HOW TO "ZERO TRUST" YOUR:

MOBILE DEVICES, MOBILE APPS, CLOUD-TO-DEVICE CHANNEL, ATTRIBUTION, AUTHENTICATION

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE

HOW TO "ZERO TRUST" YOUR...

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE

–1–

HOW TO “ZERO TRUST” YOUR MOBILE DEVICES

INTRODUCTION

The impact of zero trust design on enterprise security is usually discussed in the context of reduced dependency on the perimeter. Network teams deal with zero trust objectives by rethinking how their access architecture works in the context of the major use-cases – namely, site-to-site access, third-party access, and individual access, which is increasingly arranged in a work-from-anywhere approach.It is this latter case, where it becomes super important for end-user devices to be properly protected from cyber threats, given that no external perimeter is in place to provide detection or prevention of attacks. And mobile devices certainly fall into this category of end-user device that demands to be secured against attacks. As a result, security teams must engage with an effective partner to implement the right set of controls.

INTEGRITY CHECKS ON MOBILE DEVICES

Approov is a commercial vendor specializing in mobile app security. One of the functions Approov includes in its suite of mobility protections includes a so-called “zero trust” check on the device which involves integrity checks to ensure improved security. As one would expect, this can be a valuable risk measure to take in an enterprise mobility setting.

The goal of such device checking specifically is to help safeguard mobile apps from threats such as application programming interface (API) abuse, infrastructure-in-the-middle attacks, and unauthorized usage. Approov’s device integrity checks operate by embedding security checks within the mobile app itself. When the app communicates with any backend servers, for example, Approov verifies the authenticity of the request.

THE ATTESTATION PROCESS

The core of Approov's approach is the attestation process. Each time the app makes a request, it must present a cryptographic token generated by the Approov SDK integrated into the app. This token encapsulates various integrity signals about the device and the app's runtime environment. For example, it can detect if the app is running on a rooted or jailbroken device, if debuggers are attached, or if the app code has been tampered with. These checks ensure that only legitimate and uncompromised devices can communicate with the backend APIs.

The core of Approov's approach is the attestation process.

Additionally, Approov continuously updates its detection capabilities to adapt to new threat vectors, ensuring ongoing protection. This dynamic nature of attestation, combined with robust cryptographic methods, ensures that mobile applications protected by Approov can trust the integrity of the devices they run on, thus significantly enhancing security and reducing vulnerabilities.

RECOMMENDED ACTION PLAN

The recommendation here is that enterprise teams who view the mobility ecosystem as being essential to their mission should consider connecting with Approov immediately to engage in a program that will "zero trust" their mobile devices toward greatly improved mobile security for devices, apps, and the supporting infrastructure.

HOW TO "ZERO TRUST" YOUR MOBILE APPS

INTRODUCTION

It is not uncommon for many modern organizations to value their virtual assets over their more tangible assets such as facilities or physical equipment. As a result, the mission of such companies will tend to rely heavily on their software applications, and this obviously includes mobile apps. Few observers would view such dependency as unusual, especially for organizations with a heavy IT focus on their business.

HOW APPROOV SECURES MOBILE APPS

Approov provides mobile app security by performing attestations to ensure apps are genuine, thus improving overall security. This process involves embedding the Approov SDK into the mobile application, which then works in tandem with Approov's cloud service to perform real-time, dynamic app attestations. Each time the app communicates with backend servers, it must present a cryptographic token generated by the Approov SDK. This token verifies that the app is authentic and running in a secure environment.

Each time the app communicates with backend servers, it must present a cryptographic token generated by the Approov SDK.

The attestation process includes several checks. Firstly, it verifies that the app has not been tampered with or modified since its original deployment. This involves checking the integrity of the app's code and configuration files. Secondly, Approov ensures that the app is running on a legitimate device, capable of detecting if the device is rooted, jailbroken, or if any debugging tools are present. Thirdly, it checks the app's runtime environment to detect the presence of any malicious code or unauthorized changes.

Approov's attestation mechanism also includes regular updates to address emerging threats and new attack vectors. By validating the authenticity of the app and its operating environment continuously, Approov ensures that only genuine, untampered apps can access backend resources. This significantly enhances security by preventing unauthorized access and reducing the risk of data breaches and other malicious activities.

ACTION PLAN

The recommendation here is that enterprise teams who view the mobility ecosystem as being essential to their mission should consider connecting with Approov immediately to engage in a program that will "zero trust" their mobile apps toward greatly improved mobile security for devices, apps, and the supporting infrastructure.

–3–

HOW TO "ZERO TRUST" YOUR CLOUD-TO-DEVICE CHANNEL

INTRODUCTION

The path that exists between mobile applications hosted in the cloud and the requesting mobile device – which we refer to here as the Cloud-to-Device Channel – carries obvious significance in the cybersecurity protection of any mobility-first enterprise. If this channel cannot be trusted to provide safe, secure, and reliable access, then the implications on the enterprise mission can be considerable.

Obviously, much of this responsibility will go to the mobile and broadband carriers who support the underlying network fabric. Without robust support from these vendors, obviously the channel will not be reliable. But it is the application-level attacks on this channel that we address here – and we refer to the protection process at this level as one that involves the goal to "zero trust" the Cloud-to-Device Channel.

HOW APPROOV SECURES CLOUD-TO-DEVICE CHANNEL

Approov enhances mobile application security by protecting this communication channel between the cloud and mobile devices through dynamic certificate pinning. This method ensures that data transmitted between the app and backend servers is secure from interception and tampering, thus improving overall security.

Dynamic certificate pinning involves the app verifying the server's SSL/TLS certificate during each communication session. The Approov SDK embedded in the mobile app manages this process. When the app attempts to establish a connection with the server, Approov dynamically pins the server's certificate, ensuring that only a connection with the legitimate server can be established. This prevents man-in-the-middle (MITM) attacks where attackers might use forged certificates to intercept or alter data.

By continuously validating the server's certificate and ensuring that only trusted connections are made, Approov safeguards the communication channel against interception and tampering.

Approov's dynamic approach to certificate pinning allows for flexibility and responsiveness to changes. Unlike static pinning, which can cause issues if the certificate changes (e.g., due to expiration), dynamic pinning can automatically adjust to certificate updates, reducing the risk of service disruptions while maintaining security. Approov also identifies and prevents malicious software on the device, thus preventing MitM (main-in-the-middle) attacks using tools such as *mitmproxy* installed on the client.

By continuously validating the server's certificate and ensuring that only trusted connections are made, Approov safeguards the communication channel against interception and tampering. This secure communication framework helps protect sensitive data and maintain the integrity and confidentiality of interactions between the mobile app and cloud services, significantly enhancing overall security.

ACTION PLAN

The recommendation here is that enterprise teams who view the mobility ecosystem as being essential to their mission should consider connecting with Approov immediately to engage in a program that will "zero trust" their cloud-to-device channel toward greatly improved mobile security for devices, apps, and the supporting infrastructure.

HOW TO “ZERO TRUST” YOUR ATTRIBUTION

INTRODUCTION

Cybersecurity teams have long struggled with the challenge of balancing the need for certain users to include anonymity with the requirement that security, which can include monitoring and mitigation, is enforced across the spectrum of all supported use-cases. This has long been a conundrum that has created difficulty for enterprise security teams trying to make good architectural and operational decisions.

As a result, many attempts have been made over the years by practitioners to use obfuscation tools that rely on a variety of different methods including passwords, secrets, and other on-device attributes. Practical experience has dictated that while advances have been made, many weaknesses exist in how attribution is dealt with in the context specifically of the mobility ecosystem.

HOW APPROOV SECURES ATTRIBUTION

Approov addresses the problem of insecure obfuscation tools and the threat of API secrets being extracted from mobile apps, including those stored in secure enclaves, by using a comprehensive approach to runtime secrets protection. Instead of relying on potentially vulnerable on-device storage, Approov ensures that API secrets never reside on the mobile device at all.

Approov achieves this by dynamically generating and validating cryptographic tokens that complement the need for static API keys. When an app communicates with its backend server, it must present an Approov-generated token, which the backend server verifies before allowing access to protected resources. This token is created and validated in real-time, ensuring that only legitimate, untampered apps can access the API.

When an app communicates with its backend server, it must present an Approov-generated token

By removing API secrets from the mobile device entirely, Approov eliminates the risk of secrets being intercepted by tools like Frida, even if they are stored in traditionally secure areas. The dynamic nature of the token generation process ensures that even if an attacker manages to de-obfuscate parts of the app, they cannot access or replicate the API secrets needed to authenticate with the backend server.

This approach not only secures the communication channel but also ensures that sensitive secrets remain protected in the cloud, making it significantly harder for attackers to compromise the app's security, even with advanced de-obfuscation techniques and runtime inspection tools. The other advantage is that certificates and API keys can be rotated immediately when this is required, hence maintaining service continuity.

ACTION PLAN

The recommendation here is that enterprise teams who view the mobility ecosystem as being essential to their mission should consider connecting with Approov immediately to engage in a program that will "zero trust" their attribution toward greatly improved mobile security for devices, apps, and the supporting infrastructure.

HOW TO "ZERO TRUST" YOUR AUTHENTICATION

INTRODUCTION

If there would be one security control that would provide the most foundational support for all the others, the case could be made that authentication fits that bill. Without a reliable means for determining the identity of any requesting entity, whether human or non-human, it is inconceivable that reasonable security policy enforcement can occur.

Approov addresses the shortcomings of traditional user authentication, including those with multi-factor authentication (MFA), by implementing a robust, short-lived token-based access system.

As a result, the question emerges in the context of mobility security around how authentication can be done most effectively as enterprise teams move more toward zero trust. This implies that prior reliance on centralized services that reside on the perimeter edge of a network are no longer present to provide support in this area. As a result, the question emerges how an organization can "zero trust" their mobile authentication.

HOW APPROOV SECURES AUTHENTICATION

Approov addresses the shortcomings of traditional user authentication, including those with multi-factor authentication (MFA), by implementing a robust, short-lived token-based access system to ensure that backend APIs communicate only with genuine mobile apps. This approach effectively mitigates the risk of reverse engineering and misuse of stolen credentials.

Approov's solution centers around dynamic app attestation and token generation. When a mobile app makes a request to a backend API, the Approov SDK embedded in the app generates a cryptographic token. This token is short-lived and dynamically generated, ensuring it is valid only for a limited time. The backend API then verifies this token before granting access to its resources.

This process ensures that only authentic and untampered mobile apps can obtain valid tokens, thereby accessing the backend APIs. The dynamic nature of token generation makes it extremely difficult for attackers to reverse engineer the app and use stolen credentials since the tokens are not static and cannot be reused.

Approov's tokens are closely tied to the specific instance of the app and the health of its runtime environment, adding an additional layer of security. Even if an attacker manages to steal credentials, they would not be able to generate valid tokens without passing the attestation checks performed by Approov.

By combining dynamic app attestation with short-lived token generation, Approov ensures that backend APIs interact exclusively with genuine mobile apps, significantly enhancing security and reducing the risk associated with compromised credentials and reverse engineering.

ACTION PLAN

The recommendation here is that enterprise teams who view the mobility ecosystem as being essential to their mission should consider connecting with Approov immediately to engage in a program that will "zero trust" their authentication toward greatly improved mobile security for devices, apps, and the supporting infrastructure.

For more information visit

www.approov.io

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.

The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.