امنیت تجارت الکترونیک

فصل پنجم:
سرویسهای امنیتی پرداخت

تهیه و تنظیم: دکتر آرش حبیبی لشکری

اولین نسخه: دی 1393
بروزرسانی: شهریور 1394

فهرست:

- **سرویسهای امنیتی پرداخت**
  - امنیت تراکنش پرداخت
    - ناشناس بودن - گمنامی
    - عدم قابلیت ردیابی
    - محرمانگی داده‌های تراکنش پرداخت
    - عدم انکار پیامهای تراکنش پرداخت
    - تازگی پیامهای تراکنش پرداخت
  - امنیت پول دیجیتالی
    - محافظت در برابر خرج کردن دوباره
    - محافظت در برابر جعل سکه
    - محافظت دربرابر سرقت سکه‌ها
  - امنیت چک امنیتی
    - انتقال مجوز پرداخت (پروکسی)

سرویسهای امنیتی پرداخت

سرویسهای امنیتی پرداخت

برای اقناع کامل نیازمندیهای امنیتی یک سیستم یا سامانه پرداخت الکترونیکی، مهیا کردن برخی از سرویسهای امنیتی اضافی علاوه بر سرویسهای امنیتی پایه مورد نیاز می باشد.

سرویسهای امنیتی پرداخت به سه گروه اصلی بسته به ابزار پرداخت استفاده شده، قابل تقسیم هستند:

- گروه اول مربوط به همه‌ی سیستمهای پرداخت الکترونیکی و همه‌ی ابزارهای پرداخت می‌شوند و به سرویسهای امنیتی تراکنشهای پرداخت معروف هستند.

- گروه دوم سرویسها، گروهی از سیستمهای پرداخت هستند که از پول دیجیتال به عنوان یک ابزار پرداخت استفاده می‌کنند و در اصطلاح به آنها *امنیت پول دیجیتال* می‌گویند.

- گروه سوم درواقع همان سرویسهای امنیتی ولی بر پایه تکنیکهای مخصوص سیستمهای پرداخت با چکهای الکترونیکی هستند.

سرویسهای امنیتی تراکنشهای پرداخت

- ناشناس بودن یا گمنامی کاربر: حراست از افشاء شدن شناسه‌ی کاربر در یک تراکنش شبکه‌ای.
- عدم قابلیت ردیابی مکانی: حراست از افشای منبع یا محل وقوع تراکنش پرداخت.
- ناشناس بودن شخص پرداخت کننده: حراست از افشای شناسه‌ی پرداخت کننده در یک تراکنش پرداخت.
- عدم قابلیت ردیابی تراکنش پرداخت: محافظت دربرابر اتصال یا پیوند دو تراکنش پرداخت جداگانه مربوط به یک مشتری.
- محرمانگی داده‌های تراکنش پرداخت: به صورت انتخابی از افشای بخشهای خاصی از تراکنش پرداخت برای افراد غیر مرتبط حفاظت می‌کند.
- عدم انکار پیامهای تراکنش پرداخت: حراست در برابر انکار اصل پیام مبادله شده در یک تراکنش پرداخت.
- تازگی پیامهای تراکنش پرداخت: حراست در برابر بازپخش پیامهای تراکنش پرداخت

سرویسهای امنیتی پول و چک دیجیتال

- **سرویسهای پول دیجیتال:**
- محافظت در برابر خرج کردن دوباره: از چند بار خرج کردن سکه‌های الکترونیکی جلوگیری می‌نماید.
- محافظت در برابر جعل سکه: از تولید سکه‌های دیجیتال جعلی بوسیله‌ی یک عامل غیرمجاز جلوگیری می‌نماید.
- محافظت دربرابر سرقت سکه‌ها: از استفاده سکه‌های دیجیتال توسط یک عامل غیرمجاز جلوگیری می‌نماید.

- **سرویسهای چک دیجیتال:**
- انتقال مجوز پرداخت (پروکسی): انتقال اجازه‌ی پرداخت از مسئول مجاز به مسئول دیگر که توسط مسئول مجاز انتخاب شده را ممکن می‌سازد.

گمنام سازی و عدم ردیابی مکانی

گمنام سازی کاربر قابلیت استفاده برای تمام سرویسهای شبکه را دارد. (پست الکترونیکی ناشناس یا خرید کالا بصورت ناشناخته) برای نمونه قابلیت عدم ردیابی مکانی مربوط می‌شود به گمنامی شبکه‌ی کاربر (پست الکترونیکی ناشناخته که فیلد فرستنده ندارد)، آیا آدرس IP قابل ردیابی نیست؟

از آنجا که تراکنشهای پرداخت الکترونیک در یک شبکه ارتباطی انجام می‌پذیرند، گمنامی پرداخت کننده سرویسی است که بین دو طرف ارتباطی به کار گرفته می‌شود:

بین مشتری و فروشنده - بین فروشنده و بانک فروشنده - بین بانک فروشنده و بانک مشتری

پرداخت کننده در هر جلسه ای بجز در جلساتی که با بانک خود در ارتباط است، گمنام خواهد بود.

گمنامی پرداخت کننده = گمنامی کاربر (مثل قابلیت عدم ردیابی مکانی) + مکانیزمهای دیگر

یک پرداخت کننده می‌تواند گمنام باشد به نحوی که دارای یک اسم مستعار و یا یک شناسه‌ی عددی باشد؟ اگر کسی از یک شناسه برای تمامی تراکنشهای پرداخت خود استفاده نماید، رفتار آن شخص نظارت خواهد شد که در ترکیب با اطلاعات جنبی دیگر، حتی می‌تواند هویت شخص نیز استنتاج شود.

محرمانگی، عدم انکار و تازگی تراکنشهای پرداخت

محرمانگی داده‌های تراکنشهای پرداخت: درواقع به نوعی همان محرمانگی پایه (جلسه اول) است. ولی امکان پیچیده تر شدن آن نیز وجود دارد. برای نمونه این سرویس می تواند نه تنها از افشاء داده‌های تراکنشهای پرداخت به افراد خارج از سیستم حفاظت نماید، بلکه از افشاء بخشهای انتخاب شده‌ای از داده‌ها برای شرکت کنندگان در تراکنش نیز جلوگیری نماید.

اصل عدم انکار: مشتری ادعا می‌کند که هرگز دستورالعمل پرداختی صادر نکرده یا تاجر ادعا می‌کند که هرگز پرداختی از جانب مشتری انجام نشده است.

تضمین تازگی پیامهای تراکنش پرداخت: به این معنی است که از استفاده‌ی مجدد آنها جلوگیری شود، برای نمونه می‌توان به پیامهای دستورالعملهای پرداخت اشاره نمود. اگر یک مشتری اطلاعات کارت اعتباری خود را بهمراه دستور پرداخت خود ارسال نماید، حتی اگر پیام رمزنگاری شده باشد، می‌تواند توسط حمله فرد- در- میانه استراق سمع شده و در آینده توسط مهاجم بدون اطلاع مشتری (صاحب کارت) مورد استفاده قرار گیرد.

سرویسهای امنیتی پرداخت

گمنامی کامل می‌تواند باعث ایجاد تقلب و ناتوانی در دستگیری شخص خطاکار شود. برای مثال، یک سکه‌ی الکترونیک کاملا گمنام به صورت رشته ای از بیتها است که می‌تواند به هر تعدادی که خواسته شود، تکثیر گردد. آیا بانک حتی اگر متوجه این اتفاق شود، می تواند هویت شخص را معین کند؟

در این موارد، سرویس حفاظت در برابر خرج کردن مجدد سکه ها می‌تواند یاری دهنده باشد. این سرویس می‌تواند بر اساس گمنامی شرطی اجرا شود، که شرط آن این باشد که اگر مشتری صادق باشد و هر سکه را یکبار خرج کند، هویت آن مشخص نشود. ولی اگر سعی بر دوباره خرج کردن سکه‌ها داشته باشد، شناسایی شده و در نهایت مسئولیت را بر عهده گیرد.

رشته‌های بیتی، سکه‌های الکترونیکی اگر رمزنگاری نشوند به سادگی می‌توانند دزدیده (توسط استراق سمع) شوند. اگر پرداخت کننده‌ها گمنام باشند آنگاه راهی برای دریافت کننده‌گان وجه وجود ندارد که مالک قانونی را از یک سارق که سکه‌ها را دزدیده تشخیص دهند. هرچند مکانیزمهایی برای جلوگیری از دزدیده شدن سکه‌ها وجود دارد و در پیاده سازی سرویسهای امنیتی پرداخت نیز از آنها استفاده شده‌است.

تعاملی بین میزان خطر یا ریسک و میزان حفاظت (برای مثال گمنامی شرطی)

یک چک الکترونیک با امضاء الکترونیکی مورد تایید امکان برداشت از حساب را صادر می نماید، در اینجا سرویس انتقال مجوز امنیت این تراکنش را تامین می نماید.

در دسترس بودن و قابلیت اطمینان

در دسترس بودن و قابلیت اطمینان

- یک سیستم پرداخت الکترونیک جدا از احتیاج به امن بودن، باید در دسترس و قابل اطمینان باشد. یعنی باید در همه‌ی زمانها، هفت روز هفته، 24 ساعت شبانه‌روز در دسترس باشد.

- همچنین باید در مقابل حملات ازکار- انداختن- سرویس (DOS) نیز حفاظت شود، یا اینکه حداقل توانایی تشخیص آنها را داشته و به سرعت شروع به احیای رویه‌ها نماید.

- برای تضمین قابلیت اطمینان، تراکنشهای پرداخت باید به صورت **اتومیک** باشند. به این معنی که تراکنشها یا کاملا اتفاق می‌افتند یا اصلا رخ نمی‌دهند، ولی به هیچ وجه در یک حالت ناشناخته و ناسازگار باقی نمی‌مانند.

- علاوه بر این، سرویسهای بنیادی شبکه نیز همانند اجزای سخت افزاری و نرم افزاری باید به اندازه کافی قابل اطمینان باشند.

خلاصه:

امنیت تراکنش پرداخت، ناشناس بودن،عدم قابلیت ردیابی، محرمانگی داده‌های تراکنش پرداخت، عدم انکار پیامهای تراکنش پرداخت، تازگی پیامهای تراکنش پرداخت، امنیت پول دیجیتالی ، محافظت در برابر خرج کردن دوباره، محافظت در برابر جعل سکه، محافظت دربرابر سرقت سکه‌ها، امنیت چک امنیتی، انتقال مجوز پرداخت (پروکسی)

جلسه بعدی:

امنیت تراکنش پرداخت

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