ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال هفتم)
شماره ۲۵ / بهار ۱۴۰۱ / ص ۱۷- ۱

مروری بر کاربرد رمزهای یک بار مصرف ترکیبی و حملات به ویژه فیشینگ

سمیه نصیری
فوق لیسانس مهندسی کامپیوتر گرایش نرم افزار، مدرس مدعو دانشگاه فرهنگیان پردیس الزهرا زنجان.

نام نویسنده مسئول:
سمیه نصیری

تاریخ دریافت: ۱۴۰۰/۱۰/۰۵
تاریخ پذیرش: ۱۴۰۰/۱۲/۱۶

چکیده

حملات فیشینگ گروهی از حملات هستند که امنیت کاربران و اطلاعات حیاتی آنها از جمله رمز عبور آنها را به خطر می‌اندازند و تاکنون راه حل‌های زیادی از جمله رمزهای یک بار مصرف برای جلوگیری از تهدیدات موجود ارائه شده است. علیرغم تلاش‌ها برای استفاده از رمزهای عبور یک بار مصرف برای جلوگیری از حملات فیشینگ، این هنوز یک چالش بزرگ است و تحقیقات بیشتری مورد نیاز است. بیشترین حمله برای جذب کاربران (با استفاده از تکنیک‌های مهندسی اجتماعی) به وب‌سایت‌های فیشینگ کاملاً طراحی شده است که شبیه وب‌سایت‌های سازمان‌های هدف اصلی هستند تا با پر کردن برخی فرم‌ها، اطلاعات شخصی کاربران را دریافت کنند. فیشینگ، از جمله فیشینگ نیزه‌ای، به دلیل غیرقابل پیش بینی بودن، به یک مشکل جدی تبدیل شده است. این به نوبه خود به محققان و دست اندرکاران این امکان را می‌دهد تا راه حل‌هایی برای دفاع از آن یا حداقل آگاه ساختن کاربران از خطر این پدیده بیابند. کارایی روش پیشنهادی به صورت تحلیلی با استفاده از تعریف سناریو، مدل‌سازی و شبیه‌سازی محاسبه می‌شود و بر اساس معیار نرخ پیشگیری و همچنین ضریب پیچیدگی روش پیشنهادی اندازه‌گیری می‌شود که نشان‌دهنده بعید است که توسط مهاجمان حدس زده شود.

واژگان کلیدی: فیشینگ، رمزیکبارمصرف.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۵، بهار ۱۴۰۱، ص ۱۷- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

استفاده از رمزهای عبور یکبار مصرف در اپلیکیشن های احراز هویت، علاوه بر افزایش امنیت تبادل اطلاعات و ارتباطات، می‌تواند برای جلوگیری از حملاتی که قصد فریب و سرقت اطلاعات کاربران را دارند نیز مورد استفاده قرار گیرد. امروزه این نوع حملات که عمدتاً با عنوان حملات فیشینگ شناخته می‌شوند، از تنوع زیادی برخوردار بوده و همواره امنیت کاربران را در فضای مجازی تهدید می‌کنند. در حوزه سایبری همواره با حملات، تهدیدها و چالش‌های جدیدی مواجه هستیم. حملات فیشینگ مجموعه‌ای رایج از حملات هستند که حریم خصوصی کاربران را هدف قرار می‌دهند. این حملات به طرق مختلف سعی در سرقت اطلاعات حساس کاربران دارند. مهاجم می‌تواند از اطلاعات هویت قربانی برای حدس زدن رمزهای عبور مورد نیاز استفاده کند. برای جلوگیری از چنین حملاتی به راهکارهای مناسب نیاز داریم. امروزه اهداف زیر می‌تواند به عنوان فاکتورهایی برای رسیدن به بهترین مکانیزم های ضد حملات فیشینگ مطرح گردد:

- اهمیت بسیار بالای محرمانگی اطلاعات کاربران
- پیشرفت روزافزون روش‌ها و تکنیک‌های مورد استفاده در حملات فیشینگ
- خسارت‌های مادی و معنوی ناشی از حملات فیشینگ
- عقب‌ماندگی مدافعان، نسبت به مهاجمان، در حوزه سایبری
- نیاز به ارائه راهکار جامعی که جنبه‌های مختلفی، از جمله امنیت خود رمز یکبارمصرف، را درنظر گرفته باشد.

بسیاری از تکنیک‌ها، بر اساس دیدگاه‌های مختلف، برای رویارویی با این نوع حملات مورد استفاده قرار گرفتند، مانند روش‌های لیست سیاه، واژگانی، محتوا، هویت، شباهت بصری، یا روش‌های مبتنی بر استخراج ویژگی‌های رفتاری. فهرست روش‌ها البته جامع نیست. بلکه به استخراج برخی از ویژگی‌های مفید در مورد صفحه وب یا URL مورد نظر کمک می‌کند. این روش‌های فهرست‌شده از تحلیل استاتیک/دینامیک یا هر دوی آنها استفاده می‌کنند، که نمونه راه‌حل ارائه‌شده در این مطالعه است. روش تجزیه و تحلیل استاتیک دارای استخراج است که بدون اجرای صفحه وب URL در آزمون انجام می‌شود. با توجه به تحلیل پویا، ابتدا صفحه وب قبل از پیش بینی نتیجه بارگذاری می‌شود.

ما با ارائه این پژوهش می‌خواهیم به پرسش‌هایی مانند، چه روش‌هایی برای حملات فیشینگ مورد استفاده قرار می‌گیرند؟ رمزهای یکبار مصرف کدامند؟ راه‌های مبارزه رمزهای یکبار مصرف با حملات فیشینگ چیست؟ آیا روش‌های ترکیبی جهت پیشگیری از حملات فیشینگ را می‌توان بهبود داد؟

همچنین تمامی نگارش این مقاله بر پایه فرضیات زیر می‌باشد:

- استفاده از رمزهای یکبارمصرف می‌تواند موجب پیشگیری از حملات فیشینگ شود.
- ترکیب روش‌های مختلف می‌تواند موجب بهبود پیشگیری از حملات فیشینگ شود.
- پیشگیری از حملات فیشینگ موجب ارتقاء محرمانگی اطلاعات کاربران خواهد شد.

مفاهیم اولیه

بسیاری از راه حل‌های مبتنی بر روش شناسی پیشنهاد شده است. اما آنها با یک مشکل عمده روبرو هستند که منجر به تعداد زیادی از مثبت‌های کاذب می‌شود، که عمدتاً به دلیل محدودیت چنین رویکردهایی است، هدف تحقیقات تاکنون ایجاد راه‌حلی است که می‌تواند با استفاده از تکنیک‌های هوشمند برای اجرای قوانین منطقی و مدل‌های یادگیری عمیق که به به‌روزرسانی رفتار فیشینگ کمک می‌کند، تهدیدات پیشرفته و پایدار را شناسایی و از آنها جلوگیری کند. هدف همه محققان در ارائه دانشی که به عنوان بزرگترین پشتیبان برای سازمان‌های مختلف در فرار یا مقابله با مشکل فیشینگ عمل می‌کند، متمرکز بوده است.

ISSN: 2745-3673
http://www.Rcsj.ir

احراز هویت یک مرحله‌ای

احراز هویت تک عاملی گذرواژه‌ها به طور سنتی برای جلوگیری از دسترسی افراد غیرمجاز به اطلاعات محافظت شده استفاده می‌شود .کاربر از طریق نام کاربری خود را به سیستم معرفی می‌کند و از طریق رمز عبور هویت خود را تأیید می‌کند. اگرچه احراز هویت تک عاملی رایج‌ترین نوع احراز هویت است و در بسیاری از موارد نیازهای امنیتی را برآورده می‌کند، اما معایبی نیز دارد که از جمله آن‌ها می‌توان به احتمال گم شدن، فراموشی و مهمتر از همه سرقت رمزهای عبور ثابت اشاره کرد.

احراز هویت دو مرحله‌ای

با افزودن یک فاکتور امنیتی به سیستم، می‌توان امنیت کاربر را تا حد بسیار مطلوبی ارتقا بخشید. در این روش که به احراز هویت دوفاکتوری معروف است در کنار آن نیاز به ابزاریست که بتواند صحت هویت وی را تأیید نماید.

رمز یک بار مصرف و حملات فیشینگ

رمز یکبار مصرف رمز عبور یکبار مصرف یا پویا فناوری نسبتاً جدیدی است که برای ارتقای امنیت کاربران در دنیای مجازی توسعه یافته و مورد استفاده قرار می‌گیرد. یکی از مزیت‌های اصلی رمزهای عبور پویا در مقایسه با رمزهای عبور سنتی مقاوم بودن آنها در برابر حملات مجدد است، از آنجایی که هر رمز عبور تنها در یک جلسه استفاده می‌شود، امکان استراق سمع و استفاده مجدد از آن وجود ندارد، بنابراین از ایستا بودن آنها ایمن‌تر است. کدها و برای برنامه‌هایی که نیاز به امنیت بالایی دارند مانند بانکداری اینترنتی مناسب است. فیشینگ یکی از اصطلاحاتی است که مهاجمان در زمینه ادبیات اینترنتی به کار می‌برند و به فریب کاربران برای افشای اطلاعات حساس و شخصی خود اشاره دارد.

پیشینه سوابق و تحقیقات

تحقیقات راه حل‌های بسیاری را برای استخراج ویژگی‌های مفید مورد استفاده در راه حل‌های تشخیص فیشینگ نشان داده‌اند. مرور مطالعات قبلی شامل فهرست سیاه، واژگانی، محتوایی، دیداری، هویتی و روش‌های مبتنی بر رفتار است. این نیاز به درخواست‌های دائمی کاربر و تجربه نهایی کاربر برای تجزیه و تحلیل صفحات وب دارد. این تکنیک بیشتر به مرورگر یا ابزار مورد استفاده برای دسترسی به صفحه وب بستگی دارد. بنابراین، اگر این ابزار هک شود یا به روز نشود، به تکنیک مورد اعتماد نخواهد بود. در هر صورت این ویژگی به عنوان اولین گام در سیستم ما استفاده خواهد شد اما ویژگی قابل اعتمادی محسوب نخواهد شد.

در یک تحلیل از تعداد نام دامنه‌هایی که توسط فیشرها ثبت شده‌اند، در مقابل فیش‌هایی که در دامنه‌های در معرض خطر (هک) ظاهر می‌شوند، انجام دادیم. این دسته‌بندی‌های مختلف مهم هستند زیرا گزینه‌های کاهش متفاوتی را برای پاسخ‌دهندگان ارائه می‌دهند و بینش‌هایی را درباره نحوه ارتکاب جرائم فیشارها ارائه می‌دهند. اگر دامنه‌ای برای فیشینگ در مدت زمان بسیار کوتاهی پس از ثبت گزارش شده باشد، و/یا حاوی نام تجاری یا رشته‌ای گمراه‌کننده باشد، و/یا به‌صورت دسته‌ای یا در الگویی ثبت شده باشد که نشان‌دهنده مالکیت یا قصد مشترک باشد، ما آن را به‌عنوان مخرب پرچم‌گذاری کردیم [۱].

رمزهای یکبارمصرف می‌توانند از مکانیزم‌های احراز هویت در مقابل حملات مختلف ازجمله حملات بازپخش[1] در هنگام ورود[2] محافظت کنند. با استفاده از روش پیشنهادی یک نسخه آزمایشی احراز هویت دوعاملی[3] برای تلفن‌های همراه توسعه داده شده و به صورت عملی، یک سال مورد استفاده قرار گرفته است [۳۸].

در حوزه سایبری، تکنیک استفاده شده برای سرقت اعتبار[4] کاربران، فیشینگ نامیده می‌شود. برای توقف حملات فیشینگ از تکنیک‌های تشخیص و پیشگیری زیادی استفاده می‌شود که هر کدام مزایا و معایب مربوط به خود را دارند. با استفاده از کلمه

[1] Replay Attack
[2] Login-Time
[3] two-factor authentication
[4] credentials

ISSN: 2745-3673
http://www.Rcsj.ir

کلیدی[5] اصالت صفحه وب را مشخص می‌کند با این کار از ورود کاربران به صفحات جعلی و سرقت اطلاعات محرمانه آنها جلوگیری می‌شود [۶۲].

امروزه حملات فیشینگ تهدیدی جدی برای اطلاعات محرمانه کاربران اینترنت است. یک مهاجم با ارسال پیام‌های جعلی افراد را فریب می‌دهد تا اطلاعات حساس را افشا کنند. کاربران ناآگاهی که دستورالعمل‌های پیام را دنبال می‌کنند به یک صفحه وب جعلی هدایت می‌شوند و از آنها خواسته می‌شود اطلاعات حساس خود را وارد کنند [۳۶].

هر حمله مخربی که با کمک یک صفحه وب جعلی برای تشویق کاربران به وارد کردن جزئیات امنیتی خود انجام شود، به عنوان یک حمله فیشینگ توصیف می‌شود. حملات فیشینگ به طور گسترده برای به دست آوردن رمز عبور و جزئیات امنیتی کاربران ناآگاه استفاده می‌شود. ضمن بررسی انواع روش‌های فیشینگ و همچنین اقدامات متقابل، روشی را پیشنهاد کرده‌اند که از ترکیبی از رمزهای عبور یک بار مصرف و تشخیص صدا برای جلوگیری از حملات فیشینگ استفاده می‌کند [۵۹].

پروتکل PJP از کلید امنیتی رمز عبور برای جلوگیری از یافتن رمز عبور دشمنان استفاده می‌کند. پروتکل AMP همچنین یک سیستم مدیریت حساب بهبودیافته را با در نظر گرفتن فعالیت‌های کلیدی کاربران برای تصمیم گیری در مورد قفل کردن حساب خود ارائه می‌دهد. روش پیشنهادی از تکنیک همگام سازی استاندارد MD5 برای محافظت از رمزهای عبور قبل از انتقال و ذخیره سازی استفاده می‌کند [۶۵].

در تحقیق دیگری معایب رمزهای متنی را درنظر گرفته و طرحی ارائه کرده است که از ترکیب تصاویر، برای رمز عبور استفاده می‌کند. رمزهای تصویری شامل فعالیت‌های کلیک بر روی تصاویر و درگ کردن تصاویر بوده و می‌تواند جایگزین مناسبی برای رمزهای متنی باشد [۵۰].

همچنین در تحقیق دیگری، برای حل مسئله فیشینگ در وب‌سایت‌ها، روشی ارائه کرده است که با استفاده از تصویر و رمز یکبارمصرف از یک رمزنگاری تصویری بهره می‌برد. در این روش تصویر اصلی به دو بلوک تقسیم شده و یک رمز یکبارمصرف تولید می‌شود [۴۹].

روش‌های احراز هویت مبتنی بر پیامک، پس از دریافت درخواست‌های کاربران، رمز عبور یکبار مصرف را به تلفن همراه کاربران ارسال می‌کنند. کاربران رمز عبور را در دستگاه مشتری خود وارد می‌کنند تا عملیات تأیید را انجام دهند. اگرچه این روش می‌تواند به خوبی از استفاده غیرمجاز از رمزهای عبور جلوگیری کند، مهاجم همچنان می‌تواند مجموعه‌ای از رمزهای عبور را حدس بزند که در نهایت یا منجر به حمله موفقیت آمیز یا منجر به ایجاد حساب می‌شود. مسدود. سیستمی را توسعه داده‌اند که دستگاه مشتری را قادر می‌سازد صحت یک رمز عبور یکبار مصرف را تأیید کند [۳۹].

با گسترش گوشی‌های هوشمند، سازندگان مختلف ارزهای رمزنگاری شده یکبار مصرف نیز به عنوان اپلیکیشن برای گوشی‌های هوشمند توسعه یافته‌اند و بدون هیچ هزینه اضافی امکانات زیادی را در اختیار کاربران قرار داده‌اند. این تحقیق راه حلی را توسعه داده است که از انعطاف پذیری نرم افزار و امنیت سخت افزاری استفاده می‌کند. با این کار گوشی هوشمند به ابزاری مناسب برای تولید رمزهای عبور یکبار مصرف تبدیل می‌شود و این کار بدون آسیب پذیری های امنیتی خود دستگاه و بدون تغییر در سیستم عامل انجام می‌شود [۷۸].

اگرچه گذرواژه‌های یک بار مصرف به طور گسترده برای جلوگیری از حملات فیشینگ و پخش مجدد استفاده می‌شود، اما ایمن سازی آنها نیز یک چالش مهم است. ماهتو مدلی را برای بهبود امنیت رمزنگاری یکبار مصرف ایجاد کرده است که از منحنی بیضی و رمزنگاری بیومتریک عنبیه استفاده می‌کند. از جمله مزایای این روش می‌توان به کوتاهتر بودن طول کلید نسبت به RSA و تولید کلیدهای خصوصی به صورت پویا در صورت نیاز اشاره کرد [۵۵].

حملات سایبری و انواع آن

حملات سایبری می‌توانند با اهداف و نیت‌های مختلفی انجام شوند. بنابراین دسته‌بندی‌های مختلفی نیز برای اهداف حملات می‌توان ارائه کرد. به عنوان نمونه از یک دیدگاه می‌توان اهداف حملات سایبری را به صورت زیر دسته‌بندی کرد:

[5] Code word

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۵، بهار ۱۴۰۱، ص ۱۷- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

- دسترسی به اطلاعات یک سیستم کامپیوتری
- دستبرد به اطلاعات حساس و محرمانه‌ای که در داخل یک کامپیوتر نگهداری می‌شود
- مطالعه و سرقت اطلاعات شخصی کاربران
- سرقت اطلاعات بانکی
- مطالعه و زیرنظر گرفتن یک سازمان به صورت غیر مجاز
- ایجاد اختلال در یک سرویس‌دهنده
- به کارگرفتن کامپیوتر افراد به عنوان سپر و پوششی برای اهداف آتی
- ورود به اتصال اینترنتی و استفاده از پهنای باند غیر مجاز

انواع حملات سایبری نیز عبارتند از:

- دسترسی به بدنه اصلی سیستم (Physical Access):
- قطع کردن ارتباط (Communication Interception):
- انکار سرویس (Denial Of Service):
- دسترسی غیرمجاز به شبکه (Intrusion):
- (Trapdoors)

مقایسه انواع حملات سایبری در جدول (۱) آمده است.

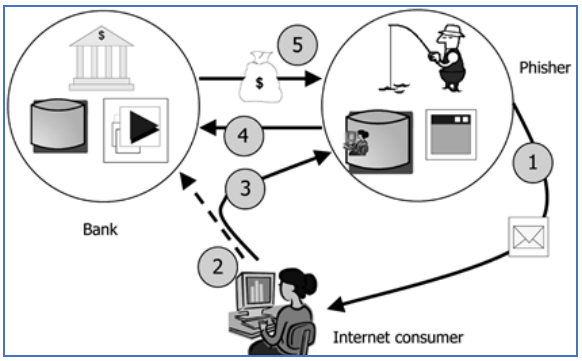
جدول ۱. نیز برخی از انواع حملات سایبری را معرفی و توضیح مختصری در مورد آنها ارائه کرده است

ردیف	نام حمله	توضیحات
۱	جعل هویت	در این نوع از حمله، دشمن خود را به عنوان یک کاربر مشروع برای سیستم جا می‌زند. او با استفاده از روش‌های مختلفی از جمله به‌دست آوردن نام کاربری و رمز عبور کاربران دیگر، این کار را انجام می‌دهد.
۲	تغییر داده‌ها	داده‌هایی که در هر سیستم و یا هر واسطی ذخیره‌سازی شده‌اند و توسط سایر سیستم‌ها مورد استفاده قرار می‌گیرند در معرض این گونه حملات قرار دارند. در صورتی که یک مهاجم بتواند این داده‌ها را تغییر دهد این نوع از حمله اتفاق افتاده است. این تغییر می‌تواند عمدی و یا سهوی باشد.
۳	انکار	اگر هیچ سابقه‌ای از فعالیت‌های انجام شده در شبکه وجود نداشته باشد آنگاه یک کاربر متقلب ممکن است عملیات واقعی سیستم را انکار کند. به این معنی که این کاربر عملیات غیرقانونی خود را انجام می‌دهد اما هیچ شواهدی مبنی بر انجام این کار ثبت نمی‌شود.
۴	افشای اطلاعات	سیاست‌های امنیتی باید طوری تنظیم شوند که اطلاعات در اختیار افراد مجاز قرار گیرند. در صورتی که افراد غیرمجاز به اطلاعات دسترسی داشته باشند آنگاه این نوع از حمله اتفاق افتاده است.
۵	منع سرویس	در این نوع از حمله، مهاجم تلاش می‌کند تا با استفاده از تکنیک‌های مختلفی در سرویس‌هایی که یک سیستم ارائه کرده، اختلال ایجاد کند و آنها را از کار بیاندازد.
۶	افزایش حق امتیاز	کاربران مختلفی که از سیستم استفاده می‌کنند دارای اولویت‌های مختلفی هستند. در صورتی که کاربری با اولویت پایین‌تر بتواند به اولویت بالاتری دسترسی پیدا کند این نوع از حمله اتفاق افتاده است. در این حالت مهاجم به داده‌ای دسترسی پیدا کرده است که حق دسترسی به آن را ندارد.

ISSN: 2745-3673
http://www.Rcsj.ir

حملات فیشینگ

معمولاً یک هکر ابتدا یک صفحه جعلی برای انجام این حمله ایجاد می‌کند. مهاجمان برای افزایش میزان موفقیت حملات سعی می‌کنند خود را به گونه‌ای معرفی کنند که مردم به آنها اعتماد کرده و آنها را به عنوان نماینده قانونی مراکز معتبری مانند بانک‌ها بپذیرند. مهاجمان پس از جلب رضایت و اعتماد کاربران، اطلاعات حساس و مهمی مانند شماره کارت اعتباری را درخواست می‌کنند. اکثر عملیات ذکر شده به صورت خودکار انجام می‌شود و با توجه به اینکه کاربران گسترده هدف اولیه هستند و درصد بسیار زیادی از آنها دانش لازم برای شناسایی و مقابله با این نوع حملات را ندارند، شانس موفقیت مهاجمان به سرقت هویت کاربران افزایش می‌یابد. برای درک بهتر حمله فیشینگ به تصویر جالب زیر توجه کنید. در ابتدا، هکر یک صفحه وب دقیقاً شبیه به صفحه اصلی وب سایت بانک قربانی طراحی کرد. هکر پس از به دست آوردن اطلاعات، اطلاعات صفحه اصلی بانک را بررسی کرده و از حساب بانکی قربانی برداشت می‌کند و در پایان پیامی از سوی هکر برای قربانی ارسال می‌شود (شکل ۱)



شکل ۱. مثالی از حمله فیشینگ

از سوی دیگر و به طور خلاصه انواع حمله فیشینگ عبارت است از:

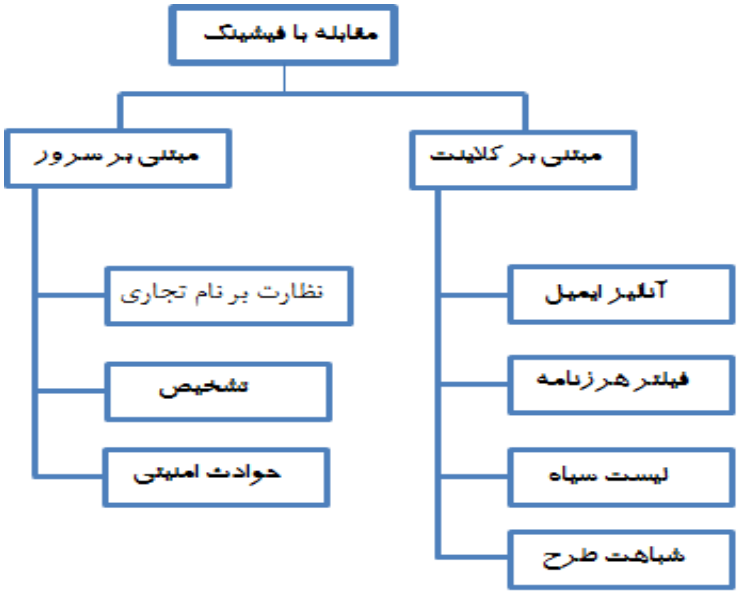
- فیشینگ فریبنده
- جعل وب‌سایت‌ها
- فیشینگ تلفنی
- قاپیدن تب

روش‌های مقابله با فیشینگ

به طور کلی برای مقابله در برابر حملات فیشینگ دو راهکار مختلف ارائه شده است. این روش‌ها عبارتند از روش‌های مبتنی بر سرور و روش‌های مبتنی بر کلاینت. شکل (۲) انواع دسته‌بندی‌های مختلف روش‌های آنتی فیشینگ را نمایش می‌دهد:

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۵، بهار ۱۴۰۱، ص ۱۷- ۱

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۲. روش‌های مقابله با فیشینگ

رمز یک بار مصرف و چگونگی محاسبه آن

هر سیستم احراز هویتی که مبتنی بر رمزعبور یکبار مصرف باشد حداقل متشکل از دو جزء است که عبارتند از:

- سرور احراز هویت
- ابزاری جهت تولید رمز پویا برای هر مشتری

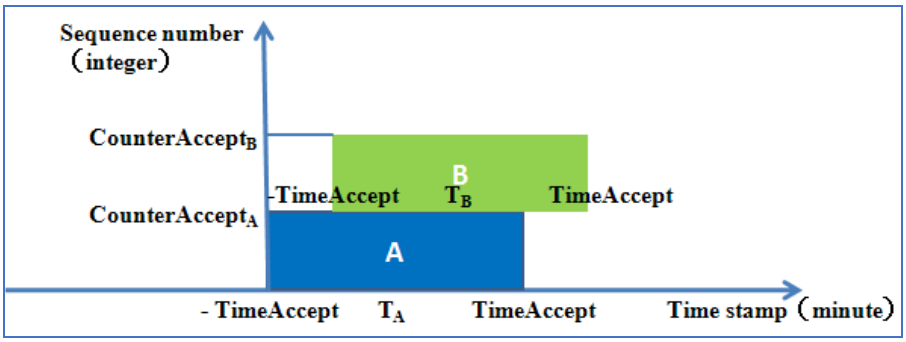
نحوه احراز هویت سرور به فناوری مورد استفاده برای تولید رمز عبور پویا بستگی دارد، اما نحوه تحویل رمز عبور می‌تواند تأثیر زیادی بر عملکرد سرور و فناوری مورد استفاده داشته باشد. در مجموع از سه روش اصلی برای تولید رمزهای عبور یکبار مصرف استفاده شده است: ایجاد رمزهای عبور پویا بر اساس فاکتور زمان: رمزهای عبور تولید شده برای هر کاربر فقط برای مدت زمان مشخصی معتبر هستند. از فناوری رمز یکبار مصرف برای انجام تراکنش‌های امن در فضای مجازی استفاده می‌شود. بر اساس کارت یا ابزاری که بانک در اختیار مشتری قرار می‌دهد، برای هر تراکنش رمزی ایجاد می‌شود که فقط برای یک بار اعتبار دارد. امنیت رمز یکبار مصرف به دلیل استفاده از ویژگی‌های رمزنگاری استاندارد بسیار بالاست.

یکی از نقاط ضعف سمت کاربر که می‌تواند باعث رمز عبور کاربران سایت شود، برنامه‌های ثبت کننده کلیدی است که ممکن است این برنامه‌ها هم به صورت سخت افزاری و هم نرم افزاری مورد استفاده قرار گیرند. بهترین راه برای مقابله با برنامه‌های key logger استفاده از رمز عبور یکبار مصرف است که می‌توان به روشی غیر از رایانه فعلی کاربر به آن دسترسی پیدا کرد. در این حالت برنامه key logger که پسوردها را ذخیره می‌کند و برای سازنده ارسال می‌کند بی اثر است زیرا رمز ذخیره شده توسط برنامه key logger فقط یک بار معتبر است و فقط یک بار قابل استفاده است. رمز یکبار مصرف تولید شده نباید توسط کامپیوتر کاربر قابل دسترسی باشد زیرا در این صورت علاوه بر کاربر، نرم افزارهای جاسوسی نیز می‌توانند به آن دسترسی داشته باشند.

محاسبه رمز یکبار مصرف

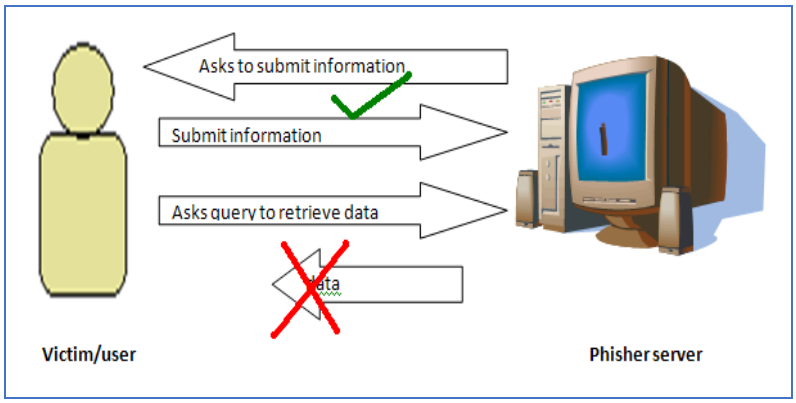
محاسبه رمز یکبار مصرف بر ایجاد یک رمز عبور جدید و منحصر به فرد برای بازبینی کننده هر سیستم احراز هویت متمرکز است. بسته به زمان ارسال پیام، زمان پردازش و حرکت ساعت، بازبینی کننده از یک پنجره دریافت استفاده می‌کند و منحصر به فرد بودن رمزهای عبور در پنجره دریافت مدیریت می‌شود. رمز عبور یکبار مصرف باید به فضای محصور که فقط یک بار احراز هویت شده است محدود شود. در شکل (۳) وضعیت پنجره پذیرش به همراه برچسب زمانی و دنباله اعداد نمایش داده شده است:

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۳. پنجره پذیرش به همراه برچسب زمانی و دنباله اعداد

با استناد به یکی از مهمترین تحقیقات [۶۲]، در بیشتر موارد فیشرها تمایل به حصول اختیار از قربانیان دارند و برای انجام این مقصود، صفحات را به گونه‌ای فیشینگ می‌کنند که صفحات فقط حاوی درخواست‌های ثبت بوده که اطلاعات کاربران را در پایگاه‌داده ثبت کرده و هیچ اطلاعاتی مربوط به کاربر یا وب‌سایت را برنگرداند. شکل (۴) نحوه تبادل اطلاعات بین سرور فیشینگ و قربانی را به خوبی نشان می‌دهد.



شکل ۴. نمایش نحوه تبادل اطلاعات بین سرور فیشینگ و قربانی

روش پیشنهادی در این مرجع دارای دو فاز زیر می‌باشد:

- فاز ثبت‌نام
- فاز ورود

تکنیک تولید کد

هر وقت که کاربر وارد وب سایت شود، پس از وارد کردن شناسه کاربری از او خواسته می‌شود که یکی از دو رقمی که از کد یکتای او به صورت تصادفی انتخاب شده‌اند را وارد کند. اگر رقم‌های وارد شده با رقم‌های کدی که در پایگاه داده ذخیره شده هستند تطابق داشته باشند، آنگاه کد کامل او بر روی صفحه نمایش، نشان داده می‌شود. سپس لازم است که کاربر کد را مورد بازبینی قرار داده تا اطمینان حاصل کند که به سایت واقعی وارد می‌شود نه سایتی که مربوط به عملیات فیشینگ است.

ترکیب پروتکل‌های PJP و AMP با رمزهای یکبارمصرف

طرحی را ایجاد کرده‌اند که از توسعه و ادغام دو پروتکل محبوب PJP و AMP با رمزهای عبور یکبار مصرف استفاده می‌کند. پروتکل PJP از کلید امنیتی رمز عبور برای جلوگیری از یافتن رمز عبور دشمنان استفاده می‌کند. ملاحظات اصلی طراحی در این طرح عبارتند از: بهبود سیستم مدیریت حساب موجود، به ویژه ویژگی قفل حساب، و جلوگیری از حمله انکار سرویس ارائه یک استراتژی مقابله‌ای برای محافظت در برابر ۱۳ حمله برجسته مرتبط با رمز عبور استفاده از یک رمز عبور یکبار مصرف

ISSN: 2745-3673
http://www.Rcsj.ir

انعطاف پذیر در برابر حملات پاسخ پیام. ۲- ۳- ۴- ۱- پروتکل PJP این پروتکل شامل استفاده از یک کلید امنیتی رمز عبور برای جلوگیری از دسترسی دشمنان به رمز عبور از متن وارد شده توسط کاربر از طریق ابزارهای key logger است [۶۵]. در هنگام ثبت نام به کاربران آموزش داده می‌شود که رمز عبور و نام کاربری خود را ارائه دهند، اما در هنگام ورود از کاربران انتظار می‌رود رمز عبور خود را به همراه کلید امنیتی رمز عبور در قسمت رمز عبور وارد کنند. کلید امنیتی رمز عبور هر دنباله‌ای از کاراکترهای دلخواه است به جز نویسه‌های رمز عبوری که کاربران در هنگام ورود انتخاب می‌کنند. طول رمز عبور در این مرجع ۸ کاراکتر است و طول کلید امنیتی رمز عبور ۴ است تا به طور قابل توجهی ثبت کننده کلید را به گمراهی بیاندازد. کاربر واقعی که رمز عبور خود را اشتباه تایپ کرده یا فراموش کرده است، انتظار می‌رود پس از کمی تلاش آن را به خاطر بسپارد.

فناوری پایه و تشخیص خطا

تحلیل استاتیکی به تشخیص خطا بدون اجرای هدف اصلی اشاره دارد. به طور کلی کمک می‌کند زیرا تجزیه و تحلیل استاتیک به نرم افزار یا سخت افزار برای اجرای این کار بستگی ندارد. در مطالعه حاضر، تجزیه و تحلیل استاتیک به استخراج کد منبع از صفحه بدون اجرای آن اشاره دارد تا در درمان سریع باشد. با این حال، گاهی اوقات ممکن است با مشکلی روبرو شوید، مانند برخی از صفحات وب، کدهای منبع رمزگذاری شده را از هر دو صفحه وب قانونی یا فیشینگ تولید می‌کنند که می‌تواند حل شود زیرا ابزارهایی برای بازیابی این کد منبع صفحه وب وجود دارد. هدف از تجزیه و تحلیل استاتیک یافتن مستقیم کلمات کلیدی یا قطعات مشخص شده است.

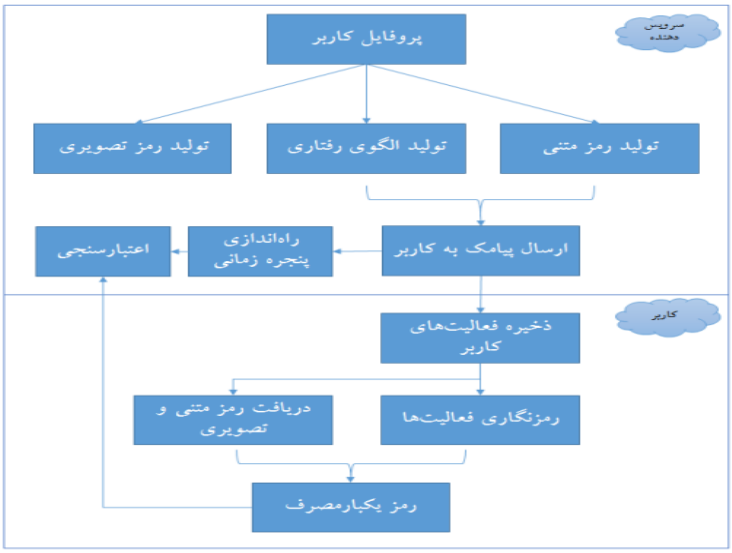
روش‌های دیگری برای جلوگیری از حملات فیشینگ به شرح زیر وجود دارد:

- استفاده از رمزهای تصویری به جای رمزهای متنی
- رمزنگاری تصویری برای حل مسئله فیشینگ
- رمز یکبارمصرف مبتنی بر پیامک
- رمز یکبارمصرف مبتنی بر گوشی هوشمند
- بهبود امنیت رمز یکبارمصرف با رمزنگاری منحنی بیضوی و بیومتریک عنبیه چشم

متدولوژی

از آنجایی که یک مهاجم از مجموعه‌ای از ابزارها و روش‌های خودکار یا کدهای آماده برای جمع آوری اطلاعات در حملات فیشینگ استفاده می‌کند، استفاده از یک راه حل ترکیبی برای ایجاد رمز عبور یک بار مصرف می‌تواند منجر به یک رمز عبور پیچیده یک بار مصرف و گزینه خوبی برای افزایش امنیت شود. در این نگارش روش جدیدی ارائه شده است که روش‌های رمزگذاری ویدئو، متن و متن را با یک راه‌حل ابتکاری، بر اساس پارامترهای رفتاری ترکیب می‌کند. همانطور که اشاره شد روش پیشنهادی یک راهکار ترکیبی است که شامل رمز تصویری، پیام متنی و الگوهای رفتاری است. شکل (۵) چارچوب کلی روش پیشنهادی را نمایش می‌دهد.

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۵. چارچوب کلی روش پیشنهادی

رمز عبور متنی نیز بر اساس اطلاعات پروفایل کاربر ایجاد می‌شود. کاربر الگوی رفتاری خاصی را برای درج رمز عبور مشخص می‌کند و فرآیند تولید الگوی رفتاری نیز بر اساس همین الگو خواهد بود. در هر مرحله از فرآیند احراز هویت، بر اساس نام کاربری که یک ویژگی منحصر به فرد برای هر کاربر است و همچنین رمز اصلی، بر اساس مشخصات کاربر، کدهای متن، تصویر و الگو ایجاد می‌شود و رمز عبور تصویر به کاربر نشان داده می‌شود. در صفحه ورود یک کد متنی همراه با دستورالعملی که الگوی رفتاری را مشخص می‌کند برای کاربر ارسال می‌شود. کاربر باید با مشاهده رمز عبور تصویر در صفحه ورود و همچنین دریافت پیامک حاوی کد متنی و الگوی رفتاری رمز عبور خود را به همراه کدهای متنی و تصویری با الگوی رفتاری مشخص شده وارد کند.

در این صفحه و در سمت کاربر، فعالیت‌های کاربر که شامل الگوهای رفتاری وی می‌شود، ذخیره و رمزگذاری شده و به همراه کدهای تصویری و متنی، رمز یکبار مصرف ایجاد و به سرور ارسال می‌شود. بخش احراز هویت در سمت سرور ابتدا پنجره زمانی را بررسی می‌کند و سپس الگوی رفتار را استخراج و رمزگشایی می‌کند. سپس در صورت تطبیق الگوی رفتاری، کدهای تصویری و متنی ارزیابی شده و در صورت تطبیق آنها با مقادیری که قبلاً تولید شده‌اند، فرآیند اعتبارسنجی نام کاربری و رمز عبور نهایی انجام می‌شود.

روش پیشنهادی بر ۱۰ گام استوار است که عبارتند از:

۱. ثبت‌نام و ایجاد پروفایل کاربر
۲. تولید رمز تصویری
۳. تولید رمز متنی
۴. تولید رمز الگوی رفتاری
۵. ارسال پیامک به کاربر
۶. راه‌اندازی پنجره زمانی
۷. اعتبارسنجی
۸. ذخیره‌سازی و رمزنگاری فعالیت‌های کاربر
۹. دریافت رمزهای متنی و تصویری
۱۰. بازتولید و ارسال رمز یکبارمصرف

کاربر هنگام ثبت نام باید یکی از دسته بندی‌ها را انتخاب کند که در این مرحله از دسته انتخابی برای تولید کد تصویری استفاده می‌شود. اگر طبق شکل دسته مورد نظر یک گل باشد و کاربر آن را به درستی انتخاب کرده باشد، عدد ۷ یک کد

ISSN: 2745-3673
http://www.Rcsj.ir

تصویری برای ایجاد رمز یکبار مصرف است. برای این منظور یکی از فیلدهای متنی در پروفایل کاربری به همراه یک عدد تصادفی ۴ رقمی برای کاربر ارسال می‌شود. در چنین حالتی اگر کاربر در شکل ابتدا شماره شناسه و سپس کد ملی ۴۵ را انتخاب کند و در صورت انجام برعکس عدد ۵۴ تولید می‌شود. در صورتی که نام کاربری «حسن» باشد و همان فیلد برای وی ارسال شده باشد، با انتخاب گزینه «نام»، از عدد ۱۰ به عنوان بخشی از رمز یکبار مصرف استفاده می‌شود. نکته بسیار مهمی که در قسمت قبل رعایت شد این است که می‌توان از الگوی رفتار کاربر به عنوان معیاری مناسب برای تولید رمز یکبار مصرف استفاده کرد. در مثال قبلی مشاهده شد که اولویت بندی فعالیت‌های کاربر می‌تواند منجر به تولید کدهای مختلف شود. به عبارت دیگر در پیامکی که برای کاربر ارسال می‌شود ترتیب فعالیت‌های وی مشخص می‌شود.

به کاربر گفته می‌شود ابتدا یک عدد تصادفی و سپس کد متنی و در نهایت کد تصویر را وارد کند. از آنجایی که طول عمر رمزهای یک بار مصرف باید محدود باشد، برای هر بار که یک رمز عبور یک بار مصرف برای کاربر ایجاد می‌شود، باید یک پنجره یک بار مصرف راه اندازی شود و اگر فرآیند احراز هویت در آن پنجره زمانی انجام نشود، آن پنجره رمز عبور زمان نامعتبر است. کاربر باید یک بار درخواست رمز عبور را دوباره ارسال کند. فرآیند اعتبارسنجی با دریافت یک رمز عبور یک بار مصرف توسط کاربر آغاز می‌شود و پس از رمزگشایی، باید به گونه‌ای عمل کند که اعتبار آن را در اسرع وقت تأیید کند تا سربار محاسباتی در سمت سرور به حداقل برسد.

ترکیب روش‌های مختلف برای تولید رمز یکبار مصرف موجب خواهد شد که حدس زدن آن برای مهاجمان مختلف از جمله حملات فیشینگ بسیار دشوار شده و در این راستا الگوهای رفتاری نقش بسیار مهمی را ایفا خواهند کرد. زیرا در بسیاری از روش‌ها و ابزارهای موجود راهکاری برای آن تعبیه نشده و بنابراین قادر خواهد بود که ضریب امنیت رمز یکبار مصرف را به طور قابل ملاحظه‌ای بالا ببرد. در این تحقیق یک راهکار ترکیبی برای تولید رمز یکبارمصرف ارائه گردید که متناسب با تعداد فاکتورهای انتخابی برای الگوهای رفتاری می‌توانند به صورت ضریبی از فاکتوریل تعداد الگوها، شانس افشاء رمزیکبارمصرف را کاهش دهد. همچنین راهکار پیشنهادی، روشی مبتی بر انتخاب تصویر و متن از جدول و ورود متن عددی با الگوی خاصی است که می‌تواند برای کاربر جذاب بوده و علی‌رغم پیچیدگی بالایی که برای رمز یکبارمصرف بوجود می‌آورد به نوعی کاربر پسند نیز باشد.

ارزیابی

در مرحله اول، داده‌های مورد نیاز برای ارزیابی روش پیشنهادی از طریق مدل‌سازی حملات مختلف جمع‌آوری شده و با استفاده از شبیه‌سازی عملکرد روش پیشنهادی در برابر حملات مختلف مشخص خواهد شد. برای هر حمله، دو حالت در نظر گرفته می‌شود، یا روش پیشنهادی می‌تواند در برابر آن مقاومت کند یا حمله موفق خواهد بود. اگر روش پیشنهادی بتواند از حمله جلوگیری کند، میزان پیشگیری آن افزایش می‌یابد و در غیر این صورت میزان پیشگیری کاهش می‌یابد. جدول (۲) مجموعه سناریوهایی که برای تولید این دادگان مورد استفاده قرار گرفته‌اند را نمایش می‌دهد.

جدول ۲. سناریوهای مورد استفاده برای شبیه‌سازی دادگان مربوط به حملات فیشینگ

ردیف	عنوان	توضیحات
۱	سناریو ۱	در این سناریو، مهاجم کاربر را به یک وب‌سایت جعلی راهنمایی کرده و تلاش می‌کند تا رمز عبور او را بدست آورد. در این حالت کاربر باید با توجه به تنظیمات خود در هنگام ثبت‌نام در سایت، متوجه جعلی بودن آن شده و از ارائه رمز عبور خودداری کند.
۲	سناریو ۲	در این سناریو مهاجم با جعل هویت کاربر به وب‌سایت مورد نظر دسترسی پیدا کرده و تلاش می‌کند با حدس زدن رمز عبور دسترسی مورد نیاز را بدست آورد. در این حالت وب‌سایت باید بتواند بر اساس الگوهای رفتاری، مهاجم را تشخیص داده و از ورود او جلوگیری کند.

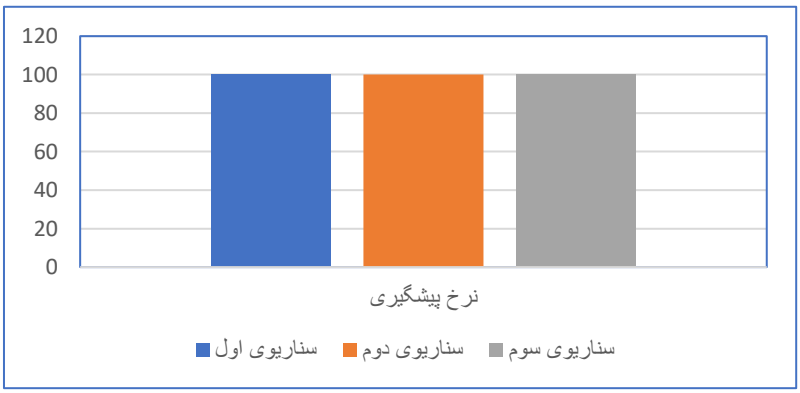
ISSN: 2745-3673
http://www.Rcsj.ir

۳	سناریو ۳	در این سناریو مهاجم با ذخیره‌سازی رمزهای یکبارمصرف قبلی کاربر تلاش می‌کند که دانش خود را از پروفایل کاربر کامل کرده و رمزهای یکبارمصرف بعدی را پیش‌بینی کند. در این حالت ضریب پیچیدگی رمز یکبار مصرف باید بتواند فعالیت مهاجم را با چالش روبرو کند.

برای انجام هر یک از سناریوهای ۳ گانه، با فرض اینکه مهاجم به صورت چرخشی به برخی از اطلاعات نمایه کاربر دسترسی دارد شبیه سازی شده است.

نتایج حاصل از انجام آزمایشات

شکل (۶) نرخ پیش‌گیری روش پیشنهادی را بر اساس آزمایشات انجام شده در تمامی سناریوهای مورد نظر نشان می‌دهد. بر اساس نمودار، نرخ پیشگیری از حملات فیشینگ در روش پیشنهادی ۱۰۰ درصد بدست آمده است که این موضوع کارایی روش پیشنهادی را در جلوگیری از حملات فیشینگ به خوبی نمایش می‌دهد.



شکل ۶. مقایسه نرخ پیشگیری روش پیشنهادی در سناریوهای مختلف

پیچیدگی یک رمز عبور نشان می‌دهد که یک رمز عبور چقدر قوی است تا مهاجم نتواند آن را حدس بزند. با فرض سناریویی که در آن یک مهاجم تمام یا بخشی از اطلاعات نمایه کاربر را به دست می‌آورد، یک رمز عبور یکبار مصرف همچنان باید بتواند بازدارنده خوبی باشد. در روش پیشنهادی با وجود حفظ سادگی و کاربرپسندی رمز یکبار مصرف، مشکل پیچیدگی آن را در چندین سطح مختلف انجام داده‌ایم که در ادامه به توضیح آن می‌پردازیم. ما الگوهای رفتاری را به عنوان دنباله‌ای از فعالیت‌های انجام شده توسط کاربر تعریف می‌کنیم و بر اساس آن ترتیب وارد کردن قسمت‌های مختلف رمز عبور یک بار مصرف را به عنوان یک الگو در نظر می‌گیریم. در این سطح، برای تعداد بخش‌های مختلف رمز یک بار مصرف، ضریب پیچیدگی بر اساس جایگشت‌های مختلف افزایش می‌یابد و بر اساس رابطه فاکتوریل، تعداد بخش‌های رمز یک بار مصرف افزایش می‌یابد. اگر از k دسته‌های تصویر مختلف استفاده شود و برای هر دسته از m تصویر متفاوت استفاده شود، پیچیدگی رمز عبور پیشنهادی به نسبت رابطه زیر افزایش می‌یابد: ضریب پیچیدگی. جدول (۳) یک مقایسه توصیفی بین روش پیشنهادی و روش‌های ترکیبی و روش‌های ساده انجام داده است.

جدول ۳. مقایسه توصیفی روش پیشنهادی

ردیف	معیار	روش ساده	روش ترکیبی	روش پیشنهادی
۱	پیچیدگی	کمتر	متوسط	بیشتر
۲	نرخ پیشگیری	کمتر	متوسط	بیشتر
۳	سادگی	بیشتر	کمتر	کمتر
۴	جذابیت	کمتر	بیشتر	بیشتر

ISSN: 2745-3673
http://www.Rcsj.ir

به طور کلی روش پیشنهادی کارایی بسیار بالایی دارد و پیشرفت‌های زیادی را به همراه داشته است. چیزی که این فعالیت را به عنوان یک تحقیق دانشگاهی برجسته متمایز می‌کند، تمرکز آن بر الگوهای رفتاری کاربر است که می‌تواند فصل جدیدی را در زمینه تولید و استفاده از رمزهای عبور برای آینده باز کند. جداسازی رمزگذاری یکبار مصرف در محاسبات، سمت سرور و کاربر از دیگر مزیت‌های ویژه روش پیشنهادی است که می‌تواند امنیت آن را حتی در صورت وجود حملات شنود به خوبی تضمین کند.

نتیجه گیری

نتیجه نهایی

رمز یکبار مصرف جایگزینی برای رمز دوم است که برای امنیت دسترسی کاربران به سیستم‌های الکترونیکی ارائه می‌شود و از قابلیت‌های رمزنگاری استفاده می‌کند. استفاده از رمزهای عبور یکبار مصرف در اپلیکیشن های احراز هویت، علاوه بر افزایش امنیت تبادل اطلاعات و ارتباطات، می‌تواند برای جلوگیری از حملاتی که قصد فریب و سرقت اطلاعات کاربران را دارند نیز مورد استفاده قرار گیرد. امروزه این نوع حملات که عمدتاً با عنوان حملات فیشینگ شناخته می‌شوند، از تنوع زیادی برخوردار بوده و همواره امنیت کاربران را در فضای مجازی تهدید می‌کنند. یکی از راهکارها برای این منظور استفاده از رمزهای یک بار مصرف است و علیرغم فعالیت‌های زیادی که تاکنون در زمینه توسعه رمزهای عبور یکبار مصرف برای جلوگیری از حملات فیشینگ انجام شده است، اما این حوزه به عنوان یک میدان باز تحقیقاتی و تحقیقاتی شناخته شده است. لازم است تحقیقات بیشتری در این زمینه صورت گیرد. راه حل پیشنهادی مبتنی بر انتخاب تصویر و متن از جدول و وارد کردن متن عددی با الگوی خاصی است که می‌تواند برای کاربر جذاب باشد و علیرغم پیچیدگی بالایی که برای رمز یک بار مصرف ایجاد می‌کند، کاربر نیز می‌باشد.

با توجه به کاربرد، دقت و قابلیت اطمینان روش، این مطالعه پیشنهاد کرد که یک فرآیند کامل برای به روز رسانی مدل و استخراج دانش جدید در مورد چگونگی تغییر پدیده فیشینگ انجام شود .این مطالعه همچنین طبقه‌بندی ویژگی‌ها را با استفاده از مدل‌های یادگیری ماشین و یادگیری عمیق با فرآیند تنظیم دقیق فراپارامتر ارائه کرد .با این حال، آموزش‌های مرتبط با شبکه‌های یادگیری عمیق به دلیل محاسبات ریاضی عظیمی که می‌توان انجام داد، به منابع بیشتری نیاز دارند و در مورد طبقه‌بندی باینری برای تشخیص حملات فیشینگ، مدل‌های موجود نه تنها عملکرد و دقت بسیار خوبی را نشان داده‌اند، بلکه همچنین به کاهش میزان خطا کمک کرد .مشارکت در مطالعه حاضر ارزشمند است زیرا روشی منحصر به فرد را با ادغام شش روش الگوریتمی مختلف ایجاد کرده است.

پیشنهادات برای تحقیقات آینده

یکی دیگر از مشکلات ارزیابی‌های امنیتی، کمبود اطلاعات در مورد الگوهای حمله و روش‌های استفاده شده توسط مهاجمان است. اگرچه کارایی راه حل پیشنهادی برای الگوی رفتاری تنظیم شده به خوبی نشان داده شده است، اما به عنوان پیشنهادی برای ادامه این تحقیق، می‌توان الگوهای رفتاری پیچیده‌تری را در نظر گرفت. هر فرآیندی مانند انتخاب متن یا تصویر را می‌توان به عنوان مجموعه‌ای از الگوهای رفتاری پیچیده‌تری تعریف کرد. استفاده از روش‌های مختلف رمزنگاری نیز می‌تواند به روش‌های جالبی منجر شود، بنابراین پیشنهاد می‌شود در تحقیقات آتی به این موضوع توجه شود. اگرچه روش پیشنهادی در آزمایشگاه عملکرد خوبی داشته است، اما نیاز به استفاده واقعی دارد و تنها در چنین شرایطی می‌توان به قابلیت‌های واقعی آن یا هر تحقیق دانشگاهی دیگری پی برد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] G.Aaron, and R. Rasmussen, Global phishing survey: trends and domain name use in 2H2014, Anti-Phishing Working Group (APWG), Lexington, MA, 2014.
[2] M. Abdalla, O. Chevassut, and D. Pointcheval, One-time verifier-based encrypted key exchange. In Public Key Cryptography-PKC 2005, Springer Berlin Heidelberg, pp. 47-64, 2005.
[3] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, How to attack two-factor authentication internet banking. In Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 322-328, 2013.
[4] I.G.N. Agung, A.K. Agung, G.M.A. Sasmita, Dynamic Mobile Token for Web Security using MD5 and One Time Password Method, International Journal of Computer Applications, vol. 55, no. 6, 2012.
[5] M.H. Almeshekah, M.J. Atallah, E.H. Spafford, Defending against Password Exposure using Deceptive Covert Communication, 2015.
[6] A.J. Atkinson, D.L. McDonald, D.L. Mcdonald, R.J. Atkinson, and C. Metz, One time passwords in everything (OPIE): Experiences with building and using stronger authentication. In In Proc, 5th USENIX Security Symposium, 1995.
[7] H. Berghel, J. Carpinter, and J.Y. Jo, Phish phactors: Offensive and defensive strategies, Advances in Computers, vol. 70, pp. 223-268, 2007.
[8] R.S. Bhuvaneshwari, and P. Anuja, Secured Password Management Technique Using One-Time Password Protocol In Smartphone, International Journal of Computer Science and Mobile Computing, IJCSMC, vol. 3, no. 3, pp. 976-981, 2014.
[9] K. Biçakci, and N. Baykal, Improving the security and flexibility of one-time passwords by signature chains, Turkish Journal of Electrical Engineering & Computer Sciences, vol. 11, no. 3, pp. 223-236, 2003.
[10] S. Brostoff, P. Inglesant, and M.A. Sasse, Evaluating the usability and security of a graphical one-time PIN system, InProceedings of the 24th BCS Interaction Specialist Group Conference, British Computer Society, pp. 88-97, September 2010.
[11] P.Chan, T. Halevi, and N. Memon, Glass OTP: Secure and Convenient User Authentication on Google Glass. In Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 298-308, 2015.
[12] G.K. Chaudhary, Development Review on Phishing: A Computer Security Threat, 2014.
[13] A.G. Chellaiah, Preventing Phishing attacks using anti-phishing prevention technique,. In International Journal of Engineering Development and Research, vol. 2, March 2014,
[14] C. Chen, C.J. Mitchell, and S. Tang, Ubiquitous one-time password service using the Generic Authentication Architecture, Mobile Networks and Applications, vol. 18, no. 5, pp. 738-747, 2013.
[15] R. Coombs, Securing the Future of Authentication with ARM TrustZone-based Trusted Execution Environment and Fast Identity Online (FIDO). ARM White Paper, 2015.
[16] O. Delgado, A. Fúster Sabater, and J.M. Sierra, Analysis of new threats to online banking authentication schemes, 2008.
[17] J.S. Downs, M. Holbrook, and L.F. Cranor, Behavioral response to phishing risk. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, pp. 37-44, October 2007.
[18] A. Dmitrienko, C. Liebchen, C. Rossow, and A.R. Sadeghi, Security analysis of mobile two-factor authentication schemes, Intel® Technology Journal, vol. 18, no. 4, 2014.
[19] M.H. Eldefrawy, M.K. Khan, K. Alghathbar, T.H. Kim, H. Elkamchouchi, Mobile one-time passwords: two-factor authentication using mobile phones, Security and Communication Networks, vol. 5, no. 5, pp. 508-516, 2012.
[20] A. Emigh, Online identity theft: Phishing technology, chokepoints and countermeasures, Identity Theft Technology Council, 2005.
[21] D. Emm, M. Garnaeva, R. Unuchek, D. Makrushin, and A. Ivanov, IT THREAT EVOLUTION IN Q3 2015, 2014.

ISSN: 2745-3673
http://www.Rcsj.ir

[22] D. Florêncio, and C. Herley, One-time password access to any server without changing the server. In Information Security, Springer Berlin Heidelberg, pp. 401-420, 2008.
[23] M.M. Gaurav, and A. Jain, Anti-Phishing Techniques: A Review, International Journal of Engineering Research and Applications, vol. 2, no. 2, pp. 350-355, 2012.
[24] E. Ghazizadeh, Z.S. Shams Dolatabadi, R. Khaleghparast, M. Zamani, A.A. Manaf, and M.S. Abdullah, Secure OpenID authentication model by using Trusted Computing. In Abstract and Applied Analysis, Hindawi Publishing Corporation, Vol. 2014, November 2014.
[25] V. Goyal, A. Abraham, S. Sanyal, and S.Y. Han, The N/R one time password system. In Information Technology: Coding and Computing, 2005. ITCC 2005, International Conference, Vol. 1, pp. 733-738, April 2005.
[26] B. Groza, and D. Petrica, One-time passwords for uncertain number of authentications. Proceedings of CSCS15, 2005.
[27] M.G. Gouda, A.X. Liu, L.M. Leung, and M.A. Alam, Single password, multiple accounts. In Proc. 3rd Int. Conf. on Applied Cryptography and Network Security. New York City, NY, USA, pp. 1-12, 2005.
[28] N. Gupta, Analysis of Issues in phishing attack and development of prevention mechanism. Journal of Global Research in Computer Science, vol. 5, no. 6, pp. 22-25. 2014.
[29] R. Gupta, and P.K. Shukla, Performance Analysis of Anti-Phishing Tools and Study of Classification Data Mining Algorithms for a Novel Anti-Phishing System, International Journal of Computer Network and Information Security (IJCNIS), vol. 7, no. 12, p. 70, 2015.
[30] R. Gupta, and P.K. Shukla, System Design, Investigation and Countermeasure of Phishing Attacks using Data Mining Classification Methods and its Analysis. International Journal of Advanced Science and Technology, vol. 78, pp. 29-40, 2015.
[31] S. Gupta, S. Sahni, P. Sabbu, S. Varma, and S.V. Gangashetty, Passblot: A Highly Scalable Graphical One Time Password System, International Journal of Network Security & Its Applications, vol. 4, no. 2, pp. 201, 2012.
[32] T.H. Gurav, and M. Dhage, Remote client authentication using mobile phone generated OTP, International Journal of Scientific and Research Publications, vol.2, no. 5, p. 4, 2012.
[33] S. Hamdare, V. Nagpurkar, and J. Mittal, Securing SMS Based One Time Password Technique from Man in the Middle Attack. arXiv preprint arXiv:1405.4828, 2014.
[34] J. Hong, The state of phishing attacks, Communications of the ACM, vol. 55, no. 1, pp. 74-81, 2012.
[35] R. Howard, R. Thomas, J. Burstein, and R. Bradescu, Cyber Fraud Trends and Mitigation. In The International Conference on Forensic Computer Science (ICoFCS), 2007.
[36] C.Y. Huang, S.P. Ma, and K.T. Chen, Using one-time passwords to prevent password phishing attacks. Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1292-1301, 2011.
[37] H. Huang, J. Tan, and L. Liu, Countermeasure techniques for deceptive phishing attack. In New Trends in Information and Service Science, 2009. NISS'09. International Conference, pp. 636-641, June 2009.
[38] Y. Huang, Z. Huang, H. Zhao, and X. Lai, A new one-time password method. IERI Procedia, vol. 4, pp. 32-37, 2013.
[39] J.J. Hwang, Y.C. Hsu, and G.Y. Liao, An SMS-Based One-Time-Password Scheme with Client-Side Validation, Journal of Digital Information Management, vol. 13, no. 2, 2015.
[40] R. Isawa, and M. Morii, One-Time Password Authentication Scheme to Solve Stolen Verifier Problem. In Proc, of Forum on Information Technology, 2011.
[41] B. Issac, R. Chiong, and S.M. Jacob, Analysis of Phishing Attacks and Countermeasures. arXiv preprint arXiv:1410.4672, 2014.
[42] M. Jakobsson, and J. Ratkiewicz, Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In Proceedings of the 15th international conference on World Wide Web. ACM.Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and

ISSN: 2745-3673
http://www.Rcsj.ir

countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, pp. 513-522, May 2006.
[43] M. Jakobsson, and A.L. Young, Distributed Phishing Attacks. IACR Cryptology ePrint Archive, p. 91. 2005.
[44] A. Jesudoss, and N. Subramaniam, A Survey on Authentication Attacks and Countermeasures in a Distributed Environment, IJCSE, vol, 5, no. 2, 2014.
[45] E. Kalaikavitha, and J. Gnanaselvi, Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology', Research Inventy: International Journal of Engineering and Science, vol. 2, no. 10, pp. 14-17, 2013.
[46] A. Kavoukis, and S. Aljareh, Efficient time synchronized one-time password scheme to provide secure wake-up authentication on wireless sensor networks. arXiv preprint arXiv:1302.1756, 2013.
[47] A.A. Khan, Preventing phishing attacks using one time password and user machine identification. arXiv preprint arXiv:1305.2704, 2013.
[48] M. Kim, B. Lee, S. Kim, and D. Won, Weaknesses and improvements of a one-time password authentication scheme, International Journal of Future Generation Communication and Networking, vol. 2, no. 4, 2009.
[49] P.P.N. G. Kumar, and R.J. Mathew, An Advanced Anti Phishing Approach Based On Two-Tier Validation, IJRCCT, vol. 3, no. 9, pp. 1015-1017, 2014.
[50] B.K. Kushwaha, An approach for user authentication One Time Password (Numeric and Graphical) Scheme, Journal of Global Research in Computer Science, vol. 3, no. 11, 2012.
[51] M.A. Kute, Modern Method for Detecting Web Phishing Using Visual Cryptography (VC) and Quick Response Code (QR code), International Journal of engineering Research and Applications, vol. 1, no. 5, pp.1-5, 2015.
[52] Y. Lee, and H. Kim, Insider Attack-Resistant OTP (One-Time Password) Based on Bilinear Maps. International Journal of Computer and Communication Engineering, vol. 2, no. 3, p. 304, 2013.
[53] Z. Li, W. He, D. Akhawe, and D. Song, The emperor's new password manager: Security analysis of web-based password managers, In 23rd USENIX Security Symposium (USENIX Security 14), pp. 465-479, 2014.
[54] A.Y. Lindell, Time versus Event Based One-Time Passwords, Aladdin Knowledge Systems, 2007.
[55] D. Mahto, and D.K. Yadav, Security Improvement of One-Time Password Using Crypto-Biometric Model. In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. Springer India, pp. 347-353, 2016.
[56] R. Manning, and G. Aaron, Phishing Activity Trends Report. Anti-Phishing Working Group (APWG), Rep, 1st Quarter 2014, 2014.
[57] R. Manning, and G. Aaron, Phishing Activity Trends Report. Anti-Phishing Working Group (APWG), Rep. 1st-3rd Quarter 2015, 2015.
[58] R. Manning, and G. Aaron, Phishing Activity Trends Report, Anti-Phishing Working Group (APWG), Rep. 4th Quarter 2015, 2016.
[59] K. Marimuthu, D.G. Gopal, H. Mehta, and A.R.P. Boominathan, A NOVEL WAY OF INTEGRATING VOICE RECOGNITION AND ONE TIME PASSWORDS TO PREVENT PASSWORD PHISHING ATTACKS, International Journal of Distributed and Parallel Systems, vol. 5, no. 4, p. 11, 2014.
[60] C.J. Marinakis, and N.N. Karanikolas, Strengthening the security of e-banking transactions. The case of NBG, Current Trends in Informatics, pp. 559-570, 2007.
[61] J. Milletary, and C.C. Center, Technical trends in phishing attacks, Retrieved December, vol. 1, pp. 3-3, 2005.
[62] M. Mishra, J.A. Gaurav, and A. Jain, A Preventive Anti-Phishing Technique using Code word, International Journal of Computer Science and Information Technologies, vol. 3, no. 3, pp. 4248-4250, 2012.

ISSN: 2745-3673
http://www.Rcsj.ir

[63] C. Mulliner, R. Borgaonkar, P. Stewin, and J.P. Seifert, SMS-based one-time passwords: attacks and defense. In Detection of Intrusions and Malware, and Vulnerability Assessment, Springer Berlin Heidelberg, pp. 150-159, 2013.
[64] P.J. Nero, B. Wardman, H. Copes, and G. Warner, Phishing: Crime that pays. In eCrime Researchers Summit (eCrime), pp. 1-10, November 2011.
[65] A. Onashoga, A. Sodiya, and A. Afolorunso, A One-Time Server-Specific Password Authentication Scheme. CIT, Journal of Computing and Information Technology, vol. 20, no. 2, pp. 85-93, 2012.
[66] D. Oswald, B. Richter, and C. Paar, Side-channel attacks on the Yubikey 2 one-time password generator. In Research in Attacks, Intrusions, and Defenses, Springer Berlin Heidelberg, pp. 204-222, 2013.
[67] H. Parmar, N. Nainan, and S. Thaseen, Generation of secure one-time password based on image Authentication. Computer Science & Information Technology, 195206, 2012.
[68] Y. Patel, and M.S.C. Diana, Fingerprint Authentication Technique to Prevent Phishing using Pattern Matrix, International Journal of Engineering Research and Development, Volume 6, Issue 8, pp. 88-92, April 2013
[69] B. Parno, C. Kuo, and A. Perrig, Phoolproof phishing prevention. Springer Berlin Heidelberg, pp. 1-19, 2006.
[70] A. Perrig, The BiBa one-time signature and broadcast authentication protocol. In Proceedings of the 8th ACM conference on Computer and Communications Security, pp. 28-37, November 2001.
[71] M.V. Prakash, P.A. Infant, and S.J. Shobana, Eliminating vulnerable attacks using one time password and passtext analytical study of blended schema, Universal Journal of Computer Science and Engineering Technology, vol. 1, no. 2, pp. 133-140, 2010.
[72] S. Purkait, Phishing counter measures and their effectiveness-literature review. Information Management & Computer Security, vol. 20, no. 5, pp. 382-420, 2012.
[73] H. Raddum, L.H. Nestås, and K.J. Hole, Security analysis of mobile phones used as OTP generators. In Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, Springer Berlin Heidelberg, pp. 324-331, 2010.
[74] C.J.N. Rani, L. Joseph, and E.R. Naganathan, Secure One Time Password Generation for Website Security using Mobile Phone with Biometrics, 2013.
[75] D.D. Rao, G. Kour, and D. Jyoti, One Time Password Security through Cryptography for Mobile Banking, 2011.
[76] A.D. Rubin, Independent one-time passwords. Computing Systems, vol. 9, no. 1, pp. 15-27, 1996.
[77] M. Slyman, An evaluation of hypothetical attacks against the PassWindow authentication method [Electronic resource]. The PassWindow method.–2009.–Available at:http://www.passwindow.Com/evaluation_of_hypothetical_attacks_against_passwindow. Pdf.
[78] H. Sun, K. Sun, Y. Wang, and J. Jing, TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens, InProceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 976-988, October 2015.
[79] A. Tandon, R. Sharma, S. Sodhiya, and P.M. Vincent, QR Code based secure OTP distribution scheme for Authentication in Net-Banking, International Journal of Engineering & Technology, pp. 0975-4024, 2013.
[80] R. Van Rijswijk-Deij, Simple Location-Based One-time Passwords.Utrecht: Technical Paper, 2010.
[81] I.R. Widiasari, Combining Advanced Encryption Standard (AES) and One Time Pad (OTP) Encryption for Data Security, International Journal of Computer Applications, vol. 57, no. 20, 2012.
[82] M. Wu, R.C. Miller, and S.L. Garfinkel, Do security toolbars actually prevent phishing attacks? In Proceedings of the SIGCHI conference on Human Factors in computing systems, pp. 601-610, April 2006.
[83] S. Yadav, and B. Bohra, A review on recent phishing attacks in Internet. In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1312-1315, October 2015.