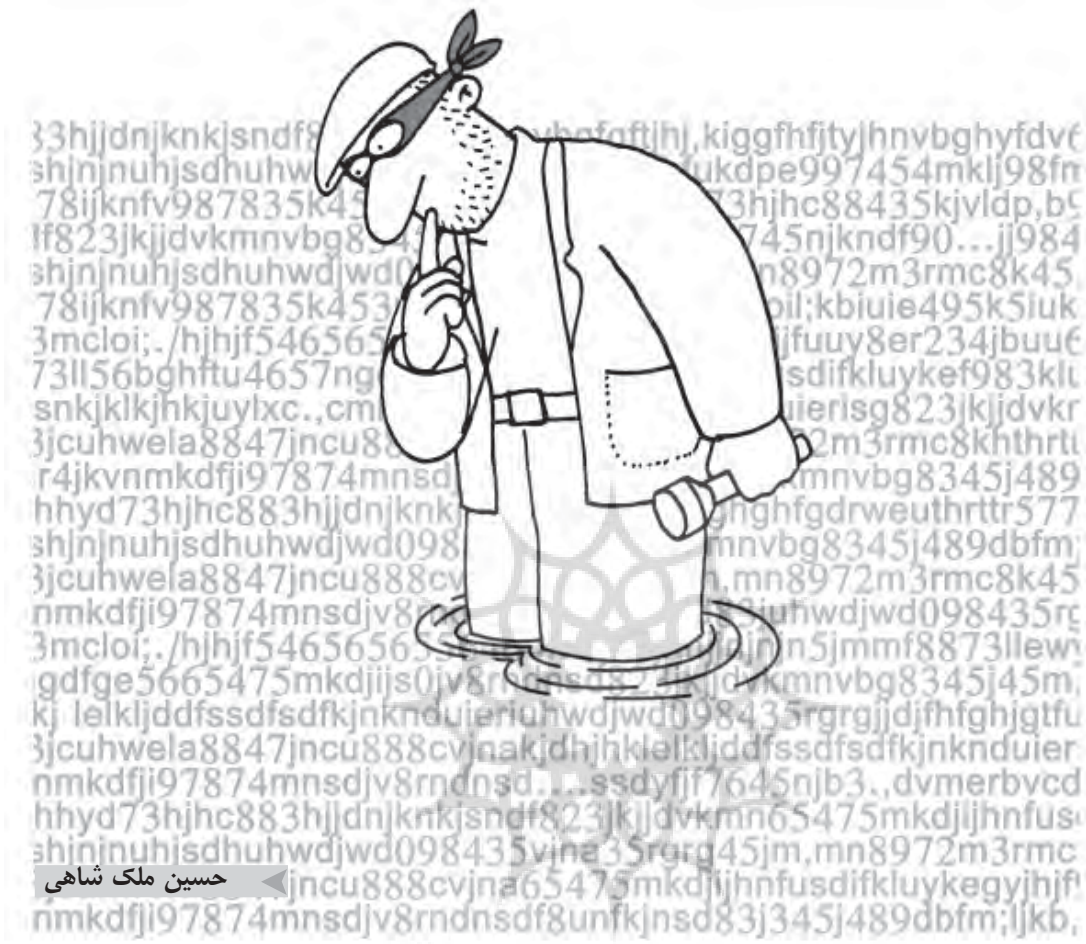
امنیت در بانکداری الکترونیک با استفاده از کلمات عبور یک بار مصرف



حسین ملک شاهی

رشد روزافزون فن آوری اطلاعات و نفوذ آن به تجارت موجب تغییر در بازارهای پولی شده و روش های بانکداری را متحول کرده است. با گسترش معاملات از طریق تجارت الکترونیک نیاز به حضور بانکداری الکترونیک برای پوشش نقل و انتقال وجوه و منابع مالی بیش از پیش احساس می شود و بدون بانکداری الکترونیک پیاده سازی تجارت الکترونیک غیرممکن خواهد بود. در این گیر و دار بانک هایی که بتوانند ساختارهای داخلی خود را با سرعت بیشتر سازگار کنند، سود سرشاری به دست خواهند آورد و در مقابل، اگر نتوانند تغییرات را به درستی اعمال کنند، متحمل زیان های جبران ناپذیری خواهند شد. یکی از عواملی که بیش از عوامل دیگر خود را در پیاده سازی بانکداری الکترونیک نمایان می سازد مسئله امنیت است. چراکه اگر سیستم طراحی شده از امنیت کافی برخوردار نباشد، ضمن وارد کردن خسارات غیرقابل جبران به سازمان، مشتریان را در استفاده از بانکداری الکترونیک گریزان می کند. بر اساس تجزیه و تحلیل حملاتی که ممکن است روی سیستم اتفاق بیافتد، می توان یک خط مشی امنیتی را تعریف نمود تا ریسک های مورد نظر را تحت پوشش قرار داده و یا تا حد قابل قبولی کاهش دهد.

روش هایی که برای منظور مورد استفاده قرار می گیرند، مکانیزم‌هایی از قبیل رمزنگاری، تصدیق، امضای دیجیتالی، تعیین هویت، تمامیت داده، کنترل دسترسی و ... هستند. برای استفاده از این مکانیزم ها استانداردهای خاصی تعریف شده و سخت افزار و نرم‌افزارهای ویژه‌ای به وجود آمده است. یکی از مواردی که در بانکداری الکترونیک باید مورد توجه قرار گیرد، مکانیزم "تعیین هویت" است. استفاده از کلمه "عبور" ساده ترین روش در اثبات هویت در سیستم امنیتی است، اما بسیار نا امن است و در عین حال کارکرد فوق العاده راحتی دارد. برای اینکه از کلمات عبور استفاده کرده و سیستم نیز از امنیت کافی برخوردار باشد، کلمات "عبور یک بار مصرف" (OTPS) معرفی می شوند. ساخت این کلمات عبور دارای فن آوری‌های متنوعی است که از آنها می توان در نقل و انتقال وجوه بین بانکی با استفاده از شبکه شتاب و "سامانه تسویه ناخالص آنی" و با

استفاده از اینترنت، تلفن ثابت و همراه استفاده کرد. در این مقاله به بررسی این فن آوری‌ها می‌پردازیم.

1- Cryptography
2- Authentication
3- Digital Signature
4- Data Integrity
5- Access Control
6- Identification
7- Password
8- One Time Passwords (OTPS)
9-Real-Time Gross Sottlement (RTGS)

کلمات عبور یک‌بار مصرف

استفاده از کلمات عبور یکی از روش های متداول در تعیین هویت است. برای مثال هنگامی که شخصی می‌خواهد از طریق اینترنت از موجودی حساب بانکی خود مطلع شود، باید به طریقی خودش را به بانک معرفی کند تا ثابت کند اجازه دریافت چنین اطلاعاتی را دارد. ساده ترین روش برای انجام دادن این کار استفاده از یک کلمه عبور است. اما استفاده از کلمه عبور خطرناک است، زیرا یک مزاحم غیرمجاز[1] که دارای وقت و تلاش کافی باشد، می‌تواند تماس بین ثابت کننده[2] و تصدیق کننده را دنبال کرده و کلمه عبور را به دست آورد. با تغییر مداوم کلمه عبور، این حمله ضعیف می شود و با به کار بردن کلمات یک‌بار مصرف این حمله دیگر کارایی نخواهد داشت. کلمات عبور یک‌بار مصرف برای یک بار تعیین هویت به کار می روند و برای تعیین هویت بعدی باید از کلمه عبور دیگری استفاده شود. به طور اساسی سه نوع کلمه عبور یک‌بار مصرف وجود دارد. اولین نوع از یک الگوریتم ریاضی استفاده کرده و کلمه عبور جدید را از روی قبلی تولید می‌کند. نوع دوم بر پایه همسان سازی زمانی[3] بین تصدیق کننده و ثابت کننده کار می‌کند. نوع سوم نیز از یک الگوریتم ریاضی استفاده کرده و بر پایه یک چالش[4] مثل یک عدد تصادفی[5] و یا جزئیات تراکش[6] کلمه عبور تولید می‌کند.

قبل از اینکه نحوه کارکرد هر یک از انواع بالا را ذکر کنیم، با انواع امنیت آشنا شده و قضیه زیر را در مورد امنیت کامل بیان می کنیم.

امنیت کامل(۷) : به طور کلی دو نوع امنیت برای یک دستگاه رمزنگاری وجود دارد که عبارتند از:

۱- امنیت محاسباتی: در این امنیت آن دسته از دستگاه های رمز نگاری پیشنهاد می شوند که بر اساس نظریه پیچیدگی کار می کنند. امنیت این دستگاه های رمز نگاری به قدرت محاسباتی رایانه های زمان بستگی دارد.

۲- امنیت غیر مشروط : یک دستگاه رمز نگاری دارای امنیت غیرمشروط است اگر به هیچ وجه شکسته نشود، حتی اگر دارای منابع محاسباتی بینهایت باشیم. برای به دست آوردن امنیت غیرمشروط نیاز به امنیت کامل داریم. طبق قضیه، اگر فضاهای رمز و کلید و پیغام با هم برابر باشند یک دستگاه رمز نگاری امنیت کامل ایجاد می‌کند، اگر و فقط اگر برای هر پیغام و رمز شده آن فقط یک کلید وجود داشته باشد. سیستم یکبار ورنام نمونه‌ای از دستگاه‌های رمزنگاری است که امنیت کامل برقرار می‌سازد. در ادامه به توضیح در مورد آن می‌پردازیم.

سیستم یک‌بار ورنام

یکی از دستگاه های رمزنگاری که می تواند امنیت کامل ایجاد کند، در سال ۱۹۱۷ به همت "جیلبرت ورنام"[7] برای رمزنگاری خودکار پیغام‌های تلگراف معرفی و ثبت شد. این دستگاه رمز به صورت زیر است:

فرض کنید $n \geq 1$ یک عدد صحیح بوده و داشته باشیم $P=C=K=(Z_2)^n$ که در اینجا P و C و K به ترتیب فضاهای پیغام و رمز و کلید هستند، در این صورت برای $x=(x_1,x_2,\ldots,x_n)\in P$ و $k=(k_1,k_2,\ldots,k_n)\in K$ ، تابع رمزگذار $e_k(x)$ را به صورت زیر تعریف می کنیم :

$$e_k(x)=(x_1+k_1,x_2+k_2,\ldots,x_n+k_n) \bmod 2$$

و برای $y=(y_1,y_2,\ldots,y_n)\in C$ ، تابع رمزگشای $d_k(x)$ به صورت زیر تعریف می شود :

$$d_k(x)=(x_1+k_1,x_2+k_2,\ldots,x_n+k_n) \bmod 2$$

در این دستگاه اگر یک کلید برای رمز کردن چند پیغام به کار رود، دستگاه امنیت خود را از دست می دهد، زیرا مزاحم با حمله متن ساده - معلوم[8] می تواند کلید را پیدا کند.

با توجه به اینکه دستگاه های رمز یک‌بار مصرف (OTP) نیز برای هر پیغام یک رمز تولید می کنند، می توانند دارای امنیت کامل باشند.

حملاتی که ممکن است روی سیستم اتفاق بیافتد، می توان یک خط مشی امنیتی را تعریف نمود تا ریسک های مورد نظر را تحت پوشش قرار داده و یا تا حد قابل قبولی کاهش دهد

انواع دستگاه رمز یک‌بار مصرف

سه نوع دستگاه OTP وجود دارد که عبارتند از:

دستگاهOTP نوع اول: این دستگاه ها بر اساس الگوریتم‌های ریاضی کار می کنند. یکی از روش ها برای ساخت این دستگاه‌ها منسوب به "لزلی لمپرت[9]" بوده و از یک تابع یک طرفه[10] به نام f استفاده می کند. به این نحو که از یک مقدار اولیه s استفاده کرده و کلمات عبور را به صورت زیر تولید می کند:

$$f(s),\ f(f(s)),\ f(f(f(s))),\ \ldots$$

برای به دست آوردن کلمه عبور بعدی در این دنباله از روی کلمات عبور قبل، نیاز به پیدا کردن راهی برای محاسبه تابع معکوس f^{-1} است. از آنجا که f را به عنوان تابع یکطرفه انتخاب کرده ایم، یافتن تابع معکوس f^{-1} به طور محاسباتی غیرممکن است. بنابر این دستگاه OTP نوع اول ، امنیت محاسباتی ایجاد می کند.

دستگاه OTP نوع دوم : این دستگاه‌ها معمولا "توکن‌های[11]" سخت‌افزاری هستند. به این بیان که هر کاربر یک دستگاه رمز شخصی دارد که کلمه عبور یکبار مصرف تولید می‌کند. درون این token ها یک زمان سنج دقیق وجود دارد که با زمان سنج تصدیق کننده همزمان می شود. کاملا مشخص است که زمان سهم مهمی از الگوریتم این دستگاه ها را در تولید کلمه عبور دارد، چرا که تولید کلمه عبور جدید بر پایه زمان جاری است، به جای اینکه بر پایه کلمه عبور قبلی یا یک کلید مخفی باشد. شایان ذکر است که تلفن‌های همراه و "دستیارهای شخصی دیجیتالی[12]" نیز می توانند برای تولید یک کلمه عبور یکبار مصرف از این نوع مورد استفاده قرار گیرند و نیز دستگاه را می توان طوری طراحی کرد که امنیت کامل برقرار سازد .

دستگاه OTP نوع سوم : استفاده از کلمات عبور یک‌بار مصرف نیازمند آن است که کار بر چالشی همزمان را فراهم کند که معتبر باشد. برای انجام دادن این کار می توان از خود کلمه عبور استفاده کرد و برای اجتناب از تکرارها یک شمارنده نیز اضافه کرد تا چنانچه موردی پیش آید که در آن یک چالشی دوبار حاصل شود، باز هم به کلمات عبور یک‌بار مصرف متفاوتی منجر شود. EMV از این روش استفاده کرده و تراشه هایی را برای استفاده در کارت های اعتباری در اروپا طراحی کرده است .

نتیجه گیری

دستگاه های OTP غیر همزمان دارای ساعت نیستند و در نتیجه نیازمند شارژ باطری مداوم نخواهند بود و لذا در هزینه استفاده از این نوع فن آوری صرفه جویی خواهد شد.

از طرفی کلمات عبور یک بار مصرفی که همزمان نیستند، نسبت به کلاهبرداری آسیب پذیرتر هستند. البته باید توجه داشت که حتی کلمات عبور یکبار مصرف همزمان نیز نسبت به حمله شخص ثالث آسیب پذیر هستند و هرگز نباید کلمات عبور در اختیار اشخاص ثالث قرار گیرد. در مجموع برای یک نصب گسترده، انتظار می رود دستگاه OTP همزمان انتخاب گرانتری باشد . زیرا نسبت به دستگاه های غیر همزمان هزینه مازادی برای کلمات عبور صرف می شود و همچنین تهیه توکن ها هزینه ای بر مشتریان تحمیل می کند، اما از آنجا که می توانند امنیت کامل ایجاد کنند، انتخاب مناسبی هستند، این دستگاه های رمز همچنین دارای حق اختراع بوده و الگوریتم آن در اختیار عموم قرار نمی گیرد و اصل امنیت از طریق نداشتن شناخت را نیز پشتیبانی می کنند. از طرفی یکی از مکانیزم‌های امنیتی، امضای دیجیتال است که از موارد مطرح در زمینه بانکداری الکترونیک محسوب می شود. با استفاده از این دستگاه ها می توان اقدام به صدور امضای دیجیتال کرد. بنابر این با توجه به ویژگی‌های این دستگاه‌ها می‌توان آنها را به منظور استفاده فراگیر معرفی و در کنار آنها از قراردادهایی نظیر SSL و SET استفاده کرد. کما اینکه این دستگاه ها از طرف بعضی بانک‌ها برای انتقالات داخلی مورد استفاده قرار می گیرند. با آموزش همگانی می توان از حمله شخص ثالث نیز جلوگیری کرده و نقل و انتقالات وجوه بین بانکی را که قسمت عمده ای از تراکنش های بانکی را تشکیل می‌دهند، به صورت الکترونیک و بدون حضور در شعبه و با امنیت بالا انجام داد.

منابع:

[1] Buchmann Johannes A.,"Introduction to Cryptography", Springer-Verlag, 2001.

[2] Stinson, Douglas R.,"Cryptography: Theory and Practice", CRC Press, 1995.

[3] Menezes, Alfred J. and van Oorshot, Paul C. and Vanstone, Scot A., "Handbook of Applied Cryptography", CRC Press, 2001.

پی نوشت ها:

1-Unauthorized Intruder
2-Prover
3-Time Synchronization
4-Challenge
5-Random Number
6-Transaction Details
7-Gilbert Vernum
8-Known Plaintext Attack
9-Leslie Lamport
10-One-way Function
11-Tokens
12-Personal Digital Assistants