a window into cyber

August 2021

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

In a business awash with abbreviations and acronyms, a simple explanation is always welcome. This month, our guest author Freaky Clown deconstructs APIs (Application Programming Interfaces) for us. APIs have been around for a long time, but with the burgeoning popularity of mobile apps and more sophisticated web development technologies, there's a growing dependence on them for all kinds of data processing.

But the increasing prevalence of APIs is (unsurprisingly) accompanied by heightened risk, with hackers becoming adept at exploiting their weaknesses to access sensitive information. High profile victims include the interactive exercise equipment company Peloton, which made the news recently when its unsecured API exposed user account data, including private accounts.

The potential consequences of API security flaws can be costly: from a battered reputation and lost business to penalties and fines imposed by regulators. All the more reason to keep informed and up to date – and here at Brit, we're happy to help.

this month's author: **FreakyClown**

Co-CEO and Head of Ethical Hacking, Cygenta

*@_freakyclown_*

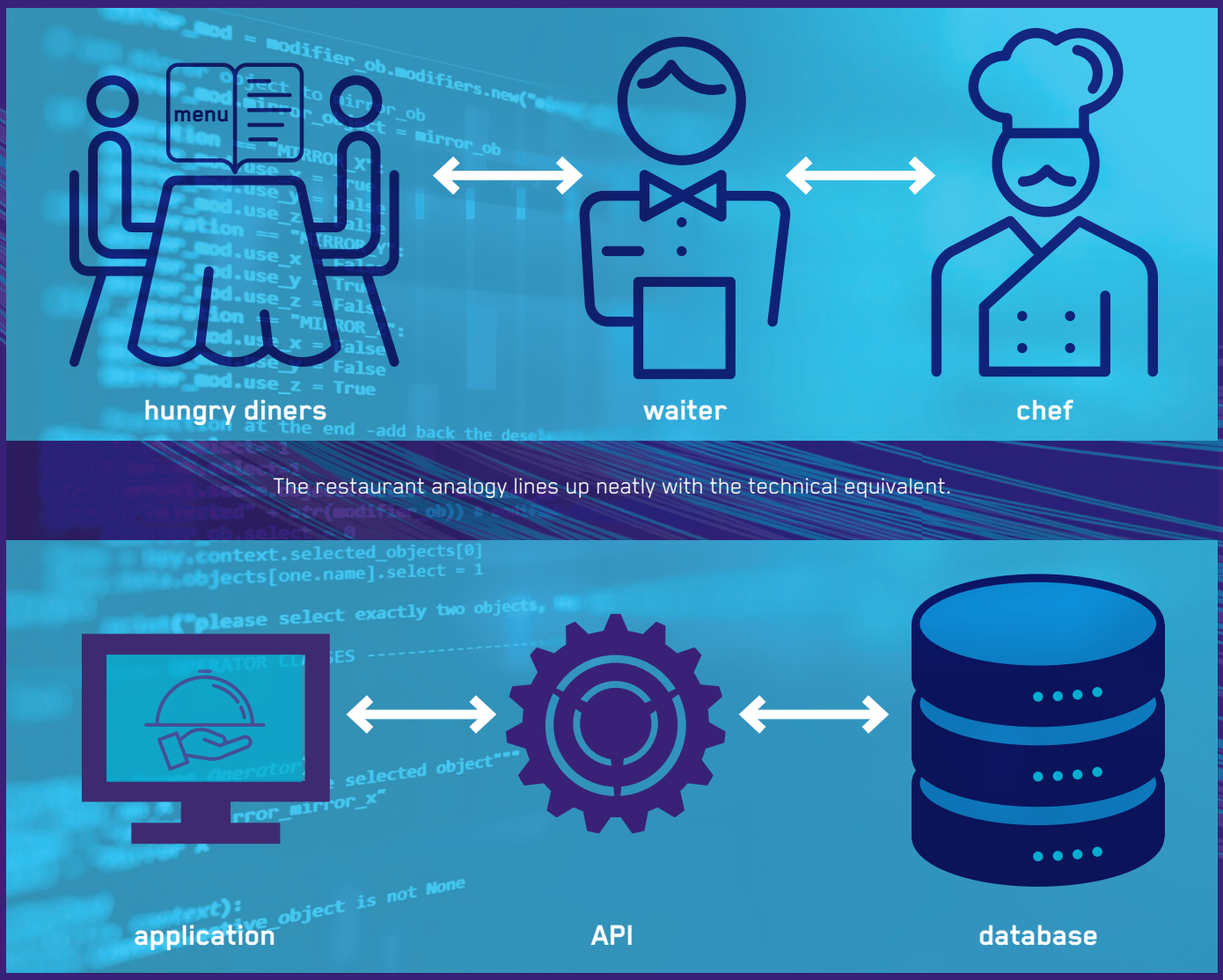
FC has worked in the Information Security field for over 20 years as an ethical hacker and social engineer. He performs valuable research into vulnerabilities, 'breaking into' hundreds of global banks, offices and government facilities to demonstrate weaknesses in physical, personnel and digital controls, and help organisations improve their security. As former Head of Cyber Research at Raytheon Missile Systems, FC has collaborated with intelligence agencies and assisted governments against national security threats.

Why APIs are the most important thing you've never heard of

APIs have been around since the 1940s, yet they only really became used as we know them in the 1960s. Unfortunately, they've taken a while to become recognised for the powerful tool they are.

So, what is an API? In technical terms, it's an Application Programming Interface: essentially a standardised method of communication between computer systems, or an intermediary between two applications.

A well-known example of how to understand how APIs work is the restaurant analogy. A restaurant (service provider) offers meals (services) and needs a way to tell their customers (end users) what they offer. Since they don't want to let the customer into the kitchen to see their secret recipes, they share their services with a menu (documentation). The customer (API client) selects from the menu and tells the waiter (API call), who relays the order to the chef (API server) and returns with the meal (API response) – all without the customer entering the kitchen.



The restaurant analogy lines up neatly with the technical equivalent.

continued on next page

The actual technology used to serve and respond doesn't matter: it's the standardised method that's important. Just as Morse code can be sent via light or sound, it's the code itself that's important, not the method of sending and receiving.

Another huge benefit of APIs is that they strip away everything that's not really needed. For example, take a website that allows you to search for a recipe. The page is made from HTML and other code; it contains forms, photos and maybe adverts. A single page might be around 2-3MB once you add in all the menus with JavaScript and CSS that make it look appealing on screen. An API version of the same site has none of these: the API call requests a recipe – and only the recipe is sent back; a fraction of the size and amounting to a few kilobytes.

The fact that APIs deal only in the data actually needed makes them sleek and fast. They also have another invaluable benefit: flexibility for the end user.

Take streaming media services such as Netflix, Amazon Prime or Disney+ as an example. They all offer the same type of data (movies and TV shows), searching and favourites lists, but they display the end results in different ways. What if you wanted to change the look and feel – and even the functions offered? If they provided direct access to their API, you could build any front-end system you wish. APIs simply provide the data; what you do with it is up to you – and no one is forced to use it in a specific way. Allowing end users to do what they want creates innovation opportunities.

continued on next page

But what about the security considerations when building your own API? We've seen data breaches in the past due to lack of API security from companies such as Facebook, Google, Venmo, T-Mobile and even the US postal service.

Most attacks against APIs are not the standard ones prevalent in web applications. They're mostly business logic flaws or access control failures. Automated tools tend not to pick up on these, hence professional testing should be sought.

The first step in helping secure an API endpoint is to require an API key. This is essentially a unique code given to the end application builder, which is checked by the API before processing the call. It's also important to document all endpoint functions – but not as important as checking what the function returns. In the Facebook data breach, the API returned private data that exposed millions of users for over 20 months before it was fixed. Google's API breach resulted in a shutdown of Google+; T-mobile users were victims of SIM-swapping.

So whilst APIs are extremely powerful, just like any other technology they require vigilance and security, since a data exposure can be catastrophic.

news from Datasafe

Datasafe delivers the latest risk management resources so clients can proactively manage their data protection and privacy risk.

Test your backups – now!

Backups are a good ransomware prevention strategy. But to be effective, they must be tested regularly to ensure successful and timely restoration in the event of an attack.

Check out Datasafe's tips on best backup practice, click here

Scammers target ransomware victims' customers

Cybercriminals are upping their game – again. This time by specifically targeting cyberattack victims' customers. Criminals are now using alleged specialised knowledge of a data breach to establish their credibility and effect a scam.

If you've been notified by a business partner or other entity that your information may have been compromised in a data breach, stay on high alert for scammers attempting to use the information against you. ALWAYS verify the caller or email using known contact information before responding in any way. And never give up sensitive information (such as login and passwords) without first verifying the communication with known contact information.