کوپن های الکترونیکی:

سیستم میکرو پرداخت کارآمد، امن و قابلیت محول کردن به غیر

چکیده

در این مقاله، یک طرح میکرو پرداخت کارآمد و امن جدید، به نام کوپن های الکترونیکی ارائه می دهیم که می تواند از قابلیت تفویض هزینه های خود را به دیگر کاربران و یا دستگاه های خود را مانند لپ تاپ، PDA، تلفن همراه و نقاط دسترسی به خدمات این چنینی را تسهیل کند. این طرح وعده تبدیل به یک توانمندساز برای خدمات مختلف مبتنی بر اینترنت است که شامل پرداخت واحد معقول است. این امر به کاربران انعطاف پذیری برای مدیریت قابلیت پرداخت هزینه در کل نقاط مختلف در دسترس برای خدمات خاص بدون اخذ مجوز برای هر نقطه دسترسی از یک بانک تسهیلاتی ارائه می دهد. این انعطاف پذیری که در طرح های پرداخت میکرو وجود دارد، برای دسترسی در همه جای خدمات الکترونیکی و دیگر برنامه های کاربردی مبتنی بر اینترنت ضروری است. تسهیلات واگذاری در رابطه با اثبات و یا تایید مجوز واگذاری و امنیت ارائه شده برای پرداخت کلیت ناچیزی را مطرح می سازد. پرداخت تسهیلات مسئولیت مخارج کل را از بین می برد. مقاله طراحی پروتکلی را مطرح می کند و تجزیه و تحلیل عملکرد سیستمی را فرام می کند.

کوپن های الکترونیکی بر اساس PayWord ، زنجیره مخلوط یک طرفه تک پیگردی برای پرداخت واحد معقولانه، TESLAبرای امنیت پرداخت و SPKI / SDSI به عنوان چارچوب PKI زمینه ای برای ویژگی نمایندگی منحصر به فرد آن است. نتایج به دست آمده از اجرای کوپن الکترونیکی کاملا قابل قبول و در نزدیک به زمان واقعی پاسخ را نشان می دهد. طرح ما از زنجیره هش یک طرفه چند پیگردی برای پرداخت واحد معقول استفاده می کند. علاوه بر

این، انتقال بخش زنجیره های پرداخت به دیگران را مجاز می سازد. چون قابلیت هزینه های این کاربر می توان از نقاط دسترسی در سرویس های مختلف برای دسترسی خدمات مشترک، به صورت همزمان مورد استفاده قرار گیرد.

کلید واژه ها. میکرو پرداخت، امنیت، نمایندگی، تابع هش یک طرفه، PayWord، TESLA، SPKI / SDSI

1. مقدمه

تجارت الکترونیک طیف گسترده ای از معاملات متفاوت، از معاملات کلان تا خرد را پوشش می دهد. در معاملات کلان ، در حالی که ارزش هر معامله بسیار بالا است، چالش در ارائه درجه بالاتری از احراز هویت، امنیت پرداخت، و غیر انکار بودن معاملات نهفته است. در معاملات خرد، در حالی که نیاز به تهیه کردن حجم معاملات بزرگ با ارزش مالی ذاتاً پایین وجود دارد، چالش نگه داشتن هزینه هر معامله برای حداقلی به طور متوسط است.

معاملات خرد شامل خدمات اینترنتی فعال مانند جریان های چند رسانه ای، دسترسی به قدرت محاسباتی شبکه، نرم افزار های قابل بارگذاری، نرم افزار پلاگین / رابط های برنامه کاربردی، تماسهایVoIP ، کتابخانه الکترونیکی، اخبار و کالاهای غیر ملموس مختلفی است که می توان از طریق اینترنت تحویل داد (برای مثال از میان آنها، اخبار رایگان است). مشترکین به چنین خدماتی از طریق نقاط مختلف سرویس ها دسترسی دارند و همواره مایل به فاش کردن مجموعه ای از نقاط دسترسی نیستند. ارائه دهندگان خدمات با ابزارهای موجود موفق به شارژ خدمات خود نمی شوند. از این رو، آنها خدماتی را به کاربران بصورت رایگان ارائه می کنند و یا مکانیسم های دیگر نسبت به یک سیستم پرداخت میکرو بکار می برند. ارائه دهندگان خدمات هزینه تبلیغ و یا اشتراک انبوه را با استفاده از احراز هویت بر اساس آدرس IP میزبان و / یا کوکی های مرورگر و غیره بازیابی می کنند. مکانیزم میکرو پرداخت مستقیم مکمل عالی و ابزاری کوچک برای فروشندگان هستند. علاوه بر این، انگیزه های پراکنده ای برای کاربران پراکنده فراهم می کند که یک اشتراک تمام وقت برای برخی از خدمات پرداخت نمی خواهند. بر خلاف پرداخت کلان، ارزش پولی هر میکرو پرداخت بسیار کم است و خطر درگیر قابل قبول است. در حالی که پرداخت های کلان بر

امنیت، غیر قابل انکار بودن و ظرفیت جایگزینی معامله، سیستم های میکرو پرداخت هدف کارآمد، کم هزینه بودن و راه اندازی امن تاکید دارند. کاربران آماده پذیرش سیستم های میکرو پرداخت با عوامل خطر منطقی مرتبط با آن هستند. در این مقاله، ما نگران طراحی و ساخت یک سیستم معامله میکرو هستیم که کاربران را به طور مستقیم مطابق با الزاماتی از قبیل امنیت، کم هزینه بودن هر معامله و امکانات نمایندگی حمایت می کند.

چندین روش پرداخت الکترونیکی ارائه شده در متون و مقالات گذشته وجود دارد: PayWord و MicroMint ، (ریوست و شامیر[1]، 1996)؛MilliCent ، (گلاسمن[2] و همکاران، 1995)، MiniPay، (هرزبرگ و یوچای[3] 1997)، NetBill، (پروژه تجارت الکترونیک NetBill، 1995)؛ Net-Card، (اندرسون[4] و همکاران، 1996 NetCash (مدوینسکی و نیومن[5]، 1993)؛ Agora، (گبر و سیلبرشاز[6] 1996)، MPTP، (هالام- بیکر[7]، 1995)؛iKP ، (بلار[8] و همکاران، 2000) مبتنی بر میکرو پرداخت، و غیره. این طرح ها را می توان بطور گسترده در دسته ها بر خط و خارج از خط متمایز کرد، به اساس نوع اعتبار سنجی پرداخت که استفاده شده است. در روش خارج از خط، خطری که به طور طبیعی مطرح می شود اعتبار سنجی فوری انجام نشده است.NetBill ، NetCash، MiniPay، MilliCentاز برخط و یا نوع نیمه آنلاین اعتبار پرداخت استفاده می کنند که به طور کلی پر هزینه است.

NetBillبرای خرید کالای اطلاعاتی از طریق اینترنت با تاکید بر امنیت و ظرفیت جابجایی معاملات طراحی شده است. سرور مورد اعتماد مرکزی در هر معامله ای در گیر است. اقتصاد خرد و مقیاس پذیری به دلیل ترافیک شبکه گسترده ای مورد نیاز در معامله و تعامل با سرور NetBill مرکزی پرسش بر انگیز است. NetCash طرح بر خط دیگری است که یک چارچوب برای سیستم پرداخت زمان واقعی امن و تا حدی ناشناس ارائه می دهد. ساختار اصلی NetCash شامل سرور ارز توزیع مستقل، با یک لینک بین جریان الکترونیکی ناشناس و خدمات غیر ناشناس است. سرور جریان نقد ارائه دهنده خدمات به مشتریان است، مانند تشخیص هزینه دو برابر، تبادل سکه برای موارد

[1] Rivest & Shamir
[2] Glassman
[3] Herzberg & Yochai
[4] Anderson
[5] Medvinsky & Neuman
[6] Gabber & Silberschatz
[7] Hallam-baker
[8] Bellare

غیر قابل پیگیری، خرید سکه با چک و بازخرید سکه برای چک. ویژگی هایMiniPay با هزینه کم، تاخیر قابل اغماض، رابط کاربری طبیعی، طراحی مقیاس پذیر، پشتیبانی از ارزهای مختلف و امنیت بالا از جمله عدم انکار، پیشگیری از ولخرجی و محافظت در برابر انکار سرویس. معماری MiniPay شامل چهار تا شش بخش در راه اندازی آن است. کلیدهای عمومی برای تأیید هویت بخش ها آن استفاده می شود و مبتنی بر روابط همکار با همکار است که در آن کلید های عمومی با استفاده از روابط موجود بین همسالان تبادل و تصدیق می شوند. MilliCent سیستم تجاری ریز دیجیتال اختصاصی است. این سیستم خاص تجاری ضامن، به نام رسید موقت، یک شکل از نشانه ای است که تنها با یک تاجر خاص برای یک دوره زمانی محدود معتبر است. معاملات MilliCent ناشناس نیستند و عمدتا خارج از خط هستند. PayWord خارج از خط، بسیار کارآمد، طرح میکرو پرداخت مبتنی بر اعتبار است. این یک طرح سه جانبه است که شامل یک بانک، فروشنده و کاربر است. بانک تسهیلات اعتباری به کاربران می دهد و این اطمینان را به فروشندگان می دهد تا با کاربران ثبت شده پرداخت انجام شود. طرح های میکرو پرداخت دیگری عبارتند از؛ IKP میکرو ، NetCard، MPTP تا حد زیادی بر اساس PayWord پیشنهادی است. دیگر طرح های میکرو پرداخت از بحث ما خارج هستند (مانندMONDEX ، CAFE)که بر روی سخت افزار های خاص مانند کارت هوشمند تکیه می کنند.

طرح میکرو پرداخت های بالا با هدف پرداخت امن و / یا کارآمد برای کالاهای غیر ملموس در پرداخت/ پرداخت به ازای هر کلیک/ پرداخت به عنوان اساس طراحی شده اند. طرح ها هم به شدت بر برنامه های کاربردی کلید نامتقارن تکیه دارند و یا برای این بانک در شرایط سنگین تر ضرب سکه و تایید بر روی خط بودن هستند. علاوه بر این، بسیاری از این طرح ها با توجه به طراحی متمرکز مقیاس پذیر نیستند. در حال حاضر تقاضا برنامه های کاربردی روز بسیار بیشتر از آنچه است که در این طرح فراهم می شود. امروزه، کاربران از ربات نرم افزار برای خرید بابت موارد بالا استفاده می کنند. کاربران انتظار دارند خدمات مشترک آنها از نقاط دسترسی مختلف در دسترس باشند (به طور همزمان پذیرفتنی). ما در حال حاضر دو نمونه از سناریوهای میکرو پرداخت را ارائه دادیم که به خوبی با طرح های موجود مورد بحث بطور راضی کننده ای راه اندازی نمی شوند.

سناریوی 1 : کنسرسیومی از موسسات دانشگاهی خود را برای انتشار الکترونیکی خدمات مختلف موظف ساختند. مدیریت کنسرسیوم حاضر برای فریب دیگر نهادهای غیر عضو برای اشتراک موقت و یا به صورت دائم است. بدین منظور، برای مدیر کنسرسیوم لازم است تا به ویژگی هایی مانند نمایندگی جزئی از قدرت به دیگر نهاد و یا فردی را دااشته باشد در حالی که بهره وری و امنیت سیستم را حفظ می کند.

سناریو 2: یک کاربر یک نرم افزار چندگانه و موضوعاتی با استفاده از رابط های مختلف برنامه کاربردی خارجی / پلاگین (رابط برنامه نرم افزار)، بر اساس اشتراک کاربر دارد. ابزار پرداخت یکپارچه مانع اجرای موضوعات بطور موازی خواهند شد.

یکی از دلایل اصلی آن این است که پرداخت میکرو موجود اجازه نمی دهد تا کاربر اختیارات خود را کاملا و یا جزئی به اشخاص ثالث واگذار کند. بسیاری از این حالات وجود دارد که در آن رشد تجارت الکترونیک به دلیل در دسترس نبودن کارآمد دچار رکود می شود و طرح میکرو پرداخت امن که تسهیلات واگذاری به غیر را برای کاربران به منظور قابلیت پرداخت هزینه های خود فراهم می کند. در این مقاله، ما باید طراحی و پیاده سازی آدرس یک سیستم میکرو پرداخت را با رسیدن به شرایط زیر بیان کنیم: امنیت، کم هزینه بودن در هر معامله، بازده و ارائه قابلیت واگذاری مخارج. طراحی ما از ویژگی های PayWord (ریورس و شامیر 1996)، TESLA (Perrig (پرینگ و همکاران، 2002؛ پرینگ و همکاران، 2001)، و SPKI / SDSI (کلارک و همکاران، 2001) استفاده کردند. به عبارت دیگر، ما چارچوب PayWord را گسترش می کنیم (ریورس و شامیر، 1996) که مسئولیت رسیدگی به قابلیت هزینه کرد کاربران را از طریق SPKI / SDSI اداره می کند و امنیت از طریقTESLA را اداره می کند.

طرح ما یک طرح مبتنی بر اعتبار و خارج از خط است. همچنین، سکه/ paywords (واحد ابتدایی پرداخت) فروشنده خاص و نه کاربر خاص هستند، بر خلاف PayWord. برای حفظ کوین تنها فروشنده خاص و نه کاربر خاص به عنوان کوین قصد تغییر دست ها را دارد. یکی از نیازها برای تامین امنیت کوین نسبت به یک تهدید این است که می توان آنها را در حمل و نقل و در زمان واقعی به فروشنده ارائه کرد. ما از پروتکل TESLA اصلاح شده برای این هدف استفاده می کنیم. این نه تنها یک روش کارآمد برای احراز هویت منبع فراهم می کند بلکه امنیت

مقرون به صرفه ای را تعیین می کند و از حملات فرد میانجی و انکار خدمات جلوگیری می کند. ما از / SPKI (SDSIکلارک و همکاران، 2001؛ الیسون، 2002) به عنوان یک چارچوب زیرساخت کلید عمومی رضایت بخشی نیازهای (به خصوص واگذاری مجوز) از طرفین در راه اندازی خود استفاده می کنیم. اجرای ما کارآمد ، امن و قادر به رسیدگی نمونه سناریوهای میکرو پرداخت بالا با سهولت توصیف مدیریت، توانایی و تعمیر و نگهداری است.

بقیه مقاله به شرح زیر است: در بخش بعدی، یک نمای کلی از پروتکل های را بطور جداگانه ارائه می دهیم به عنوان مثال، PayWord، TESLA، و SPKI / SDSI در بخش 3 و 4 پیشنهاد شده است، پسگیری می شود. بخش 7 تجزیه و تحلیل دقیق از پروتکل های ما از نظر جنبه امنیتی، عوامل خطر و عملکرد ارائه می دهند. این مقاله با یک بحث در بخش 8 به نتیجه گیری می رسد.

2. بررسی اجمالی

در این بخش، خلاصه ای از طرح ها مانندPayWord ، TESLAوSPKI / SDSI را ارائه می دهیم که طرح ما بر آنها استوار است.

PayWord 2.1

این یک طرح خارج از خط میکرو پرداخت مبتنی بر اعتبار است که از زنجیره payword مقادیر استفاده می کند (هش یک طرفه ارائه دهنده واحد های پولی اولیه). محور طرح در به حداقل رساندن تعداد کلید عمومی عملیات مورد نیاز در هر پرداخت و در نتیجه دستیابی به بهره وری استثنایی نهفته است (ریوست و شامیر، 1996). این یک مکانیزم سه جانبه است که شامل یک کاربر U که باعث پرداخت می شود، یک فروشنده V که پرداخت را دریافت می کند و یک کارگزارB (واسطه مالی) که حساب را برای طرفین مرتبط نگه می دارد. کارگزار طرف قابل اعتماد است و تسهیلات اعتباری را برای معامله با فروشندگان به کاربران می دهد. پس از رسیدن به یک قرارداد

اعتباری رسمی بین B وU ، B به V وعده بازخریدpayword های صرف شده توسط U در فواصل منظم از زمان را می دهد.

قبل از هر گونه پرداخت به فروشنده، کاربر یک زنجیره payword تولید می کند که کاربر خاص و فروشنده خاص هستند. کاربر زنجیرهpayword در جهت معکوس با چیدن آخرین payword wn به طور تصادفی تولید می کند و سپس هرpayword $wi = h(wi+1)$ را برای$i = n - 1, n - 2, \ldots, 0,$ محاسبه می کند که در آن hیک تابع هش قوی و w0 ریشه آن زنجیره payword نامیده می شوند (تعهد). این کاربر باید چنین زنجیره paywordرا با فروشنده قبل با استفاده از زنجیره ای به عنوان یک ابزار پرداخت ثبت کند. کاربر ارزش تعهد زنجیره payword را (W0) همراه با

مجوز (گواهی PayWord) تصدیق می کند که کاربر برای تولید چنین ابزار پرداختی توانمند می سازد.

در تایید موفقیت آمیز طرف فروشنده، کاربر می تواند زنجیره payword را برای ثبت فعالیت خرید واحد عاقلانه استفاده کند. در حالی که پرداخت واحد عاقلانه با استفاده ازpayword های تولیدی است، پرداخت i م (برای $i = 1, 2, \ldots, n$) از u به v متشکل از جفت (wi , i) است که V می تواند استفاده از Wi-1 را با کمک یک طرفه تابع هش، h بررسی کند. هر یک از این پرداخت ها به محاسبات توسط کاربر نیازی ندارند، و تنها یک عملیات رشته هش منفرد توسط فروشنده برای تأیید لازم است. فروشنده می توانید پرداخت را با محاسبه هش payword تایید کند و برای تعهد payword مربوطه ریشه برای مناقصهpayword اول برابر است.

برای بازپرداخت paywordهای انباشته شده، فواصل منظم فروشنده با بانک های تسهیل کننده و آخرین گزارش متعامل است (بالاترین نمایه) پرداخت (wl , l) از هر کاربر ثبت نام شده پس از آخرین گزارش دریافت می شود، همراه با یک تعهد مربوطه. در تأیید این مسئله، بانک کاربر حساب L را شارژ می کند و سپرده آن را به حساب فروشنده واریز می کند. توجه داشته باشید که بنابراین برای بانک، نگهداری پایگاه داده های بزرگ غیر ضروری است.

رابطه بانک، کاربر، فروشنده: بگذاریدکلید عمومی بانکB ، کاربرانU و فروشنده V را با KB ، KU، KV کنیم و کلید های خصوصی آنها را با $K_B^{-1}, K_U^{-1}, K_V^{-1}$– مشخص کنیم. تعامل بین سه طرف به شرح زیر است:

B ↔ U:کاربر U با جزئیات آدرس دریافتی به B نزدیک می شود (AU) و برخی از اطلاعات اضافی را (IU) برای بدست آوردن گواهی PayWord دارد که در آن E تاریخ انقضاء گواهی است CU= $\{B, U, A_U, K_U, E, I_U\}_{K_B^{-1}}$ یعنی تاریخ تا آنجا که خدمات برای مشترک می توان در دسترس باشد.

U ↔ V:، U زنجیره w1, . . . , wn ریشه w0 را محاسبه می کند و سپس تعهدی برای زنجیره payword ایجاد می کند $M = \{V, C_U, w_0, D, I_M\}_{K_U^{-1}}$ که در آن D تاریخ جاری و IM برخی از اطلاعات اضافی مورد نظر هستند. payment $P = (w_i, i)$ از U به V از یک payword و شاخص آن تشکیل شده است.

V ↔ B:در فواصل زمانی منظم، فروشندهV paywordهای انباشته را با B بانک بازپرداخت می کند. در هر یک از این درخواست های بازپرداخت، Vهر مشترکpayword را با زنجیره CU مربوطه دریافت شده از مشترک U تولید کرد (اگر در حال حاضر انجام نمی شود پس در بازپرداخت قبلی در خواست می شود) و پرداخت آخرین (L ، P WL) = از هر کاربر دریافت کرده است. در تایید تعهدات امضا دریافت، B کاری را محاسبه می کند، یعنی واحد L را از حساب U کسر و آن را به حساب V اعتبار می دهد. این توافق پرداخت خارج از سیستمPayWord قرار می گیرد. PayWord برای توالی پرداخت خرد بهینه سازی شده است، اما امن و به اندازه کافی انعطاف پذیر به حمایت از پرداخت متغیر با ارزش بزرگتر مناسب است، بسته به اینکه بانک و فروشنده حاضر هستند چقدر طر کنند. این طرح زنجیره کاربر خاص، فروشنده خاص payword است و از این رو، تضا و و اختلاف هیچ نفعی در سرقت آن ندارد در حالی که تبادل شده یا دوبرابر هزینه می شود. در نتیجه، PayWordنمی تواند ناشناس ماندن به معاملات را فراهم کند. زمانی که کاربر به زنجیره payword های متعدد برای مثال استفاده از آن برای دسترسی به خدمات مشترک از طریق دستگاه های متعدد نیاز دارد (کامپیوتر،لپ تاپ، PDA، تلفن همراه، و غیره،) به طور جداگانه آن را درخواست و برای هر دستگاه ثبت نام کرده اند که باعث می شود سیستم ناکارآمد باشد زیرا تعامل اولیه با بانک هزینه را افزایش می دهد.

TESLA 2.2

TESLA(جریان کارآمد از دست دادن تحمل تأیید هویت بهنگام) یک پروتکل احراز هویت با ارتباطات کم و سربار محاسباتی منبع کارآمد است (پریج و همکاران، 2002، 2001). توابع رمزنگاری متقارن خالص (MAC -پیام تایید کد است (اشنایر، 1996) توابع) و رسیدن به خواص نامتقارن از طریق هماهنگی آزادانه و افشای کلیدی تاخیر. با استفاده از این اختلاف زمان بین فرستنده و گیرنده برای دستیابی به عدم تقارن استفاده می شود.

پروتکلTESLA در زیر خلاصه شده است: فرستنده پیام MAC را به هر خروجی محاسبه بسته با استفاده از یک کلید k محاسبه می کند که فقط برای فرستنده مشخص است. گیرنده در بافر مانند بسته پیش می رود و آنها را اعتبار می بخشد و به زودی به عنوان فرستنده k را در انتقال بعدی آن افشا می کند. در فواصل به طور منظم، تغییرات فرستنده کلید K برای محاسبات MAC استفاده می شود. این مقادیر k از تابع هش یک راه مقاوم در برابر برخورد در چنین راهی به دست آمده اند که ارزش بعدی می تواند در جهت معکوس تصدیق شده است. با توجه به چنین استفاده از مقادیر زنجیره هش یک راه برای محاسبه MAC بیش از بسته های خروجی، گیرنده می تواند از حملات انکار سرویس و پخش شده به سادگی به دنبال در بسته زمان مهر و موم آن را خنثی کند، کلید توسط فرستنده در آن زمان فاش می سازد، و می تواند از بسته مشکوک چشم پوشی کند (پریج و همکاران، 2002). پروتکل اصلی در زیر خلاصه شده است.

قبل از شروع انتقال واقعی، گیرنده و فرستنده آزادانه وقت خود همگام سازی می کنند. در حین این فرایند، گیرنده علاقه مند به محاسبه حداکثر زمان خطای همزمان سازی هستند. گیرنده زمان محلی آن TR را ثبت می کند و به عنوان یک هماهنگ سازی زمان درخواست به فرستنده عنوان می شود. فرستنده با یک پیام امضای دیجیتالی را پاسخ می دهد

$\{t_S, Nonce\}_{K_S^{-1}}$ ، جایی که TS و K-1S به ترتیب زمان محلی فرستنده و کلید خصوصی هستند. تأیید صحت موفقیت آمیز فعلا توسط فرستنده، گیرنده محاسبه بالا در زمان کنونی فرستنده به عنوان TR ≤ TS محدود + TR -

TS، بازمی گردد که در آن TR زمان کنونی گیرنده است. پس از این فرآیند، زمان واقعی خطای همزمان سازی δ، است که تفاوت بین فرستنده و گیرنده محاسبه می شود.

حالا فرستنده زمان را به فواصل مدت زمان یکنواخت و اختصاص مقادیر یک طرفه زنجیره ای هش [رجوع به ضمیمهA] پی در پی به هر زمان فاصله برای تولید MACها در طول بسته داده فواصل زمانی مربوطه تقسیم می کند. فرستنده تعریف زمان d را برای مقادیر زنجیره ای یک طرفه تعریف می کند و آن را وسیله انتقال به گیرنده می داند. در دریافت بسته های اضافه شده به MACها بیش از آن که توسط فرستنده محاسبه شود، گیرنده موارد زیر را انجام م دهد: از آنجا که برنامه برای افشای کلید شناخته شده و ساعت ها آزادانه هماهنگ، گیرنده بررسی می کند که کلید مورد استفاده برای محاسبه MAC هنوز مخفی است که فرستنده نمی تواند فاصله زمانی را افشای کند. اگر MAC کلیدی است که هنوز هم پنهان است، سپس گیرنده بسته را بافر می کند. فرستنده تازی ترین زنجیره ارزش یک طرفه را ارسال می کند که آن را می توانید با هر بسته افشا کرد. چک گیرنده که کلید فاش درست به موجب اموال زنجیره های یک طرفه است، و سپس صحت MAC از بافر بسته های اطلاعاتی بررسی می شود که در فاصله زمانی کلیدی ارسال فاش می شود. گیرنده بسته تنها در صورتی MACارسال شده توسط فرستنده را می پذیرد که منطبق با ارزش محلی محاسبه شده باشد.

TESLAسربار محاسبه کم برای نسل و تایید اطلاعات احراز هویت و سربار ارتباطی پایین دارد. بافر محدود برای فرستنده و گیرنده مورد نیاز است، از این رو احراز هویت به موقع برای هر بسته صورت می گیرد. افشای کلید رمزنگاری و دستیابی به اموال محرمانه بودن اطلاعات و احراز هویت کارآمد استفاده می شود که به طور کلی توسط که توسط روش رمزنگاری TESLA نامتقارن ارائه می شود. TESLA نمی تواند نیاز مهم برای غیر قابل انکار معاملات مالی را فراهم کند. امنیت TESLA نیز متکی به این واقعیت است که کلید زودتر پس از یک دوره کار در زمان کنار گذاشته شود.

SPKI / SDSI 2.3

SPKIو SDSI دو تلاش جداگانه آغاز شده برای غلبه بر پیچیدگی، حفظ حریم خصوصی و اعتماد مرتبط با مسائل مواجه شده سنتی زیرساختهای کلید عمومی بسیار متمرکز هستند(الیسون، 2002). بعد این طرح با هم ادغام شدند و نام SPKI یا SPKI / SDSI داشتند. این طرح را برای بیان ساختمان های داده ای استفاده می کنند که کاربر شفافیت مورد نیاز را فراهم می کند و ASN.1 جلوگیری می کند (چکیده نحو نشانه گذاری (ASN.1) . برخلاف طرح نامگذاری جهانی بکار رفته در سلسله مراتب زیرساختهای کلید عمومی، آن را با فضاهای نام محلی در ارتباط با هر کلید عمومی استفاده می کنند. به طوری که هر مدیر می تواند موضوع / تعریف کلید اتصالات محلی را داشته باشد. اصول می تواند تعاریف جدید اتصال کلید اصلی دیگر و یا بر اساس نام اعتماد او حاضر برای قرار دادن، مانند PGPوب سایت از اعتماد به (PGP) ایجاد کند. این طرح به پیروی از روش پایین به بالا، بر خلاف رویکرد بالا به پایین X.509 است (فورد و باوم، 2002)، و دارای مقررات به جای ریشه جهانی مقامات صدور گواهینامهاست .(CAS)همچنین، جدایی مجوز نامگذاری مانع غیر ضروری مجوز کاربر است که در حالی که اجرای یک مقام خاص صورت می گیرد، مورد نیاز است. این ممکن نیست که گواهی بازی نامگذاری و اتصالات مجوز های متعدد با هم باشند. علاوه بر این، گواهینامه حدود و گواهی گروه اجازه می دهد یک مدیر امنیتی برای کنترل سیاست به روش ها دسترسی داشته باشد [رجوع به پیوست اول].

طرح کاربردی مختصری با استفاده از سناریوی زیر: اجازه دهید اصل K به عنوان یک ارائه دهنده منابع نشان داده توسط منابع و مشخص ACL برای دسترسی K در نظر بگیریم . اصولK1 ، K2، K3به عنوان خرده فروشان برای عمل خود سرویس در نظر میگیریم. یک اصل Ks به مشترک برای منابع خدمات از طریق یکی از خرده فروشان صورت می گیرد. بیایید ببینیم چگونه مشترک KS می آید تا اجازه دسترسی به منابع و چگونه صاحب منابع K را اثبات کندو از گواهینامه های گروه و نام طولانی به نحو احسن و مدیریت دسترسی به منابع استفاده کند. طراحی برای چنین سیاستی است در زیر با استفاده از نمادهایSPKI داده شده است

$K \quad my\_retailers \longrightarrow \{K_1, K_2, K_3\}$ _ گروه "خرده فروشان i" توسط مدیرK

تعریف شده است و می تواند برخی سیاست مشترک در تمام سه مدیر موضوع تنها با روایت سیاست بیش از تعریف نام خرده فروشان را اعمال کند.

$K \ my\_customers \longrightarrow \{K_A, K_B, K_3 \ customers\}$ یکی دیگر از تعریف گروه های محلی

توسط K اصلی، که در آن شامل یکی دیگر از گروه به عنوان مثال، مشتریان K3 جدا از KA وKB است که در آن مشتریان به KP}→ - K3 ، Kq، KR، KS جدا می شوند.

- K اصلی گروه های آن تحکیم و ایجاد یک تعریف جدید، Kگروه های → myretailers K i -}، مشتریان KMY} و سبب می شود با ساخت یک تعریف مجوز اعضای خود را به دسترسی به منابع فراهم کند، K → KRESOURCE- گروه های i، که در آن نشان می دهد واگذاری بیشتر از اصول موضوع مجاز است.

دنباله ای از پیام ها، بین کنترل منابع Kو درخواست KS در زیر آورده شده است:

- KS درخواست دسترسی برای منابع می فرستد. کنترل کننده Kخواستار Ks برای برآوردن سیاست کنترل دسترسی

اجرا شده توسط KRESOURCE قانون K → - گروه های i است.

-KSدرخواست برای تعریف K گروه های i است.

K -تعاریف گروه های آن گروه های i، خرده فروشان i، i و مشتریان را فراهم می کند. در K تعریف مشتریان i، KS می یابد لینک مجوز از دست رفته باشند.

- اثبات کشف زنجیره گواهی Ks به صورت زیر است:

$K_{\text{RESOURCE}} \longrightarrow K \ my\_groups \ \square$
$K_{\text{RESOURCE}} \longrightarrow K \ my\_customers \ \square$; since
$\underline{K \ my\_groups} \longrightarrow$
$\{K \ my\_retailers, \underline{K \ my\_customers}\} K_{\text{RESOURCE}} \longrightarrow$
$K_3 \ customers \ \square$; since

$$\underline{K\ my\_customers} \longrightarrow \{K_A, K_B, \underline{K_3\ customers}\}$$
and
$$\underline{K_3\ customers} \longrightarrow \{K_p, K_q, K_r, \underline{K_s}\}$$
$$\therefore\ K_{\text{RESOURCE}} \longrightarrow K_s\ \square$$

-در این روش، KSثابت می کند اعتبار دسترسی خود را بیش از منابع است و قادر به تفویض قدرت بیشتر است. اما در دسترسی تعریف کنترل منابع Ksبه واگذاری محدودتر منتهی خواهد شد.

چنین زیرساخت های امنیتی توزیع در طراحی و مدیریت امنیتی مدل های پیچیده را تسهیل می کنند. توانایی خود را به کاربران اجازه می دهد به صورت محلی نام خود را تعریف و مجوز اتصال کمک می کند تا در دستیابی به مدل اعتماد طبیعی، به شدت وابسته به CAهای ریشه جهانی نیست، برسند. طرح های میکرو موجود به نظر می رسد به این معنا تکیه بر یک مرجع صدور گواهینامه متمرکز زیرساخت است که مشکلات مقیاس پذیری و روابط اعتماد سلسله مراتبی رو به رو است.

3. کوپن های الکترونیکی: عمومی طرح

در این مقاله، نگرانی اصلی ما طراحی و پیاده سازی یک سیستم میکرو پرداخت با ویژگی های زیر است:

1. سیستم حداقل باید در تاریخ همتراز با سیستwordpay، از نظر بهره وری و امنیت باشد،

2. باید کاربران اجازه داد تا قابلیت واگذاری هزینه های خود را داشته باشند.

قلب ساخت و ساز ما پروتکل یک PayWord فروشنده خاص فعال منبعTESLA همراه با احراز هویت و محرمانه بودن مکانیزم برای paywords است. هر چند اجرای شبیه به PayWord به جای تولید یک زنجیره payword و صرف آن را بیش از مدت زمان، کاربر زنجیر payword های متعدد تولید و از یک رویکرد مدیریت آماری استفاده می کند (که از کاربران متفاوت به کاربران بر اساس الگوهای هزینه های خود را) برای هزینه آن را بیش از غیر متناقض فواصل زمانیSPKI / SDSI است.چارچوب نه تنها خواص مانند غیر قابل انکار کردن را فراهم می کند بلکه از ویژگی های مهم واگذاری است. پروتکل ما یک پروتکل خارج از خط است که یکی از ویژگی های بسیار مهم از هر گونه طرح میکرو پرداخت است.

در ادامه، ما باید پروتکل اساسی را بدون از ویژگی های واگذاری توصیف کنیم. ویژگی های هیئت پروتکل به طور جداگانه در بخش 4توضیح داده شد. معاملات پروتکل پایه در میان سه طرفین در شکل 1توصیف شد و جزئیات هر مرحله معامله شرح داده شد:

- **یک درخواست برای گواهی PayWord** با استفاده از استاندارد پروتکل پرداخت کاربر یک جلسه با بانک ایجاد و یک حالت مناسب برای پرداخت را انتخاب می کند. اطلاعات کارت اعتباریCCU ، کلید عمومی و کاربر سایر اطلاعات KU ازIU بانک با استفاده از یک پروتکل پرداخت استاندارد ارسال می شود حمایت می کند. جزئیات مورد نیاز این کاربر توسط بانک برای معامله تناسب در اینجا به کار می رود.

- **صدور گواهی بر اساس PayWord** اعتبار کاربر، بانک و یا مسائل مربوط به یک PayWord CUگواهی به را رد می کند. کاربران را قادر می سازد این کاربر زنجیر payword به صورت محلی تولید کندکه تضمین بازپرداخت بانک برای paywordsصرف شده توسط کاربر با یک فروشنده وجود دارد. پاسخ امضا شامل اطلاعات مربوط به اعتماد سازی برای فروشنده، به عنوان مثال، PayWordبانک صادر کنندهB، نام کاربر، کلید عمومی، گواهی زمان انقضایE و سایر اطلاعات IUاست (حد زنجیرهpayword). س از دریافت گواهیPayWord ، کاربران paywords"با انتخاب یک شماره تصادفی وR از یک استاندارد مقاوم در برابر، برخورد، رمز نویسی امن یک طرفه تابع هش استفاده می کنند، بیش از آن پی در پی بیش از یک طیف توسط بانک در گواهیPayWord مشخص شده است. به عنوان مثال، (R) = WN، (WN) = WN-1برای n + 1 بار و ساعتW0 = (W1) ؛ W0 به نام ریشه یا دوزهای همراه با تعهد از زنجیرهpayword ، که به عنوان یک payword استفاده نمی شود (رجوع به شکل 2).

- **ثبت نام C با فروشنده.** فرایندی که در آن کاربران یک پیام دیجیتالی امضا شده حاوی نام فروشندهV ، اعتبار PayWordآنCU، زنجیره ای payword ریشه / و اطلاعات اختیاری i را می فرستد (طول رشته W به عنوان کلید رمزنگاری payword مثال استفاده 56-بیتی یا 64 بیتی). فروشنده امضای کاربر و صحت CU گواهی PayWordمحصور در M فروشنده را نیز برای وجود ارزش دوزهای همراه توسط کاربر تایید می کند.

- **درخواست هماهنگ سازی زمان**. قبل از دادن یک سیگنال متهور کاربر ، فروشنده زمان خود را با کاربر هماهنگ می کند به طوری که می توان آن را علف به بسته های جعلی از بافر و تصدیق منبع بسته باقی مانده دانست. این اولین گام در TESLA آغاز شده فروشنده برای ثبت زمان محلی TRو رمز شده با کلید خصوصی به عنوان یک درخواست هماهنگ سازی زمان امن است.

$$\begin{array}{lllll}
\mathrm{U} & \longrightarrow & \langle CC, K_U, I_U \rangle_{SSL} & \longrightarrow \mathrm{B} & \ldots \text{ⓐ Macro-Payment for PayWord Certificate} \\
\mathrm{U} & \longleftarrow & C_U = \{B, U, K_U, E, I_U\}_{K_B^{-1}} & \longleftarrow \mathrm{B} & \ldots \text{ⓑ User receives the PayWord Certificate}
\end{array}$$

$$\begin{array}{lllll}
\mathrm{U} & \longrightarrow & M = \{V, C_U, w_0, I\}_{K_U^{-1}} & \longrightarrow \mathrm{V} & \ldots \text{ⓒ Registration of PayWord chain with Vendor} \\
\mathrm{U} & \longleftarrow & \langle Nonce \rangle_{K_V^{-1}} & \longleftarrow \mathrm{V} & \ldots \text{ⓓ Time Synchronization Request} \\
\mathrm{U} & \longrightarrow & \langle t_U, Nonce, T_{int}, d \rangle_{K_U^{-1}} & \longrightarrow \mathrm{V} & \ldots \text{ⓔ Response and Agreement} \\
\mathrm{U} & \longrightarrow & \{\langle w_i \rangle_{w_i}, MAC(w_i), w_{i-d}\} & \longrightarrow \mathrm{V} & \ldots \text{ⓕ Micro-Payments} \\
\mathrm{U} & \longrightarrow & \{\langle w_{i+1} \rangle_{w_{i+1}}, MAC(w_{i+1}), w_{i+1-d}\} & \longrightarrow \mathrm{V} & \ldots \text{ⓖ} \quad \downarrow \\
\mathrm{U} & \longrightarrow & \{\langle w_{i+2} \rangle_{w_{i+2}}, MAC(w_{i+2}), w_{i+2-d}\} & \longrightarrow \mathrm{V} & \ldots \text{ⓗ} \quad \downarrow
\end{array}$$

شکل. 1. مراحل پروتکل کوپن های الکترونیکی.

$$\begin{array}{l}
\longmapsto \ \textit{generation sequence} \ \longmapsto \qquad\qquad\qquad \longmapsto \\
\boxed{w_n, w_{n-1}, w_{n-2}, \ \ldots \ \ldots \ w_{200}, w_{199}, w_{198} \ \ldots \ w_2, w_1, w_0} \\
\longleftarrow \qquad\qquad \longleftarrow \textit{spending sequence} \longleftarrow
\end{array}$$

شکل. 2. تولید زنجیرهPayWord

(e) **پاسخ**. در پاسخ به هماهنگ سازی زمان درخواست از فروشنده، کاربر رمزگذاری پیام متشکل از وقت محلی آن tu را می فرستد، زمان فاصله Tint که یک کلید برای استفاده رمزگذاری خواهد بود، و عدد صحیح d که بر فواصل زمانی دلالت می کند که کلید مخفی باقی خواهد ماند. پس از موفقیت در بررسی ارزش فعلی بازگردانده شده توسطU ، فروشنده حداکثر هماهنگ سازی زمان خطا Δ را محاسبه می کند. همانطور که در بخش 2.2 توضیح داده شد.

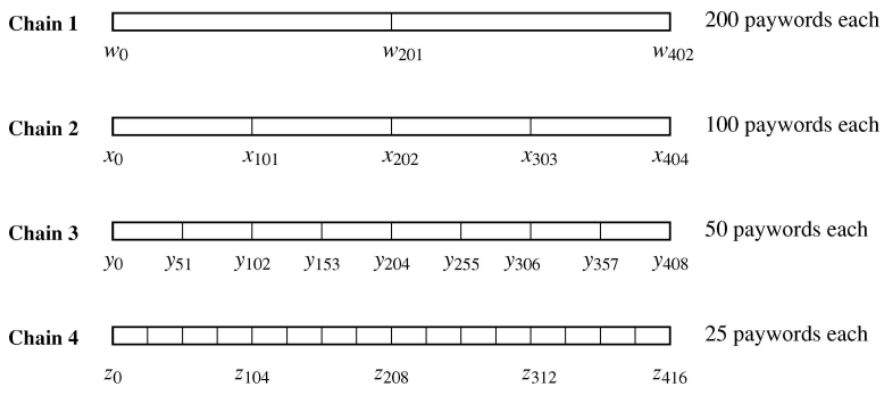
(f),(g),(h) پرداخت امن. در حال حاضر، فروشنده آماده پذیرش payword است. به جای ارسال paywords در قالب ساده، کاربر هرpayword را به عنوان یک کلید رمزنگاریpayword کد گذاری می کند یعنی $\langle w_i \rangle_{w_i}$. رمزگذاری payword با MAC آن ارسال می شود، با استفاده از payword به عنوان کلید محاسبه می شود و کلید اخیر که کاربر می تواند نشان دهد. برای اولین d پیام های کاربر هیچ کلیدی را آشکار نمی سازند. از (D + 1) STپیام، کاربر افشای کلید های مناسب را شروع خواهد کرد. بنابراین، فروشنده پیام dگذشته با بافر می کند و به اولین payword به عنوان کلید فاش توسط کاربر در پیام ST (D + 1) اعتبار می بخشد . بنابراین، هر تایید paywordبا فواصلd تاخیر می کنند که به طور کلی یک عدد صحیح با ارزش کوچک است. با به کارگیری مکانیسمTESLA ، فروشنده به بسته اعتبار می بخشد و برای تأیید payword ، تابع هش h را در طی payword بکار می برد و آن را در برابر آخرینpayword ارسال شده توسط کاربر بررسی می کند. بنابراین، احراز هویت و تایید payword دست به دست با تاخیر d کوچک پیش می رود.

4. کوپن های الکترونیکی: طرح با واگذاری

واگذاری یک ویژگی مهم است که در طرح های پرداخت میکرو موجود از دست رفته اند زیرا کاربران دستگاه های مختلفی برای دسترسی به یک سرویس اشتراک دارند. بدیهی است ثبت نام تمام دستگاه های ممکن با فروشنده و قراردادهای قبلی جداگانه با بانک قابل توصیه نیست. هدف ما باید به حداقل رساندن محاسبات گران به ویژه برای دستگاه های دستی با منابع محدود است. طرح ما اجازه می دهد تا کاربر ثبت نام را از کامپیوتر خود شروع کند و قابلیت تفویض مخارج به دستگاه های خود و یا حتی به کاربران دیگر را داشته باشد. ما قابلیت واگذاری هزینه از طریق چند زجیره payword با استفاده از مجوزSDSI / SPKI بدون مزاحمت بیشتر با عملیاتPKI را بدست آوردیم.

در ادامه، ما مسیر واگذاری یکپارچه شده در کوپن های الکترونیکی را مشخص خواهیم کرد. برای این کار، اجازه دهید گواهی زیر را فرض کنیم.

$$K_U\ Chain1_{[201-402]} \longrightarrow K_{agent3}\blacksquare$$



شکل. 3. تولید زنجیرهای payword چند دانه

از طریق این مجوز، اصل KU اختیارات خود را به بخشی از زنجیر 1 به Kagent3 واگذار می کند. پرچم واگذاری نهایی در گواهی به معنی این است که Kagent3 می تواند مجوزی را اعمال کند اما نمی تواند واگذار بیشتر آن را به دیگران انجام دهد.

بنابراین، در سیستم کوپن های الکترونیکی ما، یک کاربر مایل به استفاده از امکانات واگذاری است که با درخواست بانک برای یک گواهی PayWord شروع می شود و همچنین بانک را در مورد الزامات نسل payword چند دانه آن مطلع می سازد، به طوری که بانک بیش از یک ثبت نام توسط کاربر با یک فروشنده با استفاده از مقادیر متعدد از یک زنجیره payword را به عنوان تعهد پیش بینی می کند. بانک گواهی PayWord مربوط به کاربر را صادر می کند و کاربر تولید زنجیره payword را شروع می کند. ارائه طرح نمونه از زنجیره payword چند دانه ای در شکل. 3نشان داده شده است و بعضی ار بخش های این زنجیره paywordچند دانه ای به شرح زیر به سه عامل مختلف واگذار شد:

$$\begin{aligned}
&\text{User} \longrightarrow \{w_0, K_{agent1}, E, I_U, \langle w_l \rangle_{K_{agent1}}\} &&\longrightarrow \text{agent1}\\
&\text{User} \longrightarrow \{x_0, K_{agent2}, E, I_U, \langle x_{100} \rangle_{K_{agent2}}\} &&\longrightarrow \text{agent2}\\
&\text{User} \longrightarrow \{w_{201}, K_{agent3}, E, I_U, \langle w_{402} \rangle_{K_{agent3}}\} &&\longrightarrow \text{agent3}
\end{aligned}$$

کاربر عوامل نرم افزاری خود را برای هزینه بابت صدور یک گواهی مجوز شامل اطلاعات زیر تایید کرد: تعهد برای عامل، محدودیت هزینه، تاریخ انقضاء، عامل کلید عمومی و برنامه های دیگر داده های خاص.

این عوامل / کاربران فرعی لازم نیست که به طور تصادفی یک عدد را انتخاب و زنجیره ای خود را محاسبه کنند، اما ارزش های شروع و پایان زنجیره ای توسطU ارائه خواهند شد. مقدار ریشه در گواهی و ارزش سقف بالا محصور (WL)به agent1 در فرمت های رمزگذاری شده ارسال می شود، یعنی $\langle w_l \rangle_{K_{agent1}}, agent1$ با استفاده از تابع هش h در طی WL برای L بار شروع می شود و مقدار ریشه ها توسطU تعریف شده است. به محض این که کاربر چنین اختیاری را در بخشی از زنجیرهpayword واگذار کند، آن زنجیره را از دسترسی بیشتر قفل می سازد تا بخشی از زنجیره به طور کامل صرف و یا منقضی شود. بنابراین، درخواست payword بعدی از یکی دیگر از کاربران فرعی از یک زنجیره payword قفل نشده مختلف بکار گرفته می شود. بنابراین، توانایی کاربر برای تفویض اختیارات جزئی برای زنجیره payword است که توسط تعدادی از زنجیره های payword قفل نشده با کاربر محدود شده است. عوامل / کاربران فرعی قدرت صرفpaywords از زنجیر های payword مختلف را دارند که می تواند به صورت همزمان مبادله شوند. در صورتی که دانش پیشینی در مورد الگوی درخواستی از کاربران فرعی داشته باشد، می تواند هوشمندانه زنجیره payword را با محاسبه مناسب تقسیم بندی کند.

مرحله ثبت نام © کمی متفاوت خواهد بود، یعنی اینکه

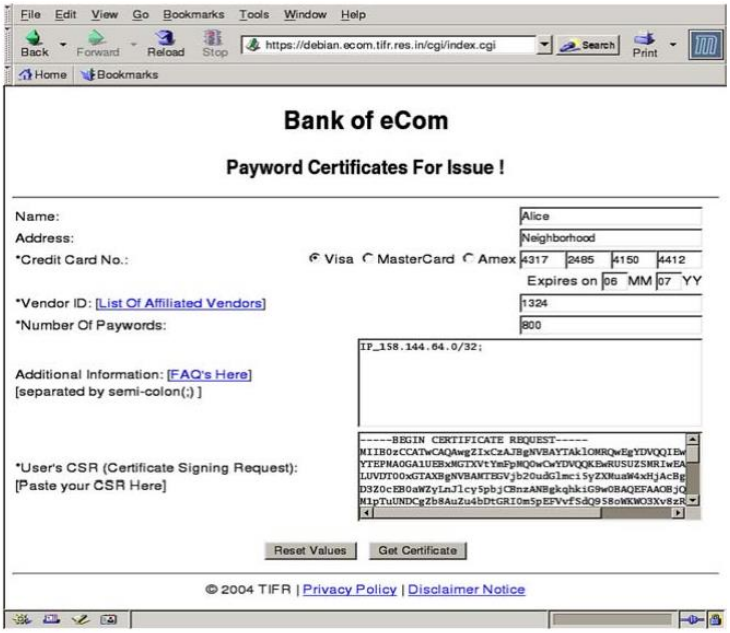
$$\text{agent3} \longrightarrow \{V, X, w_{201}, I_{agent3}\}_{K^{-1}_{agent3}} \longrightarrow \text{Vendor}$$

در آن X اثبات agent3 از مجوز در SPKI / SDSI است و w201 ارزش ریشه payword زنجیره ای است که agent3 خواهان صرف هزینه است. فروشنده امضا در طی پیام ثبت نام و اثبات چک اصالت ارائه شده توسط متقاضی و درآمد حاصل بیشتر را تأیید می کند.

در فواصل دوره ای، فروشنده همه امضاهای تعهدات به بانک را مطابق با بالاترین ارزش payword هزینه و شاخص آن را تسلیم می کنند. بانک این اطلاعات ارائه شده توسط فروشنده خارج از خط را تایید می کند و بر این اساس پول حساب فروشنده از حساب کاربر را معتبر می سازد.

قبل از توجه به تجزیه و تحلیل طرح کوپن های الکترونیکی پرداخت میکرو ، ما باید به طور خلاصه تعهدات بازیگران در پروتکل، یعنی بانک، فروشنده، و کاربر را بیان کنیم.

بانک طرف قابل اعتماد در این راه اندازی است. بانک به عنوان یک تسهیل کننده برای فروشندگان و کاربران عمل می کند.



شکل. 4. رابط بانک برای صدور گواهی PayWord به کاربران.

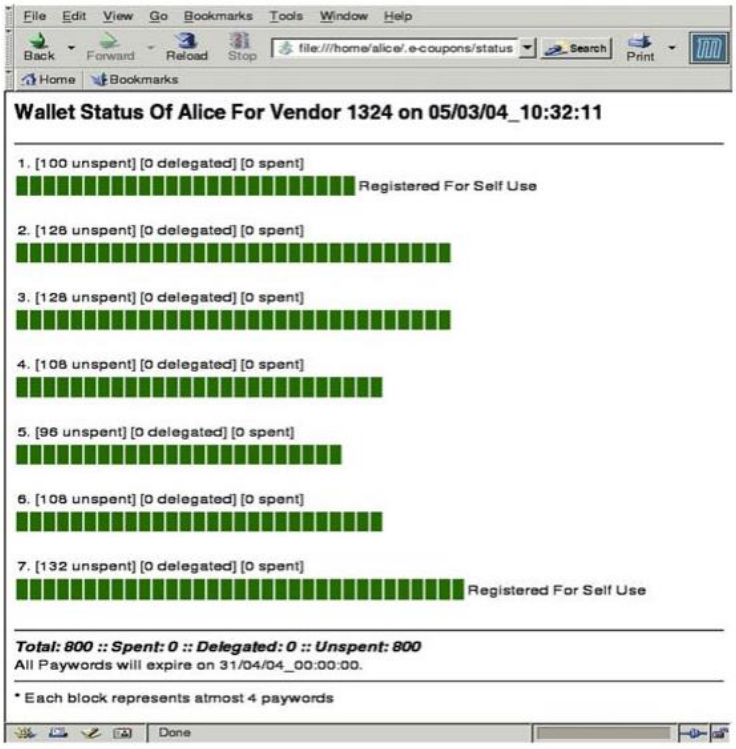
بانک ها به طور مستقل وارد توافق قانونی با دو نهاد دیگر می شوند که به رفتار صادقانه توافق می کردند. بانک فروشندگان شرکت کننده برای بازپرداخت paywordهای هزینه شده توسط کاربران ثبت نام را تضمین می کرد. فروشندگان ملزم به تحویل کالا به دریافت مبلغ پرداختی مورد توافق هستند. کاربران به هزینه payword خود زنجیره ای در جهت معکوس از ایجاد آن نیاز دارد و مسئول مدیریت زنجیره ای خود payword است، و خطر از دست دادن paywords هایی که از ترتیب زیر پیروی نمی کنند را باید بپردازند.

5. کوپن های الکترونیکی: اجرا

در این بخش، باید اجرای دست اول دیدگاه سیستم خود را به دنبال چند عکس فوری توضیح دهنده رابط سیستم برای آن کاربران ارائه دهیم. ساخت کوپن های الکترونیکی در سه مکانیسم مبتنی بر لینوکس GNU / ماشین آلات اینتل پنتیوم برنامه های بانک، فروشنده، کاربر و یک لپ تاپ به عنوان یک نقطه دسترسی خدمات اضافی برای کاربر انجام شد، تا واگذاری paywords از کامپیوتر خود به لپ تاپ را نشان دهد.

توسعه نرم افزار کوپن های الکترونیکی ادغام سه ماژول اصلی؛ یعنیPayWord ، TESLA اصلاحشده و / SPKI SDSIاست. اجرای این ماژول با استفاده ازC ، PerlCGI، و دیگر زبان های برنامه نویسی، پایگاه داده mySQL برای بانک و فروشنده انجام می شود، آپاچی به عنوان یک سرور وب برای بانک و کتابخانه OpenSSL برای رمزنگاری است. ما راه اندازی نهاد های فردی کوپن های الکترونیکی را در ادامه توصیف کرده ایم:

-**بانک**: برای سیستم امری محوری است. این نهاد مورد اعتماد برای کاربران با صدور گواهی تایید می شود. ماژول SPKI / SDSIروی دستگاه بانک به عنوانCA قابل اجرا است. رابط بانک برای کاربران بسته بندی پوشانده شده در اطراف ابزار مت فردت است (کمبریجMIT). این رابط با SSL آپاچی سرور میزبان فعال است که ورودی را از کاربران می پذیرد و Payword گواهی را با پذیرش پرداخت توسط ضامن تایید می کند. ورودی از کاربر برای هدایت سپر sdsi2shتوسط اسکریپت های Perl-CGI جمع آوری شده اند. بیان گواهی بر این اساس برای کاربران ارائه شده است، در حالی که یک کپی ذخیره شده در پایگاه داده بانک وجود دارد. شکل. 4، یک نگاه اجمالی از تعامل کاربر با بانک را نشان می دهد. سرور بانک به پورت 2344 برای درخواست بازپرداخت از فرشونده ها گوش فرا می دهد.



شکل5. رابط کیف پول کاربر: وضعیت اولیه در زمانt0 .

این برنامه داده ها را (تعهدات کاربر و / یا شاخص های payword) از فروشندگان و فروشگاه های تعهدات برای جدول پایگاه داده فروشنده مربوطه و بازپرداخت حساب فروشنده را با توجه به شاخصpayword بعد از اعتبار ارزش آن می پذیرد. این محاسبات با بستگی اولویت کمتری بر بار و سرور انجام می شوند.

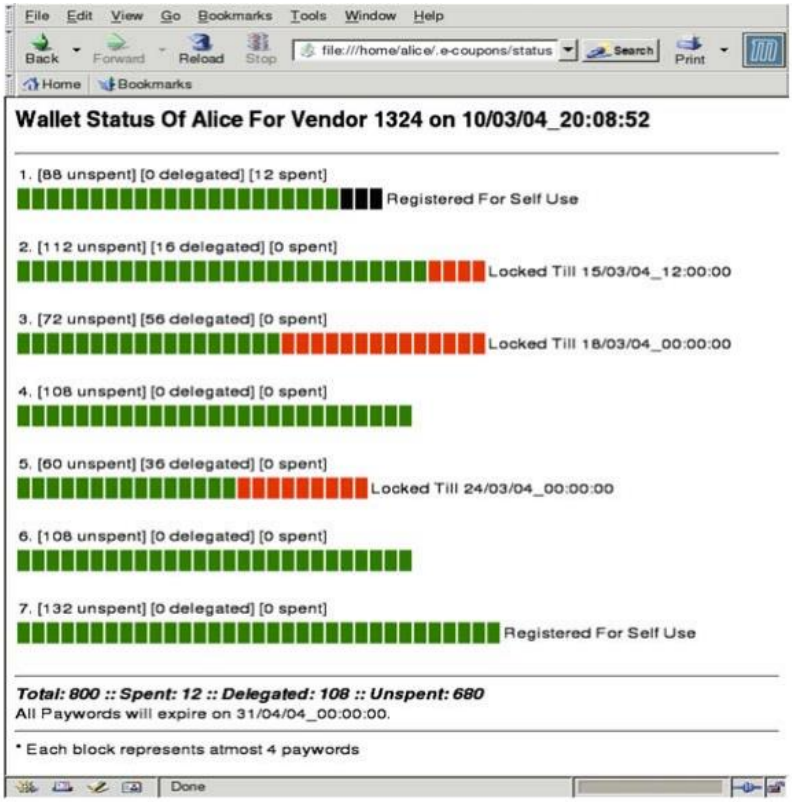
- **کاربر**: پس از پرداخت کلان برای خدمات خاص یک فروشنده، کاربر اختیاراتی را از طریق گواهی PayWord، برای جعل paywords برای هدف پرداخت دریافت می کند. این گواهی در $HOME/.e-coupons/certificates/دایرکتوری با نامVENDORID.crt $ ، به طور پیش فرض ذخیره می شود. به کاربران یک برنامه تعاملی ارائه شده است که آنها به تولید زنجیر payword مختلف بر اساس نیازهای خود کمک می کند. برنامه برای عدم وجود یک فایل VENDORID.lock $ در / HOME $ کوپن المترونیکی / وضعیت / استفاده-گواهی ها قبل از ایجاد زنجیره payword برای فروشنده خاص هدایت می شوند. پس از اجرا موفق آن قفلی را تولید می کنند و زنجیره های تولید شده در فایل های جداگانه تحت-e. / HOME $ / VENDORID $ / coupons/chainsذخیره می سازد. با توجه به فضای مورد نیاز برای ذخیره سازی paywordsبه یک فایل و زمان مورد نیاز برای دسترسی به هر یک از فایلهای paywordدر مقابل تولید ارزش paywordنو مقدار قبلی را در CPU به راحتی در دسترس قرار می دهند، برنامه ما فقط نتایج متوسط و مربوط به شاخص برای فایل payword جدا از مقادیر مرزی زنجیره ای را ذخیره می کنند. پس از تولید(paywordsشکل 5، وضعیت کیف پول اولیه کاربر را نشان می دهد)، کاربر می تواند هم زنجیرهایی برای استفاده خود یا نماینده زنجیر، در کلیت و یا جزئی، برای دیگران ثبت می کند. برای استفاده از زنجیره ای برای استفاده خود، کاربر مقدار ریشه زنجیره ای را به عنوان تعهد امضا می کند و آن را با فروشنده بعد از سرور TESLA بر روی پورت 2345 برای اداره درخواست های زمان هماهنگ سازی ناشی از سمت فروشنده مقدار اولیه را ارائه دادند. کاربر نیز با سپر sdsi2sh برای قابلیت واگذاری هزینه مجهز شد. شکل. 6، استفاده از ابزار ارائه شده برای کاربران به منظور قابلیت تفویض و واگذاری هزینه را نشان می دهد. رابط کاربری کامل برای کاربران از سیستم برای مدیریت کیف پول ارائه

شده است. شکل های 7، 8، 9، وضعیت کیف پول کاربر در فواصل زمانی مختلف را نشان می دهد، paywordها را در کد رنگ متمایز بطور برجسته نشان می دهد، paywordهای "هزینه نشده"، "واگذار شده" و "هزینه شده."

-**فروشنده**: در اجرای ما، سرور پخش موسیقی را به عنوان سرویس فروشنده یکپارچه ساختیم که بر روی پورت 6666 درخواست کاربر را گوش می داد.

```
File  Edit  View  Terminal  Go  Help
[alice@Knuth alice]$ delegate_coupons

Usage: delegate_coupons   [--paywords=NUMBER] [--dir=DIRECTORY]
                          <--file=FILENAME | --lname=LOCALNAME>
                          <--certnum=CERTNUM> <--chain=CHAINNUM>
                          <--vendorid=ID> [--help | DEFAULT]

 -p, --paywords=NUMBER          Number of Paywords
 -f, --file=FILE                File containing public-key
 -d, --dir=DIRECTORY            Directory containing certificates of the user
                                Default ~/.e-coupons/certificates/
 -l, --lname=LOCALNAME          Local Name of Delegatee as in SDSI2

 -vi, --vendorid=ID             Specify vendor id
 -cn, --certnum=CERTNUM         Certificate Number
 -ch, --chain=CHAINNUM          Chain Number

[alice@Knuth alice]$ delegate_coupons --lname="Self Laptop" --vendorid=1324 --certnum=3 --chain=2
Certificate stored in /home/alice/.e-coupons/certificates/1324/3/Self_Laptop.crt
[alice@Knuth alice]$
```

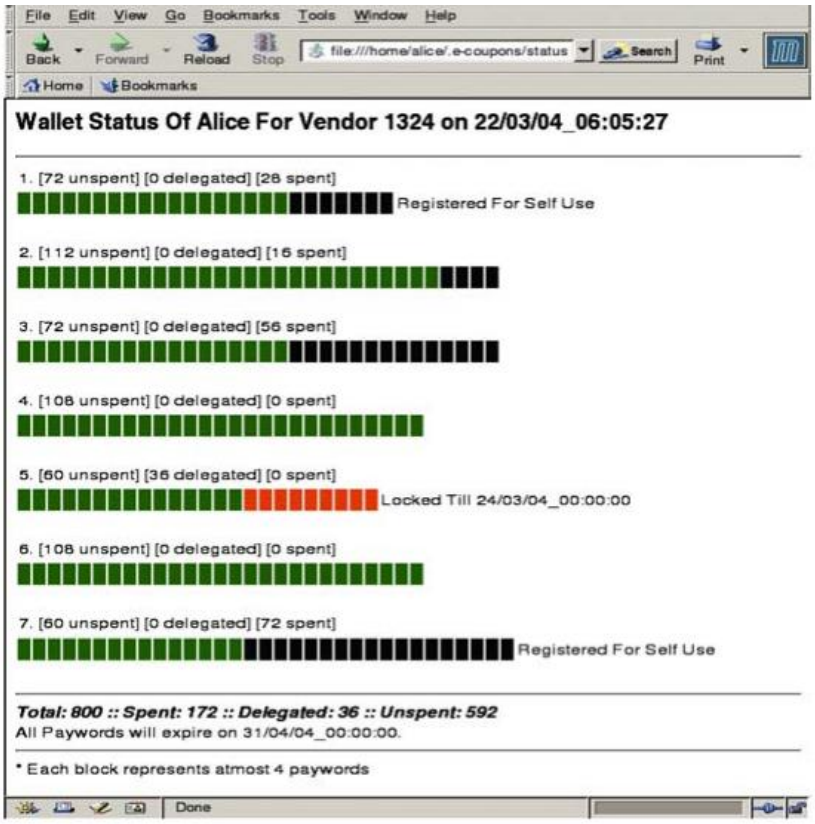
شکل. 6. کاربر قابلیت هزینه کرد را واگذار می کند.



شکل7. وضعیت کیف پول کاربر در زمان t1 .

فروشندگان ممکن است از روش های مختلف برای پیاده سازی رابط کاربری خود برای کاربران داشته باشند. فروشنده با مکانیزم راستی آزمایی SPKI / SDSI مجهز می شود و یک پایگاه داده اطلاعات کاربر را ذخیره می سازد.

کاربران با ارسال تعهدات امضا شده همراه با اثبات هزینه های قابلیت واگذاری یا از تسهیل به دست آمده از بانک و یا یک کاربر مجاز ثبت نام می کنند.



شکل 8. وضعیت کیف پول کاربر در زمان t2 .

با دریافت درخواست ثبت نام، فروشنده مکانیسم تصدیق را اجرا می کند. این فرآیند شامل اعتبارنامه کاربر (تک گواهی PayWord یا زنجیره ای از گواهی در مورد واگذاری) تأیید و تایید فروشگاه های فروشنده نسبت به تعهد کاربر در پایگاه داده در برابر ورود کاربر بصورت موفق است. فروشنده این اطلاعات برای مدت زمان کافی حفظ می کند تا ولخرجی کاربر و تلاش ها برای برداخت دو برابر را خنثی کند. قبل از مقدار پرداخت اولیه معامله، فروشنده

خود را با کاربر و با ارسال یک درخواست به پورت کاربر 2345 همزمان می سازد. همانند پردازش های تراکنش ها، فروشنده ذخیره سازی بالاترین شاخص هایpayword دریافت شده از کاربر را ادامه می دهد.

فروشنده بصورت دوره ای تعهدات انباشته و شاخصهای payword را برای تسهیل بانک برای بازپردات می فرستد. بانک ممکن است وجود تلاش ها برای هزینه دو برابری کاربر خاص را گزارش کند. فروشنده بلافاصله چنین کاربرانی را از پایگاه داده کاربران ثبت نامی خالی می سازد.

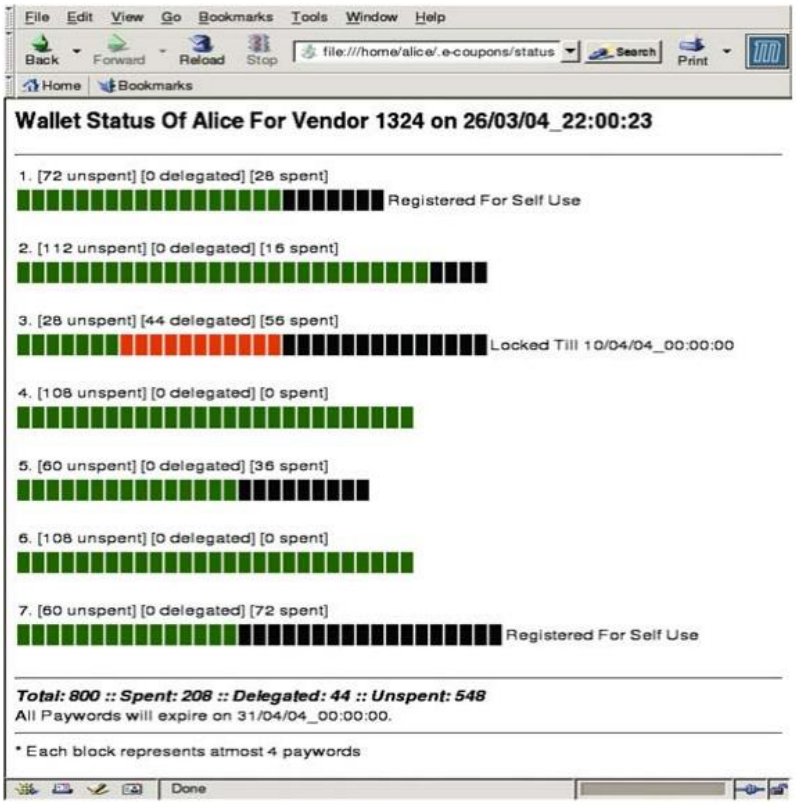
6. کوپن های الکترونیکی: برنامه های کاربردی

در این بخش، ما یک سناریوی برنامه کاربردی معمولی سیستم کوپن های الکترونیکی را ارائه می دهیم که نمی تواند استفاده از طرح های موجود را پیش بینی کند. اما دامنه کوپن های الکترونیکی باید به حالات نمونه محدود در نظر گرفته شود که در این مقاله مطرح شده است. توانایی کوپن های الکترونیکی برای حمایت از پرداخت همزمان برای یک سرویس مشترک از نقاط دسترسی در سرویس های مختلف به طور همزمان یکی از ویژگی های مهم آن است. این قابلیت با کمک مثال زیر توضیح داده شده است.

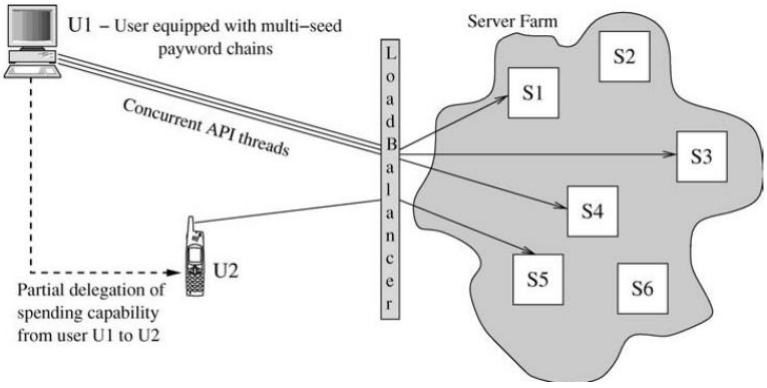
گوگل، یک موتور جستجوی پیشرو، به نرم افزار برنامه نویسان اجازه می دهد تا به اطلاعات جستجو از طریق رابط های برنامه کاربردی دسترسی دشته باشند (برنامه کاربردی رابط). در حال حاضر گوگل دسترسی رایگان به اطلاعات را از طریق رابط های برنامه کاربردی با هر کاربر، در هر محدودیت های دسترسی در هر هفته فراهم می کند. ممکن است به دلیل عدم وجود یک طرح مناسب میکرو پرداخت، گوگل به حالت پرداخت تغییر نکند. کوپن های الکترونیکی به صورت کامل مناسب برای این سناریو مناسب هستند.

اجازه دهید فرض کنیم، یک کاربر "U1" برای چنین سرویس API با کمک یک بانک تسهیل کننده مشترک باشد. کاربر یک برنامه چند رشته ای می نویسد که در آن هر موضوع به صورت جداگانه به سرویس اشتراک API و قابلیت پرداخت خود نیاز دارند. از آنجا که، سیستم های بزرگ توازن بار بین سرور را اجرا می کنند، بنابراین درخواست API

به صورت تصادفی در میان سرورهای سیستم توزیع می شوند [رجوع به شکل. 10] (از این رو زنجیره ای payword منفرد برای چنین حالاتی مناسب نیست). یک



شکل 9. وضعیت کیف پول کاربر در زمان t3.



شکل. 10. پرداخت همزمان برای برنامه های کاربردی چند رشته ای

فردی ممکن است در مورد ساخت خود "متعادل کننده بار" به عنوان پرداخت برای سرویسAPI استدلال کند، به جای سرور های فردی که در واقع درخواست API را فراهم می کنند. اما چنین رویکرد محاسباتی بار "متعادل کننده

بار" و ارتباط بین "متعادل کننده بار" و سرور در پشت آن را بطور فوق العاده افزایش خواهد داد. همچنین ممکن است استدلال شود که به جای هر موضوع پرداخت به صورت جداگانه، به منشاء این موضوعات اجازه پرداخت داده می شود. اما چنین رویکردی استقلال موضوعات را محدود می سازد، در حالی که برای پارامترهای مانند "کیفیت خدمات" مذاکره می شود.

علاوه بر این، کاربر به دسترسی به خدمات یک دستگاه موقت قرض گرفته شده نیاز دارند یا ممکن است به کاربر دیگری استفاده از خدمات در شکل محدود را اجازه دهد (مشابه کوپن هدیه). این نیاز در شکل 10به تصویر کشیده است که در آن کاربر "U1" مجوز گواهی به "U2"را صادر می کند. به غیر از مدت زمان اعتبار، این گواه شامل مقادیر مرزی یک زیر زنجیره ای، برداشت شده توسط "U1" از مجموعه قفل نشده چند زنجیر payword است، همانطور که در بخش 4 نشان داده شده است. سناریو در بالا شباهت نزدیک با بسیاری از برنامه ها را در محاسبات توزیع شده، به خصوص در محاسبات شبکه ای را، قیمت گذاری در MANET و غیره را نشان می دهد. علاوه بر این، امکان واگذاری کاربران را قادر می سازد تا با هدیه دادن آن به دیگران، به جای پرداخت نشده منقضی از paywords به طور کامل استفاده کنند.

7. تحلیل طرح کوپن های الکترونیکی

در این بخش، تجزیه و تحلیل کوپن های الکترونیکی را با توجه به مسائلی مانند خطر درگیری، امنیت و عملکرد را برای دنبال کردن یک مقایسه اجمالی سیستم با سیستم های پرداخت میکرو موجود توضیح می دهیم.

7.1 تجزیه تحلیل خطر

کوپن های الکترونیکی هیچ خطر اضافی را جذب نمی کنند در حالی که پرداخت واحد عاقلانه صورت می گیرد. هر چند ساخت paywords های رایگان از کاربر خاص شامل خطر از سرقت payword در مبادلات است، اما امنیت کافی از طریق یک فرایند رمزگذاری نسبی و مکانیزم احراز هویتTESLA برای چنین تلاش هایی خنثی است . خطر

در سطح پایین با همه طرف های درگیر در ارتباط با پروتکل همراه است. از آنجا که بانک برای بازپرداخت در برابر paywords تسهیلات اعتباری به کاربران و تضمین به فروشندگان می دهد، تلاش های بدجنسانه ولخرجی توسط کاربر بانک را در معرض خطر نگه می دارد. با این حال قراردادهای حقوقی بین بانک و کاربر بازدارنده خواهد شد. خطر دریافت نکردن کالای یک کاربر وجود دارد که او برای آن کالا پرداخت انجام داده است. این خطر با کاربران پایینی همراه است زیرا پرداخت واحد عاقلانه هستند، اما فروشنده در معرض خطر بزرگ از دست دادن شهرت خود قرار دارد.

ما درک کردیم که استفاده از کلید برای رمزنگاری هدف و برای محاسبه MAC ممکن است به نقاط ضعف رمزنگاری پروتکل منجر شود. ولی ما به ارائه محرمانهpayword ها برای یک بازه زمانی کوتاه در طول انتقال خود نیازمندیم که با استفاده یک زیر رشته 64 بیتی از payword انجام می شود.

در حالی که فروشنده آزادانه زمان خود را با فرستنده در پروتکلTESLA منطبق می سازد، تاخیر پخش درخواست هماهنگ سازی زمان بسته را نمی داند، پس فرض بر این است که خطا هماهنگ سازی زمان Δ است. برای باقی می ماند در طرف امن ما زمان رفت و برگشت کامل بسته را در نظر گرفتیم. حتی اگر فروشنده یکی از بسته های ورودی معتبر را از دست دهد، می تواند ارزش آن را با موفقیت در بسته بعدی دریافت کند، زیرا ماهیت خود تصدیقی هویت paywords ها در زنجیره وجود دارد. فروشنده همیشه می تواند به بالاترین ارزش payword به سمت ارزش تعهدی پیش برود. با چنین امکانات ارائه شده ای، فروشنده آماده پذیرش خطر از دست دادن بسته به دلیل اشتباهات شبکه می باشد.

همچنین، فروشنده به بافر بسته نیاز دارد تا در طول تاخیر قبل از آن بتوان آنها را تصدیق کرد. و گاهی به علت بار سنگین فروشنده، رها کردن بسته زمانی به سادگی خطرناک می شود زمانی که منابع (فضای بافر ورودی) به طور کامل استفاده شده باشند. این مشکل می تواند با نگه داشتن تعهد بافری کردن بسته در طول تاخیر افشا بر کاربران حل شود. علاوه بر این، با متصل کردن مقادیر هش paywords آینده، یک بسته زود هنگام به تصدیق هویت داده ها در payword بعدی تا حد ممکن کمک خواهد کرد. بنابراین تایید می تواند در زمان واقعی انجام شود.

خطر payword های دو برابر هزینه را می توان با دو روش خنثی کرد. یا فروشنده باید یک بافر از ارزش تعهد ثبت نام شده را حفظ کند و هر یک از ثبت نام های جدید در برابر این بافر را بررسی کند و یا آن را به منظور بررسی هر یک از زنجیره ارزشpayword تعهدی با بانک انتخاب کند. گزینه بعد است بر خط و هزینه بر است. این یک تصمیم سیاسی راه اندازی بر اساس توافق بین بانک و فروشنده خواهد بود. ما ورزش مدل شهرت در دنیای واقعی برای بررسی

سوء رفتار از نهادهای درگیر در راه اندازی. شهرت بد به دلیل عدم تحویل کالا در مورد پرداخت موفق توسط کاربران به فروشنده از لحاظ از دست دادن کسب و کار است. و بانک را برای بدرفتاری کاربران (تلاش های هزینه دو برابر) با امتناع

به صدور گواهی PayWord در زمان تجدید اشتراک جریمه می کند.

7.2 تجزیه و تحلیل امنیت

در پروتکل PayWord از paywords کاربر و فروشنده خاص هستند، به طوری که آنها تهدید را تحمل نمی کنند در حالی که تهدید به سرقت رفتن بر خلاف کوپن های الکترونیکی است که در آنpaywords کاربران خاص نیست. هر پیام که در آن دشمن ممکن است به استفاده از کلیدهای رمزگذاری کم بیتی علاقه داشته باشد. امنیت برای هر paywoed فرستاده شده با فرشنده ارائه شده است زیرا payword ها کاربران خاص و آسیب پذیر برای سرقت در زمان تبادل نیستند.

جدول 1. تجزیه و تحلیل عملکرد و ارزیابی مقایسه ای

	No. of Asymmetric key operations required signature/encryption		No. of Symmetric key operations required payword encryption/decryption		No. of Hashes required payword gen./verification, MAC computations	
	User	Vendor	User	Vendor	User	Vendor
Chain 1	$1+E$	D	400	400	$(402 \times 2)+400$	$404+400$
Chain 2	$1+E$	D	400	400	$(404 \times 2)+400$	$408+400$
Chain 3	$1+E$	D	400	400	$(408 \times 2)+400$	$416+400$
Chain 4	$1+E$	D	400	400	$(416 \times 2)+400$	$432+400$
Single Chain (1600 paywords)	1	1	0 no security required, since	0 coins are vendor and user-specific	$1601+0$	$1601+0$

ما امنیت را با کمک احراز هویت منبع کارآمد مکانیزم TESLA و به طور همزمان با رمزنگاری هر payword با خود آن ارائه کردیم. TESLAبه یک سربار تبدیل نشده است، زیرا ما هش های زنجیره ای جداگانه یک طرفه برای محاسباتMAC تولید نمی کنیم و به راحتی برای هویت زنجیره payword در دسترس را از زنجیره یکی دیگر از مقادیر هش یک طرفه تصدیق نمی کنیم. دو-هزینه های paywords امکان پذیر نمی باشد زیرا paywordها فروشنده خاص هستند.

اطلاعات کارت اعتباری کاربر توسط پروتکل پرداخت استاندارد ارسال می شود، در حالی که روش رمزگذاری مورد استفاده برای محرمانه بودن payword نسبتا ضعیف است. از آنجا که رمزگذاری 56 بیتی به اندازه کافی رضایت بخشی برای اعتماد در برابر حملات را برای استفاده ناشیانه برای یک دوره زمانی فراهم می کند که به اندازه کافی برای payword توسط گیرنده تایید می شود، از استفاده از طول کامل payword به عنوان کلید رمزنگاری جلوگیری می کند. چون چنین امنیتی عملی برای پرداخت پوشش داده می شود، کاربر می تواند به ارسال paywordsاز فرقه بالاتر فکر کند.

7.3 تجزیه و تحلیل عملکرد و مقایسه ارزیابی

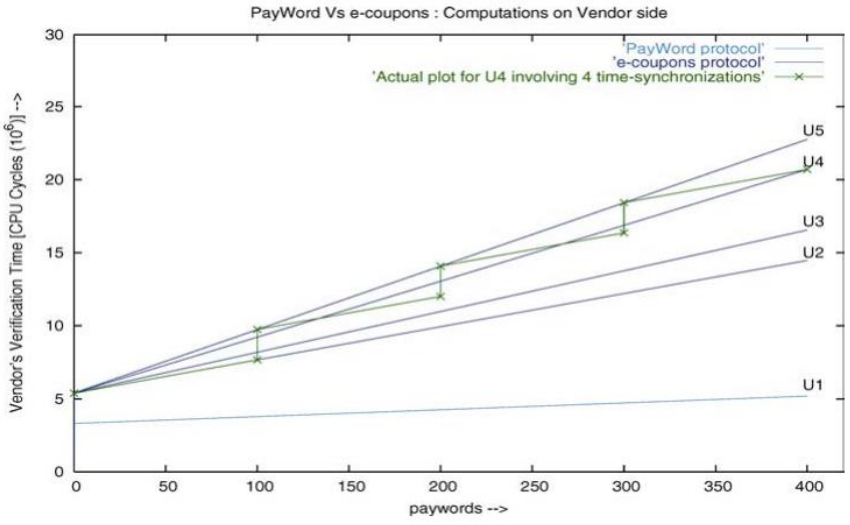
ارزیابی عملکرد سیستم ما در برابر پروتکل PayWord اصلی در حالی است که یک از کاربر خاص و فروشنده یکپارچه خاص زنجیره ای payword به یک فروشنده خاص پرداخت چند دانه در جدول 1. داده شده در این جدول ، نشان دهنده تعداد دفعاتی رمزنگاری مقصود فعلی است انجام به عنوان یک درخواست هماهنگ سازی زمان از یک فروشنده به یک کاربر و E نشان دهنده پاسخ های رمزگذاری شده از کاربر برای فروشنده است. ارزش هر دو Dو E به تعداد کل مراحل معامله شروع بین آنها برابر است، به عنوان هماهنگ سازی زمان اولین قدم در انجام این کار میکرو معاملات این است. عملیات کلید متقارن (رمزگذاری / رمزگشایی با استفاده از 64 بیتیDES) درگیر در اجرای ما در مرحله ارسال paywords و تایید خود را در دریافت پایان یافت.

این تحلیل بر اساس تفویض اختیار payword تا عمق1 است، یعنی کاربران فرعی که مجوز payword را دریافت کرده اند قدرت خود را هر بیشتر واگذار می کنند که مورد کلی خواهد بود. بنابراین، در ستون هش از جدول 1، طول زنجیره payword کاربر در 2 ضرب شده است؛ صاحب زنجیره اصلی ارزش استفاده از هش تابع ساعت و نمایندگان برخی از این زنجیره های کاربران فرعی را تولید می کنند و کاربران دوباره مقادیر بین طیف ها را محاسبه می کنند. از این رو، ضریب d + 1 افزایش می یابد که در آن d عمق واگذاری است.

همچنین، تفویض اختیار payword توسط یک کاربر به یک کاربر را هم یک گواهی به مجوز اثبات (X) از کاربر فرعی می افزاید. این مجوز زمان تایید فروشنده را افزایش خواهد داد. بنابراین، عمق واگذاری و زمان برای مجوز تایید شده توسط فروشنده خطی متناسب مورد نیاز است.

از اجرای طرح ما، یک نمودار از "تعدادpayword ها "در برابر "زمان تایید مورد نیاز توسط خریدار برای PayWordو کوپن های الکترونیکی پروتکل برای اثبات ادعای ما (شکل 11) تولید کرده اند. از نمودار بدیهی است که کوپن های الکترونیکی در سمت فروشنده برای اعتبار سنجی نسبت به پروتکل PayWord نیاز به زمان بیشتری دارند، اما انعطاف پذیری را به کاربران مدیریت قابلیت واگذاری هزینه ها فراهم می کند.

عملیات هش توسط زیر کاربر برای ایجاد payword با محاسبه دوباره ارزش اجرا می شود، پیش از آن توسطواگذار کننده محاسبه می شود. بنابراین، تصمیم گیری سیاسی خواهد بود، چه به مقادیر محاسبه کاربر و یا فقط مقادیر مرزی ارائه شود. اگر یک کاربر از برخی paywordih و معاملات یک بعدی بدون معامله ای بگذرد، کاربر می تواند پرداخت مقدار بالاتری را در یک معامله بررسی کند.



شکل. 11. ارزیابی محاسباتی کوپن های الکترونیکی در برابر فروشنده.w.r.t. payword

فروشنده هنوز هم می تواند با استفاده مکرر از عملکرد هش اعتبار را از payword بررسی کند. در حالی که با اجرای اقدامات در برابر هزینه دو برابر، روند می تواند در کارایی آن با استفاده از رای گیری احتمالی بهبود یابد(جارکی و اولدیزکو 1997). در حال حاضر، اجازه دهید تا کوپن های الکترونیکی با طرح های موجود دیگر را ارزیابی کنیم.

1. طرح پرداخت میکرو برای احراز هویت و غیر انکار SPKI نیاز به PKI دارد. PKI امکانات بدوی مورد نیاز را فراهم می کند. به خاطر همین چارچوب برای ما معرفی مفهوم هزینه های قابلیت واگذاری به کاربران دیگر ممکن است .این مرکز در تمام طرح های میکرو پرداختی دیگر وجود ندارد. بدیهی است، یکی نمی تواند payword کاربر خاص را حفظ کند اگر فرد بخواهد اختیارات paywords خود را به دیگران واگذار کند. این تغییر به طرح PayWord اصلی تهدید paywords هایی را ارائه می دهد در حالی که در معامله قرار دارند. ما نشان داده ایم که چگونه TESLA امنیتی برای paywords در حمل فراهم می کند. این تغییرات تدریجی به طرح اصلی PayWord باعث می شود ما طرح کمی کمتر از پرداخت ساده طرح Payword کارآمد باشد. اما طرح اصلیPayWord فاقد امکانات مورد نیاز برای قابلیت واگذاری هزینه هستند.

2. در میان متنوع موجود طرح های میکرو پرداخت تلاش برای ارائه پرداخت کم هزینه از طریق اینترنت، بیشتر وابسته به طرح PayWord و MiniPay ما است. هر دوی آنها طرح خارج از خط و مناسب برای برنامه های کاربردی پردات آنی هستند. اما طرح ما از آنها بطور قابل ملاحظه از نظر امکانات مانند واگذاری و روشی که در آن ما امنیت برای معاملات تامین می شود فرق می کند.

3. از آنجا که طرح PayWord فروشنده خاص و کار بر خاص است، کاربر اشتراک خاصی را به نقطه دسترسی ثبت نام محدود می کند که کاملا غیرطبیعی است. در عمل، اگر یک کاربر یک سرویس خاص مشترک داشته باشد، کاربر باید آزادی کامل برای دسترسی به خدمات صرف نظر از نوع دسترسی داشته باشد. بر خلاف Payword، طرح امنیت برآمده است و مسائل زیبایی هزینه دو برابر هستند.

4. بر خلاف معماری سه جانبه PayWord (شامل یک بانک، فروشنده و کاربران)، سیستمMiniPay باید از چهار تا شش طرف برخوردار باشد (کاربران، دسترسی شامل ارائه دهنده سیستم های صدور صورت حساب کاربران، بانک، فروشنده، سیستم ارائه دهنده خدمات اینترنت برای صدور صورت حساب فروشنده، یک داور). از آنجا که اعتماد انتقالی نیست، تعداد نهادهای در معماری عمومی به خاطر امکانات مانند پشتیبانی ارز چندگانه درخواست و غیره، افزایش می یابد، اعتماد کلی در میان اشخاص نسبت به سیستم کاهش می یابد. در عوض پشتیبانی از ارزهای مختلف می تواند توسط بانک بدون به کار گرفتن تلاش های قابل توجهی در طراحی اداره شود. ارز واحد اضافی برای پرداخت و فروشنده استفاده کردیم که چنین واحدهایی می توانند از ارز مورد نظر بین ارز ها به گرو در آورد که در آن کاربر را برای کلمه مجوز و ارز مورد نظر توسط فروشنده پرداخت می نماید.

5. در پروتکلMiniPay ، تهدید انکار خدمات توسط کاربر نهایی اعمال نمی شود اما با تسهیلات میانی یعنی ارائه دهنده در دسترس و ارائه دهنده خدمات اینترنت اعمال می شوند. آن ادعا می کند که همه طرفین از بسته شدن محافظت می شوند. در مقابل، مکانیزم TESLA در پروتکل ما به خریدار و فروشنده اجازه انجام احراز هویت منبع در هر بسته ورودی در زمان واقعی را می دهد. در این روش، پاکت های ساختگی ورودی برای انکار سرویس حمله در نظر گرفته شده است.

8. نتیجه گیری

در این مقاله، ما طراحی و پیاده سازی از یک طرح میکرو پرداخت کارآمد را مطرح مرده ایم که از واگذاری قابلیت صرف هزینه به دیگران و اقدامات امنیتی بسیار سبک و ذاتی حمایت می کند. از نظر ما، این اولین ابتکار در چنین مواردی است. طرح کم هزینه ، قوی و تاخیر ناچیز در زمان پاسخ دارد. طرح ما تلاش های هزینه دو برابری را تشخیص می دهد، تلاش انکار کننده خدمات و حملات افراد میانجی را خنثی می سازد. نتایج حاصل از اجرای طرح ما رضایت بخش است و بهره وری بهبود یافته را نشان می دهد در حالی که طرح یکپارچه احتمالاتی دیگر را تایید می کند (شامیر، 1995).

از نظر اعتماد در ارتباط با سه طرف به عنوان مثال، بانک، کاربران و فروشنده خطری در این پروتکل درگیر است، طرح ما به خوبی طرح PayWord است. علاوه بر این، PayWord فروشندگان را قابل اعتماد فرض می کند، در حالی که کاربران لازم نیست قابل اعتماد باشد. طرح ما نیز تحت همان محیط اعتماد و بی اعتمادی کار می کند. با این حال، طرح ما ویژگی های عملی تری به معاملات پرداخت های میکرو می دهد، مانند توزیع نسبی بیش از قابلیت هزینه به روبات برنامه و یا ارائه مقدماتی اشتراک محدود به پتانسیل مشتریان که بخشی از این قبیل راه اندازی نیست. معرفی ویژگی های واگذاری هیچ گونه خطری را متحمل نمی شود، بنابراین تسهیل واگذاری قابل دوام است.

نقش SPKI / SDSI به واگذاری محدود نمی شود، اما موارد ضروری سیستم PKI برای ارائه کلید ها عمومی و اعتبار گواهی، را تایید می کند. بنابراین ما باید یک سیستم میکرو پرداخت عالی داشته باشیم که امن، نسبتا کارآمد باشد و یک لایه غیر مستقیم را فراهم کند (در حالی که کاربران تفویض اختیارات می کنند) که منجر به گمنامی معامله می شود.

طرح ما اجازه می دهد تا کاربر امنیت ارائه شده برای پرداخت را پارامتری کند. برای پرداخت در فروشندگان مختلف، کاربر می تواند قدرت رمزگذاری برای پرداخت را بر اساس آسیب پذیری پروتکل اصلی (HTTP WAP)، و منابع محاسباتی در دسترس ارائه کند. این ماده کاربر را را تشویق می کند تا ارزش بالاتر با امنیت بیشتر را پرداخت کند.

عملا ایمن میکرو پرداخت با ارزش پولی نسبتا بالاتر معادل داشتن چند پرداخت کارآمد با ارزش پولی مشابه برای همان مجموعه ای از تحویل است. چنین مفادی مهم هستند چرا که آنها برای معاملات بین میکرو پرداخت و ماکرو پرداخت قرار دارند.

اجرای ما خارج از خط است، فروشنده خاص اما نه کاربر خاص و کاملا کارآمد می باشد. با فروشنده خاص، آن طرح قادر به خنثی کردن تلاش های دو هزینه ای و تبانی بین فروشندگان است. از آنجا که کاربر خاص نیست، با خطر paywordsسرقت رفته مواجه می شود در حالی که مبادله در حال اجرا است. با این مشکل ارائه یک پوشش محرمانه بودن اطلاعات زودگذر را انجام دادیم. لایه های غیر مستقیم در مجوز به کاربران پایانی ناشناس این امکان را می دهد تا زودتر از آن بهره ببرند. نیازی به گفتن نیست، حفظ حریم خصوصی از ویژگی های بسیار خواسته شده برای تجارت الکترونیک است.

در واقع می توان سیستم را برای فروشنده خاص با حفظ ارزش های دریافت تعهدات فروشندگان و به طور همزمان رایگان کرد (آنلاین) تا آن برای تأیید ثبت نام متعدد به بانک ارسال کنند. به این ترتیب، با توجه به استفاده از حل و فصل تناوبی فروشنده با بانک، کاربر نمی تواند زنجیره ای payword مشابه را به دو فروشنده مختلف ارائه کند.

ضمیمه

A. توابع هش یک طرفه وMAC

یک تابع هش یک تابع ریاضی است که یک رشته ورودی با طول متغیر را دارد (به نام پیش تصویر) و آن را به یک طول رشته خروجی ثابت (به طور کلی کوچکتر) تبدیل می کند (به نام مقدار هش). تابع هش یک طرفه یک تابع هش است که در یک جهت کار می کند:

```
(cert
 (issuer (name
  (hash sha1 |isEf64Sf5JpqasB4DCsR6Bn=|)
   Service-X-Subscriber-class-economy))
(subject
  (hash sha1 |Gf5tUySRhJiLk3syer0ibk3=|)
(not-before "2003-10-01_12:00:00")
(not-after "2004-10-31_11:59:59"))
```

```
(cert
 (issuer
  (hash sha1 |isEf64Sf5JpqasB4DCsR6Bn=|))
(subject (name
  (hash sha1 |isEf64Sf5JpqasB4DCsR6Bn=|))
   Service-X-Subscriber-class-economy))
(delegate) (tag (issue-payword
          (payword-limit 3000)
          (service http://xplore.ieee.org)))
(not-before "2003-10-01_12:00:00")
(not-after "2003-10-31_11:59:59"))
```

شکل. 12. نام و گواهی مجوز (صادر شده توسط بانک به یک کاربر).

محاسبه یک مقدار هش از پیش تصویر آسان است، اما برای تولید یک پیش تصویر سخت است که به یک مقدار خاص درهم می شود. خروجی به ورودی در هر راه قابل تشخیص وابسته نیست. یک بیت منفرد در تغییرات پیش تصویر به طور متوسط تغییر می کند، نیمی از بیت ها در مقدار هش هستند. با توجه به مقدار هش، برای پیدا کردن یک پیش تصویر قابل محاسبه غیر ممکن است که با آن مقدار در هم می شود. تابع هش یک طرفه نیز طلاقی آزادی است: تولید

دو پیش تصاویر با مقدار هش یکسان سخت است (اشنایر، 1996؛ لمپورت 1981). بنابراین، یک تابع هش یک طرفه یک h نقشه برداری از مجموعه ای کلمات در خود است مانند:

1. با توجه به کلمه X، محاسبه برای h(x) آسان است.

2. با توجه به کلمه Y، امکان محاسبه یک کلمه X چنان که Y =h(x) باشد، ممکن نیست.

کد تصدیق پیام یا MAC یک تابع یک طرفه وابسته به کلید هش است. MACها همان خواص توابع هش یک طرفه را دارند، اما آنها نیز شامل یک کلید هستند. تنها کسی با کلید یکسان می توانید هش (اشنایر، 1996) را بررسی کنید. آنها برای ارائه اصالت بدون پنهان کاری بسیار مفید هستند.

B. گواهی های SPKI

شکل 12، گواهی واقعی صادر شده توسط بانکB را نشان می دهد که دارای کلید عمومی مشخص شده در داخل جعبه صادر کننده به کاربر U به عنوان هدف گواهی هستند. با صدور نام این گواهی، بانک عضویت گروه را به مشترکین خود

می دهد تا گروه آنها خدمات- X- مشترک- کلاس- اقتصاد برای یک دوره از یک سال باشد. و با صدور مجوز گواهی، بانک اعضای گروه خدمات-X-مشترک - کلاس-اقتصاد را برای سکه های نو خود با محدودیت های مناسب توانمند می سازند (در این مورد 3000 می باشد، به طور مشابه می تواند تعریف دیگری از گروه به نام سرویس-X-مشترک- کلاس- منحصر به فرد با محدودیت های هزینه بالاتر باشد). به این ترتیب SPKI لبه روشنی بیش از دیگر طرحهای PKIدر مدیریت کارآمد شرایط فضای نام و مجوز دارد. همچنین، به تفاوت بین دوره اعتبار دو مجوز توجه داشته باشید. مجوز در یک ماه منقضی می شود، در حالی که اتصالات نام برای دوره زمانی دیگری باقی می ماند.