TAG CYBER

AN ATTACKER-CENTRIC APPROACH TO API AND WEB APPLICATION SECURITY USING THREATX

EDWARD AMOROSO, CHRIS WILDER,
TAG CYBER

THREATX

TAG CYBER

AN ATTACKER-CENTRIC APPROACH TO API AND WEB APPLICATION SECURITY USING THREATX

EDWARD G. AMOROSO
CHRIS WILDER

Application programming interface (API) and web application risk are challenges for organizations of all sizes. A new security approach combines visibility into the API attack surface with attacker behavior profiles to block threats before sensitive data is exploited. The ThreatX commercial offering implements this new API protection approach effectively..

INTRODUCTION

Despite considerable attention across the cybersecurity community, connecting third-party and in-house applications via APIs continues to create significant cyber risk. Misconfigured, rogue or zombie APIs can expose sensitive and personal data belonging to organizations and their consumers. Modern effective API security solutions must therefore become more proactive, and an attacker-centric mindset is emerging as a useful strategy.

The integration of APIs with third-party apps and digital services allows organizations to scale their capabilities, improve functionality and optimize efficiency and time to market. However, APIs present additional challenges as they are among the largest attack surfaces and highly prized targets for determined hackers. APIs are rarely controlled centrally and often emerge across various teams and business units with little visibility to the security organization.

In this report, we summarize the cyber risks for modern APIs and include a review of next-generation API security requirements, followed by guidance on how an attacker-centric view might be used to reduce the threat of API attacks. We use the ThreatX platform solution to demonstrate how a commercial platform can deliver visibility, real-time mitigation and attacker behavior analysis to deter API vulnerabilities and exploits.

API SECURITY RISK

The cyber risks to APIs are becoming increasingly well-known to developers, managers and security teams. While this is good news from an awareness perspective, implementing effective mitigation remains difficult. In the section below, we provide an overview of the major API security risks that have emerged. In the subsequent section, we outline a next-generation security approach that combines API visibility and analytics with focus on attacker behavior.

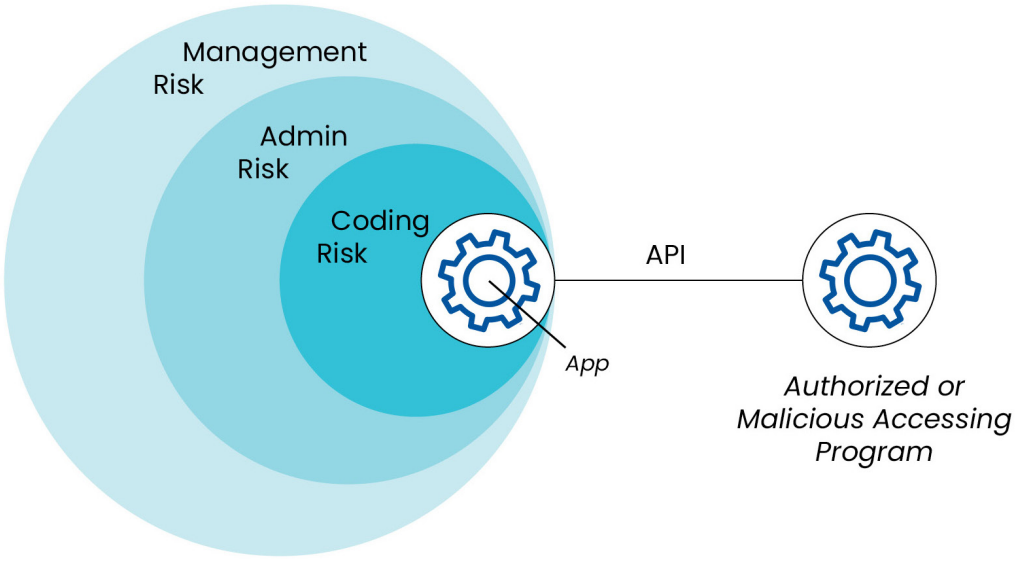

Figure 1. Three Dimensions of API Security Risk

API Coding Risks

Despite published guidance on how to avoid vulnerabilities during the coding process, many developers are just not trained in secure coding. This is a shame because frameworks such as OWASP provide valuable lists of API security errors made by programmers.[1] It includes, for example, advice on using authentication and authorization mechanisms properly in code, as well as rate limiting, managing assets and avoiding common misconfigurations.

The problem is that a lack of training, combined with business pressure to emphasize speed of delivery, has led to insecure coding practices. Even in cases where software is scanned by a static or dynamic tool, the result is usually that the more obvious vulnerabilities are removed. In these cases, subtler vulnerabilities might remain in the software that can be exploited by malicious attackers.

API Administration Risks

In addition to the risks introduced by an ever-expanding API attack surface, cyber risks also emerge in the set-up and configuration in APIs. Configuration includes environmental considerations such as logging and monitoring API usage, as well as dependence on default configurations in servers, cloud infrastructure (including storage) and other functional support mechanisms.

The responsibility of managing the configuration of core systems and services has been debated in the security community since the early days of hosting applications on Unix and Windows in the 1990s. The blame typically goes to management decisions to overwork and underfund teams tasked with system and software administration. Automation addresses some of this concern, but poorly administered APIs are still common on the internet.

API Management Risks

A third risk worth mentioning with respect to API security involves decisions made by managers, team leads and executives regarding the creation, deployment and use of APIs to support the business. In addition to the underestimation of complexity to administer software mentioned above, resource shortages are common in related areas such as training, testing and day-to-day monitoring.

Use of APIs, in particular, is often poorly managed which leads to increased risk exposure as more zombie and rogue APIs are left behind. For security, the monitoring of the behavior and use of any resource requires understanding normal versus suspicious behavior—and this is no different for APIs. Nevertheless, it remains common for APIs to be deployed and used with poor oversight and poor management of the organization's API attack surface.

NEXT-GENERATION API THREAT MITIGATION

To properly address cyber risk to APIs, we recommend a new security approach to combine visibility and analytics with detailed assessment of malicious attacker behavior. The goal is to create an accurate contextual view of an organization's entire API attack surface and to prioritize actions based on the vulnerabilities most likely to be targeted by attackers. The main components of this security approach are outlined below.

Visibility and Analytics

Creating real-time visibility into APIs and web applications allows security teams to detect evidence of runtime attacks such as cycling of IP addresses, location masking and credential stuffing. Such visibility must therefore span the DevOps lifecycle to ensure coverage against all types of threats.

The visibility obtained from observing real-time traffic to APIs can be used for a variety of analysis and reporting tasks. Further, because the traffic is observed and analyzed in real-time, rather than offline, immediate blocking of threats is possible. In this sense, API threat mitigation implements functionality that complements support from bot mitigation tools and web application firewall (WAF) platforms.

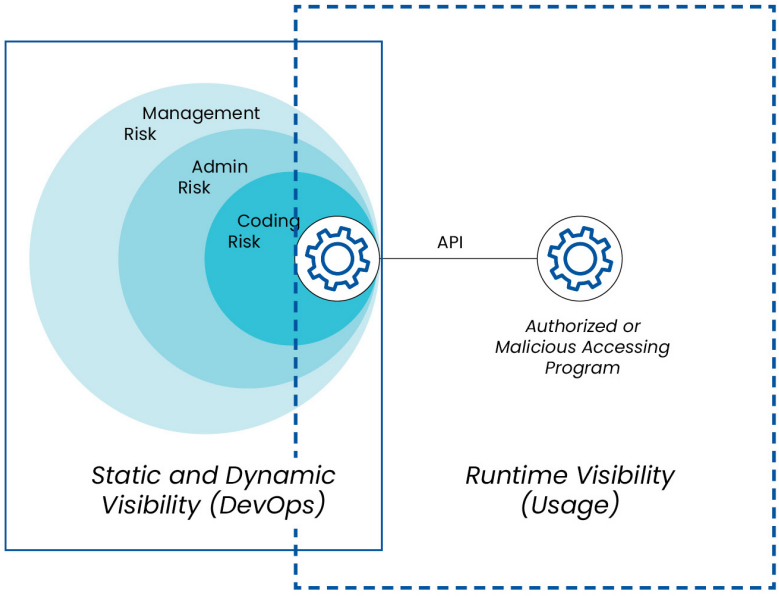

Figure 2. API and Web App Visibility and Analytics

Attacker Behavior Context

One of the most powerful methods for the detection, prevention and even response to cyberthreats involves developing profiles of expected behaviors. These profiles can then be used to measure differences in observed behavior, which can then be subjected to either pre-determined or dynamically generated thresholds. Response action would then result if a threshold has been exceeded. This differs greatly from the legacy approach, which relied on static signatures to identify and block a threat; signatures are onerous to manage and have limited long-term value in terms of mitigating risk.

Much of the modern cybersecurity discipline has evolved from this concept (arguably invented by Dr. Dorothy Denning) and one area where this has shown considerable recent progress involves profiling attacker behavior. Whether memorialized in a static framework such as MITRE ATT&CK or managed as part of a runtime view of activity, attacker behavior profiling can offer valuable context for security teams.

For API and web application security, attacker behavior would be integrated with the visibility and analytics used for mitigating cyber risk. In particular, attacker behavior would be especially valuable during the runtime visibility portion of most modern API and web application suites. This would allow for more effective detection since the objective of most security systems is to reduce risk while being mindful of keeping false-positive and false-negative rates down, versus just guessing or relying on signatures.

THREATX PLATFORM OVERVIEW

ThreatX offers a commercial platform that protects APIs from advanced threats. The ThreatX platform uses an attacker-centric approach to behavior analytics consistent with the discussion above. The solution helps enterprise teams defend vulnerable APIs and provide cyber risk mitigation for web applications. The sections below provide an overview of the solution design and enterprise deployment.

ThreatX Platform Design

The ThreatX platform is based on the design and development of a Single Risk Engine that combines API protection with bot mitigation, DDOS security and web application security functionality. The engine provides the correlation and aggregation capability required to make sense of potential attacker activity across a full range of tactics, techniques and procedures. The goal is to cover the kill chain from start to finish for full API and web application security coverage.

At the heart of the Single Risk Engine is the management of dynamic profiles of threat actors developed with the following security attributes:

- *API Protection*: This function supports discovery and analysis of APIs for a range of gateway and network architectures. Support is included for automatic threat detection and behavioral analysis.
- *Cloud Native WAF*: The WAF component offers protection of apps and APIs based on guidance from frameworks such as OWASP Top 10. The solution is agentless and public cloud agnostic.
- *DDOS Protection*: The ThreatX solution includes volumetric layer 3 (packet) to heuristic layer 7 (application) support for DDOS protection and mitigation. The service comes with 24/7 managed support.
- *Bot Management*: Bot management is a necessary function for APIs and web apps since many threat actors masquerade their breaches using automated bad bots that purport to be normal users.

- *Dynamic Profiling*: Maintaining profiles of attacker behavior requires ongoing updates using contextual information and observed patterns to create a dynamic view of applicable baselines. This is an important aspect of any profiling engine because adversaries will typically change their tactics frequently.

The result of this approach is a world-class correlation and analysis engine at the heart of the ThreatX solution that can provide strong API and web application security coverage based on an attacker-centric approach to managing risk.

ThreatX Product Offerings

The specific commercial product offerings, all consisting of agentless deployment, included in the ThreatX suite are as follows:

- *API Protection*: This function supports discovery and analysis of APIs for a range of gateway and network architectures. Support is included for automatic threat detection and behavioral analysis.
- *Cloud Native WAF*: The WAF component offers protection of apps and APIs based on guidance from frameworks such as OWASP Top 10. The solution is agentless and public cloud agnostic.
- *DDOS Protection*: The ThreatX solution includes volumetric layer 3 (packet) to heuristic layer 7 (application) support for DDOS protection and mitigation. The service comes with 24/7 managed support.
- *Bot Management*: Bot management is a necessary function for APIs and web apps since many threat actors masquerade their breaches using automated bad bots that purport to be normal users.

These capabilities are complemented by ThreatX Managed Services which results in a well-designed portfolio suite for enterprise teams that need a means for minimizing the cyber risks to their APIs and web applications.

[1] *https://owasp.org/www-project-api-security/*

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.