Application Programming Interface (API) Security

Relying on Application Programming Interfaces (APIs) is a given in any industry, but especially in finance, where APIs are connecting fintech to financial institutions (FIs) and their customers.

The FFIEC's FIL-55-2021 issued guidance for effective and secure APIs, and Deer Brook has organized this primer of points that FIs should consider for themselves and expect from their vendors.

The Threats

As more data breaches occur and make the headlines of cybersecurity news, APIs are being identified as root causes of the breaches; after all, APIs are the vector to protected data.

API data breaches have been devastating, with these five organizations all having been attacked between 2017 and 2019:

- Equifax (56% of Americans' SSNs, credit card numbers, driver licenses, names, and birthdates breached) [1]
- Capital One (100 million credit card applications breached) [2]
- Facebook (267+ million IDs, phone numbers, and names breached) [3]
- USPS (60 million accounts breached) [4]
- Venmo (200 million transactions breached) [5]

High velocity transactions can mask abnormal activity, meaning that API attacks can take anywhere from a few months to a few years to detect.

Financial institutions who develop in-house APIs need to provide a multilayered security architecture to protect data. FIs also need to verify that their fintech vendors so the same.

How do APIs work?

APIs are programs that link user requests for data to backend applications and databases.

API data can be stored completely within a protected network and service specific in-house needs, but API data is more commonly stored at the network's perimeters, providing access to external users.

Here are some real-world examples of APIs at work:

- An API is what allows an Uber driver to punch in a street address in their app, and have directions appear via a separate mapping application, powered by Google Maps.
- An API is also in place so a Venmo user can use their mobile device to send funds to the Uber driver's account.

As with any application that accepts input, hackers craft attacks to subvert the purpose of the API. Very often, APIs have been subverted to provide unauthorized access to protected data.

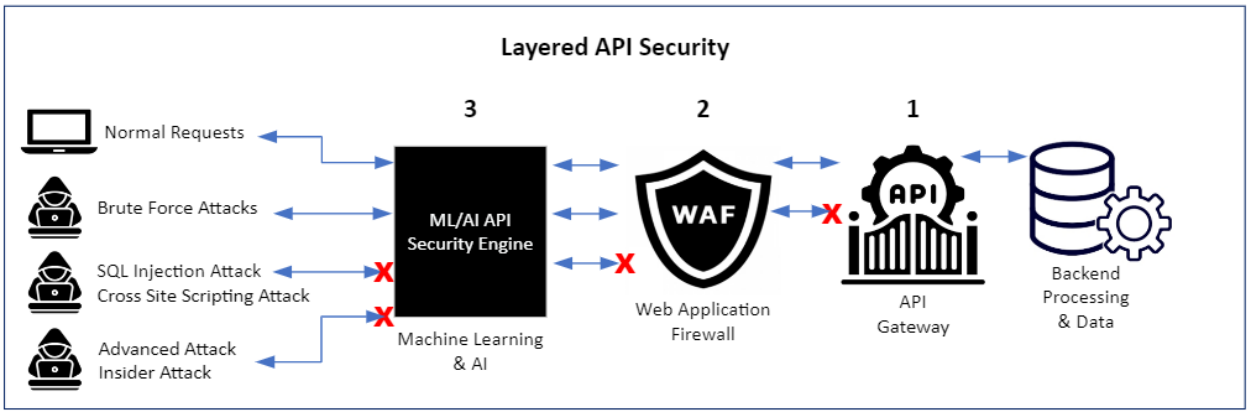
Common Attacks

Although the OWASP Top 10, a reputable security awareness document, identifies known attacks that API gateways and web application firewalls can prevent [6], there is a rise in sophisticated attacks that are quickly becoming the norm. These attacks can evade traditional API gateway and Web Application Firewalls (WAF).

Hackers are increasingly launching advanced attacks using machine learning (ML) and artificial intelligence (AI), while insider threats increase alongside them.

How to Protect APIs:

1. Assign an owner to manage your APIs. You can't protect your APIs or verify vendors' API security without first identifying them and assigning ownership to a central person or team who are accountable for them.
2. Inventory and catalog the APIs that have access to your data; both your APIs and vendor APIs.
3. Add API security to your information security policy (ISP) or program. Be consistent in its development and track the inevitable changes that happen.
4. If you develop APIs, ensure you have a comprehensive system development life cycle (SDLC). Train your developers, Information Technology (IT) staff, and Information Security (IS) staff on their responsibilities.
5. When vulnerability scanning, include APIs that you own or have permission to scan against. Use a scanner application that has API coverage.
6. Risk assess APIs, and track control exceptions or vulnerability scan results found on your APIs.
7. Implement a layered security architecture for your APIs. The following example shows three ideal lines of defense:



a. First line: Locate APIs behind an API gateway. This will protect against brute force attacks and other simple attacks.
b. Second line: Enable a WAF or Runtime Application Self-Protection (RASP) solution which can protect against attacks such as SQL injections and cross-site scripting attacks.
c. Third line: Leverage ML and AI to learn your normal transaction patterns, and to notify you of abnormal transactions. This can protect against wrongful transactions made with legitimate credentials, stolen tokens, insider threats, and other authenticated access from a bad actor.

8. Expect the same API management and security architecture from your vendors. SSAE SOC reports barely cover API security, if at all. Expect more due diligence in your vendors' reports. They might have the controls, but you own the risk.

Wrapping Up

Deer Brook provides API risk assessments and security consulting services that you can leverage for compliance requirements and, most of all, for peace of mind.

References

1. "You can now submit a claim for the $700 million Equifax…" CNBC. 25 July 2019
2. "A hacker gained access to 100 million Capital One credit…" CNN. 30 July 2019
3. "Facebook data breach sees millions of user…" TechRadar. 24 December 2019.
4. "USPS Security Flaw Exposes Personal Data of 60…" Fortune. 26 November 2018.
5. "I Scraped Millions of Venmo Payments. Your Data Is at…" Wired. 26 June 2019.
6. "Welcome to the OWASP Top 10 – 2021" OWASP. 2022.

Additional Sources

- Salt Security
- Traceable

deer-brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS