Managing API Security in the Connected Digital Economy

Key Findings from The Global State of API Security Survey 2015





Table of Contents

API Security Overview

Major API Security Concerns

API Security, a CIO Level Concern

A Missed Opportunity: Securing the API Consumer

Not Everyone Limits API Access

Nor Does Everyone Do **API** Rate Limiting

Not Enough Mobile Device Management

Attention Paid to Who is Consuming APIs and Microservices

Common API **Security Practices**

Minimum Level of Security Policy

OAuth Grant Types

APIs and Regulatory Compliance

Identity Technologies and APIs

Additional API Security Measures

Introduction

The front lines of information security risk management evolve in parallel with the dominant technologies in common use. The emergence of the Web brought Web-based threats and resulting countermeasures. The rise of SQL databases brought SQL injection and its mitigations. Now, we have the increasing usage and business importance of Application Programming Interfaces (APIs), which are vital the development of mobile applications and the digital enterprise in general. APIs, like all technologies, have security vulnerabilities. In fact, the very openness that makes them so useful in expanding the enterprise into the digital realm can itself be an avenue of risk exposure.

API security risks are also potentially worse, in business impact terms, than earlier generations of information security risk. APIs are often a key part of fast-track application development, enabling processes such as DevOps and connecting multiple corporate entities in rapid implementation cycles. While great for business, these capabilities can also expose more than one business to risks that might have previously been limited to a single corporation. Liability and compliance risks also grow with the increases in pace and connectivity.

Akana works with many clients worldwide who are concerned about API security issues. To help them and the broader industry gain a better understanding of the state of API security, we conducted a survey of 1,200 IT professionals on the subject in May, 2015. The respondents came from a range of industries and organization sizes. The survey reveals, perhaps not surprisingly, that API security is an identified risk for many IT departments and business managers. The specific ways that companies handle API security do vary, with organizations with larger portfolios of APIs in production having more aggressive and sophisticated API security policies in effect. The size of the organization overall does not appear to have much effect on the level of API security in use.

Over 1000 Employees

Fewer than 100 Employees

101-500 Employees

501-1000 Employees

Figure 1 - Organization size of survey respondents who use APIs.

Facing API(s) Have Public Facing API(s) Only Internal API(s)

01 API Security Overview

Overall, respondents expressed confidence in the security of APIs. As Figure 3 shows, 60% felt were "confident" or "very confident" in the security of APIs. So, if you are exposing your back end systems to mobile applications using an API, you will probably have a fairly high level of confidence that connection will be secure. Yet, almost 30% of respondents unsure about the state of their API security. This shows that many IT professionals are not completely certain that security issues in APIs are

being adequately addressed. Respondents are neutral on the issue, most likely because they don't feel they have enough information to make a judgment one way or another. Only 6% lacked confidence in API security.



47% Confident

15% Very Confident

7% Unconfident

3% Very Unconfident

Figure 3 - What is your confidence level in the security of API(s)?

Major API Security Concerns

IT professionals indeed do have many API security worries, as captured in Figure 4, which asked respondents to identify their top Open Web Application Security Project (OWASP) associated concerns. 53% selected an XML bomb, JSON Scheme, DDoS and SQL Injection. A high level of concern about XML bombs, DDoS and SQL injection mirrors the current spate of data thefts and destructive hacking incidents that are affecting major corporations. APIs are simply the latest and most open interfaces into corporate information assets.

Answer Choices Responses XML bomb, JSON Schema, DDoS, SQL Injection 53.25% XML firewall, message-level security, encryption... 42.86% 37.66% Cros site scripting 36.36% XML attacks 35.06% Impersonation Phishing 25.97% 25.97% **Brute Force** Malicious Code Injections 42.86% Auto disabling of API credientals after N failed auth... 20.78%

As Figure 4 shows, IT professionals worry about cross-site scripting, phishing, impersonation, malicious code injections and more. Almost any threat can be an API threat. They all need to be addressed.

Respondent Profiles

The majority (58%) of respondents came from organizations with more than 1,000 employees. The remainder were spread among smaller firms, with 23% coming from organizations with fewer than 100 employees. Respondents reported a mix of public, internal, and partner-facing API use cases. Figure 2 shows the breakdown of use cases, with 60% of respondents indicating that they have public-facing APIs and 64% partner-facing

Figure 2

APIs. Multiple answers were allowed. 32% had only internal facing APIs.

APIs matter to these respondents, which follows the general rise of APIs as a major means for application integration and an enabler of the mobile/digital enterprises as well as new methodologies such as DevOps. 94% said that APIs were either "Important" or "Very Important" to the growth of their businesses. 93% said that they expected to see API usage rise in the future. In terms of APIs actually in production, 42% had fewer than 10, 23% had between 10 and 50, and 30% had more than 50 APIs.

Figure 2 shows the breakdown of use cases, with 60% of respondents indicating that they have public-facing APIs and 64% partner-facing. Multiple answers were allowed. 32% had only internal facing APIs.







API Security, a CIO Level Concern

The specific worries highlighted in Figure 4 might explain why although 60% of respondents felt confident in API security, 75% reported that API security was a CIO level concern. In the abstract, yes, APIs seem secure. When looking at the specific threats, they are a cause for concern. For the CIO, the security of a new, business-critical technology such as APIs would have to be a serious concern. This is partly due to

the fact that the API is more than just a technology. It is often today the foundation of entire business strategies: the mobile strategy; the partner strategy; the customer experience strategy – all of these and more may rely significantly on APIs for their success. For this reason, the CIO is not just responsible for operating and securing a new kind of software. He or she is responsible for complete business execution.

Another way to reconcile this apparent contradiction is to consider that respondents may be confident in API security in general, but they have distinct security concerns about APIs. API security was also an issue for business managers in 65% of respondents' organizations a factor that might also explain why CIOs were concerned about API security even if most IT staffers felt the technology itself was secure.

02 A Missed Opportunity: Securing the API Consumer

The biggest takeaway from the survey results is the surprising discovery that many businesses are not taking adequate measures to secure the API consumer (e.g. a mobile app). While attention is being paid to building controls and countermeasures into the API itself. many respondents appear to be neglecting a major point of vulnerability: the app that's accessing that API.

Almost 60% of respondents indicated that they did not have processes in place to check if

the API consumer is handling the data and API securely. One interpretation of this finding is that some API owners do not consider the security of their data an issue once it leaves their domain via the API. When filtering for organizations with more than 50 APIs in production, the percentage who do not have processes for checking the security of the API consumer falls to 43%. This drop is possibly reflective of a generally more rigorous security policy in API-intensive organizations.

Industry experience underscores the potential business impact of this threat. Snapchat provides a frightening example. In the summer of 2013, the computer security research firm Gibson Security warned Snapchat about vulnerabilities that exposed them to the threat of a hack.

Snapchat apparently did not heed this warning, and in the holiday season of 2013 hackers compromise its API security and use it to look up 4.6 million phone numbers and user







Figure 5 - Do you have processes in place to check if the API consumer is handling the data and API securely?

names. Snapchat did implement some basic security, but it was not at a level that serious security professionals would recommend for such a high profile service. Their measures included some basic SSL and

token hashing. They used a hardcoded shared secret key, which was a simple string constant in the app. Moreover, they did not have mechanisms in their infrastructure to prevent

and detect anomalous behavior such as bulk queries for phone numbers and usernames originating from a single client or over a very short period of time.

Not Everyone Limits API Access

The SnapChat hack notwithstanding, not everyone limits API access. 22% of survey takers did not answer the question, "How do you limit API access?" Of those who did

answer, 48% selected the option for limiting access based on an API key, with 27% using App ID and 41% with User ID. For organizations with 50+ APIs, 65% use API keys.

Based on App ID

Based on API key

Based on User ID

Not Applicable



Snapchat ... in the Holiday season of

2013 had hackers compromise

its API security and use it to look up

4.6 million

phone numbers and user names.

Figure 6- How do you limit API access? Multiple answers allowed.



Answer Choices	Responses
If rate limits span time durations greater than per second or per minute, I persist a global count of transactions accross a cluster.	19.48%
I throttle socket connections and bandwidth in addition to message per second.	16.88%
I restrict API message sizes for requests, responses, or both.	25.97%
I recieve and alert when N(SLA Threshold) faults)401, 403, 500 errors) occur in an hour.	19.48%
Not Applicable	45.45%

Figure 7 - Do you enforce a single rate limit for all API consumers, or are rate limits configurable on a per consumer contract basis to enforce different SLAs for multiple consumers of the same API? Multiple Answers allowed.

Nor Does Everyone Do API Rate Limiting

Respondents also did not indicate a high level of rate limiting for APIs. 45% selected "Not Applicable" to the question, "Do you enforce a single rate limit for all API consumers. or are rate limits configurable on a per consumer contract basis to enforce different SLAs

for multiple consumers of the same API?" This suggests that rate limiting is not viewed as an important consideration for security. Larger organizations (1000+) and shops with 50+ APIs were more likely to use rate limiting but even then, more than 30% responded

"Not Applicable." This is alarming because rate limiting is one of the best countermeasures against distributed denial of service (DDOS attacks on APIs.)

Not Enough Mobile Device Management

Mobile devices, which can be iail broken present a potentially high-impact threat to APIs. Respondents were asked, "Do you use any mobile device management technology to protect API credentials stored on mobile applications to mitigate the risk of a jail broken device?" A surprisingly high number - 65% - of those who did answer revealed that they found mobile device management "Not Applicable." Also surprising, when filtering for

organizations with 50+ APIs, 73% answered "Not Applicable." This finding suggests that mobile device management is not viewed as a high priority for API security, even in organizations with a large portfolio of APIs. Of those who do use mobile development, 12% use AES 256 client side symmetric key encryption and 17% use a mobile application containerization approach, such as Airwatch, Good or Mobile Iron.

Answer Choices	Responses
Application Client IDs / API keys mapped to names and email addresses of owners	62.50%
X.509 certificates and keys to verify trust	18.75%
IP addresses of anonymous consumers	22.50%
Consumers are not tracked	7.50%
Not Applicable	18.75%

Figure 9 - How do you know who is consuming your APIs and Microservices? Multiple answers allowed.

Attention Paid to Who is Consuming APIs and Microservices

While rate limiting and client level security are as common as might need to be, API owners seem to want to know who is consuming their APIs

and microservices, 62% of respondents indicated that they use application client IDs - API keys mapped to names and email addresses of owners.

Another 19% use x.509 certificates and 22% use IP addresses of anonymous consumers. Only 7% said they did not track consumers at all.

03 Common API Security Practices

IT professionals are definitely working on API security, even if their approaches are not consistent and wide-reaching enough. While there was a diversity in responses regarding API security practices, there is a lot of activity. The breadth of security practices suggests that they vary with applications of the technology as well as by size of the API portfolio.

Answer Choices	Responses
API keys in URL query parameters (without SSL)	7.95%
API keys in URL query parameters (with TLS 1.0)	10.23%
API keys in URL query parameters (with TLS 1.2)	30.68%
API keys and OAuth Bearer tokens (with TLS1.0/1.2)	27.27%
API keys and OAuth MAC tokens (with TLS1.0/1.2)	11.36%
Mutual TLS, plus API keys, and any token technology for authentication and authorization	18.18%
Mutual TLS, plus API keys, and any token technology for authentication and authorization, plus HSM intergration for crypto operations and secure key mgt.	11.36%
None	11.36%
Not Applicable	13.64%

Figure 10 - What is the minimum level of security policy enforcement for runtime access to public cloud APIs? Multiple answers allowed.





Minimum Level of Security Policy

When asked about the minimum level of security policy enforcement for runtime access to public cloud APIs, respondents reported multiple solutions, as shown in Figure 10. The most

popular answer was "API keys in URL guery parameter with Transport Layer Security (TLS) 1.2." 87% of respondents use API keys in some way. 29% use manual TLS plus API keys, with

11% using manual TLS but adding HSM integration for crypto operations and secure key management.









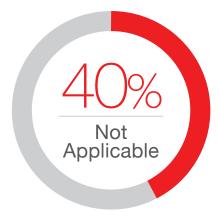


Figure 11

OAuth Grant Types

Given the importance of APIs for mobile enterprise initiatives, it's not surprising that OAuth is a popular approach to securing information that's exposed to mobile clients. Authorization code is the most popular type

of OAuth grant, as shown in Figure 11. Client credentials claims a 30% share of OAuth using respondents. Conversely, implicit grants account for just 5% of respondents. Given that OAuth is predominantly for

mobile apps, not all survey takers responded to the guestion or found it applicable. Results are similar for organizations with 1000+ employees or 50+ APIs.

APIs and Regulatory Compliance

The Payment Card Industry (PCI) security standards dominate API security practices for companies that need to adhere to regulatory frameworks. Figure 12 shows responses to the question, "Do you certify your API platform for compliance with any of the following regulatory requirements?" This

is not an issue for every industry, of course. In this case, nearly 60% of the survey takers did not answer. Of those who did, 28% certify their API platform with PCI DSS 2.0 Level 1, 17% with PCI DSS 3.0 Level 1, and 26% with PCI DSS 2.0 Level 2. The ISO 27001 certification is also popular, with 26%

of respondents certifying their API platforms with it. Again, shops with 50+ APIs have a different profile. When filtering the results for 50+ APIs, the number of respondents certifying with PSS 2.0 Level 1 or Level 2 increases to 35% and 47%, respectively.



Identity Technologies and APIs

Enterprise Active Directory and Lightweight Directory Access Protocol (LDAP) were by far the most common identity technologies used by respondents, with 61% indicating that it was what they integrated with their API gateways. 40% used custom authentication Web service or REST API. 20% use Security Assertion Markup Language (SAML).

Answer Choices	Responses
Enterprise Active Directory and/or LDAP	61.25%
IAM Product (Siteminder, Ping Identity, Oracle, Olta, other)	25.00%
Public Cloud OpenID providers (Google, Yahoo, Other)	15.00%
Custom Authentication Web Servic or REST API	40.00%
Custom SQL, noSQL Database	10.00%
Custom NoSQL Database	0.00%
SAML	20.00%
Kerberos	10.00%
Not using any API Gateway	17.50%

Figure 13 -Which identity technologies do you integrate with your API Gateways? Multiple answers allowed.

Not Applicable	23.17%
Rotate keys on demand and to schedule key rotation for API consumer credentials	8.54%
Suspended/resume access to one API consumer without impacting other API consumers	17.07%
Cross-Origin Resource Sharing (CORS) policy enforced	14.63%
Filter API message content that is written to the audit log and/or encrypt message before	20.73%
Intergration of OAuth with Active Directory/LDAP, OpenID Connect and JSON Web Tokens	45.12%
Sign and verify header and/or paylaod message signatures	32.93%
Answer Choices	Responses

Figure 14 - What additional aspects of API Security have you applied? Multiple answers allowed.

Additional API Security Measures

Respondents reported a number of additional aspects of API security. 33% sign and verify header and/or payload signatures. 48% of shops with 50+ APIs use this practice. 45% of respondents (and 56% of those with 50+ APIs) inte-

grate OAuth with Active Directory/LDAP, OpenID Connector and JSON Web tokens. 20% of respondents (and 32% of those with 50+ APIs) filter API message content that is written to the audit log, and/or encrypt messages before writing to the log.

Conclusion

API security, like APIs themselves, is still early in the industry adoption cycle. The survey's results bear this out, showing a wide range of responses to concerns about security and a diversity of security practices. For example, processes for checking if API consumers, such as mobile apps, are securely handling an organization's data, do not appear to be

in wide use. However, organizations with more APIs do seem to have more robust API security in effect. This makes sense. Regardless of organization size, a larger API portfolio appears to translate into more rigor and depth for API security. Organizations with fewer APIs may be earlier in the adoption cycle and have less mature approaches to API security.



API Management, API Security, and Cloud Integration, solutions helps businesses accelerate digital transformation by securely extending their reach across multiple channels mobile, cloud and Internet of Things. Akana enables enterprises to quickly deliver scalable applications, share data as APIs, connect and integrate applications, drive partner adoption, monetize their assets and provide intelligent insights into their business and operations. The world's largest companies including Bank of America, Pfizer, and Verizon use Akana to harness the power of their technology and transform their businesses. Akana is recognized as a leader in API Management by several analyst firms. For more information on Akana's API Platform, see http://www.akana.com. Akana was previously known as SOA Software.



