CASE STUDY

Mitigating the Risk of Credential Stuffing Attacks on Mobility Apps

"Before integrating Approov, we were concerned about the risk of credential stuffing attacks on our shared e-moped platform. We realised that we needed an out-of-the-box security solution that enabled us to focus our resources and productivity on developing our core product. Approov provided the perfect solution to our problem."

— Arthur Bloemen, Head of Product and Technology at felyx

With mobile apps being the primary means of accessing transportation mobility services, effective security measures are essential to prevent attacks on the apps and their backend APIs. By integrating Approov Mobile Security, felyx was able to prevent credential stuffing attacks and enhance the security of their platform.

The Client

felyx is an innovative and forward-thinking scale-up that is focused on revolutionizing urban transportation across the Netherlands and Belgium. They achieve this through their shared e-moped solutions that offer sustainable and efficient transportation to all. felyx's vision is to shape the cities of the future by creating a more sustainable, safe, convenient, and fun means of transportation. By connecting people through smooth, green, and shared rides, they are making it easier for people to get around while also reducing their carbon footprint.

The Challenge

felyx was concerned about the risk of credential stuffing attacks on their platform; this would involve attackers using stolen or weak credentials in an attempt to take over accounts. These types of attacks are usually fueled by large external leaks of credentials from other sites, and they can pose a serious threat to a company's platform security and user experience.

How Approov Mobile Security Helped

Credential stuffing is a type of cyber attack where attackers use automated scripts to test large volumes of username and password combinations in rapid succession against a target application. In the case of mobile apps, attackers may use stolen credentials from other breaches or test for common, weak passwords to gain access to user accounts on the app. If the attackers gain access, they can engage in malicious activities such as stealing personal information, performing fraudulent transactions, or spreading spam or malware. Credential stuffing attacks can be especially problematic for mobile apps, which often lack the advanced security features found in web applications.

Authenticating both the user and the app is essential for securing back-end services and preventing brute force attacks from bots or scripts. This, along with two-factor authentication, provides a robust defense against scripted attacks. Approov Mobile Security performs an ongoing, deep inspection of mobile apps and the devices they are

©2023 Approov | CriticalBlue Limited. All rights reserved. Version 1.0

running upon, and based on this guarantees the authenticity of requests to backend APIs and services. With the Approov integration in place, malicious traffic was blocked before reaching felyx's backend services.

The Results

Approov enabled felyx to secure their mobile app effectively by verifying the authenticity of the app while accessing backend APIs and services, effectively preventing unauthorized access and credential stuffing attacks. Arthur explains,

> ***"Before integrating Approov, we were concerned about the risk of credential stuffing attacks on our shared e-moped platform. We wanted to offer a seamless and secure experience to our users; we realised that we needed an out-of-the-box security solution that enabled us to focus our resources and productivity on developing our core product. Approov provided the perfect solution to our problem."***

The team at felyx found that implementing Approov was easy and required limited code, and it covered both iOS and Android platforms. Arthur continues,

> ***"We did need to adjust our workflow to integrate it into our automatic pipeline, but once done, it made our lives much easier. With a strong defense against scripted attacks in place we haven't encountered any issues regarding credential stuffing or other security breaches".***

Summary

felyx recognized the potential threat of credential stuffing attacks to their platform's security and user experience, which could be resource-intensive to address. Approov provided an easy-to-implement solution that secured their mobile app, ensuring the authenticity of requests to their backend APIs and services, and preventing any unauthorized access and credential stuffing attacks.

Arthur offers advice for anyone wanting to secure their platform but avoid in-house resource strain,

> ***"We highly recommend Approov to anyone looking for a reliable, out-of-the-box solution to secure their mobile app".***

approov
mobile security

Approov protects your revenue by ensuring that only your own mobile apps—running in safe environments and communicating over secured connections—can use your APIs and backend resources. Botnets, malicious scripts, tampered and fake apps are blocked.

Find out more about Approov Mobile Security: www.approov.io

©2023 Approov | CriticalBlue Limited. All rights reserved. Version 1.0