eclypses

WHITE PAPER

DevSecOps and Eclypses MTE® Technology

Why application-level security tools are essential to the modern development lifecycle

www.eclypses.com
Document ID: ECLYPSES - 1532395320-274
Version #: 2.0

Contents

Introduction

In the past, the roles of development, operations, and security were isolated to a specific team during various stages of engineering lifecycles. While this made sense when development cycles lasted months or even years, modern organizations began to see the need for rapid and agile engineering projects and DevOps was born. By automating deployment and testing, code could be delivered more efficiently and consistently. As often happens, application security remained a final stage process until organizations began shifting security toward developers and DevSecOps was coined.

DevSecOps stands for development, security, and operations. It blends process, culture, and tooling to integrate security as the responsibility of all members in the IT (Information Technology) lifecycle. To narrow it down to the biggest differences:

- It puts security first by introducing it immediately in the software development lifecycle (SDLC) by the developers.
- DevSecOps is about built-in security, not “bolt-on security” that functions as a perimeter around apps and data.
- Everyone involved has an obligation to security in the DevOps continuous integration and continuous delivery (CI/CD) workflow.
- DevOps focuses on the speed of app delivery, while DevSecOps delivers secure apps as quickly as possible.

DevSecOps Today

Today, DevSecOps is used in organizations in every vertical from Government, Healthcare, Fintech, etc. However, according to an article published by DevOps.com, “while an impressive 90% of organizations are in some phase of the journey toward DevSecOps, only 30% are implementing DevSecOps while 24% are in the planning phase, 18% are designing and 18% are still refining their DevSecOps strategy”. Granted, this is still a relatively new practice and has yet to reach maturity in many organizations but is especially important considering the recent increase in zero-day attacks.

It can be daunting to change an existing workflow. Teams need to be reorganized, retrained, or sometimes removed. Change is often resisted. Yet, the idea of integrating security into every part of the SDLC from development to production without sacrificing speed is often a very appealing prospect. Moreover, it’s an ideology with few downsides.

There are companies offering DevSecOps services from Zero-Trust Architectures built in the cloud to Integrated Development Environments (IDE). NIST has published guidelines on DevSecOps related strategies.

Securing Applications with Better Tools

"Bolt-on" application security can be a tough habit to break and has long been relied on to keep an application secure. The most ubiquitous example of this is Transport Layer Security (TLS) and its predecessor SSL. Application data is placed and secured by technology that is outside the application. Like the way application security has been "shifting left" from IT (Information Technology) to developers, it may be time to shift application security from the perimeter to the application.

Eclypses MTE (Microtoken Exchange) technology is a data security solution supplying application-level security through our MTE toolkits that are FIPS 140-3 verified. The cryptographic library and collection of patented solutions give developers many ways to add security without sacrificing speed and efficiency.

What MTE Does for Application Security

1. Encryption key management

Encryption of data-at-rest and in-transit is essential to any organization. Similarly, key management is among the most difficult processes to get right today. The options range from expensive key vaults to simple environment variables, but the problem remains the same – the key must exist somewhere.

Eclypses MKE (Managed Key Encryption) is a simple, patented process to programmatically Encrypt data by generating an Encryption Key that is:

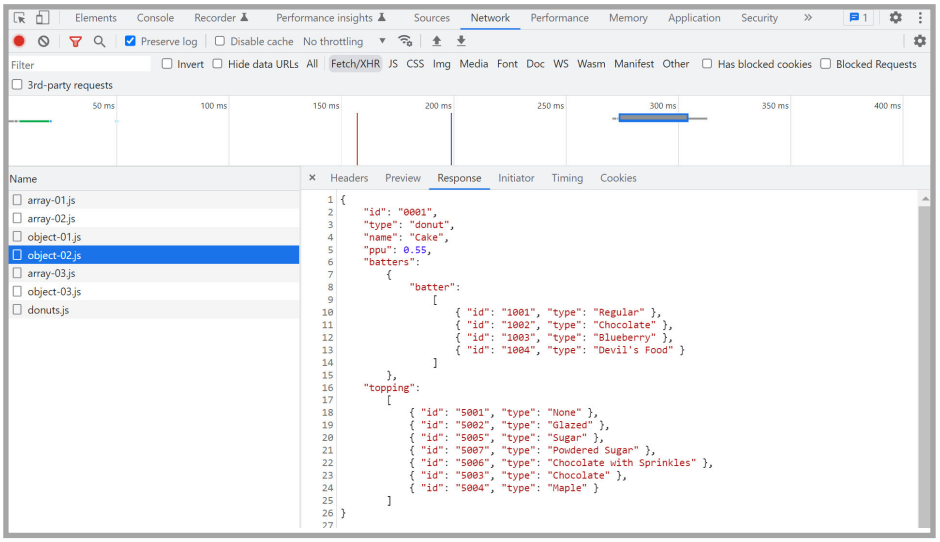
- Instantly obsolete (one-time use)
- Unique for every single transmission
- Never stored
- The data is randomized beforehand to be resistant to brute force

2. Payload inspection

One of the most common mistakes made by developers is exposing too much data (or the wrong data) in the responses from their RESTful API's. For example, in late 2021 a Missouri state website revealed teachers Social Security numbers when inspecting the data returned from a simple HTTP

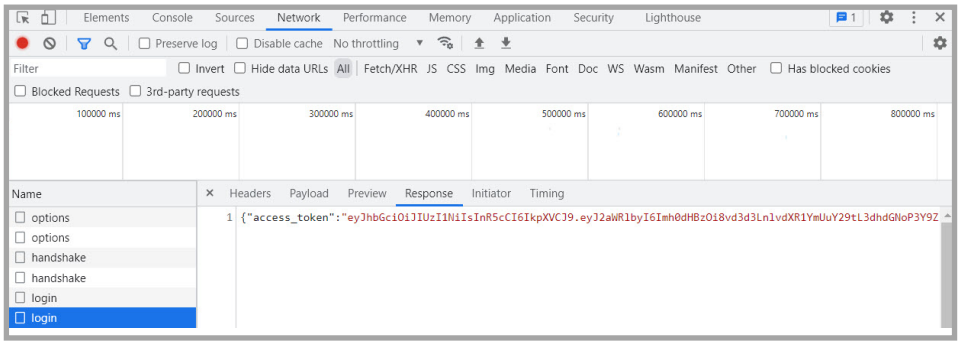
endpoint. This site was secured with HTTPS, but the unencrypted data can be reviewed in plain text by any modern browser's developer tools.

Often, data protected by HIPAA or GDPR (General Data Protection Regulation) can be found in otherwise unrelated requests and in a simpler example, integer-based identifiers can be exposed, and bad actors can attempt to request other users' data by incrementing them.



Example: serialized sample data returned in the response as integers

Eclypses MTE, because it is application-level, will render all serialized payloads completely unreadable without removing/ replacing any other security like TLS.



Example: MTE Encoded payload. Will not expose data that may be accidentally included.

3. Automatic testing of endpoints

Unit Testing and external endpoint penetration testing are essential to the DevSecOps process, but they can be very inefficient and often miss obvious vulnerabilities. The endpoints themselves are public and, while usually protected by authorization tokens, are susceptible to HTTP requests to retrieve sensitive data.

An API endpoint expecting only Eclypses MTE encoded payloads prevents anonymous or generically automated requests from bots and ensures the client is uniquely verified to be sending and requesting information.

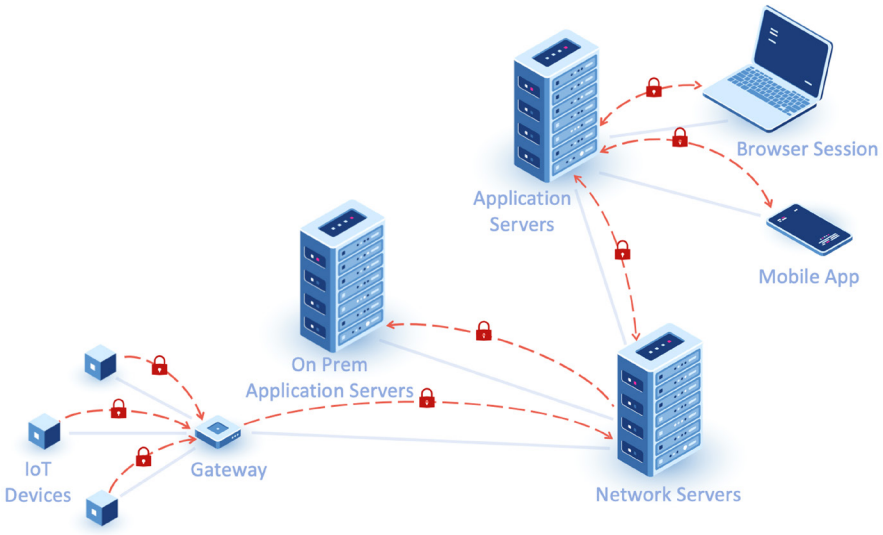
4. Quantum Resistance

The rise in Quantum computing presents many challenges to the future of public-key encryption. Most experts believe it is not if, but when. The trouble with this mentality is that some might still see this as a future issue. At Eclypses, if data can be broken in the future, it is already too late!

Eclypses MTE is a future-resistant technology that exists today. MTE is not based on traditional encryption but on patented randomization and replacement of data. Data protected with MTE today will be protected from threats in a post-quantum future.

Securing Services and Pipelines

Eclypses MTE is an application-level toolkit but has many additional uses in the DevSecOps pipeline. In cloud environments, it is recommended to encrypt data between apps and services. A container orchestration platform with integrated security features helps minimize the chance of man-in-the-middle or unauthorized access.



The engineering team at Eclypses has incorporated Eclypses MTE into nearly every aspect of our IT environment, from IoT devices, mobile applications, and VPN services. The Eclypses MTE has been validated by Penumbra, a third-party testing organization to be cryptographically secure in over fifteen different operating systems.

Conclusion

Due to the exponential growth of data and the increase in cyber-attacks, a DevSecOps approach must look towards the future and create a robust data security strategy. By giving Eclypses MTE, a strong data security solution, to the Developers, you will be able to provide a far more proactive and successful security posture today and in the future. As the responsibility for application development moves toward the developer, application-level security tools should move to the application. Eclypses MTE is the ideal “built-in” security for modern DevSecOps ideology.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies, websites, and IoT devices. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

This technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT

contact@eclypses.com
www.eclypses.com
(719) 323-6680