گزارش فعالیت‌های پروژه در هشت ماه اول

موضوع تحقیق :بررسی حملات پوششی و توسعه راهکارهای دفاعی برای مرورگرهای اندرویدی

هدف پروژه :شناسایی و تحلیل آسیب‌پذیری‌های امنیتی مرورگرهای اندرویدی و ارائه راهکارهایی برای مقابله با حملات پوششی که می‌تواند حریم خصوصی کاربران را تهدید کند.

۱ .بررسی و تحلیل ادبیات و منابع مرتبط (٪۲۰ - حدود ۲.۵ ماه)

فعالیت‌ها:

- **جمع‌آوری و مطالعه منابع** :در آغاز پروژه، مجموعه‌ای از مقالات علمی و پژوهش‌های پیشین درباره امنیت اندروید، مدل‌های مجوزدهی و حملات پوششی جمع‌آوری و مطالعه شد. منابع مطالعه شده به شناسایی راهکارهای مورد استفاده در پروژه‌های مشابه و درک بهتر از تهدیدات امنیتی کمک کردند.
- **تحلیل سیستم مجوزدهی اندروید** :سیستم مجوزدهی اندروید به عنوان یکی از پایه‌های امنیتی این سیستم عامل مورد بررسی قرار گرفت. در این بخش، مجوزهای مختلفی مانند مجوزهای عادی، خطرناک و امضا مورد تحلیل قرار گرفتند تا مشخص شود کدام دسته از مجوزها بیشتر در معرض حملات قرار دارند.
- **بررسی آسیب‌پذیری‌های مرورگرهای موبایلی** :به تحلیل تهدیدات امنیتی مرورگرهای موبایل و بررسی نوع حملاتی که می‌توانند از این آسیب‌پذیری‌ها بهره‌برداری کنند پرداخته شد. تمرکز اصلی روی حملات پوششی، به ویژه حمله‌ی"Toast Overlay" ، بود که به طور مخفیانه کاربران را به افشای اطلاعات یا انجام عملکردهای ناخواسته فریب می‌دهد.

دستاوردها:

- **ایجاد یک چارچوب نظری قوی** :این مرحله، پایه و اساس تئوری لازم برای طراحی مدل‌های تشخیصی و ابزارهای امنیتی در مراحل بعدی پروژه را فراهم کرد.
- **شناخت عمیق‌تر از آسیب‌پذیری‌ها** :به درک بهتری از ساختار سیستم مجوزدهی اندروید و نقاط ضعف آن دست یافته شد. این درک پایه‌ای برای طراحی مدل‌های پیشگیرانه‌ی امنیتی بود.
- **آشنایی با انواع حملات پوششی و تهدیدات آن‌ها** :با مطالعه روش‌های مختلف حملات پوششی، توانستیم تا تهدیدات بالقوه‌ای که این نوع حملات برای کاربران ایجاد می‌کنند را بهتر شناسایی کرده و در طراحی راهکارهای مقابله با آن‌ها گام‌های اساسی برداریم.

۲ .طراحی اولیه مدل‌های تشخیص و تحلیل امنیتی (٪۲۵ - حدود ۳.۵ ماه)

فعالیت‌ها:

- **طراحی مدل‌های تحلیل ایستا و تحلیل رفتاری** :در این مرحله، مدل‌هایی برای تحلیل ایستا و رفتاری طراحی و پیاده‌سازی شدند. تحلیل ایستا شامل بررسی کد و ساختار برنامه‌ها به منظور شناسایی الگوهای مشکوک بدون نیاز به اجرای آن‌ها است. تحلیل رفتاری نیز بر ردیابی رفتارهای برنامه‌ها در زمان اجرا تمرکز دارد و به شناسایی فعالیت‌های غیرعادی، به ویژه در مرورگرهای اندروید، کمک می‌کند.

- **توسعه ابزارهای اولیه تشخیص و امنیتی** :بر اساس مدل‌های طراحی شده، ابزارهای امنیتی اولیه‌ای توسعه یافت که بتواند به شناسایی فعالیت‌های مشکوک بپردازد. این ابزارها به صورت آزمایشی برای ردیابی رفتارهای غیرعادی مرورگرها در برابر حملات پوششی طراحی شدند.
- **بازبینی و بهینه‌سازی مدل‌ها** :پس از پیاده‌سازی اولیه، مدل‌ها با توجه به نتایج آزمایش‌های اولیه و بازخوردهای دریافتی بهینه‌سازی شدند. این بهینه‌سازی شامل تغییرات در الگوریتم‌ها و پارامترهای شناسایی بود تا دقت و کارایی مدل‌ها افزایش یابد.

دستاوردها:

- **توسعه مدل‌های پایه‌ای تشخیص** :مدل‌های طراحی شده قادر به شناسایی فعالیت‌های مشکوک و الگوهای پوششی در مرورگرهای اندرویدی هستند. این مدل‌ها پایه‌ای برای توسعه ابزارهای امنیتی پیشرفته‌تر در آینده خواهند بود.
- **ایجاد زیرساخت تشخیص امنیتی برای مرورگرها** :زیرساختی فراهم شد که می‌تواند به صورت پویا فعالیت‌های مرورگرها را رصد کرده و در صورت بروز رفتارهای غیرعادی هشدار دهد. این زیرساخت به مرورگرها اجازه می‌دهد که تهدیدات امنیتی را سریع‌تر شناسایی کنند.
- **بهینه‌سازی مدل‌ها برای افزایش دقت و سرعت تشخیص** :بازخوردهای دریافتی از آزمایش‌های اولیه به ما کمک کرد تا دقت و سرعت تشخیص مدل‌ها را افزایش داده و نقاط ضعف آن‌ها را برطرف کنیم.

۳ .شبیه‌سازی و آزمایش حملات پوششی (۱۵٪ - حدود ۲ ماه(

فعالیت‌ها:

- **شبیه‌سازی حملات پوششی** :حملات پوششی مانند "Toast Overlay" و "UI Redressing" در نسخه‌های مختلف اندروید (تا نسخه ۱۲) شبیه‌سازی شد تا نقاط ضعف مرورگرها و عملکرد مدل‌های تشخیصی مورد ارزیابی قرار گیرد. این شبیه‌سازی‌ها نشان دادند که چگونه کاربران بدون اطلاع در معرض خطر قرار می‌گیرند و چگونه مدل‌ها می‌توانند به شناسایی سریع این حملات کمک کنند.
- **آزمایش مدل‌ها در شرایط واقعی** :مدل‌های تشخیصی در محیط‌های واقعی آزمایش شدند تا دقت و کارایی آن‌ها در شناسایی حملات پوششی بررسی شود. داده‌های جمع‌آوری شده از این آزمایش‌ها برای بهینه‌سازی مدل‌ها و ابزارهای تشخیصی استفاده شد.
- **تجزیه و تحلیل نتایج** :داده‌های حاصل از شبیه‌سازی‌ها و آزمایش‌ها به دقت تجزیه و تحلیل شدند. این تحلیل‌ها نقاط ضعف مرورگرها و سیستم مجوزدهی اندروید در برابر حملات پوششی را آشکار کرد و ما را قادر ساخت تا اصلاحاتی را در مدل‌های تشخیصی اعمال کنیم.

دستاوردها:

- **شناسایی حساسیت مرورگرهای اندرویدی به حملات پوششی** :نتایج شبیه‌سازی‌ها نشان دادند که مرورگرهای اندرویدی به حملات پوششی حساس هستند و بهبودهای امنیتی در آن‌ها ضروری است.
- **اعتبارسنجی مدل‌های تشخیصی اولیه** :مدل‌های اولیه در شناسایی حملات پوششی در محیط‌های واقعی توانستند کارایی خود را نشان دهند. این اعتبارسنجی به ما کمک کرد تا نقاط ضعف مدل‌ها را شناسایی کرده و اصلاحاتی برای بهبود عملکرد آن‌ها اعمال کنیم.
- **جمع‌آوری داده‌های مهم برای بهینه‌سازی مدل‌ها** :داده‌های حاصل از آزمایش‌ها و شبیه‌سازی‌ها برای بهینه‌سازی و ارتقای دقت مدل‌های تشخیصی استفاده شدند و به ما کمک کردند تا بهبودهایی در سیستم تشخیصی اعمال کنیم.

جمع‌بندی

در این ۸ ماه، ٪۶۰ از پروژه با موفقیت به اتمام رسید. این فعالیت‌ها شامل مطالعه و تحلیل منابع، طراحی و پیاده‌سازی مدل‌های اولیه تشخیص، و شبیه‌سازی و آزمایش حملات پوششی بود. این دستاوردها به ما کمک کرد تا دانش و ابزارهای لازم برای بهبود امنیت مرورگرهای اندرویدی را به دست آورده و مسیر را برای توسعه مدل‌های پیشرفته‌تر در مراحل بعدی پروژه هموار کنیم.