سومین کنفرانس انجمن رمز ایران
دانشگاه صنعتی اصفهان
۱۶و۱۷ شهریورماه ۱۳۸۴

بررسی امنیتی پروتکل پرداخت *3D Secure*

مسعود کلینی
دانشگاه صنعتی اصفهان
masoudkoleini@yahoo.com

مهدی برنجکوب
دانشگاه صنعتی اصفهان
brnjkb@cc.iut.ac.ir

محمد دخیل‌علیان
دانشگاه صنعتی اصفهان
Mdalian@cc.iut.ac.ir

چکیده

با گسترش روزافزون مبادلات مالی از طریق اینترنت، آمار تقلب نیز به شدت رو به گسترش است. این تقلبها را می‌توان سرقت شماره کارت اعتباری و خرید کالا و یا دریافت خدمات از طریق آن، سرقت پول الکترونیکی یا خرج دوباره آن، شنود کردن کلمات عبور و موارد دیگر دانست. تلاشهای متعددی برای حل این مشکل انجام شده و پروتکلهای مختلفی برای مبادلات اینترنتی از جمله مبادلات کارت اعتباری پیشنهاد و پیاده‌سازی شده است. از جمله این پروتکلها، پروتکل *3D Secure* است که توسط شرکت ویزا طراحی و پیاده‌سازی شده است. در این مقاله پروتکل *3D Secure* مورد تحلیل قرار گرفته و نقاط ضعف و قوت آن برشمرده می‌شود. در پایان نیز یک سناریوی حمله به این پروتکل معرفی می‌گردد.

واژه‌های کلیدی: کارت اعتباری، *3D Secure*، *SSL*، پروتکل پرداخت، کارت ویزا

۱- مقدمه

معاملات کارت اعتباری هم اکنون گسترده ترین وسیله خرید اینترنتی محسوب می‌شوند. از طریق این روش خرید، مشتری می‌تواند با باز کردن یک حساب بانکی، به انجام معامله و خرید اینترنتی بپردازد. در این سیستمها، مشتری می‌تواند خرید اینترنتی خود را انجام داده و در پایان هر ماه، صورتحساب خود را پرداخت نماید. هم اکنون سیستمهای معاملاتی اعتباری و بدهی[1]، گسترده ترین ابزار خرید اینترنتی به حساب می‌آیند و تقریبا همه بازرگانان از انجام خرید اینترنتی توسط این سیستم حمایت می‌کنند. خرید توسط کارت‌های اعتباری و بدهی بسیار ساده است و مشتری صرفا با ارائه یک شماره کارت اقدام به خرید اینترنتی می‌نماید.این مسئله موجب عدم وابستگی معاملات به مکان می‌گردد. حجم و مبالغ بالای معاملات کارت اعتباری، نیاز به یک پروتکل امن برای این معاملات را بطور جدی مطرح می‌کند. در این مقاله ابتدا پس از معرفی اصول و تاریخچه پروتکلهای پرداخت کارت اعتباری، پروتکل *3D Secure* که هم اکنون توسط شرکتهای معتبر کارت اعتباری پیاده سازی شده معرفی شده و ضعفهای آن مورد تجزیه و تحلیل قرار می‌گیرد. در پایان حمله‌ای به این پروتکل ارائه می‌گردد.

[1] *Credit and Debit*

۲- مروری بر تاریخچه و اصول حاکم بر معاملات کارت اعتباری

برای انجام معاملات کارت اعتباری، نخستین تلاش اساسی را شرکتهای *IBM*، مسترکارت، *Europay* و نت اسکیپ برای استاندارد سازی پروتکل *SET*[1] انجام دادند و در سال ۱۹۹۷ شرکتهای ویزا و مسترکارت این پروتکل را استاندارد و پیاده سازی کردند [۱]. پروتکل *SET* از لحاظ نظری، قدرتمندترین پروتکل پرداخت اینترنتی به شمار می‌رفت. این پروتکل هر سه موجودیت بازرگان، مشتری و بانک را درگیر دریافت گواهینامه و استفاده از سیستم *PKI*[2] می‌کرد. این پروتکل به دلیل پیچیدگی پیاده سازی و هزینه بری مورد استفاده مشتریها و بازرگانان قرار نگرفت [۲] و از دور رقابت با روش خرید دیگری که با وجود امنیت ناچیز خود، سادگی معاملاتی بالایی داشت کنار رفت. این روش خرید، روش مبتنی بر *SSL*[3] است. در این روش، بازرگان و مشتری پیش از وارد کردن اطلاعات توسط مشتری با همدیگر ارتباط *SSL* برقرار می‌کنند و از آنجا به بعد، مشتری شماره کارت و دیگر اطلاعات مورد نیاز را به صورت رمز شده برای بازرگان می‌فرستد. اگر چه این روش در دسترس است، با این حال مشکلات خاص خود را دارد. بطور مثال اشخاصی که شماره کارت و تاریخ اعتبار را مورد دستبرد قرار دهند به راحتی می‌توانند از طریق آن به خرید اینترنتی بپردازند. خود بازرگان ممکن است از شماره کارت سوء استفاده کرده و یا با ایجاد یک صفحه خرید تقلبی، می‌توان اطلاعات مشتری را سرقت نمود. این مشکلات شرکتهای ارائه دهنده خدمات کارت اعتباری را به سمت پیاده سازی پروتکلهای دیگری سوق داد که علاوه بر پیاده سازی ساده تر نسبت به پروتکل *SET*، حتی‌الامکان بتوان مشکلات ناشی از خرید جنس با شماره کارت سرقت شده و یا سوء استفاده از شماره کارت توسط بازرگان را کاهش داد.

بطور کلی مزایای خرید به وسیله کارت اعتباری را میتوان استفاده از یک شماره کارت برای انجام معامله که موجب آسان شدن خرید اینترنتی می‌گردد و گستردگی زیاد جغرافیایی به دلیل عدم نیاز خریدار به امکانات خاص برای خرید اینترنتی عنوان کرد. با این حال این معاملات دارای مشکلات خاص خود نیز هستند، از جمله اینکه هر کسی که شماره کارت و تاریخ اعتبار آن را سرقت کند یا بازرگانی که شماره کارت برای وی ارسال می‌شود می‌تواند از آن سوء استفاده کند. بنابراین به نظر می‌آید که در صورتی که بتوان به نحوی شخصی که قصد معامله با کارت اعتباری را دارد احراز اصالت کرد و ثابت کرد که کسی که هم اکنون در حال معامله با کارت است خود صاحب کارت می‌باشد، می‌توان مشکل دستبرد شماره کارت را تا حد زیادی حل نمود. این کار موجب می‌شود که بازرگانان نیز حتی اگر به شماره کارت مشتری دسترسی پیدا کنند، نتوانند بدون داشتن اطلاعات خاص مشتری که می‌تواند امضای دیجیتال او و یا یک نام کاربری و کلمه عبور باشد، از شماره کارت سوء استفاده کنند.

موجودیتهای زیر در انجام معاملات کارتهای اعتباری درگیر هستند:

دارنده کارت[4] (که مشتری نیز نامیده می‌شود) مالک قانونی کارت اعتباری است که می تواند از طریق رایانه شخصی و اینترنت، کالای مورد نیاز خود را خریداری نماید. بازرگان[5] که شخص یا سازمانی است که کالا یا خدمات خود را از طریق وبگاه خود به مشتریها عرضه می‌کند. بازرگان می‌تواند کارت اعتباری شرکتهای مختلف را قبول نماید. صادرکننده[6]، موسسه‌ای است که قابلیت صدور کارت اعتباری را دارا می باشد. این موسسه، مسئولیت بدهی مالی مشتری را بعهده دارد. بانک بازرگان[7] که یک موسسه مالی است که برای بازرگان حساب باز کرده و کسب مجوز جابجایی مالی و عملیات پرداخت را به عهده دارد. از آنجایی که بازرگانان ممکن است چند نوع کارت اعتباری مختلف را قبول کنند و مایل به درگیری با موسسات مختلف برای تسویه‌حساب

---

[1] *Secure Electronic Transaction*
[2] *Public Key Infrastructure*
[3] *Secure Socket Layer*
[4] *Cardholder*
[5] *Merchant*
[6] *Issuer*
[7] *Acquirer*

نیستند، بانک بازرگان مسئولیت ارتباط با موسسات مالی مختلف را نیز به عهده می‌گیرد. سرویس دهنده‌های پرداخت اینترنتی[1] که برخی مواقع با نام دروازه پرداخت نیز شناخته می‌شوند.سرویس دهنده ها که می‌توانند بخشی از بانک فروشنده یا یک موجودیت دیگر باشند، در پروتکل پرداخت، وظیفه ارتباط موجودیتهای مختلف را بعهده دارند. از طرف دیگر سرویس دهنده های پرداخت می‌توانند وظایف نرم افزاری بازرگان را به عهده گرفته و عملیات مربوط به بازرگان در پروتکل را به نمایندگی از وی انجام دهند. مرجع صدور گواهینامه[2] که یک موسسه شناخته شده است موجودیتی است که گواهینامه را برای دارندگان کارت، بازرگانها و موسسات مالی صادر می‌کند. استاندارد متداول برای این منظور، استاندارد *X.509* است.

تلاش برای ارائه جایگزین عملی برای پروتکل *SET* منجر به طراحی پروتکلهای دیگری گردید که مهمترین آنها، دو پروتکل *UCAF/SPA*[3] از شرکت مسترکارت و پروتکل *3D Secure* از شرکت ویزا می‌باشد. هم اکنون پروتکل *SET* بطور کامل کنار رفته و هر دو شرکت ویزا و مسترکارت پروتکل *3D Secure* را پیاده سازی کرده و در حال ترویج آن هستند.

۳- معرفی پروتکل *3D Secure*

پروتکل *3D Secure* در سال ۲۰۰۱ توسط شرکت ویزا طراحی شد و مدتی بعد شرکت مسترکارت نیز ویرایشی از آن را پیاده سازی کرد. شرکت ویزا در توجیه طراحی این پروتکل بیان کرده که تا ماه ژولای سال ۲۰۰۱، برگشت پول در معاملات اینترنتی چند برابر متوسط سیستم شده بود *[۳]* . در تحقیقاتی که شرکت ویزا انجام داد این نتیجه بدست آمد که در صورتی که در زمان انجام معامله، دارنده کارت به درستی احراز اصالت شود، ۸۰ درصد از برگشت پول و تقلب در معاملات کاهش خواهد یافت *[۳]*. در این پروتکل، موجودیتهای درگیر در سه دامنه تقسیم شده اند. این دامنه ها عبارتند از دامنه صادرکننده ،دامنه میانی[4] و دامنه بانک بازرگان.

دامنه صادرکننده شامل موجودیتهای دارنده کارت، صادرکننده و کارگزار کنترل دسترسی میباشد.

دامنه بانک بازرگان شامل موجودیتهای بازرگان، کارگزار *MPI*[5] که روند تراکنش از جمله پیامهای مربوط به احراز اصالت شماره کارتی که از نرم افزار وبگاه[6] بازرگان برای وی فرستاده شده است و همچنین بررسی امضای صادرکننده را بعهده دارد و بانک بازرگان می‌شود.

دامنه میانی شامل کارگزار راهنما (*DS*)[7] (یک پایگاه داده که کلیه شماره کارتهای صادرشده توسط صادرکننده ها را در درون خود دارد)، مرجع صدور گواهینامه تجاری و مرجع صدور گواهینامه ویزا، کارگزار ثبت اطلاعات احراز اصالت و همچنین شامل *VisaNet*(یک شبکه بین‌المللی تحت نظارت شرکت ویزا که دریافت پیام مجوز از بانک بازرگان و ارسال آن برای بانک صادر کننده و برگرداندن جواب آن و همچنین جابجایی مالی بین بانکها را به عهده دارد) است.

پروتکل *3D Secure* دو بخش دارد. بخش اول، ثبت نام است که در آن دارنده کارت باید وارد وبگاه صادرکننده کارت خود شده و اطلاعات شخصی خود را با صادرکننده هماهنگ نماید. این بخش تنها یک بار انجام شده و دیگر نیازی به تکرار ندارد. بخش دوم، پروتکل پرداخت اینترنتی است که در آن دارنده کارت عملیات خرید از وبگاه بازرگان را انجام می‌دهد.

عملیات ثبت نام به صورت زیر انجام می‌پذیرد:

---

[1] *Internet Payment Service Provider*
[2] *Certificate Authority*
[3] *Universal Cardholder Authentication Field/ Secure Payment Algorithm*
[4] *Interoperability Domain*
[5] *Merchant Plug In*
[6] *Web Page*
[7] *Directory Server*

مرحله اول: مشتری وارد وبگاه صادرکننده کارت اعتباری شده و وارد بخش مربوط به ثبت نام در پروتکل 3D Secure می‌شود. پس از آن، مشتری به کارگزار ثبت نام متصل می‌شود.

مرحله دوم: مشتری برای اثبات موجودیت خود، شماره کارت اعتباری و دیگر اطلاعات شخصی خود را (که قبلا و در زمان انعقاد قرارداد برای دریافت کارت اعتباری به صادرکننده داده بود) را وارد می‌کند. سپس یک کلمه عبور و یک پیام اطمینان شخصی[1] با صادرکننده خود هماهنگ می‌کند.

مرحله سوم: صادرکننده بررسی می‌کند که آیا اطلاعات دارنده کارت صحیح است یا خیر.

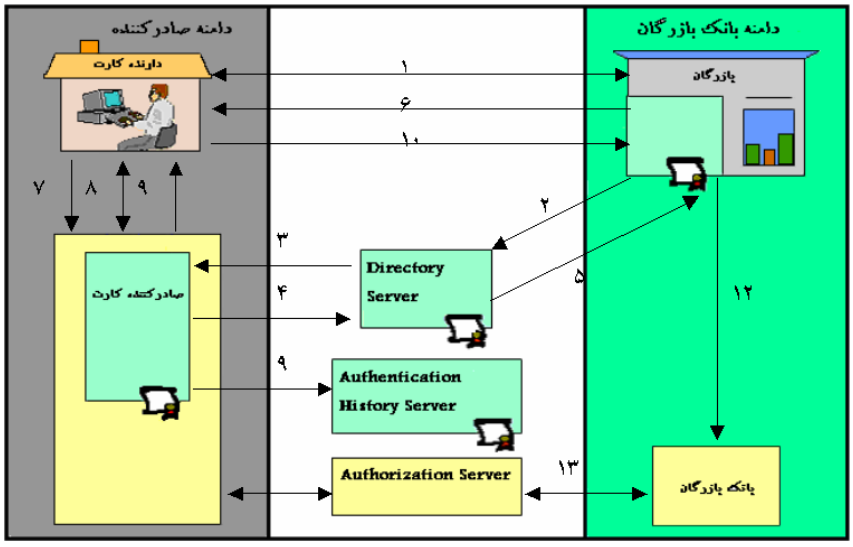
مرحله چهارم: در صورت صحت، اطلاعات در یک پایگاه داده ذخیره می‌شود و نتیجه آن به مشتری اطلاع داده می‌شود. حال مشتری می‌تواند از طریق سیستم *3D Secure* به معامله بپردازد.

ابزاری که برای ایجاد امنیت در مسیر مبادلات و جلوگیری از شنود شماره کارت اعتباری، کلمه عبور و دیگر اطلاعات استفاده می‌شود، *SSL/TLS* است. در پروتکل *3D Secure*، بر استفاده از *SSL/TLS* در کلیه مسیرها تاکید شده است. این *SSL/TLS* باید ۱۲۸ بیت یا بیشتر را حمایت کند، با این حال همانگونه که خود شرکت ویزا اظهار داشته ، به دلیل عدم امکان صادرات ابزار رمز نگاری قدرتمند، مسیرهای ارتباطی مشتری می‌تواند از رمزنگاری با قدرت ٤٠ بیت استفاده نماید*[٤]*.

مراحل تراکنش در پروتکل *3D Secure* که بصورت شماتیک در شکل ۵-۱ نشان داده شده است به شرح زیر است:

مرحله اول: دارنده کارت وارد وبگاه بازرگان می‌شود و خرید خود را انجام می‌دهد.وی پس از مطمئن شدن از کالا و قیمت خرید خود، شماره کارت، تاریخ انقضا و آدرس خود را وارد می‌نماید.

مرحله دوم: نرم افزار وبگاه بازرگان از *MPI* می‌خواهد که صحت شماره کارت و ثبت نام را بررسی کند. *MPI* یک درخواست بررسی ثبت نام برای *DS* می‌فرستد. این پیام *VEReq*[2] نام دارد.



شکل ۱ : روند تراکنش در پروتکل *3D Secure*

مرحله سوم: *DS* ابتدا محتویات پیام و صحت اطلاعات آن را بررسی می‌کند. سپس *DS* بررسی می‌کند که آیا این شماره کارت معتبر بوده و متعلق به یکی از صادرکننده‌ها می‌باشد یا خیر. در صورت وجود این شماره کارت، *DS* از پیام *VEReq* که بازرگان برای وی فرستاده، کلمه عبور را برداشته و آن را برای کارگزار کنترل دسترسی ارسال می‌کند.

---

[1] *Personal Assurance Message*
[2] *Verify Enrollment Request*

مرحله چهارم: کارگزار کنترل دسترسی به پایگاه داده خود مراجعه می‌کند تا ببیند که آیا شماره کارت مذکور قبلا مراحل ثبت نام را پشت سر گذاشته است یا خیر. سپس پاسخ را به *DS* برمی‌گرداند. این پاسخ *VERes*[1] نام دارد.

مرحله پنجم: *DS* این پیام را برای بازرگان ارسال می‌کند. *MPI* پیام را دریافت کرده و صحت و عدم صحت شماره کارت را بررسی می‌کند.

مرحله ششم: بازرگان یک پیام درخواست احراز اصالت برای صادرکننده کارت اعتباری مشتری می‌فرستد. او این کار را از طریق رایانه کاربر و با پست کردن پیام خود به کارگزار صادرکننده انجام می‌دهد. این پیام *PAReq*[2] نامیده می‌شود.

مرحله هفتم: کارگزار کنترل دسترسی پیام درخواست احراز اصالت را از رایانه مشتری دریافت کرده و صحت آن را بررسی می‌کند.

مرحله هشتم: کارگزار کنترل دسترسی یک صفحه روی رایانه مشتری باز می‌کند. در این صفحه، صادرکننده نشان ویزا، نشان خودش، نام بازرگان، مبلغ معامله، چهار رقم آخر شماره کارت و پیام اطمینان شخصی را به مشتری نشان می‌دهد. سپس از مشتری می‌خواهد که در صورتی که این اطلاعات را قبول دارد، کلمه عبور خود را وارد کند. مشتری در صورت تایید، کلمه عبور را وارد کرده و کلید تایید را فشار می‌دهد. اطلاعات برای صادرکننده فرستاده می‌شود. در صورتی که کلمه عبور مشتری درست باشد، صادرکننده پیام پاسخ احراز اصالت را ایجاد کرده و آن را امضا می‌کند(*PARes*)[3].

مرحله نهم: صادرکننده پاسخ را برای بازرگان ارسال می‌کند. این کار از طریق وبگرد مشتری انجام می‌پذیرد.

مرحله دهم: *MPI* صحت ساختار پیام پاسخ احراز اصالت را بررسی می‌کند.

مرحله یازدهم: وارسی امضای صادرکننده، عملی است که در این مرحله انجام می‌شود. این کار می‌تواند توسط *MPI* بازرگان و یا توسط کارگزاردیگری که قابلیت انجام این کار را دارد، انجام می‌شود.

مرحله دوازدهم: این مرحله مربوط به روند جابجایی مالی است. در این مرحله بازرگان اطلاعات را برای بانک خود می‌فرستد تا عملیات جابجایی مالی با بانک بازرگان را پیگیری نماید.

با توجه به اجباری بودن استفاده از *SSL* در مسیرهای تراکنش، آنچه که برای کلیه موجودیتهای پروتکل به غیر از مشتری اجباری است، داشتن گواهینامه کارگزار *SSL*[4] و گواهینامه کارفرمای *SSL*[5] می‌باشد. با این شرط، هر دو موجودیتی که بخواهند با همدیگر ارتباط *SSL* داشته باشند نیازمند گواهینامه هستند و تنها در صورتی که گواهینامه طرفین معتبر باشد امکان برقراری ارتباط *SSL* وجود دارد. بنابراین طرفین ارتباط می‌توانند مطمئن باشند که مخاطب آنها شخص مورد نظر است. این مسئله در مورد مشتری صدق نمی‌کند. وبگردهای رایانه های خانگی معمولا فاقد گواهینامه معتبر هستند. این مسئله موجب می‌شود که مشتری برای معامله نیازی به داشتن گواهینامه روی رایانه خود نداشته باشد. از جمله مزایای *SSL* این است که می‌تواند بدون نیاز به گواهینامه کارفرما ارتباط را ایجاد نماید و نتیجتاً نیاز مشتری به نصب گواهینامه روی رایانه را از بین می‌برد و امکان انجام معامله روی هر رایانه‌ای را برای وی فراهم می‌آورد.

٤- ضعفهای پروتکل *3D Secure* و پیشنهاداتی جهت رفع آنها

از ابتدای آوریل سال ۲۰۰۳ میلادی، بانکهای بازرگان در تمامی نقاط دنیا موظف به پذیرش پروتکل *3D Secure* برای

---

[1] *Verify Enrollment Response*
[2] *Payer Authentication Request*
[3] *Payer Authentication Response*
[4] *SSL Client Certificate*
[5] *SSL Server Certificate*

بازرگانان اینترنتی خود شدند*[٥]*. شرکتهای بزرگ دیگر مانند مسترکارت نیز به سمت پیاده سازی این پروتکل روی آوردند تا جایی که به نظر می‌رسد که پروتکل *3D Secure* بعنوان مطرح‌ترین پروتکل پرداخت کارت اعتباری حال حاضر دنیا در حال باز کردن جای خود است. بنابراین بررسی نقاط ضعف این پروتکل نیز می‌تواند اهمیت ویژه‌ای داشته باشد. در این بخش به بررسی برخی نقاط ضعف *3D Secure* و ارائه پیشنهاداتی در رابطه با آن پرداخته می‌شود.

۴-۱ شنود در گره مشتری

پروتکل امنیتی *SSL* تنها امنیت در طول کانال ارتباطی را تضمین می‌کند . امنیت در گره‌ها از جمله گره مشتری توسط این پروتکل تضمین نشده است. بنابراین یکی از اهداف حمله می‌تواند گره مشتری باشد که ناامن ترین گره در شبکه معاملاتی است. با توجه به ماهیت متکی بودن بر کلمه عبور در پروتکل، یکی از حملاتی که می‌توان علیه این پروتکل طرح کرد نصب یک شنودگر صفحه کلید روی رایانه در مکانهای عمومی خرید است. این حمله را به هر سیستم پرداخت می‌توان اعمال کرد. یکی از روشهایی که برای این مشکل پیشنهاد شده است استفاده از کلمات عبور یکبار مصرف[1] می‌باشد. این کلمات عبور یکبار مصرف نه تنها برای این منظور قابل استفاده هستند، بلکه برای جلوگیری از هرگونه شنود اینترنتی نیز قابل استفاده می‌باشند. این مشکل برای *SET* وجود ندارد، زیرا *SET* بجز در رایانه شخصی که گواهینامه شخص بهمراه کیف پول نصب شده باشد قابلیت معامله ایجاد نمی‌کند. از طرفی با فرض نصب بودن نرم افزار *SET* روی رایانه های عمومی، جابجا کردن گواهینامه توسط خریدار و نصب آن روی رایانه عمومی امری خطرناک و کاملا ناامن می‌باشد. بنابراین این حمله را نه فقط در رابطه با پروتکل *3D Secure*، بلکه برای سیستمهای کارت اعتباری دیگر که بر مبنای کلمه عبور احراز اصالت انجام می‌دهند نیز می‌توان تصور کرد. به مشتری توصیه می‌شود که هر بار پس از انجام عمل خرید در یک مکان عمومی، در اولین فرصت نسبت به تعویض کلمه عبور و پیام اطمینان شخصی خود اقدام کند.

۴-۲ حمله در مسیر بازرگان-مشتری و مشتری-صادرکننده کارت

سست ترین مسیرهای ارتباطی در پروتکل *SSL* ، مسیر بازرگان- مشتری و مسیر مشتری- صادرکننده کارت است. این مسیرها معمولا به دلیل عدم استفاده مشتری از *SSL* ۱۲۸ بیتی ، ناامن ترین بخش پروتکل می‌باشد. پروتکل *SSL* روی رایانه های شخصی از سال ۲۰۰۰ به بعد ۱۲۸ بیتی شده است، ولی در وبگردهای صادراتی، ۸۸ بیت، شناخته شده و تنها ٤٠ بیت از دید دشمن تصادفی می‌باشد که براحتی قابل شکستن و شنود است. بنابراین از آنجا که در رد و بدل کردن پیامها، ساختار پیامها کاملا از طرف ویزا مشخص شده است، اعمال یک حمله جستجوی کامل از طرف سازمانها یا اشخاصی که امکانات نسبتا مناسبی داشته باشند، چندان مشکل به نظر نمی‌رسد. از آنجایی که داشتن *SSL* ۱۲۸ بیتی برای هر شخص، نیازمند خرید آن و داشتن گواهینامه‌های مربوط می‌باشد و یکی از اهداف طراحی سیستم *3D Secure* ساده شدن کار برای مشتری و قابلیت انجام معامله در هر مکان دلخواه است، امنیت پروتکل در این بخش با سادگی معامله، معاوضه شده است.

۴-۳ ارسال داده های غلط توسط بازرگان برای اجناس خریداری شده

پیام *PAReq* که بازرگان برای کارگزار کنترل دسترسی می‌فرستد، حاوی داده ها و توافقهایی با مشتری است که توسط وی قابل مشاهده نمی‌باشد. این داده ها می‌توانند برخلاف توافق با مشتری برای کارگزار کنترل دسترسی فرستاده شوند. از جمله این

[1] *One Time PIN*

اطلاعات دامنه توصیف سفارش[1] است.

دو مشکل در این رابطه وجود دارد. یکی اختیاری بودن ارسال دامنه توصیف سفارش و دیگری پنهان بودن دامنه توصیف سفارش از دید خریدار. این دامنه در حین فرایند احراز اصالت مشتری از سوی کارگزار کنترل دسترسی الزاما در اختیار مشتری قرار نمی‌گیرد[۶].

برای جلوگیری از ارسال داده های غلط در توصیف سفارش بوسیله بازرگان، باید صادرکننده ملزم به نمایش مختصر توصیف سفارش در صفحه احراز اصالت باشد. بنابراین در صورت هرگونه عدم تطابق محتویات با خرید مشتری، مشتری از وارد کردن کلمه عبور خودداری می‌کند. در صورتی که مشتری مایل به ثبت اطلاعات خرید خود نباشد (محرمانه بودن اطلاعات خرید از دید صادرکننده)، می‌تواند در این مورد با بازرگان توافق کند. بازرگان در یک دامنه جداگانه در پیام احراز اصالت توافق با مشتری را به اطلاع صادرکننده می‌رساند. در این حالت در صفحه احراز اصالت بجای نمایش لیست اجناس خریداری شده، صادر کننده به مشتری پیام می‌دهد که وی درخواست عدم ثبت سفارشات خود را داشته است. مشتری در صورت عدم توافق و یا پشیمانی می‌تواند از وارد کردن کلمه عبور خود خودداری کند.

۴-۴ جعل صفحه احراز اصالت صادرکننده از طرف بازرگان

بازرگان می‌تواند حتی بدون اینکه عضوی از سیستم *3D Secure* باشد اطلاعات مشتری را بدست آورد، به این صورت که مشتری وارد سایت بازرگان شده و اطلاعات کارت اعتباری و دیگر اطلاعات را وارد می‌کند. پس از آن، بازرگان می‌تواند بجای ارسال اطلاعات برای دامنه میانی و بررسی ثبت نام مشتری، خود را به جای صادرکننده جا زده و در رایانه مشتری، یک صفحه احراز اصالت مانند صفحه صادرکننده کارت باز نماید و از وی درخواست کند که کلمه عبورخود را وارد نماید. مشتری به تصور اینکه این صفحه از طرف صادرکننده کارت باز شده است کلمه عبور خود را وارد می‌نماید. پس از فشار کلید تایید از طرف مشتری، اطلاعات بجای ارسال برای صادرکننده، برای بازرگان فرستاده می‌شود.

شرکت ویزا با وقوف به امکان وجود چنین حمله ای، سعی در برطرف کردن آن داشته است، به این صورت که مشتری در زمان ثبت نام و وارد کردن اطلاعات در سایت شرکت صادرکننده کارت، یک پیام اطمینان شخصی را وارد می‌کند. از این پیام بعنوان اطلاعات مشترکی که تنها دارنده کارت و صادرکننده از آن اطلاع دارند استفاده می‌شود و هدف این است که مشتری پیش از وارد کردن کلمه عبور، به پیام اطمینان شخصی نگاه کرده و اگر پیامی بود که خود او در زمان ثبت نام در وبگاه صادرکننده وارد کرده بود، مطمئن شود که این صفحه از طرف صادرکننده کارت باز شده و پس از اطمینان، کلمه عبور خود را وارد کند. علیرغم بکارگیری تمهید مذکور باز هم ایراداتی باقی می‌ماند:

۱- اگر چه اکیدا توسط شرکت ویزا توصیه شده که پیش از ورود کلمه عبور، پیام اطمینان شخصی کنترل شود، ولی همه مشتری ها در هنگام وارد کردن کلمه عبور به این نکته توجه نمی‌کنند.

۲- باز هم روشی برای بدست آودن پیام اطمینان شخصی توسط بازرگان یا هر شخص حمله کننده دیگر وجود دارد و آن روش بریدن صفحه[2] می‌باشد. در این روش، اطلاعات صفحه نمایش رایانه دارنده کارت شنود می‌شود. نرم افزارهای برش صفحه نیز به وفور روی شبکه اینترنت یافت می‌شود و بنابراین انجام این حمله کار بسیار سختی نخواهد بود.

همانگونه که دیده شد، بازرگان می‌تواند با استفاده از تکنیکهای خاص، حتی از پیام اطمینان شخصی خریدار اطلاع یابد. پس از بدست آوردن پیام اطمینان شخصی، او می‌تواند در مراجعه بعدی مشتری، صفحه احراز اصالت را بطور کامل جعل کرده و

---

[1] *Order Description Field*
[2] *Screen Scrapping*

کلمه عبور مشتری را به دست آورد. هر چند که شماره کارت اعتباری به تنهایی برای انجام معامله کافی نیست، با این حال شرکتهای ارائه کننده کارت اعتباری، برای فاش نبودن شماره کارت، ارزش امنیتی قائل بوده و یکی از ایراداتی که به *3D Secure* می‌گیرند، فاش بودن شماره کارت اعتباری در این پروتکل برای بازرگان می‌باشد*[۷]*. بنظر می‌آید در صورتی که بتوان حتی بخشی از شماره کارت اعتباری را از دید بازرگان مخفی کرد، می‌توان امنیت بیشتری به معامله و دلگرمی بیشتری به خریدار بخشید. برای این منظور ساختار شماره کارتهای اعتباری مورد بررسی قرار می‌گیرد:

رقم شروع شماره کارتهای اعتباری نشان دهنده نوع کاربردی است که صادرکننده بر مبنای آن کارت را صادر کرده است.به این رقم که اولین رقم سمت چپ شماره کارت است، نشانگر اصلی کاربرد (*MII*)[1] گفته می‌شود. ٦ رقم سمت چپ شماره کارت اعتباری (مشتمل بر *MII*)، نشانگر صادرکننده می‌باشد. این ٦ رقم دارای یک پیشوند شرکت ارائه دهنده کارت می‌باشد. باقیمانده این ۶ رقم می‌تواند به صادرکننده‌هایی که کارت اعتباری این شرکتها را ارائه می‌دهند تعلق گیرد. با توجه به این مسئله، شرکت ویزا که پیشوند تک رقمی ۴ را دارد، با توجه به باقی ماندن ۵ رقم دیگر قادر است به ۱۰۰۰۰۰ شرکت، مجوز صدور کارت اعتباری خود را بدهد. پیشوند شرکت مسترکارت، ۵۱ و ۵۵ می‌باشد. بجز رقم آخر در شماره کارت اعتباری که برای اثبات صحت ساختار شماره کارت اعتباری بکار می‌رود، دیگر ارقام باقی‌مانده، شماره حساب می‌باشند.بنابراین در یک شماره کارت اعتباری ١٦ رقمی ویزا، ۹ رقم مربوط به شماره حساب است و هر صادرکننده کارت اعتباری ویزا می‌تواند تا یک میلیارد شماره صادر کند. شماره آخر در کارتهای اعتباری به رقم کنترل[2] معروف است.

یک روش پیشنهادی برای عدم ارسال ارقام به طور کامل، ارسال بخشی از شماره کارت اعتباری بجای شماره کامل آن است. بطور مثال، فرض کنید که ۵ رقم سمت راست از یک شماره کارت ١٦ رقمی ویزا در صفحه اینترنتی بازرگان وارد نشود. از آنجا که رقم آخر ، رقم کنترل می‌باشد، آشکار بودن این رقم برای بازرگان، فضای جستجوی وی را کاهش داده و وی تنها به دنبال شماره کارتهایی می‌گردد که رقم کنترلی مطابق با رقم کنترل ارسال شده را تولید کند. با توجه به اینکه رقم کنترل می‌تواند توسط الگوریتم خاصی و از روی دیگر ارقام شماره کارت بدست آید، عدم ارسال ۵ رقم آخر، ٤ رقم مجهول (۱۰۰۰۰ شماره مختلف) برای بازرگان ایجاد می‌کند. بدیهی است که بازرگان برای تحقق سوء استفاده خود می‌تواند با ارسال شماره های متعدد و بررسی ثبت نام آنها در پایگاه اطلاعاتی ویزا ، به شماره کارت صحیح دست پیدا کند. در واقع این راه حل، وسیله‌ای برای سخت‌تر کردن کار بازرگان و یا هر سایت خرید جعلی است که قصد بدست آوردن اطلاعات مشتری را دارد.

بنظر می‌آید که عدم ارسال تعدادی از ارقام شماره کارت، جستجوی شماره کارت در *DS* و بررسی ثبت نام آن در صادرکننده را با مشکل روبرو کند. با این حال بررسی انجام شده در مرجع [۸] نشان می‌دهد که عدم ارسال تعداد محدودی از ارقام شماره کارت عملا تاثیری بر روند بررسی وضعیت کارت اعتباری نخواهد داشت.

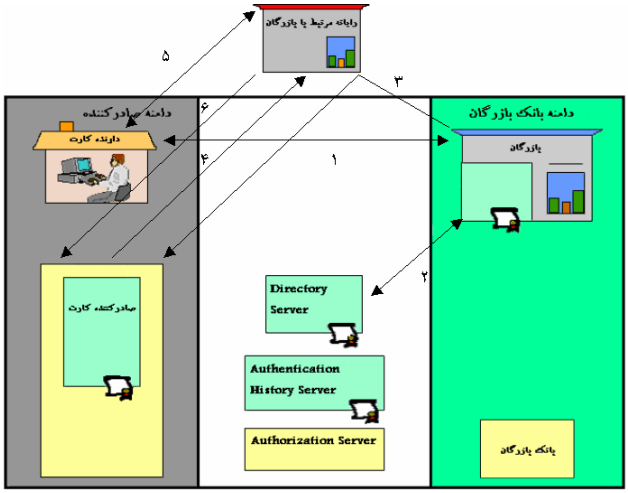
۵- طراحی یک حمله به پروتکل *3D Secure*

ویژگیهای خاصی که پروتکل *3D Secure* بر مبنای آن طراحی شده است، نقاط ضعف عمده ای را برای آن فراهم می‌کند. گذشته از موارد ذکر شده در بخش قبل، از جمله نقاط ضعف این پروتکل این است که عدم وجود کیف پول روی رایانه مشتری که بتواند روی جابجایی پیامها نظارت داشته باشد می‌تواند مشکلاتی را برای این سیستم فراهم کند. این مشکل بویژه در هنگام ارسال پیام درخواست احراز اصالت که بازرگان از طریق رایانه مشتری برای صادرکننده می‌فرستد خود را نمایان می‌کند. ارسال این پیام توسط مشتری قابل مشاهده نمی‌باشد و بنابراین مشتری اطلاعی از ردوبدل شدن این پیام و مقصد آن پیدا نمی‌کند. در

---

[1] *Major Industry Identifier*
[2] *Check Digit*

ادامه و بر اساس نقطه ضعف مذکور حمله‌ای به این پروتکل مطابق روند شکل ۱ ارائه می‌گردد.



شکل ۱ : روند حمله به پروتکل *3D Secure*

مرحله اول: مشتری وارد سایت بازرگان شده و اطلاعات خرید خود را وارد می‌کند (شماره کارت و تاریخ اعتبار)

مرحله دوم: بازرگان به *DS* مراجعه کرده و از صحت شماره کارت و ثبت نام مشتری مطمئن می‌شود.

مرحله سوم: بازرگان بجای آنکه پیام درخواست احراز اصالت را از طریق رایانه مشتری به صادرکننده بفرستد، آن را از طریق یک رایانه مرتبط با خود که در مکان دیگری مستقر است می‌فرستد.

مرحله چهارم: صادرکننده صفحه احراز اصالت خود را در رایانه مرتبط با بازرگان باز می‌کند.در این زمان، بازرگان به پیام اطمینان شخصی مشتری دسترسی پیدا می‌کند.

مرحله پنجم: با دانستن پیام اطمینان شخصی، رایانه مرتبط با بازرگان این بار ازطرف صادرکننده یک صفحه روی رایانه مشتری باز می‌کند که همراه با نشان دادن پیام اطمینان شخصی از وی درخواست وارد کردن کلمه عبور را می‌نماید. مشتری با وارد کردن کلمه عبور، اطلاعات خود را بطور کامل در اختیار بازرگان قرار می‌دهد.

مرحله ششم: رایانه مرتبط با بازرگان کلمه عبور را در صفحه مربوط به صادرکننده قرار می‌دهد. این صفحه برای صادرکننده فرستاده می‌شود.

مرحله هفتم: بازرگان کالا را برای مشتری می‌فرستد. بنابراین مشتری هیچگونه شکی به روند انجام معامله نمی‌کند و در نتیجه شکایتی نیز علیه بازرگان وجود نخواهد داشت.

مرحله هشتم: هم اکنون بازرگان کلیه اطلاعات مشتری را دارا می‌باشد. هر گونه استفاده از اطلاعات مشتری با توجه به دارا بودن کلمه عبور، موجب استرداد مبلغ توسط صادرکننده و زیان وی خواهد شد.

نکته ای که در رابطه با این حمله به چشم می‌خورد این است که ارتباطی که رایانه واسط با رایانه مشتری ایجاد می‌کند، *SSL* نمی‌باشد. در این صورت نشانه قفل *SSL* در پایین وبگرد مشتری دیده نمی‌شود. در صورتی که مشتری از ارتباط امن و *SSL* اطلاع داشته باشد، متوجه مشکلی در ارتباط امن با صادرکننده خواهد شد. ولی در حالت کلی این مورد توسط عموم مردم قابل شناسایی نیست. بویژه این ویژگی که خریدار پیام اطمینان شخصی خود را در صفحه احراز اصالت می‌بیند و بنابراین احتمال ظنین شدن او به روند معامله بسیار کم خواهد بود. شرکت ویزا به دارنده‌های کارت خود توصیه کرده است که در کنار بررسی پیام اطمینان شخصی، آدرس اینترنتی بالای صفحه احراز اصالت خود را کنترل کنند تا مطمئن شوند که صفحه از طرف صادرکننده کارت آنها باز شده است. با این حال، حمله کننده می‌تواند *IP* صادرکننده را جعل کرده و صفحه را با *IP* صادرکننده برای مشتری بفرستد. در کنار آن، صفحه نیز به گونه ای طراحی می‌شود که فشار کلید تایید از طرف مشتری، اطلاعات او را به *IP* رایانه واسط برگرداند.

در صورتی که حمله کننده بخواهد ارتباط وی با خریدار ارتباط *SSL* باشد تا باز هم شک کمتری ایجاد نماید، این کار امکان پذیر خواهد بود. در این هنگام، روند حمله اندکی تفاوت خواهد کرد. به این صورت که در مرحله سوم و زمانی که بازرگان پیام درخواست احراز اصالت را از مسیر رایانه میانی برای صادرکننده می‌فرستد، یک پیام دلخواه نیز از مسیر رایانه دارنده کارت به رایانه میانی ارسال می‌دارد. رایانه میانی باید مجهز به کارگزار *SSL* و گواهینامه باشد. برای ارتباط *SSL* نیازی به معتبر بودن گواهینامه نیست. با این حال به مشتری ناشناس بودن گواهینامه اطلاع داده می‌شود و اجازه ورود به صفحه یا عدم ورود از وی خواسته می‌شود.مشتریهایی که بدون دقت لازم، اجازه ورود به صفحه را بدهند، وارد صفحه ای می‌شوند که از نظر ظاهری هیچگونه تفاوتی با صفحه صادرکننده نخواهد داشت. با این حال اگر کسی ریشه *SSL* را با کلیک کردن قفل پایین صفحه بررسی کند، می‌تواند از ناشناس بودن گواهینامه اطلاع حاصل نماید. با این حال در حالت کلی و از لحاظ ظاهری، صفحه اینترنتی با صفحه صادرکننده تفاوتی نخواهد داشت. این حمله می‌تواند توسط کنترلهای خاص مشتری از جمله بررسی گواهینامه و یا وجود یا عدم وجود ارتباط *SSL* شناسایی شود. ولی با توجه به اینکه عموم از این ابزار اطلاعی ندارند، این حمله در اکثر مواقع موفقیت آمیز خواهد بود.

نکته دیگر این است که این حمله می‌تواند از طرف یک حمله کننده غیر از بازرگان نیز انجام پذیرد. جزئیات این حمله در مرجع [۸] آورده شده است.

٦- نتیجه‌گیری

در این مقاله ملاحظه شد که پروتکلهای متعددی برای خرید اینترنتی توسط کارت اعتباری طراحی و پیاده‌سازی شده‌اند. هر کدام از این پروتکلها مزایا و معایب خاص خود را دارند. پروتکل *SET* بعنوان قدرتمندترین پروتکل کارت اعتباری که براساس امضای دیجیتال کار می‌کرد وارد عمل شد و بسرعت نیز از صحنه رقابت با پروتکلهای ساده‌تر کنار رفت. پروتکلهای ساده معمولاً پروتکلهایی هستند که دارنده کارت را بر اساس کلمه عبور احراز اصالت می‌کنند. این مسئله موجب می‌شود که انجام معامله برای کاربر ساده‌تر شود. بنابراین سعی شرکتهای ارائه دهنده کارت اعتباری بر این شد که به سمت پروتکلهایی حرکت کنند که علاوه بر مبتنی بودن بر کلمه عبور، امنیت قابل قبولی نیز به کاربر خود ارائه دهند. هم اکنون کاربرد پروتکل *3D Secure* که توسط شرکت ویزا طراحی شده است در حال گسترش است، به نحوی که شرکت مسترکارت نیز ویرایشی از این پروتکل را پیاده‌سازی نموده است. در این مقاله، پروتکل *3D Secure* به عنوان یک پروتکل پیشرو مورد بررسی قرار گرفت و نقاط ضعف و قوت آن مطرح شد. در ادامه پیشنهاداتی در راستای بکارگیری با حاشیه امنیتی بیشتر این پروتکل مطرح و در نهایت سناریوی جدیدی برای حمله به پروتکل مذکور ارائه شد که به خوبی گویای باز بودن عرصه تحقیق و توسعه به منظور دستیابی به پروتکل پرداخت امن و کارآمد است.

مراجع

[1] Bellare, M., Garay, J. A., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., Herreweghen, V., Waidner, M., "Design, Implementation, and Deployment of the iKP Secure Electronic Payment System", IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 4, April 2000*

[2] Gpayments Inc. "Visa 3D Secure vs. Mastercard SPA, A comparison of online Authentication Standards", Authentication and Payment Solutions whitepaper*, March 2002*

[3] Visa International, "3D Secure Introduction", Visa International Service Association, *Publication 70001-01, Version 1.0.2, September 26, 2002.*

[4] Visa International, "3D Secure Protocol Specifications, Core Functions", Visa International Service Association, *Publication 70000-01, Version 1.0.2, July 16, 2002, Errata as of January 20, 2004.*

[5] Nakagawa, C., "Securing ePayment, A Survey", GIAC Security Essentials Certification (GSEC), September 20, 2004.

[6] Visa International, "3D Secure Functional Requirements, Access Control Server", Visa International Service Association, *Publication 70002-01, Version 1.0.2, July 16, 2002, Errata as of January 20, 2004.*

[7] European Committee for Banking Standards, "Secure Card Payments on The Internet", Version 1.0, November 2002.

[۸] کلینی، م. *امنیت در پروتکلهای پرداخت الکترونیکی*، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، پایان نامه کارشناسی ارشد، فروردین ۱۳۸۴