TAG

HOW 42CRUNCH ADDRESSES SCALING REQUIREMENTS FOR API SECURITY IN TELECOMMUNICATIONS

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG

42crunch

HOW 42CRUNCH ADDRESSES SCALING REQUIREMENTS FOR API SECURITY IN TELECOMMUNICATIONS

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG

This TAG report introduces the scaling requirements that exist to support application programming interface (API) security for large telecommunications firms. Commercial cybersecurity company 42Crunch is shown to effectively support these scaling requirements for API security.

INTRODUCTION

Telecommunications firms (telecoms), like all major industries, are now using application programming interfaces (APIs) to drive increased efficiencies through automation of their business processes. Such usage typically involves provision of services such as location data, billing information services, voice and video content, and number porting services to consumers through telecom-hosted APIs, but it also involves consumption by ISPs of API-provided services from other entities such as public cloud providers.[1]

The security aspects of this API landscape for telecoms are greatly complicated by the size, scope, and scale of their businesses. In fact, it is easy (and common) to underestimate the reach of the Tier 1 service providers. In the United States, for example, Verizon and AT&T work with virtually 100% of the Fortune 500 and provide mobile services to hundreds of millions of individual consumer customers. Such coverage can only be described as massive.

What this means is that securing telecom infrastructure comes with a set of functional requirements to support massive scale. Such requirements are reviewed here in the context of API security, both in terms of provision and consumption of APIs by telecoms. To illustrate the practical application of these concepts, cybersecurity vendor 42Crunch is shown to effectively support these scaling requirements for API security in the context of telecom usage.

[1] *This author, while working as the CISO for a large telecommunications firm, first experienced the massive scaling requirements that exist in this industry for the first iPhone launch, soon after which, new mobile app developers desired API-based access to location data from this iconic device, them operating over 2G networks.*

It is also worth reinforcing the obvious and potentially lucrative target that telecommunications firms represent for malicious cyber actors. The reach of telecommunications firms and Internet service providers across so many different industries provides adversaries with the ability to scale their attacks beyond just one target – but rather to a broad assortment of downstream customers of the service provider.

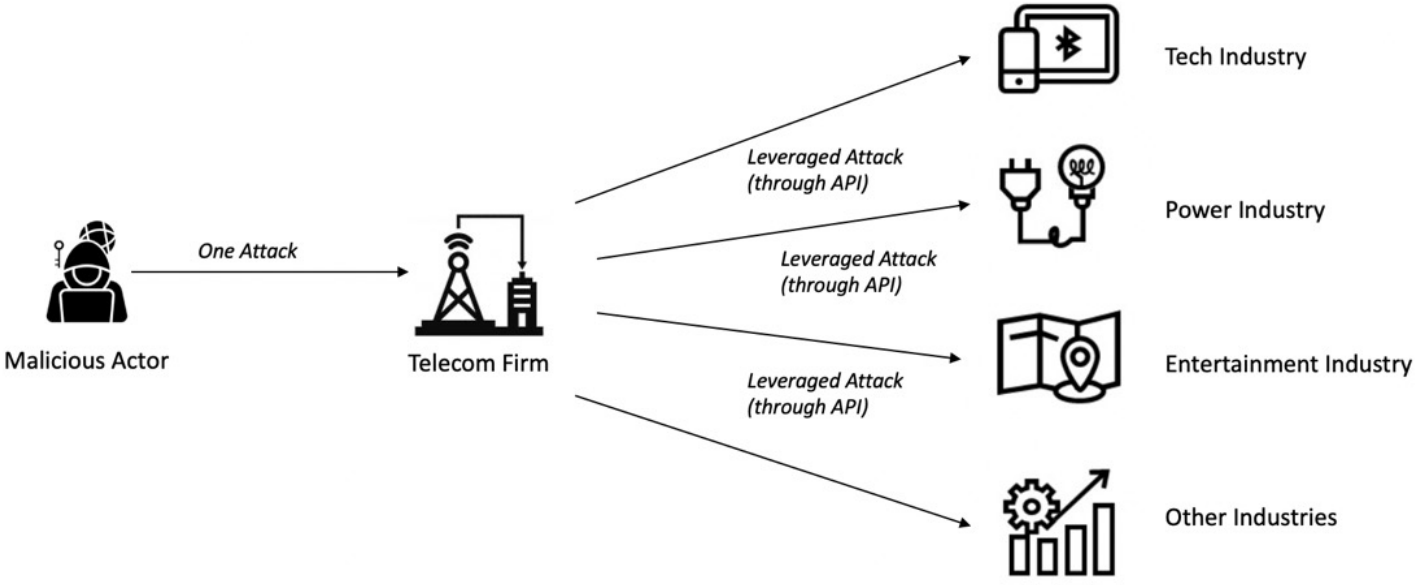

Figure 1. Attack Leverage Gained When Targeting a Telecom Firm

It is also worth mentioning that the global telecommunications industry handles vast amounts of sensitive customer data, making it imperative to adhere to global data protection regulations such as CCPA and GDPR. Additionally, there is an urgent need to comply with industry specific standards such as PCI-DSS for payment and NIST CSF and ISO 27001 for implementation of network security services.

Identifying and mitigating vulnerabilities early ensures that systems are more stable and secure, minimizing the risk of downtime, and ensuring that APIs are robust and secure. Such focus also supports consistent service availability, which is crucial for maintaining customer satisfaction and adherence to Service Level Agreements (SLA) from the outset of the software development cycle.

The leverage that emerges with an attack on a telecom firm is perhaps best achieved through APIs connecting the service provider with its customers. Using such target allows for offensive actors to take advantage of the automation, pre-integration, and convenience of API connectivity between telecoms and their enterprise users. This underscores the importance of implementing proper cybersecurity across telecom infrastructure.[2]

TELECOM SCALING REQUIREMENTS FOR API SECURITY

The primary over-arching requirement to scale API security for telecoms is automation. That is, unlike environments where there might be certain use-cases in which manual processes will suffice to address a given issue, in telecom environments this is never possible. Scale implies large numbers, and any security expert in this industry understands that without automation, workflow, and continuous processing, large gaps can emerge in security coverage.

An additional over-arching requirement that emerges with this industry is complexity. Anyone who spends even a modest amount of time working to secure telecommunications infrastructure and services (as has this author for decades) immediately recognizes the staggering complications that

[2] *In the twelve months preceding publication of this report, there have been several high-profile API-targeted attacks against telcos that have resulted in the exposure of sensitive customer ID. Information on these attacks is available at https://apisecurity.io/issue-203-optus-data-breach-api-security-guide-authn-authz-vulnerabilities/.*

arise with transport services, control services, maintenance support, application interfaces, data storage, customer support, and on and on.

Let's now focus more specifically on the security requirements for APIs. It should come as no surprise that telecoms utilize APIs to streamline the automated coordination, service implementation, and data sharing with ecosystem components such as vendor services, tiered support, adjacent network infrastructure, customer networks, and standard industry services that support key functions such as naming, routing, and other network capabilities.

In each case, the API – whether provided by a telecom for its ecosystem partners or utilized by the telecom to interact with external services – represents a point of attack by a malicious adversary. This implies the need to perform automated API security testing and to support a program of API threat protection. Three specific functional requirements that arise for such a need in the context of telecom usage are listed below:

1. **Vast API Ecosystem**: As implied above, telecoms will manage a plethora of APIs, each serving different purposes, from user authentication to data transmission. Ensuring the security of this extensive API ecosystem demands the ability to scale.

2 **Constantly Changing Environment:** The telecommunications industry is dynamic, with new services and technologies being introduced regularly, not to mention frequent mergers and acquisitions. API security must adapt to these changes seamlessly.

3. **Global Reach:** Most telecoms serve customers worldwide, which means that their APIs are accessed from diverse locations and devices. Security solutions must be globally scalable and adaptable to regional variations in security requirements.

An important consideration in the context of API security for telecoms is the degree to which their infrastructure has shifted toward a more software-defined approach. Previous generations of telecom infrastructure, especially supporting mobility, required expensive upgrades to equipment as speeds, capacities, and features improved with each successive new generation of service.

With the global advent of 5G, however, telecom infrastructure is highly software-defined, which underscores the relevance of APIs in how interactions occur between telecoms, their customers, their environment (including other telecoms), and the major service providers supporting cloud and software as a service (SaaS). API security thus emerges as a primary component of overall telecom security.

HOW 42CRUNCH SUPPORTS API SECURITY FOR TELECOMS

Commercial cybersecurity vendor 42Crunch provides an innovative API security solution that includes the right set of capabilities to address the unique scaling needs of telecommunications firms referenced above.[3] 42Crunch addresses the API Security challenge by supporting a Shift-Left approach in its platform. Capabilities are delivered to provide a range of tools and solutions that help organizations secure their APIs throughout the entire software development lifecycle, from design and development to deployment and monitoring.

42Crunch achieves its objectives by providing the following comprehensive suite of commercial tools and protection features designed to scale with the industry's tough functional requirements:

1. **API Audit for Design-Time Security Testing:** 42Crunch's API Audit is well-suited to the need of telecommunications firms as they make development investments in their infrastructure. The 42Crunch capability offers instant security scoring for APIs during the design phase. This proactive

[3] *More detailed technical and architectural information on 42Crunch can be obtained from the company's public website at 42crunch.com.*

approach allows teams to identify and prioritize security issues early in the development process, reducing the risk of vulnerabilities making their way into production.

2. **API Scan for Conformance and Vulnerability Detection:** 42Crunch's API Scan is a powerful tool that scans APIs to ensure conformance to best practices. This not only ensures that APIs meet telecommunications industry standards but also helps detect vulnerabilities at both testing time and runtime. With hundreds of cybersecurity checks, 42Crunch provides a comprehensive assessment of API security.

3. **Actionable Reports with Zero False Positives:** 42Crunch's reports are designed to be actionable, which is essential for telecommunications teams. The 42Crunch solution provides clear insights into cybersecurity issues, prioritizing them based on severity. Moreover, the API security solution is engineered to minimize false positives, ensuring that telecommunications teams can focus their efforts on genuine security concerns.

4. **Integration with IDEs and CI/CD Pipelines:** To meet the complex demands of the telecommunications industry, 42Crunch seamlessly integrates with development environments (IDEs) and continuous integration/continuous deployment (CI/CD) pipelines. This means that API security is not an afterthought but an integral part of the development process, which has emerged as a requirement in the context of any software project.

5. **Instant Visibility and Early Detection of OWASP API Security Top 10 Issues:** 42Crunch offers instant visibility for telecommunications teams into their API security status. This allows such teams to proactively address security issues, including those outlined in the OWASP API Security Top 10, which is commonly used by telecommunications teams to protect their infrastructure from common vulnerabilities during the software development process.

6. **Runtime Threat Protection:** 42Crunch also offers an API firewall that can be deployed in production environments to monitor and protect APIs from malicious traffic and attacks. While this is more focused on runtime security, it complements the proactive approach by providing security coverage throughout the API lifecycle.

TELECOM API SECURITY CASE STUDY

A specific telecommunications case study was shared by 42Crunch with the TAG team during the analysis associated with this report. The company involved is a leading US service provider that has responsibility to protect its internal and external API-based services. The service provider uses APIs throughout its infrastructure to enable a variety of internal and external facing services for employees, partners, and customers.

As part of a defence-in-depth strategy, the provider sought out an API security specialist that could complement their DevSecOps approach to creating applications. After initially reviewing their existing WAF and API Gateway providers' solutions, they selected the 42Crunch API security platform as being well-suited and capable of directly addressing their API security testing and threat protection requirements.

The project involved 300 software professionals working on 800 APIs. Both the 42Crunch API Audit and Scan services were adopted to successfully enable the development and application security teams to implement a shift-left approach to coding in security from API design time in both the IDE and CI/CD pipelines. Key outcomes from the project included the following:

- Senior executives recognized the value of adopting a positive security model based on standardized API contracts for their APIs. This led to the adoption on a large scale of a DevSecOps API security program across the entire telecom organization with improved visibility and control for security.

- The automation of Static and Dynamic API security testing was enabled across the SDLC through integration in all CI/CD pipelines at scale.
- Compliance objectives were achieved via adoption of API standards and governance of all API-based services.
- A reduction of security bottlenecks and development timeframes occurred, leading to faster times to market for new API-based services.
- Cost reduction was achieved for application security testing tasks engaged by red and blue teams.

API SECURITY ACTION PLAN FOR TELECOMS

As explained above, automated, commercial API security platforms are essential for telecommunications firms dealing with massive infrastructure requirements. 42Crunch's impressive suite of tools and features, including API Audit and API Scan, offers scalable and highly adaptable support to address the massive size, scope, and scale required by developers working in the telecommunications industry.

We recommend that telecommunications teams take the following steps to ensure that they are leveraging API security capabilities such as those from 42Crunch:

1. **Inventory –** First, developing an accurate inventory of currently deployed API security tools and platforms is a useful step.
2. **Requirements –** A cross referencing of current API security methods against key scaling and functional requirements is advised next.
3. **Platform –** Review of the best platform for implementation of API security, and we recommend inclusion of 42Crunch in such review, will help to ensure a good result.

These three API security planning steps would appear to be well-suited to the needs of modern telecoms in 2024 and beyond, as their services continue to serve as the backbone for emerging hybrid enterprise networks.

ABOUT TAG

TAG is a trusted next generation research and advisory group that utilizes an AI-powered SaaS platform to provide on-demand industry insights and recommendations on cybersecurity, artificial intelligence, and climate science/sustainability. Founded in 2016, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on thousands of engagements with clients and non-clients alike—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributor: Dr. Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-.com to discuss this report. You will receive a prompt response.