Security Threat Model

پروژهMetrogo – Urban Mobility & Digital Payment Platform :

1.هدف و جایگاه Threat Model در پروژهMetrogo

این سند صرفاً برای «چک‌لیست امنیتی» یا گذر از یک الزام دانشگاهی تهیه نشده است Threat . Modelدر پروژه Metrogo به‌عنوان یک ابزار حفاظت از سرمایه، برند و تداوم کسب‌وکار طراحی شده است Metrogo .با داده‌های حساس کاربران، اطلاعات پرداخت و رفتار حرکتی در فضای شهری سروکار دارد؛ بنابراین هر ضعف امنیتی می‌تواند پیامدهایی فراتر از یک باگ فنی ساده داشته باشد.

در سیستم‌های پرداخت شهری، شکست امنیتی می‌تواند منجر به توقف سرویس، مداخله رگولاتور، از دست رفتن اعتماد عمومی و حتی مسئولیت حقوقی مستقیم برای تیم شود. به همین دلیل، این سند تلاش می‌کند تهدیدها را پیش از وقوع شناسایی کند و نشان دهد تیم Metrogo امنیت را یک ریسک قابل مدیریت می‌داند، نه یک اتفاق تصادفی.

2. دارایی‌های حیاتی (Critical Assets) در Metrogo

اولین گام در Threat Modeling شناسایی دارایی‌هایی است که باید محافظت شوند. در Metrogo ، دارایی‌ها فقط شامل سرورها یا کد نیستند، بلکه شامل عناصر ناملموسی می‌شوند که مستقیماً با اعتماد کاربر و عملیات شهری گره خورده‌اند.

دارایی‌های حیاتی Metrogo شامل مواردی مانند اطلاعات هویتی کاربران، وضعیت حساب و اعتبار، توکن‌های پرداخت، لاگ‌های تراکنش، کلیدهای رمزنگاری و حتی الگوریتم‌های تصمیم‌گیری برای مجوز عبور هستند. از دست رفتن یا دستکاری هرکدام از این دارایی‌ها می‌تواند پیامدهای مالی، حقوقی و اعتباری جدی ایجاد کند.

این سند فرض می‌کند که همه این دارایی‌ها هدف بالقوه حمله هستند و هیچ‌کدام به‌صورت پیش‌فرض امن در نظر گرفته نمی‌شوند.

.3مهاجمان محتمل(Threat Actors)

درMetrogo ، تهدیدها فقط از سمت «هکر حرفه‌ای» نمی‌آیند Threat Model .مهاجمان را بر اساس واقعیت‌های عملیاتی سیستم پرداخت شهری تعریف می‌کند.

یکی از مهاجمان محتمل، کاربر متقلبی است که تلاش می‌کند بدون پرداخت واقعی از مترو عبور کند. این مهاجم ممکن است دانش فنی محدودی داشته باشد، اما انگیزه بالایی برای سوءاستفاده از ضعف‌های منطقی سیستم دارد. مهاجم دیگر می‌تواند یک شخص ثالث با دسترسی محدود (مانند اپراتور یا شریک فنی) باشد که از دسترسی خود فراتر می‌رود.

همچنین، مهاجمان سازمان‌یافته‌تر مانند حمله‌کنندگان به زیرساخت پرداخت، یا حتی تهدیدهای داخلی (اشتباه یا سوءنیت اعضای تیم) نیز در نظر گرفته شده‌اند. این سند فرض می‌کند که تهدید می‌تواند هم خارجی و هم داخلی باشد و امنیت فقط با اعتماد حل نمی‌شود.

4.سطح حمله (Attack Surface) درMetrogo

سطح حمله Metrogo شامل تمام نقاطی است که یک مهاجم بالقوه می‌تواند با سیستم تعامل داشته باشد. در پروژهMetrogo ، سطح حمله به‌صورت طبیعی گسترده است، زیرا سیستم شامل اپلیکیشن کاربر، APIهایBackend ، ارتباط با سرویس‌های پرداخت و تعامل با زیرساخت شهری است.

هر API که در معرض اینترنت قرار دارد، هر ورودی کاربر، هر توکن QR و هر ارتباط شبکه‌ای بخشی از سطح حمله محسوب می‌شود. این سند فرض می‌کند که هر نقطه‌ای که داده وارد سیستم می‌شود یا از آن خارج می‌شود، باید به‌عنوان یک نقطه بالقوه حمله در نظر گرفته شود.

تمرکز Threat Model در Metrogo کاهش سطح حمله از طریق محدودسازی دسترسی‌ها، ساده‌سازی مسیرهای حیاتی و حذف وابستگی‌های غیرضروری است.

.5تهدیدهای مرتبط با پرداخت و عبور شهری

یکی از مهم‌ترین دسته‌های تهدید درMetrogo ، تهدیدهایی هستند که مستقیماً به پرداخت و مجوز عبور مربوط می‌شوند. این تهدیدها شامل تلاش برای دوبار استفاده از یک مجوز، جعلQR ، replay کردن درخواست‌ها و دستکاری وضعیت پرداخت هستند.

در یک سناریوی واقعی، حتی تأخیر کوتاه در اعتبارسنجی پرداخت می‌تواند باعث شود کاربر یا مهاجم از سیستم سوءاستفاده کند. این سند نشان می‌دهد که Metrogo این تهدیدها را به‌صورت صریح شناسایی کرده و آن‌ها را جزو ریسک‌های سطح بالا در نظر می‌گیرد.

6.کنترل‌های امنیتی (Security Controls) در Metrogo

کنترل‌های امنیتی در Metrogo به‌گونه‌ای طراحی شده‌اند که متناسب با مرحله MVP باشند، اما ریسک‌های فاجعه‌بار را پوشش دهند. این کنترل‌ها شامل اعتبارسنجی ورودی‌ها، محدودسازی نرخ درخواست‌ها، بررسی وضعیت توکن‌ها و کنترل دسترسی مبتنی بر نقش هستند.

هدف این کنترل‌ها جلوگیری از حملات پیچیده در حد سیستم بانکی نیست، بلکه جلوگیری از سوءاستفاده‌های محتمل در محیط واقعی مترو است. کنترل‌ها به‌صورت لایه‌ای طراحی شده‌اند تا شکست یک لایه منجر به شکست کامل سیستم نشود.

.7مدیریت کلیدها و رمزنگاری(Key Management & Encryption)

درMetrogo ، کلیدهای رمزنگاری یکی از حساس‌ترین دارایی‌ها محسوب می‌شوند. این کلیدها برای امضای توکن‌ها، محافظت از داده‌ها و جلوگیری از جعل استفاده می‌شوند. سیاست پروژه این است که هیچ کلید حساسی در کد یا مخزن ذخیره نشود.

داده‌های حساس در حالت انتقال و ذخیره‌سازی رمزنگاری می‌شوند. هدف این رمزنگاری جلوگیری از دسترسی غیرمجاز حتی در صورت نفوذ محدود به سیستم است. این سند نشان می‌دهد که تیم Metrogoمدیریت کلید را یک مسئله عملیاتی جدی می‌داند، نه یک تنظیم پیش‌فرض.

8.کنترل دسترسی (Access Control) درMetrogo

کنترل دسترسی در Metrogo بر این اصل بنا شده است که هیچ کاربر یا سیستمی بیش از آنچه نیاز دارد نباید دسترسی داشته باشد. این اصل که به «حداقل سطح دسترسی» معروف است، در پروژه Metrogoاهمیت دوچندان دارد، زیرا هر دسترسی اضافی می‌تواند به سوءاستفاده از داده‌های حساس یا اختلال در عملیات شهری منجر شود.

درMetrogo ، نقش‌ها به‌صورت شفاف تعریف شده‌اند؛ کاربر نهایی، اپراتور پشتیبانی، توسعه‌دهنده و سرویس‌های سیستمی هرکدام سطح دسترسی متفاوتی دارند. کاربر نهایی فقط به داده‌ها و عملیات مرتبط با حساب خود دسترسی دارد و هیچ اطلاعات سیستمی یا داده‌ی کاربران دیگر برای او قابل مشاهده نیست. اپراتورهای پشتیبانی نیز تنها به اطلاعاتی دسترسی دارند که برای پاسخ‌گویی به کاربر ضروری است و امکان انجام عملیات مالی مستقیم ندارند.

کنترل دسترسی در سطح API به‌صورت متمرکز اعمال می‌شود تا از دور زدن منطق امنیتی جلوگیری شود. این رویکرد باعث می‌شود حتی اگر یک بخش از سیستم دچار ضعف شود، مهاجم نتواند به‌راحتی به کل سیستم دسترسی پیدا کند.

9. لاگ‌گیری (Logging) و مانیتورینگ امنیتی

در Metrogo ، لاگ‌گیری صرفاً برای دیباگ فنی انجام نمی‌شود، بلکه یک ابزار امنیتی و عملیاتی کلیدی است. هدف از لاگ‌گیری این است که هر رفتار غیرعادی یا مشکوک بتواند قابل ردیابی و تحلیل باشد.

سیستم لاگ Metrogo رویدادهای مهمی مانند تلاش‌های ناموفق پرداخت، استفاده مکرر از یک QR ، خطاهای اعتبارسنجی و دسترسی‌های غیرمجاز را ثبت می‌کند. این لاگ‌ها به‌گونه‌ای طراحی شده‌اند که داده حساس کاربر را افشا نکنند، اما اطلاعات کافی برای تحلیل حادثه فراهم کنند.

مانیتورینگ بر اساس این لاگ‌ها انجام می‌شود تا الگوهای غیرعادی شناسایی شوند. به‌عنوان مثال، افزایش ناگهانی خطاهای پرداخت یا تلاش‌های تکراری برای استفاده از یک مجوز می‌تواند نشانه حمله یا سوءاستفاده باشد. در Metrogo ، چنین الگوهایی به‌عنوان هشدار تلقی می‌شوند و نیازمند بررسی فوری هستند.

10. شناسایی و پاسخ به حادثه (Incident Detection & Response)

هیچ سیستمی مصون از حادثه نیست، به‌ویژه در مرحله MVP. به همین دلیل، Metrogo فرض می‌کند که حادثه امنیتی ممکن است رخ دهد و تمرکز Threat Model فقط بر پیشگیری نیست، بلکه بر واکنش سریع و کنترل‌شده نیز هست.

Incident Response در Metrogo شامل شناسایی سریع حادثه، محدودسازی اثر آن، بررسی علت ریشه‌ای و بازیابی سرویس است. این فرآیند به‌گونه‌ای طراحی شده که حتی در شرایط فشار عملیاتی (مثلاً ساعات اوج ترافیک مترو) تیم بداند چه اقداماتی باید انجام دهد و چه تصمیم‌هایی نباید به‌صورت واکنشی گرفته شود.

وجود این فرآیند باعث می‌شود یک حادثه امنیتی به بحران کنترل‌نشده تبدیل نشود و اثر آن بر کاربران و عملیات شهری به حداقل برسد.

11. سناریوهای بحران امنیتی محتمل در Metro

Threat Model بدون سناریوی واقعی ناقص است. در Metro ، چند سناریوی بحران به‌صورت آگاهانه در نظر گرفته شده‌اند؛ از جمله اختلال گسترده در پرداخت، سوءاستفاده از QR یا نشت محدود داده.

برای هر سناریو، این سند مشخص می‌کند چه بخشی از سیستم درگیر می‌شود، چه اقدام فوری لازم است و چه ذی‌نفعانی باید مطلع شوند. این شفافیت باعث می‌شود تیم در زمان بحران به‌جای حدس و گمان، بر اساس برنامه عمل کند.

هدف از این سناریوسازی ایجاد ترس نیست، بلکه کاهش زمان واکنش و جلوگیری از تصمیم‌های هیجانی است.

12.امنیت داده‌های حساس و حریم خصوصی کاربران

Metrogoبا داده‌هایی سروکار دارد که ترکیبی از اطلاعات مالی و رفتاری هستند. این داده‌ها نه‌تنها از نظر فنی، بلکه از نظر حقوقی و اجتماعی حساس محسوب می‌شوند. این سند فرض می‌کند که هرگونه نشت داده می‌تواند پیامدهای جدی برای برند و اعتماد عمومی داشته باشد.

به همین دلیل، سیاست امنیت داده در Metrogo بر محدودسازی دسترسی، رمزنگاری و حداقل‌سازی داده ذخیره‌شده تمرکز دارد. فقط داده‌هایی نگهداری می‌شوند که برای عملکرد سرویس ضروری هستند و دسترسی به آن‌ها به‌صورت کنترل‌شده انجام می‌شود.

13. ارتباط امنیت با ریسک حقوقی و برند

امنیت ضعیف در Metrogo صرفاً یک مشکل فنی نیست، بلکه یک ریسک حقوقی و اعتباری است. هر حادثه امنیتی می‌تواند منجر به شکایت کاربران، مداخله نهادهای نظارتی یا حتی توقف موقت سرویس شود. این سند نشان می‌دهد که تیم Metrogo این ارتباط را درک کرده و امنیت را بخشی از مدیریت ریسک کلان پروژه می‌داند.

با مستندسازی Threat Model و کنترل‌ها، تیم نشان می‌دهد که در صورت بروز حادثه، اقدامات معقول و مسئولانه‌ای انجام داده است. این موضوع می‌تواند در کاهش تبعات حقوقی و حفظ اعتبار برند نقش کلیدی داشته باشد.

14.امنیت به‌عنوان توانمندساز رشد، نه مانع آن

یکی از باورهای غلط رایج این است که امنیت سرعت توسعه را کاهش می‌دهد. درMetrogo ، امنیت به‌عنوان ابزاری برای افزایش اعتماد به تصمیم‌گیری و رشد پایدار در نظر گرفته می‌شود. وقتی تیم بداند ریسک‌های اصلی شناسایی و کنترل شده‌اند، با اطمینان بیشتری می‌تواند محصول را توسعه دهد.

این Threat Model نشان می‌دهد که امنیت در Metrogo بخشی از طراحی محصول است، نه یک وصله‌ی دیرهنگام.

جمع‌بندی نهایی Threat Model پروژهMetrogo

این سند Threat Model نشان می‌دهد که تیم Metrogo امنیت را به‌صورت سیستماتیک، واقع‌بینانه و متناسب با مرحله MVP مدیریت می‌کند. تهدیدها شناسایی شده‌اند، مهاجمان محتمل در نظر گرفته شده‌اند و کنترل‌های عملی برای کاهش ریسک‌ها تعریف شده‌اند.

هدف این سند ادعای امنیت کامل نیست، بلکه اثبات این است که Metrogo امنیت را می‌فهمد، آن را جدی می‌گیرد و برایش برنامه دارد.