بسم الله الرحمن الرحیم

پروپوزال

واسط امن سامانه‌های تحت وب

Saman Web Shield

نسخه ۱.۰

شرکت مهندسی ارتباطی پیام‌پرداز

پیام‌پرداز
پیشران اطلاعات و ارتباطات امن

تیرماه ۱۴۰۲

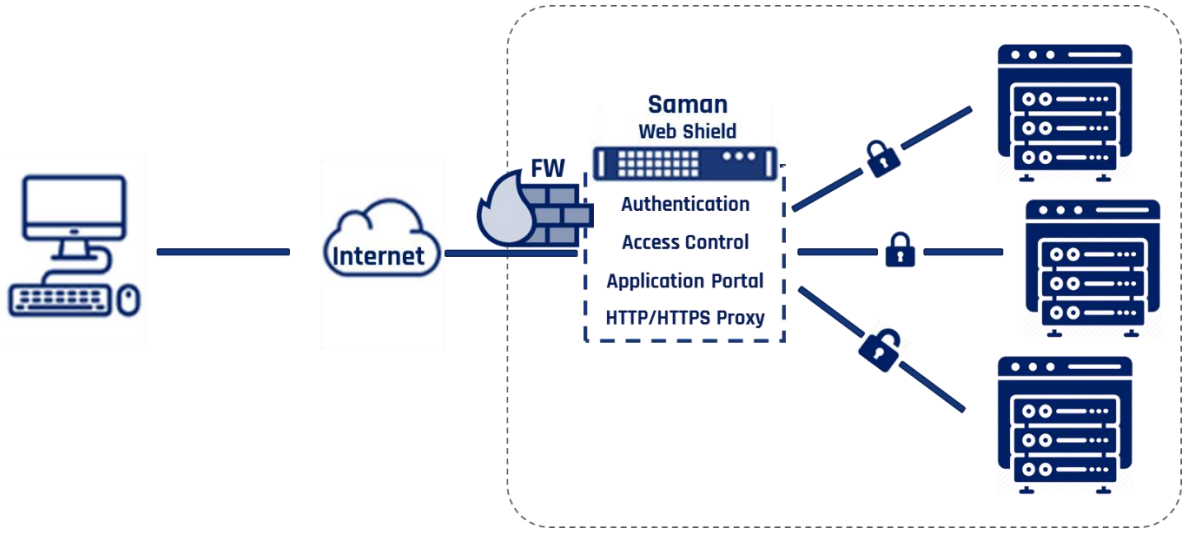
شرکت مهندسی ابل رایان پویا نماینده رسمی شرکت مهندسی ارتباطی پیام پرداز

فهرست مطالب

مقدمه

مطالعات و بررسی‌های انجام‌شده توسط موسسه Verizon در سال ۲۰۲۲ نشان می‌دهد؛ از میان حملات و نفوذهای امنیتی صورت گرفته به سازمان‌های مختلف در دنیا، مهم‌ترین هدف حملات سایبری در سال ۲۰۲۲ (با حدود ٦٥ درصد) سامانه‌ها و نرم‌افزارهای تحت وب بوده است. از میان این حملات، بیش از ۸۰ درصد آن‌ها از طریق پسوردهای ضعیف و لورفته و حدود ۱۵ درصد ناشی از آسیب‌پذیری[1]های نرم‌افزار بوده‌است و منشا کلیه این حملات، حمله‌کننده‌های خارجی[2] بوده‌است. بنابراین و با توجه به گزارش مذکور، حفاظت از سامانه‌های تحت وب منتشرشده در اینترنت به مهم‌ترین دغدغه‌ی سازمان‌ها تبدیل شده‌است.

خانواده محصولات سامان تلاش می‌کند با رفع دغدغه‌های گزارش‌شده و همگام با مفاهیم به‌روز Zero Trust و دفاع در عمق، امنیت سامانه‌های تحت وب را برای سازمان به ارمغان آورد. از این رو، محصول واسط امن سامانه‌های تحت وب سامان (با نام تجاری سامان وب‌شیلد (ساوش)) تلاش می‌کند، از دسترسی مستقیم حمله‌کننده‌ها به سامانه‌های تحت وب جلوگیری نموده و تنها در صورتی که کاربران فرآیند احراز اصالت چندعاملی را طی کرده باشند، آن سامانه در دسترس کاربر قرار می‌گیرد. مطابق شکل زیر، ساوش، به عنوان یک واسط، درخواست‌های ارسالی به سمت سامانه‌های تحت وب سازمان را پایش کرده و تنها به کاربران مجاز اجازه دسترسی خواهد داد.



شکل ۱. معماری قرارگیری ساوش در شبکه سازمان‌ها

بر خلاف راهکارهای دسترسی راه‌دور نظیر VPNها، تمرکز سامان وب‌شیلد بر تجربه کاربری ساده است و از این رو کاربران سامان **بدون نیاز به نصب نرم‌افزارهای ثالث** بر روی کامپیوتر شخصی خود و حتی بدون تغییر چشم‌گیر در فرآیند استفاده از سامانه‌های مورد نظیر خود، به استفاده از سامانه ادامه می‌دهد. همچنین، سامان از طریق تنوع روش‌های احراز اصالت چندعاملی، دسترسی امن‌تر کاربران به سامانه‌های تحت وب را تضمین می‌کند.

برخی از مهم‌ترین ویژگی‌های فنی سامان-SWP عبارتند از:

[1] Vulnerability
[2] External Attackers

سبک، سریع و قدرتمند

مقیاس‌پذیری بالای سامانه برای استفاده در سامانه‌های تحت وب با تعداد کاربران میلیونی

احراز اصالت قوی

به‌کارگیری ویژگی‌های سامان-MFA برای تامین به‌روزترین روش‌های احراز اصالت چندعاملی

کنترل دسترسی

امکان محدود کردن دسترسی کاربران به سامانه‌ها بر اساس نقش و گروه آن‌ها

ورود یکباره

پشتیبانی از روال‌های استاندارد ورود SAML، CAS، OpenID Connect، NTLM، Basic Auth و ... برای حذف فرایند قدیمی ورود سامانه‌های محافظت‌شده

جلوگیری از حملات وب

جلوگیری از حملات حوزه جعل هویت، جلوگیری از دسترسی حمله‌کننده به آسیب‌پذیری‌های سامانه‌های محافظت شده و جلوگیری از حملات brute force

ممیزی و گزارش‌گیری

امکان مشاهده لاگ و گزارشات کلیه درخواست‌های کاربران در سامانه‌های مختلف و امکان ارسال لاگ‌ها برای سامانه‌های SIEM

سهولت کاربری بالا

دسترسی ساده کاربران به سامانه‌های تحت وب بدون نیاز به نصب نرم‌افزارهای اضافه و طی‌کردن فرآیندهای پیچیده

مبتنی بر استانداردهای به‌روز

مبتنی بر فلسفه‌های امنیتی Zero Trust و دفاع در عمق

قابل اتکا

پایداری و اتکا پذیری بالا، خدمات ۵x۸ و ۷x۲۴، ارائه راهکار برای شرایط بحرانی، اتکاپذیری 99.999%

۱- احراز اصالت چندعاملی

همانطور که گفته شد استفاده از سامان وب‌شیلد گام مهمی در راستای امن‌سازی ارتباط امن کاربران با سامانه‌های تحت وب است و از طریق کاربران تنها زمانی اجازه دسترسی به سامانه‌های مد نظر را خواهند داشت که فرآیند احراز اصالت را طی کرده باشند. هر چند سامانه پیشنهادی از پروتکل‌ها و مکانیزم‌های امنیتی استاندارد برای حفظ امنیت در تمامی مراحل احراز اصالت استفاده می‌کند، اما همواره غفلت کاربران در نگهداری از کلمه عبور می‌تواند امنیت سازمان را با خطراتی مواجه کند. در صورتی که یک کاربر در نگهداری از کلمه عبور خود غفلت کند، هر فردی با دانستن کلمه عبور وی می‌تواند در تمامی سامانه‌های مربوطه (که کاربر به آن‌ها دسترسی دارد)، لاگین کند. احراز اصالت چندعاملی پاسخی برای رفع این دغدغه به شمار می‌رود.

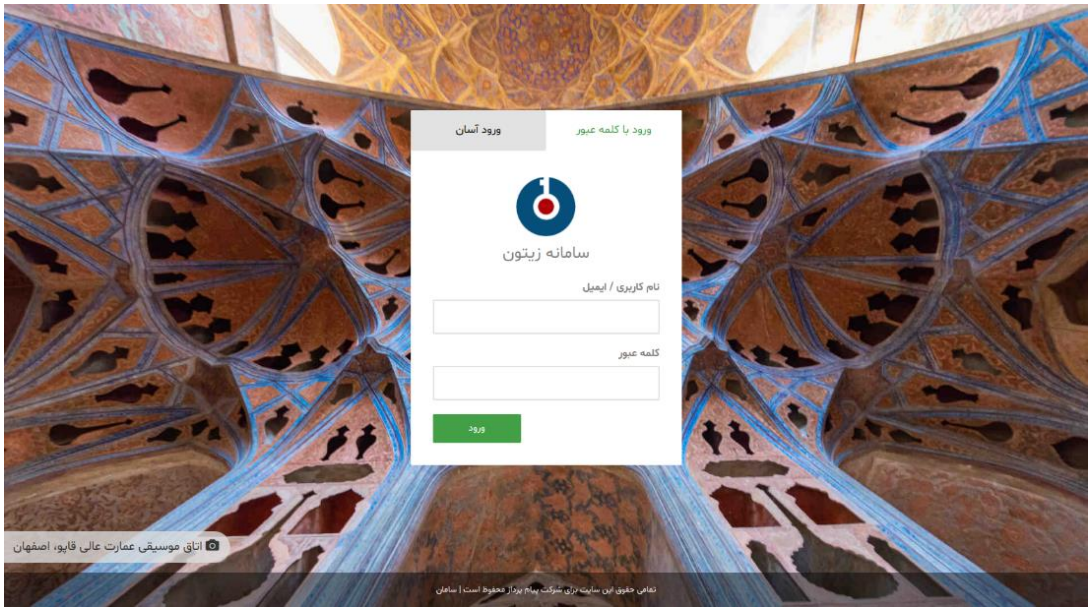
سامانه پیشنهادی به منظور تامین احراز اصالت چندعاملی از سیستم احراز اصالت چند عاملی[۳] سامان (با نام تجاری Saman-MFA) استفاده می‌کند. Saman-MFA متشکل از مجموعه کاملی از روش‌ها و فرآیندهای استاندارد، قابل اعتماد، امن و کاربرپسند برای احراز اصالت است که با هدف تحقق مفهوم احراز اصالت قوی[۴] ورود کاربران به سامانه‌ها، تجهیزات و برنامه‌های کاربردی در سطح سازمان توسعه یافته است.

از نظر تجربه کاربری، تمرکز سیستم احراز اصالت Saman-MFA بر روی تلفن‌های همراه هوشمند است. چرا که از یک سو این دستگاه‌ها همواره در دسترس کاربران هستند و از سوی دیگر از انعطاف‌پذیری و قدرت پردازشی قابل قبولی برای تحقق روال‌ها، پروتکل‌ها و الگوریتم‌های امن برخوردار می‌باشند. سیستم احراز اصالت Saman-MFA، فرآیندهای احراز اصالت استاندارد مبتنی بر پیام‌های Push، کدهای TOTP و HOTP، و همچنین روال

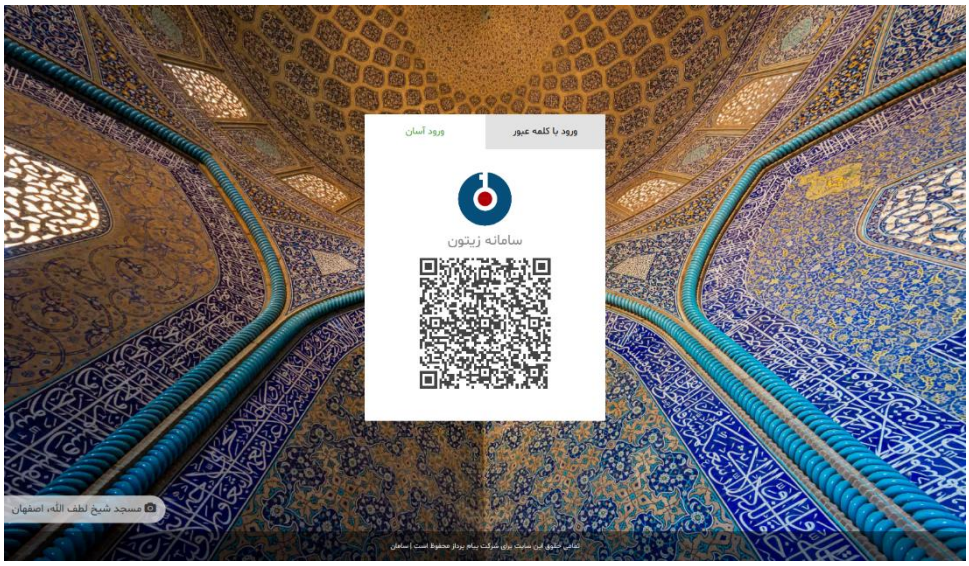
[۳] Multi-Factor Authentication
[۴] Strong Authentication

بدون کلمه عبور مبتنی بر QR-Code را در قالب اپلیکیشن موبایل اختصاصی بر روی انواع تلفن‌های همراه ارائه می‌دهد.

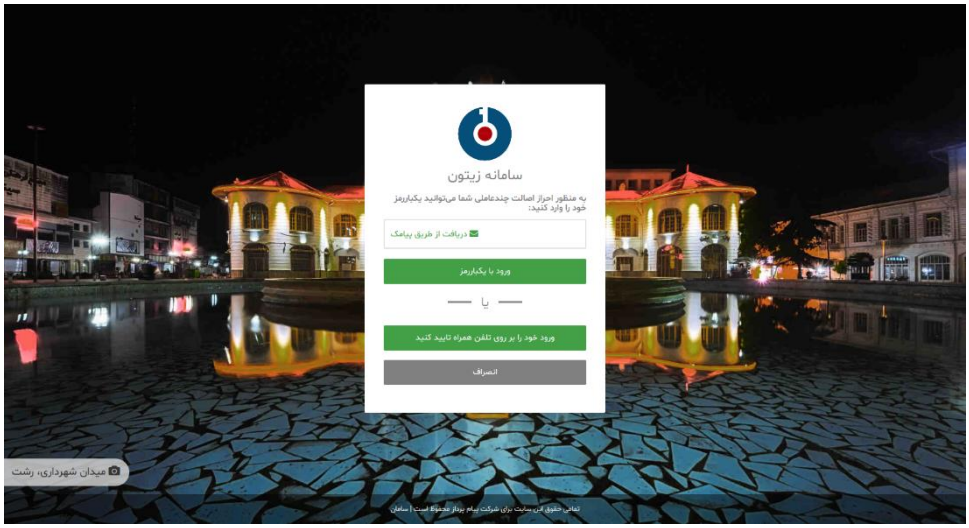
شکل‌های زیر صفحات ورود سامان وب‌شیلد به صورت چندعاملی را نمایش می‌دهد.



شکل ۲. صفحه‌ی ورود در سامان-IAM

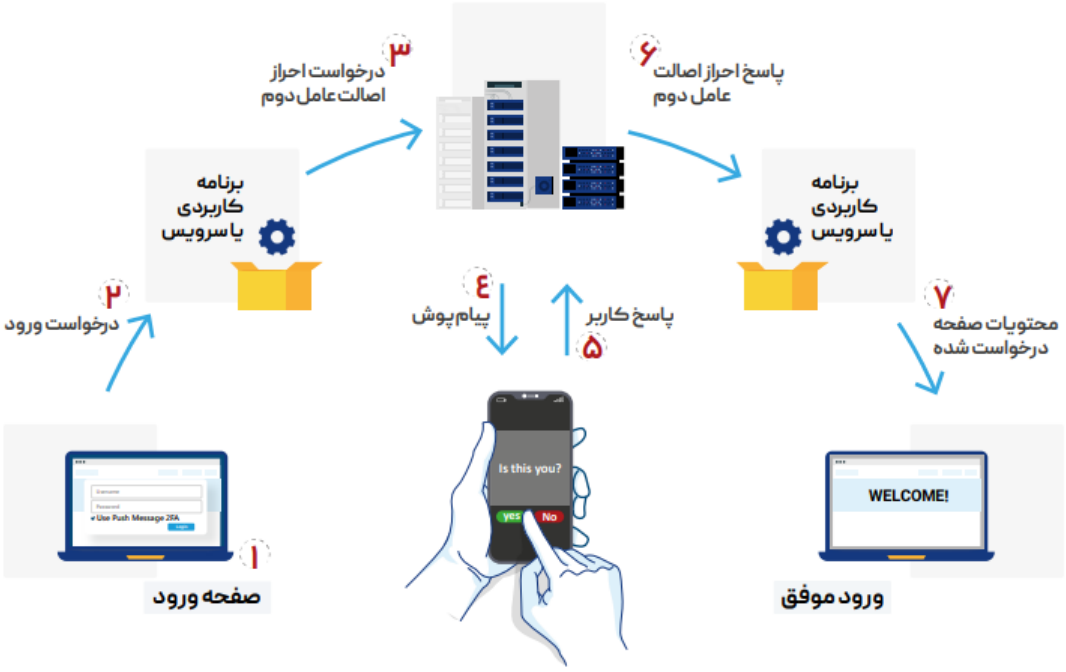


شکل ۳. صفحه‌ی ورود آسان (ورود با QRCode)



شکل ٤. صفحه انتخاب روش‌های چندعاملی ورود از طریق سامان-IAM

لازم به ذکر است با استفاده از Saman-MFA علاوه بر چندعاملی نمودن فرآیند احراز اصالت ورود یکباره، می‌توان فرآیند احراز اصالت تجهیزات، سامانه‌ها و سیستم‌عامل‌های سازمان را (حتی در حالتی که به SSO Server متصل نباشند) نیز چندعاملی نمود. برای بهره بردن از این امکان می‌توان از APIها، Agentها و SDKهای Saman-MFA استفاده کرد. به عنوان نمونه شکل زیر فرآیند احراز اصالت چندعاملی یک کاربررا از طریق پیام‌های پوش نمایش می‌دهد. در این شکل، برنامه‌ی کاربردی می‌تواند هر یک از تجهیزات زیرساختی، سیستم‌های عامل، سامانه‌های تحت وب و ... باشد.



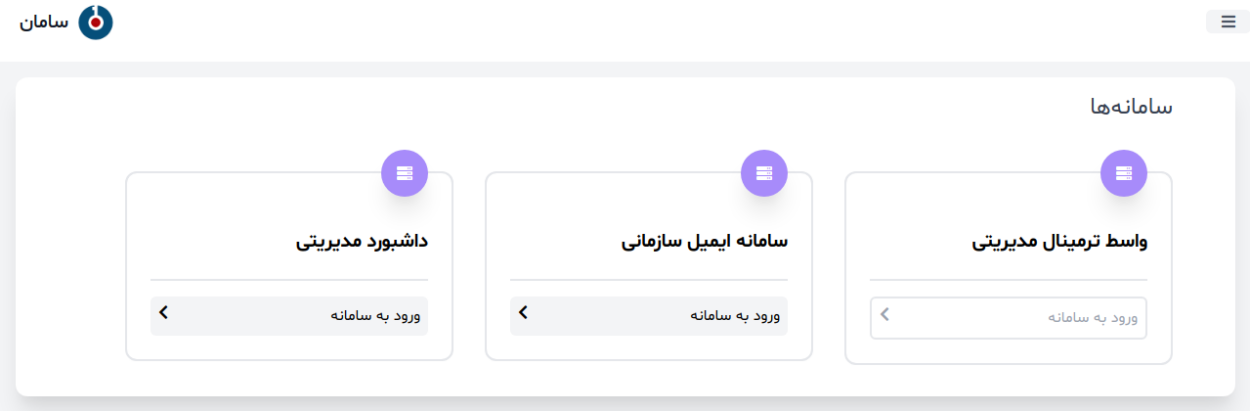
شکل ۵. سناریو نمونه استفاده از سامان-MFA برای احراز اصالت چندعاملی مبتنی بر روش پیام پوش

لازم است خاطر نشان نماییم استفاده از محصول سامان-MFA در فرایند احراز اصالت محصول سامان-IAM کاملا رایگان است، اما استفاده از آن برای احراز اصالت چندعاملی سیستم‌عامل‌ها، سامانه‌ها، تجهیزات زیرساختی، سامانه‌های دسترسی راه‌دور و ... **نیازمند تامین لایسنس مستقل** است.

در ادامه به بررسی جزئی‌تر ویژگی‌های سامان وب‌شیلد می‌پردازیم.

۲- پرتال

در سازمان‌هایی که مجهز به سامانه‌های متعدد هستند، کاربران همواره با به خاطر سپردن آدرس سامانه‌ها مشکل دارند، به این منظور سامانه پیشنهادی از طریق یک پرتال به کاربران اجازه می‌دهد پس از لاگین، لیست سامانه‌هایی که به آن‌ها دسترسی دارند را مشاهده نموده و از میان آن‌ها سامانه مد نظر خود را انتخاب نمایند.



شکل ٦. نمایی از پرتال و سامانه‌های در دسترس کاربر

۳- داشبوردهای هوشمندی کسب‌وکار

به منظور گزارش‌گیری، استفاده از یکی از داشبوردهای هوشمندی کسب‌وکار در کنار سامانه پیشنهادی توصیه می‌شود. به این منظور اطلاعات خام احراز اصالت کاربران، دسترسی‌ها و ... را توسط یک View[۵] فقط خواندنی[٦] برای استفاده در داشبورد مربوطه ارائه می‌شود. به این ترتیب می‌توان گزارش‌های مورد نظر را طریق این داشبورد آماده نموده و نمایش داد. در این پروژه به صورت رایگان و در صورت درخواست سازمان ۵ گزارش در داشبورد هوشمندی کسب‌وکار آماده‌سازی می‌شود.

٤- دسترسی‌پذیری، مقیاس‌پذیری و کارایی

نیاز است سامانه مدیریت شناسه و دسترسی مذکور بتواند روزانه تعداد بالایی درخواست را سرویس دهد. به این منظور نیاز است سامانه بتواند به‌راحتی Scale up و Scale out شود.

یکی دیگر از ویژگی‌های مهمی که این نرم‌افزار باید به آن پایبند باشد بحث دسترسی‌پذیری به میزان ٪۹۹/۹۹ است. از این رو این سامانه باید امکان توزیع‌پذیری بر روی سرورها و دیتاسنترهای مختلف را نیز داشته باشد.

[۵] منظور دستور View در پایگاه‌های داده است که یک پرس‌وجو را به صورت فقط خواندنی در دسترس کاربران غیر مدیر قرار می‌دهد. عمدتا این دستور برای گزارش‌گیری استفاده می‌شود.

[٦] Read only

۵- متدلوژی توسعه نرم‌افزار

از آن‌جایی که استفاده از متدلوژی نرم‌افزاری چابک[۷] به منظور تقریب هر چه بیشتر نرم‌افزارهای توسعه‌یافته به نیازمندی‌های کارفرمایان، بسیار محبوب و کاربردی است، در این پروژه نیز همانند پروژه‌های دیگر از متدلوژی چابک استفاده خواهد شد. این متدلوژی به کارفرما اجازه می‌دهد در بازه‌های زمانی کوتاه یک نسخه افزایشی[۸] از نرم‌افزار را مورد بررسی قرار داده و تحقق نیازمندی‌ها را مورد بررسی قرار دهد.

۶- کنترل کیفیت نرم‌افزار

به منظور کنترل کیفیت نرم‌افزار از روش‌های مرسوم مدیریت کنترل کیفیت کد با استفاده از ابزارهایی نظیر SonarQube و رعایت استانداردهای کدنویسی مانند PEP8 و ... استفاده می‌شود. همچنین برای رعایت اصول کدنویسی امن استانداردهای امنیتی نظیر CWE مورد استفاده قرار خواهد گرفت. مهم‌ترین استانداردهای کنترل کیفیت که در این پروژه رعایت می‌شود عبارتند از:

- ✓ استانداردهای MISRA و CERT-C برای نرم‌افزارهای نوشته شده به زبان C
- ✓ استاندارد PEP8 برای نرم‌افزارهای نوشته شده به زبان پایتون
- ✓ استانداردهای گوگل و SonarQube برای زبان برنامه‌نویسی جاوا
- ✓ استانداردهای کدنویسی امن؛ نظیر CWE، OWASP و SANS Top 25

علاوه بر رعایت و بررسی مداوم استانداردهای کدنویسی صحیح، در این پروژه تلاش می‌شود انواع روش‌های آزمون واحد[۹]، یکپارچگی[۱۰]، سیستم (انتها به انتها[۱۱]؛ چه دستی و چه اتوماتیک) و پذیرش استفاده شود. همچنین دائما میزان پوشش نمونه آزمون[۱۲] مورد نظارت قرار گیرد.

همچنین آزمون‌های تحمل بار[۱۳] و خرابی[۱۴] نیز به منظور بررسی دسترسی‌پذیری و پایدار سیستم طبق استانداردها و با ابزارهای مربوط انجام خواهد شد. در ضمن آزمون‌های مربوط به آسیب‌پذیری نرم‌افزاری نیز از طریق ابزارهای مطرح انجام شده و در صورت نیاز توسط تیم خارجی مورد نظر کارفرما نیز صورت خواهد گرفت.

علاوه بر روش‌های سنجش کنترل کیفیت نرم‌افزار و آزمون‌های مربوط به پذیرش، در این پروژه تمامی زیرساخت‌های لازم برای بررسی و سنجش نظرات کاربران و آماده‌سازی مقدمات برای بهبود بیش از پیش نرم‌افزار را آماده می‌نماید. از همین زیرساخت‌ها برای سنجش رضایت کاربران، جانمایی اجزای UI و تغییر احتمالی برخی از فرآیندهای احراز اصالت در فاز پایلوت استفاده خواهد شد.

مستندات کنترل کیفیت نرم‌افزار با تکیه بر آزمون‌های سیستم، پذیرش، بار، تحمل خرابی و امنیت در فاز پایانی از پروژه در قالب سند آزمون به کارفرما ارائه خواهد شد.

---

[۷] Agile Software Methodologies
[۸] Incremental
[۹] Unit Test
[۱۰] Integration
[۱۱] End to End (E2E)
[۱۲] Test Coverage
[۱۳] Load Tolerance
[۱۴] Fault Tolerance

۷- پیشینه، تجربیات و محصولات مشابه شرکت پیام‌پرداز

شرکت مهندسی ارتباطی پیام‌پرداز در سال ۱۳۷۵ با هدف ارائه خدمات تخصصی در زمینه امنیت اطلاعات و ارتباطات تأسیس گردید. هسته اصلی تشکیل‌دهنده شرکت، ترکیبی از زبده‌ترین پژوهشگران و کارشناسان رمزنگاری و امنیت اطلاعات بود که تا قبل از سال ۱۳۷۵ در قالب «حوزه مخابرات امن جهاد دانشگاهی» در دانشگاه صنعتی اصفهان به فعالیت‌های تحقیقاتی اشتغال داشتند. این شرکت از نخستین شرکت‌های خصوصی محسوب می‌شود که به صورت تخصصی و حرفه‌ای در زمینه امنیت اطلاعات و ارتباطات و با انگیزه پاسخ‌گویی به نیازهای فنی کشور در این عرصه، فعالیت خود را آغاز نموده است. این شرکت طی سنوات گذشته توانسته است با جذب برجسته‌ترین فارغ‌التحصیلان و نخبگان دانشگاهی و با افزایش توانمندی‌ها و قابلیت‌های تخصصی خود، نقش موثری در اجرای پروژه‌های تحقیقاتی و ساخت محصولات انحصاری بازار امنیت فضای تبادل اطلاعات (افتا) کشور ایفا کند.

در حال حاضر دامنه فعالیت شرکت پیام‌پرداز، کلیه حوزه‌های مشاوره، طراحی و اجرا را در برگرفته است و از طرح‌های پژوهشی همچون طراحی و تحلیل الگوریتم‌های رمزنگاری تا پروژه‌های پیاده‌سازی نرم‌افزاری و سخت‌افزاری گسترش یافته است.

حوزه هویت یکی از حوزه‌هایی است که شرکت پیام‌پرداز در چند سال اخیر به صورت جدی بر روی آن تمرکز داشته است. در همین راستا، این بخش شامل اهم محصولات، فعالیت‌ها و تجربیات مشابه شرکت پیام‌پرداز در این حوزه است:

۷-۱- محصول سامان-MFA

سیستم احراز اصالت چندعاملی سامان (با نام تجاری Saman-MFA) متشکل از مجموعه کاملی از روش‌ها و فرآیندهای استاندارد، قابل اعتماد، امن و کاربرپسند برای احراز اصالت است که با هدف تحقق مفهوم احراز اصالت قوی ورود کاربران به سامانه‌ها، تجهیزات و برنامه‌های کاربردی توسعه‌یافته است. فرآیندهای احراز اصالت سیستم Saman-MFA، بدون نیاز به تغییر در روال‌های جاری احراز اصالت سیستم‌ها (که به طور عمده احراز اصالت مبتنی بر کلمه عبور هستند) بر روی آن‌ها قرار گرفته و یک لایه امنیتی قابل اطمینان برای احراز اصالت، تشکیل می‌دهند.

از نظر تجربه کاربری، تمرکز سیستم احراز اصالت Saman-MFA بر روی تلفن‌های همراه هوشمند است. چرا که از یک سو این دستگاه‌ها همواره در دسترس کاربران هستند و از سوی دیگر از انعطاف‌پذیری و قدرت پردازشی قابل قبولی برای تحقق روال‌ها، پروتکل‌ها و الگوریتم‌های امن برخوردار می‌باشند. سیستم احراز اصالت Saman-MFA، فرآیندهای احراز اصالت استاندارد مبتنی بر پیام‌های Push، یکبارمزهای پیامکی، کدهای TOTP و HOTP، و همچنین روال احراز اصالت بدون کلمه عبور مبتنی بر QR-Code را در قالب اپلیکیشن موبایل اختصاصی بر روی انواع تلفن‌های همراه ارائه می‌دهد.

در شکل ۷ روند احراز اصالت مبتنی بر پیام پوش با استفاده از سیستم احراز اصالت سامان در یک سناریوی نمونه نشان داده شده است. همانطور که در شکل مشاهده می‌شود، سیستم سامان بدون کاستن از ویژگی‌های امنیتی احراز اصالت بر اساس کلمه عبور، یک لایه احراز اصالت که مستلزم تعامل مستقیم اما کمینه کاربر با تلفن همراه است را اضافه می‌نماید.

لازم به ذکر است که سامان-MFA در طراحی قسمتی از سامانه پیشنهادی این پروژه استفاده شده است، اما کارکردهای این محصول تنها محدود به این پروژه نشده و امکان ارائه سرویس احراز اصالت چندعاملی به انواع سیستم‌های عامل، تجهیزات شبکه، سامانه‌های نرم‌افزاری و ... را دارد.

اطلاعات تکمیلی این محصول در قالب پیوست ارسال شده است.

شکل ۷. نحوه کارکرد سامان-MFA

۷-۲- محصول سامان-IAM

سیستم جامع مدیریت شناسه و کنترل دسترسی سامان (با نام تجاری Saman-IAM) راهکاری امن، کارآمد و مقیاس‌پذیر است که سرویس‌های متنوع مورد نیاز برای مدیریت شناسه را برای استفاده سازمانی فراهم می‌نماید. این محصول می‌تواند به سادگی در سازمان استقرار یافته و درزمانی اندک با روال‌های جاری سازمان، برنامه‌های کاربردی درون‌سازمانی، سرویس‌های وب سازمان و سایر سرویس‌ها ادغام شود.

فرآیندهای مرتبط با شناسه‌ها، موجودیت‌های مختلفی از سازمان (کارکنان عادی، بخش فناوری اطلاعات، بخش‌های مرتبط با مدیریت نیروی انسانی و برخی مدیران) را درگیر می‌کند. از این رو، طراحی و پیاده‌سازی این فرآیندها مستلزم توجه به ملاحظات مختلفی از نظر رعایت نکات امنیتی، تسهیل به‌کارگیری و کارآمدی است. سیستم‌های مدیریت شناسه و دسترسی (IAM) با هدف پیاده‌سازی امن و کارآمد روال‌ها و سرویس‌های مرتبط با شناسه در سطح سازمان به‌وجود آمده‌اند. این سیستم‌ها با خودکارسازی بسیاری از فرآیندها، تسهیل کار با شناسه‌ها از طریق واسط‌های کاربری مناسب و یکپارچه‌سازی و همگام‌سازی داده‌ها و پردازش‌های مرتبط با شناسه‌ها در سرویس‌ها و برنامه‌های کاربردی سازمان، باعث ساده‌سازی مدیریت و استفاده از شناسه‌ها می‌شوند.

هرچند استفاده از یک سامانه جامع و یکپارچه مدیریت شناسه و دسترسی، فارغ از اندازه سازمان برای هر سازمانی پرفایده است، اما به‌کارگیری آن در سازمان‌های بزرگ حیاتی است. افزایش پیچیدگی فرآیندهای مرتبط با

شناسه‌ها با افزایش تعداد کارکنان، تعدد نقش‌ها و سمت‌های سازمانی، پیچیدگی روابط داخلی و خارجی سازمان، تعدد سرویس‌ها و برنامه‌های کاربردی و میزان گسترش فناوری اطلاعات در سازمان، به‌طور فزاینده‌ای افزایش می‌یابد. این امر موجب می‌شود راهکاری جامع، مبتنی بر استانداردها و دارای امنیت یکی از نیازهای اساسی چنین سازمانی باشد.

از دید امنیت اطلاعات سازمان، سیستم مدیریت شناسه و دسترسی یکی از مهمترین خاکریزهای امنیتی سازمان محسوب می‌شود. سیستم مدیریت شناسه در صورت پیاده‌سازی و استقرار به‌صورت امن و به‌روزرسانی و پشتیبانی مستمر می‌تواند بسیاری از حملات و نفوذها را به‌سادگی خنثی نماید و از هزینه‌های به‌وجود آمده در نتیجه حملات جلوگیری کند. برای مثال، حمله شایع Phishing با بکارگیری راهکارهای دقیق احراز اصالت تا حد بسیار خوبی قابل پیشگیری است. به همین ترتیب حملات مبتنی بر مهندسی اجتماعی نیز با استفاده از راهکارهای دقیق احراز اصالت و کنترل دسترسی قابل پیشگیری هستند. علاوه بر این، چنین سامانه‌هایی از طریق فراهم‌کردن روش‌های متعدد برای اعمال سیاست‌های دسترسی به منابع سازمان از فعالیت‌های بدکارانه عناصر داخل سازمان و یا نیروهایی که اخیرا از سازمان جدا شده‌اند نیز جلوگیری می‌نمایند.

لازم به ذکر است که این محصول علاوه بر نیازمندی‌های مطرح‌شده در این پروژه ویژگی کنترل دسترسی را نیز برای سازمان‌ها به ارمغان می‌آورد.

مستندات تکمیلی این محصول به پیوست ارسال می‌شود.

۳-۷- توکن‌های امنیتی کیا

توکن امنیتی کیا، یک ماژول امنیتی سخت‌افزاری داخلی است که جهت افزایش سطح امنیت کاربردهای متنوع رایانه‌ای طراحی شده است. این ماژول از طریق پورت USB به رایانه متصل می‌گردد و سرویس‌های امنیتی مورد نیاز را به برنامه‌های کاربردی ارائه می‌نماید. از جمله سرویس‌های امنیتی ارائه شده توسط کیا می‌توان به انواع سرویس‌های محرمانگی، صحت، احراز اصالت و دیگر خدمات استاندارد مطرح در زیرساخت کلید عمومی اشاره نمود.

با استفاده از امکانات امنیتی توکن کیا، توسعه‌دهندگان نرم‌افزار می‌توانند امنیت کاربردهای مختلف انتقال، پردازش و ذخیره اطلاعات حساس را فراهم آورند. همچنین امکان امضای دیجیتال، رمزنگاری متقارن و نامتقارن، احراز اصالت کاربران و قفل‌گذاری نرم‌افزارها، با سهولت هرچه بیشتر توسط کیا فراهم می‌گردد.

لازم به ذکر است که سامانه پیشنهادی در این مستند امکان یکپارچه‌سازی و استفاده از توکن‌های امنیتی کیارا نیز خواهد داشت.