امنیت تجارت الکترونیک

فصل هفتم:
امنیت پول دیجیتالی

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

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

عدم قابلیت ردیابی تراکنش

وقتی یک مشتری از یک ATM یا بانک پول برداشت می کند، معمولا شماره سریال اسکناسها ثبت نشده اند. به همین دلیل نمی توان تراکنشهای پرداخت را به یک مشتری خاص ربط داد.

سکه های دیجیتالی شماره سریال دارند و گاهی اوقات به جهت برآوردن برخی شرایط خاص، با شماره های خاصی نشان داده می شوند.

از آنجایی که این شماره ها به شکل الکترونیکی هستند، ایجاد یک لیست که بیانگر این باشد که کدام مشتری کدام شماره سریال را دریافت کرده، خیلی آسان است.

امضای کور

D. Chaum یک مکانیزم رمزنگاری پیشنهاد کرده است که می توان برای کور کردن ارتباط بین سکه های صادر شده و شناسه مشتری که آنها را دریافت کرده استفاده کرد.

مکانیزم مذکور، که هر دو عامل گمنامی پرداخت کننده و قابلیت عدم ردیابی تراکنش پرداخت را فراهم می کند، بر اساس امضای RSA بوده و چون امضا کننده نمی تواند ببیند چه چیزی را امضاء می‌نماید به *امضای کور* معروف است.

امتیاز آن به نرم افزار پرداخت اینترنتی eCash اعطا شده است. البته امضای کور در پروژه CAFE نیز به کار گرفته شده بود.

عدم قابلیت ردیابی تراکنش

سناریو اصلی همان سناریویی است که در RSA موجود است:

- ✓ d کلید خصوصی امضاء کننده
- ✓ e و n هم کلیدهای عمومی امضاء کننده
- ✓ یک پارامتر اضافی بنام فاکتور مخفی سازی **k نیز** وجود دارد که توسط ارائه دهنده‌ی پیام (برای مثال، شماره سریالهای پول دیجیتال) انتخاب می‌شود.

ارائه دهنده پیام **M** را کور می‌کند:

$$M' = M\, k^e \bmod n$$

امضاء کننده در اینجا امضاء به اصطلاح کور را محاسبه می‌نماید:

$$S' = (M')^d \bmod n = k\, M^d \bmod n$$

تهیه کننده فاکتور مخفی سازی را حذف می‌نماید:

$$S = S' / k = M^d \bmod n$$

حال امضاء کننده معمولا می‌خواهد بررسی کند که آیا پیام **M** (برای مثال، یک رای یا سکه دیجیتال) معتبر است یا خیر:

برای این منظور ارائه دهنده **n** پیام آماده می‌کند و هر کدام را با یک فاکتور مخفی سازی جداگانه کور می‌کند.

سپس، امضاء کننده **n-1** پیام را بصورت تصادفی انتخاب کرده و از ارائه دهنده می‌خواهد که فاکتور کوری متناظر را ارسال نماید.

امضاء کننده **n-1** پیام را بررسی می‌کند؛ اگر صحیح باشند، پیامهای باقی مانده را بررسی می‌نماید.

سکه های الکترونیکی که به این روش گمنام سازی می‌شوند فقط در سیستم پرداخت آنلاین قابل استفاده می‌باشند. به منظور جلوگیری از خرج کردن دوباره، باید در یک پایگاه داده‌ی مرکزی بررسی شوند که آیا در حال حاظر سکه‌ها خرج شده‌اند یا نه.

تبادل سکه ها

تبادل سکه‌ها:

سیستم NetCash توسط موسسه‌ی علوم اطلاعات دانشگاه کالیفرنیای جنوبی توسعه داده شده است: گمنامی کاربر و مکانیزم عدم ردیابی تراکنش پرداختی در اینجا بر اساس سازمانهای واسط قابل اعتماد، فراهم می‌شود.

شبکه‌ای از سرویس‌دهنده‌های پولی وجود دارد که تبادل سکه‌های شناسه- محور برای سکه‌های گمنام را، بعد از تایید صحت و حصول اطمینان از عدم خرج کردن دوباره، انجام می‌دهد.

این نوع گمنامی "ضعیفتر" از مکانیزم امضای کور است، زیرا:

- با امضای دیجیتال، تعیین شناسه‌ی کاربر ممکن نیست، حتی اگر تمام شرکت کنندگان برای انجام این امر مشارکت کنند (توطئه کنند)
- (با سرویس‌دهنده‌های پولی)، اگر تمام شرکت کنندگان از جمله سرویس‌دهنده‌های پولی درگیر در تراکنش توطئه کنند، امکان این هست که تشخیص دهیم چه کسی پول را خرج کرده است

در NetCash مشتری آزاد هست تا سرویس‌دهنده پولی که مورد اعتماد است، را انتخاب نماید. اما، حداقل باید یک سرویس‌دهنده قابل اعتماد و صادق به منظور تبادل سکه‌ها برای مشتریان وجود داشته باشد، درغیر اینصورت مکانیزم گمنامی کار نخواهد کرد.

البته مکانیزم برپایه امضای کور نیازی به شخص سوم ندارد.

خرج کردن مجدد سکه الکترونیکی

حفاظت دربرابر خرج کردن مجدد

سکه‌ها دراصل اعداد الکترونیکی ذخیره شده هستند

- پرداخت کننده یک سکه‌ی معتبر را از راه قانونی بدست می آورد
- این امکان وجود دارد که برای خرج کردن بیشتر از یکبار آن بصورت غیرقانونی اقدام نماید.

روش اول: گمنامی شرطی با استفاده از بریدن- و- انتخاب کردن:

مکانیزمهای گمنامی شرطی فقط برای مشتریان غیرقابل اعتماد "فعال" می‌شود و شناسه‌ی مشتریان غیرقابل اعتماد که سعی بر خرج کردن مجدد سکه‌ها دارند، فاش خواهد شد.

(برای پولهای دیجیتالی با شماره سریالهای از قبیل **eCash** که از امضاهای کور استفاده می‌کنند، بکار میرود)

مکانیزمی تحت عنوان *جداسازی مخفی* : پیام **M** را به چند بخش تقسیم می کنیم، لذا تمام بخشها باید کنار هم قرار گیرند تا **M** دوباره شکل گیرد (در یک طرح مخفی به اشتراک گذاری فقط یک زیرمجموعه از بخشها ممکن است برای دوباره شکل گیری **M** کافی باشند).

یک روش ساده پیدا کردن M_1 و M_2 است بطوری که:

$$M=M_1 \oplus M_2$$

حفاظت دربرابر خرج کردن مجدد

این امر با انتخاب یک M_1 تصادفی که هم طول M باشد و محاسبه M_2 بصورت زیر قابل انجام است:

$$M2=M \oplus M_1$$

در مفاهیم پول دیجیتالی، به هر سکه یک شماره سریال و N جفت رمزنگاری شده‌ی گوناگون (I_1 , I_2) (که برای مثال، با کلیدهای مختلف رمز شده‌اند) اختصاص داده شده، بنابراین شناسه‌ی مشتری بصورت زیر قابل فاش شدن است:

$$I=I_1 \oplus I_2$$

- وقتی مشتری به فروشنده با سکه الکترونیکی عملیات پرداخت را انجام می‌دهد، فروشنده از او می-خواهد که یا I_1 و یا I_2 را از هر جفت رمزگشایی نماید (انتخاب تصادفی).
- اگر از الگوریتم کلید عمومی استفاده شده باشد، فروشنده می‌تواند تصدیق نماید که آیا نتیجه‌ی رمزگشایی معتبر بوده یا خیر؟
- اگر مشتری سعی بر دوباره خرج کردن یک سکه داشته باشد، خیلی محتمل است که، برای N (برای مثال، N=100)، حداقل یک قسمت-I متناظر با یک قسمت-I که در خرج کردن بار اول فاش شده بود (برای مثال، از همان جفت) آشکار شود

حفاظت دربرابر خرج کردن مجدد

روش دوم: امضاء کور

سیستم بر اساس امضاء کور همانطور که در بخش قبل گفته شد، باید شماره سریالهای تمام سکه‌های خرج شده را در یک پایگاه داده به منظور بررسی خرج کردن مجدد، ذخیره نمود.

- یک مشکل جدی در مقیاس بزرگ را مطرح می‌کند.
- از آنجاییکه از پایگاه داده در هر پرداختی که سکه خرج شود باید پرسش شود، این مدل فقط برای سیستمهای پرداخت آنلاین مناسب است.

روش سوم: تبادل سکه

برای حفاظت از گمنامی کاربر در سیستم NetCash، یک سکه در یک سرویس‌دهنده پولی قابل اعتماد می‌تواند مبادله شود.

فقط شماره سریالهای تمام سکه‌های صادر شده و نه سکه‌های خرج شده، باید در پایگاه داده یک سرویس-دهنده پولی ذخیره شوند و به محض اینکه سکه خرج شود، شماره سریال آن از پایگاه داده حذف خواهد شد.

- این سیستم، دارای مقیاس پذیری بالاتری نسبت به سیستم امضاء کور که در بالا بیان شد، خواهد بود.
- از آنجاییکه حداقل یک سرویس‌دهنده پولی باید برای کاربرقابل اعتماد باشد، گمنامی نسبت به امضاء کور که نیاز به وجود یک عضو قابل اعتماد ندارد، ضعیفتر خواهد بود.
- چون به ازای خرج کردن هر سکه باید از پایگاه داده قبل از خرج شدن پرسش شود، لذا سیستم تبادل سکه‌ها فقط در سیستم پرداخت آنلاین قابل استفاده خواهد بود.

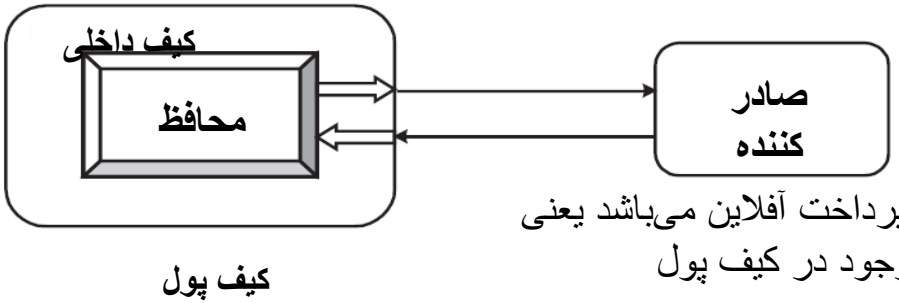
حفاظت دربرابر خرج کردن مجدد

روش چهارم: محافظ

مکانیزمهای نسبتا پیشرفته‌ای که از خرج کردن مجدد سکه‌ها در یک سیستم پرداخت آفلاین حفاظت می‌نماید

مکانیزمهای مشابه در **"T wallet"** که یک کیف پول الکترونیکی است و در پروژه **CAFE** توسعه داده شده است، به کار گرفته شده‌اند.

ایده‌ی اصلی در تصویر روبرو آمده است: صادرکننده یک سازمان بانکداری می‌باشد که پول دیجیتال صادر می‌کند. کیف پول خود شامل دو بخش است، یک کیف داخلی که نشان دهنده دارایی بوده و مورد تایید پرداخت کننده است و یک محافظ و نگهبان که مورد تایید صادر کننده است:



- محافظ یک تراشه‌ی ریزپردازنده است که هم می‌تواند در یک کیف پول قرار داده شود و هم می‌تواند روی یک کارت هوشمند سوار شود.
- نقش آن حفاظت از پول صادر کننده، طی تراکنش پرداخت آفلاین می‌باشد یعنی جلوگیری از خرج کردن مجدد، بیشتر از دارایی موجود در کیف پول
- محافظ یک دستگاه *غیر قابل تغییر*یا مقادم دربرابر تغییر بوده و برای پرداخت کننده، تغییر عملکرد محافظ از راه فیزیکی یا الکترونیکی، سخت یا غیرممکن باشد
- کیف پول به شکل یک کامپیوتر کوچک قابل حمل به همراه تامین کننده برق، صفحه کلید و نمایشگر جداگانه است که نقش آن حفاظت از موارد مورد توجه پرداخت کننده (گمنامی و قابلیت عدم ردیابی) می‌باشد. (کیف پول تمام اعمال مربوط به محافظ را بررسی می‌کند)
- محافظ، فقط از طریق کیف پول می‌تواند با دنیای بیرون ارتباط برقرار کند، بنابراین کیف پول قابلیت بررسی تمام پیامهای ورودی و خروجی را خواهد داشت

حفاظت دربرابر خرج کردن مجدد

امضاء محافظ:

وقتی یک پرداخت کننده از یک حساب سکه ای، سکه ی الکترونیکی برداشت می کند و کیف پولش را شارژ می کند،:

- یک "بخش" از هر سکه به کیف داخلی که نشان دهنده‌ی دارایی است داده می‌شود
- "بخش" دیگر به محافظ داده خواهد شد

وقتی پرداخت کننده بخواهد سکه ای در یک تراکنش پرداخت خرج نماید، محافظ نیز باید موافقت نماید. به عبارت دیگر، هر دو "بخش" سکه باید "ترکیب" شوند تا یک سکه قابل قبول بدست آید. در واقع "ترکیب" سکه ها توسط نوع خاصی از امضاء الکترونیک پیاده سازی می شود.

امضاء صادر کننده:

برای فراهم آوردن قابلیت عدم ردیابی پرداخت، امضاء روی سکه که کیف داخلی از صادر کننده می گیرد، باید کور باشد (شبیه به آنچه که در بخش قبل گفتیم). کیف داخلی باید پیام و چالش را از طریق امضای پایه ای پنهان یا به اصطلاح کور نماید.

جعل سکه الکترونیکی

حفاظت در برابر جعل سکه

جعل پول سنتی نسبتا سخت است:

- اسکناسها باید خصوصیات فیزیکی خاص، گران و یا خصوصیاتی که به راحتی قابل تولید نیستند داشته باشند (برای مثال، چاپ یا رنگ خاص).
- حداقل شماره‌های سریال و توالی باید واقعی به نظر برسند. در حالیکه شماره‌های سریال در واقع جعلی هستند و با بررسی شماره سریال در مرکز قانونی صدور اسکناس براحتی قابل تشخیص خواهند بود

در مورد پول دیجیتال، مسئله‌ی قابلیت تکثیر فیزیکی خودنمایی نمی‌کند.

- شماره‌های سریال می‌توانند قبل از خرج کردن پول در سیستمهای آنلاین بررسی شوند (که نه عملی و نه مقیاس پذیر خواهد بود)
- تنها گزینه‌ی موجود، صدور سکه با شماره سریالهایی است که دارای خصوصیات خاص محاسبات ریاضی باشند.

راه حل پیشنهادی :سکه‌هایی با هزینه‌ی تولید بالا است

- اگر تولید سکه‌های کم ارزش هزینه‌ی بالایی داشته باشند، یا اگر سازماندهی تولید سکه نیاز به سرمایه گذاری عظیمی داشته باشد، جعل سکه سودمند نخواهد بود

MicroMint یک سیستم پرداخت خرد، اعتبار محور، آفلاین می‌باشد.

در پس الگوی MicroMint که توسط River و Shamir ارائه شده است، نظریه گران بودن سکه های کم ارزش قرار داشت.

- خصوصیت آن این است که، تولید تعداد زیادی سکه نسبت به تولید تعداد کمی سکه، ارزانتر است.
- الگوی اساسی از رمزنگاری کلید عمومی استفاده نمیکند، تنها تابع درهم سازی رمزنگاری استفاده میشود
- دراصل، یک سکه با تلاقی یک تابع درهمساز نمایش داده می‌شود.

دزدیدن سکه دیجیتالی

حفاظت دربرابر دزدی سکه

یک راه مشخص برای حفاظت از دزدیده شدن سکه‌های دیجیتالی، استفاده از رمزنگاری است.

- سکه‌ها بطور معمول دارای ارزش بسیار کمی می‌باشند (برای نمونه، یک دلار)
- در نتیجه، در موارد زیادی استفاده از مکانیزم رمزنگاری نسبتا غیر کارآمد و پرهزینه به نظر می‌رسد.

روش اول : سفارشی کردن سکه ها

سفارشی کردن سکه باعث ایجاد محدودیتهایی مانند اینکه چه کسی قادر به خرج کردن آن است، میشود. راه ساده برای سفارشی کردن یک سکه، افزودن اطلاعات شناسه‌ی مشتری به آن است.

- البته قابل فهم است که گاهی اوقات مشتریان در قبال قبول خطر از دست دادن چند سکه ترجیح می دهند گمنام بمانند.
- در مواردی که سکه‌ها مختص- فروشنده می شوند، احتمال دزدیدن آنها کاهش می یابد.

سکه‌های مختص- مشتری و همچنان گمنام

مکانیزم نمونه NetCash بعنوان یک سیستم پرداخت آنلاین

یک سکه سفارشی شده، قابلیت به کارگیری توسط یک مشتری مشخص در مدت زمان معین را دارد

بعلاوه، مکانیزم حافظ گمنامی کاربر بوده و از دوباره خرج شدن پول جلوگیری نموده، و به مشتری ضمانت می‌دهد که رسید دریافتی از فروشنده معتبر است

حفاظت دربرابر دزدی سکه

مختص مشتری نمودن سکه ها:

روش اول : تبدیل نمودن سکه به سکه‌ی مختص- گروه:

- گروه شامل تعدادی از مشتریان است
- گروه نباید زیاد بزرگ باشد، چراکه در این صورت ممکن است سکه‌ها از عضوی از گروه دزدیده شده و به عضوی دیگر فروخته شوند
- گروه خیلی هم نباید کوچک باشد، زیرا این امر نیازمند محاسبات زیادی برای واسط معاملات جهت برآورده کردن نیازمندیهای همه مشتریان خواهد بود

اگر سکه‌های مختص- مشتری قابلیت خرج کردن تنها نزد یک فروشنده را داشته باشند، دزدیدن سکه ها جذابیت خود را از دست خواهد داد، چرا که فروشنده به سادگی می‌تواند تشخیص دهد که آیا سکه‌ها در حال حاظر برای کالاها یا خدماتش خرج شده‌اند یا خیر.

روش دوم: تبدیل سکه به سکه مختص- مشتری و سپس تبدیل سکه به سکه فروشنده توسط مشتری

خلاصه: امنیت تراکنشهای پول الکترونیک، عدم قابلیت ردیابی تراکنش، امضاء کور، تبادل سکه ها، حفاظت دربرابر خرج کردن مجدد، گمنامی شرطی توسط بریدن- و- انتخاب کردن، امضاء کور، تبادل سکه ها، محافظ، امضاء محافظ، امضاء صادر کننده، حفاظت در برابر جعل سکه، سکه‌هایی با هزینه‌ی تولید بالا، حفاظت در برابر دزدی سکه-ها، سکه‌های سفارشی شده، سکه‌های مختص- مشتری و همچنان گمنام، سکه‌های مختص- مشتری

جلسه بعدی: امنیت چک الکترونیکی و پروتکل تجارت باز الکترونیکی

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