Oracle's Response to OCN's Questionnaire

This document provides answers to ONC's questionnaire.

Introduction

Generally speaking, there are two types of APIs:

- **Internal APIs**: APIs exposed by product vendors to allow customers to customize or extend the vendor's product and integrate the product with third-party applications. This type of APIs is used by the vendor's customers and also by third party vendors wanting to integrate their products with the API provider (e.g., Oracle).
- **External APIs**: Two sub-categories (1) APIs exposed by companies to allow other parties to leverage their services, e.g., FedEx, Walgreen, etc., and (2) APIs exposed by companies to allow other companies to integrate functionality without having to develop it themselves, e.g., Twilio or SendGrid.

Typically, APIs are made public in open source or vendor documentation. For example, Twilio exposes their API publicly (https://www.twilio.com/docs/api/rest/making-calls). By making APIs publicly available, enterprises can improve partner connectivity (mash-ups) and cloud integration.

Based on the above, Oracle only provides what is referred to as **internal APIs.** Oracle products expose APIs that allow our customers to integrate, customize, and extend our products. Oracle API documentation is publicly accessible.

In addition, Oracle also offers products designed to manage and secure APIs. These products are sold to customers (government, financial institutions, healthcare, manufacturing, pharmaceutical, etc.) seeking to improve API security and management in their companies.

Answers to Questionnaire

1. Does your organization use APIs for apps which are available internally or to third parties?
[Marc Chanliau] Yes.
If so:
a. Do you publish your documentation online or make it available to third party

developers?
[Marc Chanliau] Oracle APIs are available to third-party developers wishing to customize, extend, or integrate Oracle products.
i. How do you determine who can get access to your API?
[Marc Chanliau] Because Oracle APIs are public, anybody can access them.
ii. Do they need to be “certified” for privacy or security standards by your organization to use?
[Marc Chanliau] Oracle APIs come with Oracle products.
b. Are there terms of use that include specific language for privacy and security?
[Marc Chanliau] Oracle APIs are subjected to the same intellectual property laws as Oracle products since these APIs are designed by and are the property of Oracle.
2. Are there production deployments of these APIs / third party applications using APIs?
[Marc Chanliau] Because Oracle APIs are used for Oracle products, Oracle APIs are deployed in production.
3. Are there any well-known threats or vulnerabilities associated with APIs themselves that should be addressed (e.g., security engineering considerations / best practices)?
[Marc Chanliau] Oracle APIs are subjected to the same Oracle Coding Practices that Oracle applies to all of its products.
a. As APIs are gaining adoption, are there steps organizations need to take to mitigate any additional threat vectors to data?
[Marc Chanliau] As mentioned previously, Oracle APIs are subjected to the same Oracle Coding Practices that Oracle applies to all its products.
b. Are these just specific to APIs in general? What might be unique / specific to healthcare?
[Marc Chanliau] N/A
c. How does the issuer of the API ensure that the API won’t become a tool used for malicious activitiy which could compromise the data source?
[Marc Chanliau] As mentioned previously, Oracle APIs are subjected to the same Oracle Coding Practices that Oracle applies to all its products.
4. How are APIs distributed in a way that the recipient / end-user of the API can trust the API is authentic?
[Marc Chanliau] Oracle APIs are part of Oracle products.
5. How to improve consumer experience with the third party apps using the APIs:
a. User stories / use cases
[Marc Chanliau] N/A
6. Is there a catalogue or store of tools that are built for the APIs for third parties to access?
[Marc Chanliau] N/A. However, Oracle does provide an API Management product for its customers, but this is not related to Oracle products’ APIs. (see http://www.oracle.com/technetwork/middleware/api-manager/overview/index.html**)**

Marc Chanliau’s Bio

Marc Chanliau has been in the software industry for over 40 years. Chanliau first started as a developer (Assembly language and C in those days), and then managed teams of developers distributed across multiple countries. Over the past fifteen years, Chanliau has been substantially involved in industry standards and protocols for Java security and XML security. In particular, Chanliau was one of the original designers of the Security Assertion Markup Language (SAML) and a key contributor to the WS-Security and WS-Policy standards. Chanliau has been with Oracle for over 10 years and is currently an Oracle Consulting Solutions Director focusing on security and identity and access control products. Chanliau is a frequent speaker at international conferences on identity management and web security, he is also a regular contributor to technical magazines / blogs covering web security in the enterprise and in the Cloud. Chanliau has a post-graduate degree in computational linguistics from the University of Paris (Pierre et Marie Curie).