابع درهم ساز تصادفی درSET
- محرمانگی داده ها
  - تابع درهم سازی تصادفی در iKP
  - امضاء دوگانه در SET
- عدم انکار
  - امضاء الکترونیکی
- تازگی پیام
  - شماره‌های یکبار مصرف
  - برچسب های زمان

گمنامی کاربر و عدم توانایی ردیابی مکانی

گمنامی کاربر و عدم توانایی ردیابی مکانی به صورت مجزا قابل تامین هستند.

یک سرویس امنیتی گمنامی کاربر، از فاش شدن شناسه‌ی یک کاربر محافظت می‌کند. که این امر با بکارگیری نام‌های مستعار برای کاربران به جای نامهای واقعی آنها، قابل دستیابی است.

اما، اگر یک تراکنش شبکه‌ای قابل ردیابی تا میزبان اصلی باشد و اگر میزبان فقط توسط کاربر شناخته شده استفاده شود، آنگاه این نوع از گمنامی کافی نخواهد بود. لذا راه چاره چیست؟

یک سرویس امنیتی عدم توانایی ردیابی مکانی از فاش شدن مبداء پیام محافظت خواهد نمود. یکی از راه‌حلهای ممکن، جهت دهی ترافیک شبکه به سمت مجموعه ای از میزبانهای ناشناس است که آنوقت چنین به نظر می‌رسد که این ترافیک توسط یکی از این میزبانها تولید شده است.

البته به شرط آنکه حداقل یکی از میزبانها در مسیر شبکه، قابل اطمینان باشد، اگر منبع ترافیک بخواهد به درستی گمنام باشد.

گمنامی کاربر و عدم توانایی ردیابی مکانی

اولین مکانیزم ترکیبی گمنامی کاربر و عدم توانایی ردیابی مکانی توسط D. Chaum ارائه شد:

- کاملا از سیستم پرداخت جدا می باشد
- می‌تواند از تحلیل ترافیک جلوگیری و حفاظت نماید

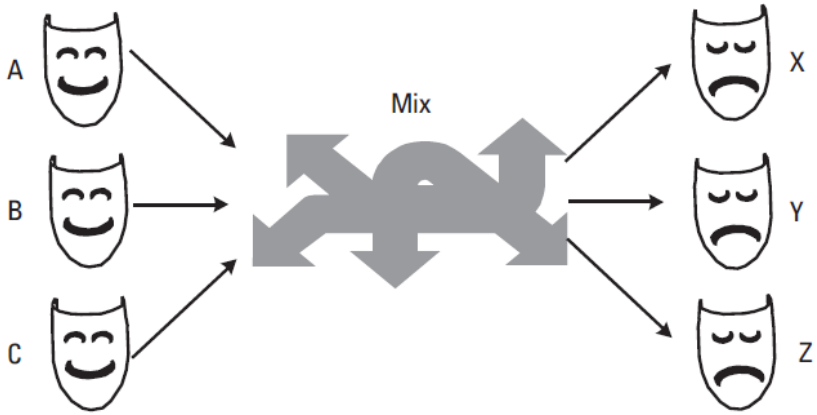
ایده اولیه در تصویر زیر آمده است:

پیامها با کلید عمومی Mix، یعنی همان E_M، رمزنگاری شده‌اند. اگر مشتری A بخواهد پیامی به فروشنده Y ارسال نماید، A دستورالعل زیر را به Mix ارسال می‌کند:

$$E_M\left(Mix, E_Y\left(Y, Message\right)\right)$$

- حال Mix می‌تواند پیام را رمزگشایی نموده و نتیجه را به Y ارسال نماید:

$$E_Y\left(Y, Message\right)$$



از آنجاییکه پیام با کلید عمومی Y که همان Ey است، رمزنگاری شده است، فقط Y می‌تواند آن را بخواند. اگر ترکیبات درست (صادق) باشند، Y ایده‌ای در مورد اینکه کجا و توسط چه کسی پیام ایجاد و فرستاده شده نخواهد داشت.

گمنامی کاربر و عدم توانایی ردیابی مکانی

اگر A از Y بخواهد که جوابی ارسال نماید، می‌تواند یک آدرس بازگشت ناشناس را در پیام خود به Y بگنجاند:

$$Mix, E_M(\mathrm{A})$$

در این روش پیام جواب در واقع به Mix ارسال می‌شود، اما فقط Mix می‌داند که آنرا به چه کسی ارسال نماید (برای مثال، نهایتا چه کسی می‌بایست آنرا دریافت کند).

یکی از ویژگی‌های دیگر طرح Mix، حفاظت در برابر تحلیل ترافیک است. که این امر از طریق ارسال پیامهای "ساختگی" از A، B و C به Mix و از Mix به X، Y و Z قابل دست‌یابی می‌باشد.

همه‌ی پیامهای، ساختگی و واقعی، می‌بایست:

- تصادفی باشند
- با طول ثابت باشند
- با نرخ ثابتی ارسال شوند
- به بلوکهایی با اندازه‌های ثابت تقسیم شوند
- به صورت رمزنگاری شده ارسال شوند

گمنامی کاربر و عدم توانایی ردیابی مکانی

ایراد اصلی این طرح آن است که Mix باید کاملا قابل اعتماد باشند؟

راه حل: استفاده از یک ماتریس (یا شبکه) از Mixها به جای یک Mix، همانند تصویر است.

هرچه ماتریس بزرگتر باشد، احتمال وجود حداقل یک Mix قابل اعتماد در مسیری که بصورت تصادفی انتخاب شده باشد، بیشتر است.

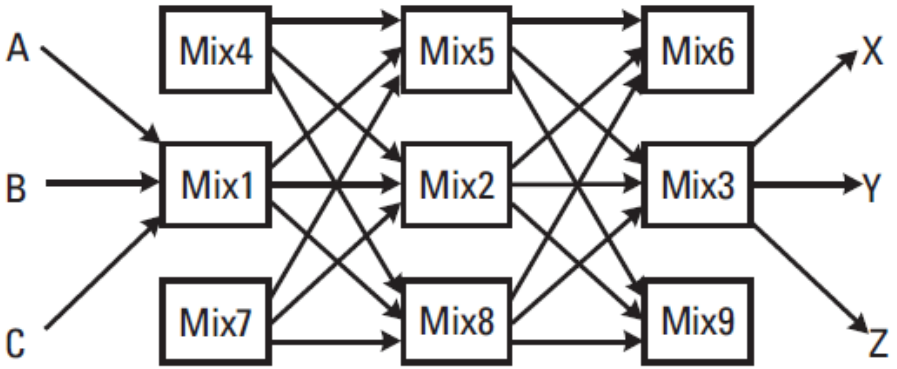
برای زنجیره‌ای از Mixها، Ei می‌تواند کلید عمومی Mix شماره i باشد که i = 1,2,3

پیام A به صورت بازگشتی به شکل زیر ساخته می‌شود:

$$E_{\text{Recipient}}(\text{Next recipient}, E_{\text{Next recipient}}(\ldots))$$

اگر A بخواهد یک پیام گمنام و غیر قابل ردیابی به Y ارسال نماید:

$$\begin{aligned}
&A \rightarrow \text{Mix1}: && E_1(\text{Mix2}, E_2(\text{Mix3}, E_3(\text{Y}, \textit{Message})))\\
&\text{Mix1} \rightarrow \text{Mix2}: && E_2(\text{Mix3}, E_3(\text{Y}, \textit{Message}))\\
&\text{Mix2} \rightarrow \text{Mix3}: && E_3(\text{Y}, \textit{Message})\\
&\text{Mix3} \rightarrow && \textit{Message}
\end{aligned}$$



گمنامی کاربر و عدم توانایی ردیابی مکانی

شخص A می‌تواند یک آدرس بازگشت ناشناس را با یک ماتریس، به همان روشی که در مثال آمده، فراهم سازد. A یک مسیر بازگشت تصادفی از میان شبکه‌ی Mix انتخاب می‌نماید (مثل Mix2, Mix1) و شناسه و آدرس خود را چندین بار توسط کلید عمومی Mixها در مسیر بازگشت رمزنگاری می‌کند.

$$\mathrm{Mix2}, E_2\left(\mathrm{Mix1}, E_1(\mathrm{A})\right)$$

گیرنده‌ی پیام (Y) ، می‌تواند پیام را به اولین ترکیب ارسال نماید، و از این نقطه به بعد دقیقا شبیه همان راه از A به Yعمل می‌کند.

مشکل اصلی: پیاده سازی شبکه‌ی Mix از هر دو دیدگاه سازمانی و فنی بسیار پر هزینه و پیچیده است.

گمنامی پرداخت کننده

نام مستعار

ساده‌ترین راه استفاده از نام مستعار به جای شناسه‌ی واقعی است.

شرکت First Virtual فعالیت خود را بر اساس زیرساخت اینترنتی موجود، برای اجرای اولین سیستم پرداخت اینترنتی آغاز کرد، که این زیرساختها شامل e-mail، TELNET میباشند.

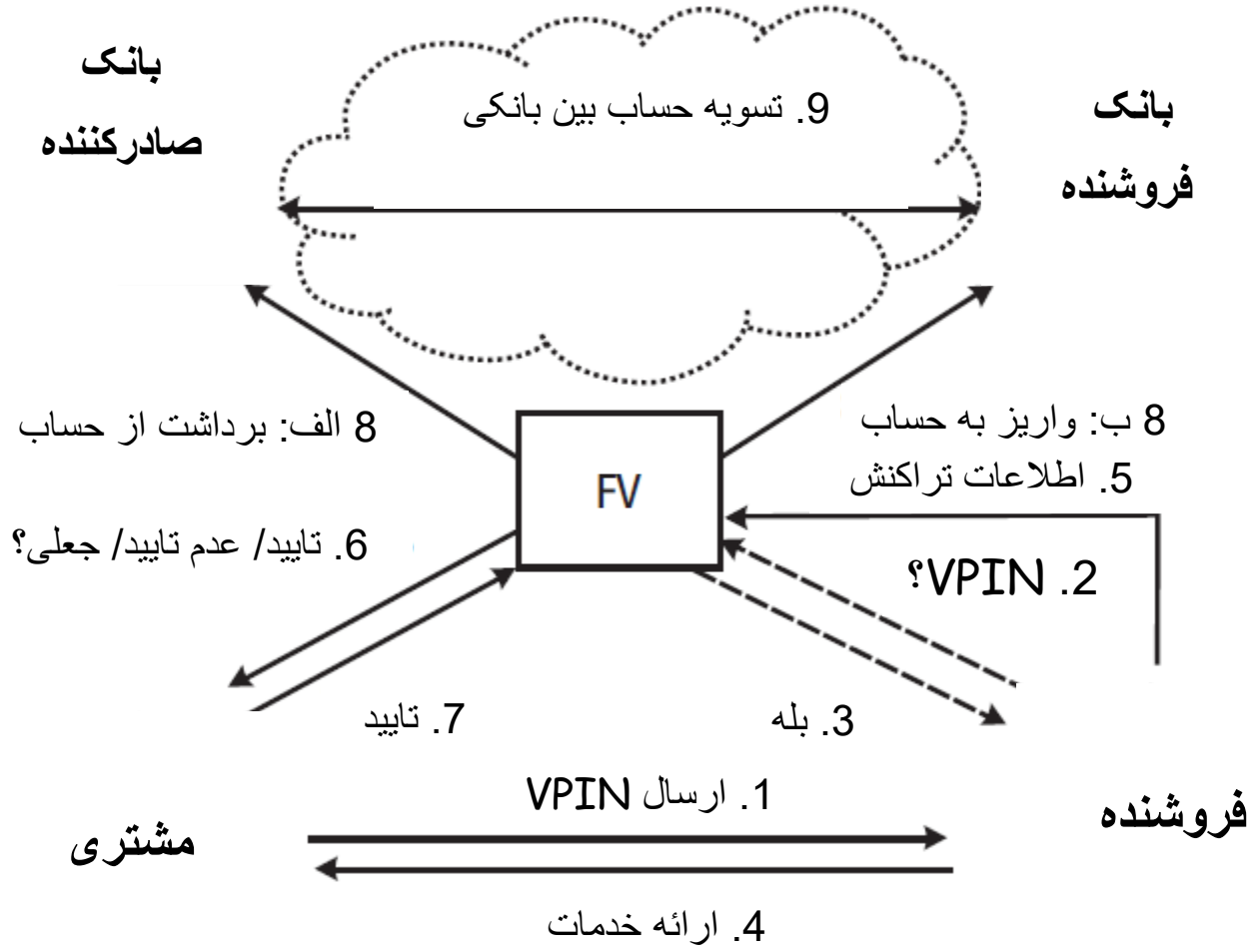
در این سیستم مشتری یک پین مجازی یا VPIN که رشته‌ای از حروف و اعداد هستند و نقش نام مستعار را برای شماره‌ی کارتهای اعتباری خواهد داشت، به روشی امن از طریق پست الکترونیکی دریافت می‌کند.

سوال: اگر ربوده شود؟

پاسخ: یک مشتری غیر مجاز در صورت ربودن نیز، نمی‌تواند از آن استفاده نماید، چرا که تمامی تراکنشها قبل ازاینکه پولی از کارتهای اعتباری برداشته شود، بوسیله‌ی پست الکترونیکی تایید خواهند شد.

تصویر صفحه بعد مراحل این کار را نمایش میدهد:

نام مستعار


بانک
صادرکننده
9. تسویه حساب بین بانکی
بانک
فروشنده
8 الف: برداشت از حساب
8 ب: واریز به حساب
5. اطلاعات تراکنش
FV
6. تایید/ عدم تایید/ جعلی؟
2. VPIN؟
7. تایید
3. بله
1. ارسال VPIN
مشتری
فروشنده
4. ارائه خدمات

نام مستعار

مراحل انجام کار:

1. مشتری سفارش خود را به همراه VPIN به فروشنده ارسال می‌نماید.
2. فروشنده درخواست مجوز دهی VPIN را به ارائه دهنده‌ی پرداخت FV ارسال می‌کند.
3. اگر VPIN قانونی باشد
4. فروشنده خدمات سفارش داده شده‌ی مشتری را تامین می نماید
5. فروشنده اطلاعات تراکنش را به ارائه دهنده‌ی FV ارسال می‌کند.
6. ارائه دهنده‌ی FV از مشتری برای پرداخت هزینه‌ی خدمات پرسش خواهد نمود (مثلا از طریق پست الکترونیک).
7. اگر مشتری اقدام به پرداخت کند، با عبارت "بله" پاسخ خواهد داد.
   - اگر انتظارات مشتری از خدمات ارائه شده برآورده نشود می‌تواند از پرداخت هزینه امتناع نماید
   - اگرخدمات از جانب مشتری سفارش داده نشده باشند، میتواند با عبارت «جعلی" این مشکل را اعلام نماید.
8. (الف:) مبلغ مورد نظر از حساب شخص برداشته شده و (ب:) به حساب فروشنده انتقال داده میشود.
9. بانکها با یکدیگر تسویه حساب خواهند نمود.

عدم قابلیت ردیابی تراکنشهای پرداخت

عدم قابلیت ردیابی تراکنشهای پرداخت

راه حل اول: استفاده از تابع درهم ساز تصادفی درSET (تراکنشهای الکترونیکی امن)

یک فروشنده در این پروتکل تنها شکل درهم شده دستورپرداخت را دریافت خواهد نمود که دستورالعملهای پرداخت، در میان دیگر اطلاعات، شامل داده‌های زیر نیز می‌باشند:

- شماره حساب اولیه یا PAN (برای نمونه شماره کارت اعتباری)
- تاریخ انقضای کارت (CardExpiry)
- یک مقدار مخفی به اشتراک گذاشته شده مابین صاحب کارت، درگاه پرداخت، و صادرکننده‌ی گواهینامه‌ی صاحب کارت (PANSecret)
- یک عدد یکبار مصرف تازه یا همان nonce برای جلوگیری از حملات لغتنامه‌ای

از آنجاییکه nonce برای هر تراکنش پرداخت متفاوت است، لذا درصورتی که دو تراکنش از یک PAN استفاده کنند، فروشنده نمی‌تواند آن دو را به یکدیگر مرتبط نماید.

عدم قابلیت ردیابی تراکنشهای پرداخت

راه حل دوم: استفاده از تابع درهم سازی تصادفی در iKP (پروتکل پرداخت کلیدی اینترنت)

در ابتدا مشتری به روش زیر یک شماره‌ی تصادفی R_C انتخاب نموده و یک اسم مستعار (یکبار مصرف) ID_C نیز می‌سازد.

$$ID_C = h_k(R_C, BAN)$$

BAN همان شماره‌ی حساب بانکی کاربر است (برای مثال، کارت پیش‌پرداخت یا اعتباری).

در اینجا h_k (?) یک تابع یک طرفه درهم سازی مقاوم در برابر برخورد است که اگر R_C به صورت تصادفی انتخاب شود، هیچ اطلاعاتی را درباره BAN ارائه نخواهد داد.

بنابراین مقدار BAN به دست فروشنده نمی‌رسد و فقط ID_C به گیرنده ارسال میشود که از طریق آن هم نمی‌توان BAN را محاسبه کرد.

در این روش برای هر تراکنش پرداخت باید مشتری یک عدد تصادفی که با دفعات پیش متفاوت است را انتخاب نماید و به همین دلیل است که فروشنده اسامی مستعار متفاوتی را دریافت می‌کند.

بنابراین برای فروشنده ممکن نیست که دو تراکنش پرداخت، که با یک BAN انجام شده‌اند را به یکدیگر مرتبط نماید.

محرمانگی داده های تراکنشهای پرداخت

محرمانگی داده ها: در SET

امضای دوگانه از محرمانگی اطلاعات سفارش خرید با توجه به درگاهای پرداخت، محافظت می‌نماید.

اگر بخاطر داشته باشید، در این پروتکل مشتری مقدار زیر را محاسبه می نماید:

$$DS = D_C\left(h(h(PI), h(OI))\right)$$

PI = Payment Instruction

OI=Order Information

فروشنده این مقادیر را دریافت می نماید:

$$OI, h(PI), DS$$

درگاه پرداخت نیز این موارد را دریافت می نماید:

$$PI, h(OI), DS$$

بنابراین هر دوی آنها می‌توانند امضای دوگانه‌ی DS را تصدیق نمایند.

البته این مکانیزم نوعی قابلیت عدم ردیابی تراکنشهای پرداخت را نیز مهیا می‌کند:

درگاه پرداخت می‌تواند تراکنشهای انجام شده توسط یک مشتری را پیوند دهد، اما نمی‌تواند ببیند که چه چیزهایی سفارش داده شده‌اند.

فروشنده هم فقط می‌تواند پرداختها را با اطلاعات سفارش پیوند دهد، ولی نمی‌تواند بفهمد کدام مشتری در پشت آنها قرارگرفته است، همانطور که یک شماره‌ی یکبار مصرف استفاده شده است.

پس تا زمانی که درگاه پرداخت و فروشنده توطئه نکنند، امضای دوگانه قابلیت عدم ردیابی تراکنش پرداخت را با پاسخگویی به فروشنده فراهم می‌نماید.

محرمانگی داده ها: تابع شبه تصادفی در iKP

داده‌های تراکنش پرداخت عموما شامل دو بخش می‌باشند: دستورالعمل پرداخت و سایر اطلاعات.

- دستورالعمل پرداخت می‌تواند شامل شماره کارت اعتباری و یا شماره‌ی حساب باشد
- اطلاعات سفارش می‌تواند نشان دهنده نوع و مقدار کالاها و خدمات سفارش داده شده و مبلغ پرداختی آنها باشد، یا اینکه فقط می‌تواند شامل شماره‌ی سفارش باشد

(مطلوب نیست که درگاه پرداخت (یا دریافت کننده) از رفتار خرید یک مشتری مطلع باشد)

مراحل بصورت زیر خواهد بود:

- در ابتدا مشتری یک عدد تصادفی بنام $SALT_c$ (برای هر تراکنش متفاوت است) را بلافاصله ارسال می‌کند (محافظت نشده).
- فروشنده با استفاده از همان تابع درهم ساز (همانند سابق) شرحی از اطلاعات سفارش (DESC) را برای دریافت کننده به روش زیر فراهم می‌کند:

$$h_k(SALT_C, DESC)$$

بنابراین دریافت کننده می‌تواند ملاحظه نماید که خروجی درهم سازی برای هر پرداخت متفاوت است، اما اطلاعات کافی برای محاسبه‌ی DESC را نخواهد داشت.

مشکل: دریافت کننده، امکان استراق سمع خطوط ارتباطی بین مشتری و فروشنده و لذا یافتن $SALT_c$ را دارد، پس اگر تعداد مقادیر ممکن DESC خیلی بالا نباشند، دریافت کننده میتواند تمام درهم سازی ها را محاسبه می‌کند؟

محرمانگی داده ها: تابع شبه تصادفی در iKP

- در این پروتکل برای ایجاد ارتباط دستورالعمل پرداخت با دریافت کننده به طریقی که فروشنده توانایی خواندن آن را نداشته باشد، *iKP* از کلید عمومی برای رمزنگاری استفاده خواهد نمود. مشتری پیامی که شامل موارد زیر است را رمزنگاری می‌کند:
  - هزینه ی اقلام سفارش داده شده
  - دستورالعمل پرداخت (برای مثال: شماره کارت اعتباری، و بصورت انتخابی PIN)
  - مقدار $h_k(SALT_c, DESC)$ به همراه داده‌های تراکنشهای معمولی درهم سازی شده
  - یک عدد تصادفی R_c برای ایجاد اسم مستعار یک بار مصرف، با کلید عمومی دریافت کننده

حال پیام رمزنگاری شده که برای فروشنده ارسال شده بود برای دریافت کننده فرستاده می‌شود.

مشتری باید گواهی کلید عمومی دریافت کننده را که از جانب صادر کننده‌ای (گواهینامه) مورد اعتماد منتشر شده، داشته باشد.

در اینجا تنها دریافت کننده میتواند پیام را رمزگشایی نموده و با R_c دریافت کننده میتواند درستی نام مستعار یکبار مصرف ID_c مشتری را نیز تصدیق نماید.

عدم انکار تراکنشهای پرداخت

عدم انکار پیامهای تراکنش پرداخت

عدم انکار ارسال و تحویل خیلی پیچیده اند و هنوز مسائل کاملا حل شده‌ای نیستند، چراکه درگیر تعامل با شبکه‌های ارتباطی هستند که به صورت بالقوه غیر قابل اعتماد می‌باشند.

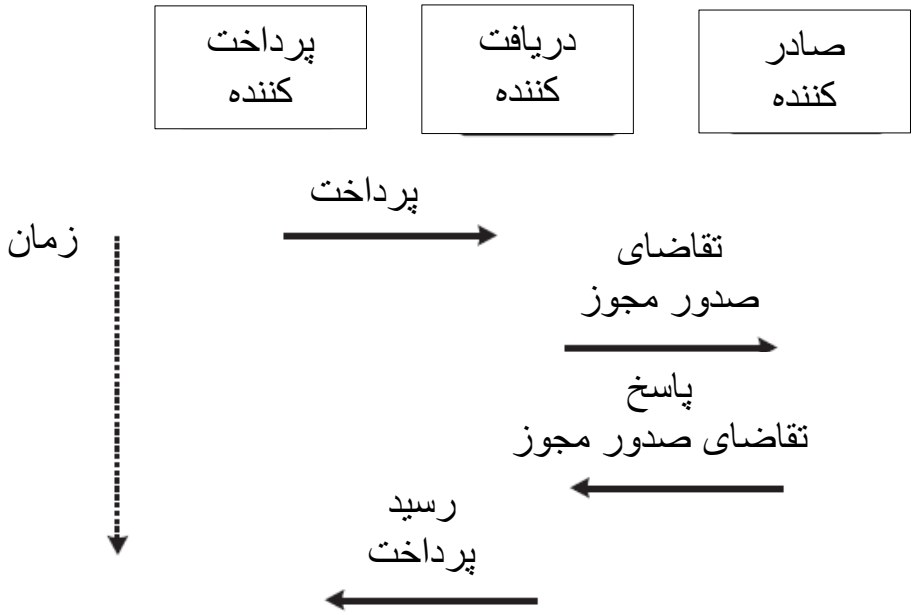
برای نمونه اگر فرستنده‌ای نیاز به اثبات این داشته باشد که واقعا پیامی را فرستاده است، احتمالا درخواست یک تایید ارسال دیجیتالی از گره‌ی شبکه را خواهد داشت. اما، در مسیر شبکه تا دریافت کننده‌ی نهایی ممکن است بیشتر از یک گره وجود داشته باشد، بنابراین ممکن است اولین گره همان را از دومی درخواست نماید و به همین ترتیب ادامه پیدا کند.

در حال حاظر هیچ زیرساختی برای فراهم کردن چنین سرویسی بطور کامل در شبکه وجود ندارد.

عدم انکار تحویل نیز مشابه است: اولین گره درخواست یک تایید تحویل امضاء شده را از دومین گره می‌نماید، و به همین ترتیب پیش می‌رود. نهایتا، آخرین گره در مسیر شبکه از دریافت کننده‌ی واقعی درخواست تایید می‌نماید.

راه حل : امضاء دیجیتالی

تصویر روبر (نمونه 3KP) یک تراکنش پرداخت ساده را نشان می‌دهد:



دریافت کننده یک درگاه پرداخت و یک بانک دریافت کننده را معرفی می‌نماید. فرض بر این است که اطلاعات سفارش (کالاها یا خدمات، قیمت، شیوه‌ی تحویل) قبل از پیام پرداخت مورد بحث و مذاکره قرار گرفته، و پیام پرداخت منحصرا دستورالعمل پرداخت را شناسایی می‌کند. پرداخت کننده پیام پرداخت را که حاوی دستورالعمل پرداخت است و شامل شناسه‌های دستورالعملهای پرداخت نیز می‌شود را به پرداخت شونده ارسال می‌نماید. برای مثال، برای یک کارت اعتباری این داده‌ها شامل بانک صادرکننده، شماره، و تاریخ انقضاء (بازه‌ی اعتبار) خواهد بود.

دریافت کننده می‌خواهد بررسی کند که آیا می‌توان از کارت مورد نظر پول برداشت نمود یا خیر، بنابراین یک پیام درخواست تایید مجوز به صادر کننده می‌فرستد.

پیام پاسخ این درخواست مجوز دهی می‌بایست حاوی نتیجه‌ی مجوز دهی باشد که اگر پاسخ مثبت باشد، دریافت کننده یک رسید پرداخت برای پرداخت کننده ارسال نموده و کالاها و خدمات خریداری شده را تحویل می‌دهد.

راه حل : امضاء دیجیتالی

تصویر روبرو پیامهای مجوز دهی فرستاده شده به هر کدام از 3 عضو شرکت کننده را نشان می‌دهد:

هر سه عضو شرکت کننده یک جفت کلید عمومی دارند. هر کلید عمومی بوسیله‌ی یک صادر کننده‌ی گواهینامه، که به صورت مستقیم و یا غیر مستقیم مورد اعتماد است، گواهی می‌شود.

دریافت کننده احتیاج به مدرک غیر قابل انکار دارد که پرداخت کننده موافقت می‌کند تا مقدار مشخصی پول بپردازد.

مدرک حاوی پیام تایید یا مجوزدهی پرداخت، پرداخت کننده می‌باشد. این پیام از طریق پرداخت کننده از عدم انکار مجوزدهی پرداخت اطمینان حاصل می‌کند.

بانک دریافت کننده و صادر کننده هم به آن مدرک، برای برداشت پول از حساب پرداخت کننده و واریز آن به حساب دریافت شونده نیاز دارند. این پیام بوسیله‌ی کلید عمومی پرداخت کننده به صورت دیجیتالی امضاء می‌شود.

راه حل : امضاء الکترونیکی

بانک دریافت کننده و صادر کننده نیازمند مدرک غیر قابل انکاری هستند که دریافت کننده ه خواستار واریز مبلغ فروش این تراکنش، به حسابش شده است. این همان هدف "مجوز دهی پرداخت به دریافت کننده" است، که پیام بوسیله‌ی کلید عمومی پرداخت شونده امضاء می‌شود.

همانطور که قبلا ذکر شد، از آنجایی که صادر کننده نیاز به مدرکی دارد که دریافت کننده تراکنش پرداخت را تایید کرده است، لذا صادر کننده از دریافت کننده درخواست "پیام تایید پرداخت" دریافت کننده را می‌نماید. این امر توسط دریافت کننده از غیر قابل انکار بودن مجوزدهی پرداخت اطمینان حاصل می‌نماید. پیام با کلید عمومی دریافت کننده امضاء می‌شود.

پیام تایید صادر کننده کارت اثبات می‌کند که دریافت کننده مجاز به جمع آوری پرداختها می‌باشد. اگر صادر کننده کارت در عین حال یک صادر کننده‌ی گواهینامه نیز باشد، پیام می‌تواند در قالب یک گواهی کلید عمومی باشد که در آن کلید عمومی پرداخت کننده نیز بصورت دیجیتال (مثل، گواهی) با کلید عمومی دریافت کننده امضاء شده باشد. در غیر اینصورت پیام می‌تواند نمایانگر یک گواهی مشخص باشد که بوسیله‌ی آن صادرکننده اجازه‌ی جمع آوری پرداختها را به دریافت شونده می‌دهد.

اگرگواهی کلید عمومی را بتوان از یک فهرست راهنما بدست آورد، این پیام ضروری نخواهد بود.

چون پرداخت کننده و دریافت کننده نباید مستقیما ارتباط برقرار کنند، گواهی به دریافت کننده فرستاده می‌شود که برای پرداخت کننده ارسال نماید.

در نهایت دریافت کننده یک رسید پرداخت برای پرداخت کننده ارسال می‌کند. حال دریافت کننده نمی‌تواند پرداخت انجام شده توسط پرداخت کننده را برای موارد خریداری شده منکر شود. رسید باید بصورت دیجیتال توسط دریافت کننده امضاء شود.

تازگی پیامهای تراکنشهای پرداخت

تازگی پیامهای تراکنش پرداخت

این سرویس محافظت در برابر حملات بازپخش را بر عهده دارد. به عبارت دیگر، از استفاده‌ی دوباره‌ی پیامهای تبادل شده طی تراکنش پرداخت توسط استراق سمع کنندگان یا شرکت کنندگان متقلب جلوگیری می‌کند.

راه حل: **استفاده از شماره‌های یکبار مصرف (شماره‌های تصادفی) و برچسبهای زمان**

به تصویر صفحه بعد (نمونه 1KP) توجه نمایید:

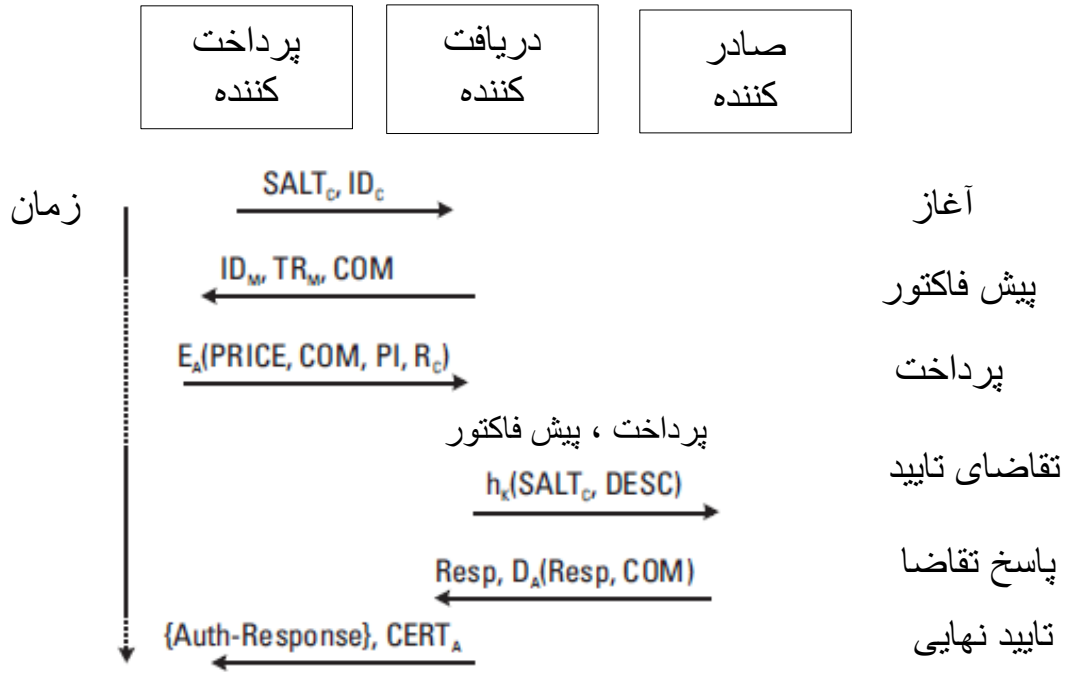
پنج مقدار وجود دارد که برای هر تراکنش پرداخت منحصر به فرد می‌باشند:

- شناسه‌ی تراکنش، ID_M، که توسط تاجر انتخاب می‌شود
- تاریخ و زمان فعلی، DATE
- شماره‌ی تصادفی، $NONCE_M$، که توسط تاجر انتخاب می‌شود
- شماره‌ی تصادفی، $SALT_C$، که توسط مشتری انتخاب می‌شود
- شماره‌ی تصادفی، R_C، که توسط مشتری انتخاب می‌شود

هدف ID_M، DATE، و $NONCE_M$ حصول اطمینان از تازگی تمام پیامهای تراکنشهای پرداخت به جز پیام آغازین می‌باشد. هر سه مقدار با هم به TR_M معروفند و تمام پیامهای تراکنش به R_C و $SALT_C$ بستگی دارند.

راه حل: شماره‌های یکبار مصرف و برچسبهای زمان

مشتری با ارسال پیام آغازین، تراکنش پرداخت را شروع می‌کند. او از یک اسم مستعار یکبار مصرف ID_C استفاده می‌نماید..



فروشنده با پیام صورتحساب پاسخ می‌دهد که ID_M شناسه‌ی آن است. مقدار COM در اینجا نشانگر یک اثر انگشت داده‌ی تراکنش عمومی است که برای همه‌ی شرکت کنندگاه شناخته شده است:

$$COM = h(PRICE, ID_M, TR_M, ID_C, h_k(SALT_C, DESC))$$

که در آن $H(.)$ یک تابع درهم‌سازی یکطرفه است.

راه حل: شماره‌های یکبار مصرف و برچسبهای زمان

پیام پرداخت با کلید عمومی دریافت کننده E_Z رمز شده است.

مشتری و فروشنده در مورد PRICE و DESC (اطلاعات سفارش) قبل از پیام آغازین مذاکره نموده‌اند.

صادر کننده می‌تواند مقدار PRICE را از پیام پرداختی که به او فرستاده شده و با کلید عمومی E_A رمز شده است، محاسبه نماید. اما از آنجاییکه پروتکل از محرمانگی اطلاعات سفارش با پاسخگویی به صادر کننده اطمینان دارد، هیچ وقت از DESC اطلاع پیدا نخواهد کرد.

در اینجا PIدستورالعمل پرداخت مشتری می‌باشد که بطور مثال حاوی، شماره کارت اعتباری و PIN مربوط به کارت خواهد بود.

پیام Auth-Request یا همان درخواست مجوز، در اصل حاوی صورتحساب و پیام پرداخت خواهد بود.

در اینجا {پیام} بیانگر محتویات پیام ارسال شده‌ی قبلی می‌باشد. مقدار $h_k(SALT_c,DESC)$، بهمراه COM، در اصل ارتباطی بین دستورالعمل پرداخت و اطلاعات سفارش ایجاد می‌کنند.

همچنین Resp، پاسخ مجوزدهی از دریافت کننده است، و اگر کارت اعتباری قابل شارژ باشد پاسخ مثبت (بله) و در غیر اینصورت پاسخ منفی (خیر) خواهد بود.

کل پیام Auto-Response توسط دریافت کننده امضاء شده است (D_A).
تاجر پیام Auto-Response را به مشتری ارسال می‌نماید. در اینجا $CERT_A$ گواهی کلید عمومی صادر کننده می‌باشد که می‌توان از یک دایرکتوری (فهرست راهنما) بصورت آنلاین آنرا بازیابی نمود.

خلاصه: گمنامی کاربر و عدم توانایی ردیابی مکانی، گمنامی پرداخت کننده، نام مستعار، عدم قابلیت ردیابی، تابع درهم سازی تصادفی در iKP، تابع درهم ساز تصادفی درSET، محرمانگی داده ها، تابع درهم سازی تصادفی در iKP، امضاء دوگانه در SET، عدم انکار، تازگی پیام

جلسه بعدی: امنیت پول دیجیتالی

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