Project number

TG4

Project title

Intelligent Web Application Firewall using Token Inspection

Study leader

Mr Tinus Green

Study leader's research group

Intelligent Systems Group

Project concept note

Next generation firewalls, also called Web Application Firewalls (WAFs), have significantly improved the defence capabilities of organisations against common web application attacks. These devices perform deep-packet inspection of traffic to detect and alert on anomalies in the HTTP requests and responses. Although these devices can detect common attacks such as Cross Site Scripting and SQL injection, they still lack the intelligence required to detect attacks masquerading as normal behaviour such as business logic flaws or authorisation bypasses.

However, with the latest move towards decentralised authentication mechanisms, such as Json Web Tokens (JWTs), which contain information such as user claims, it may be possible to incorporate this information in order to detect more complex attacks.

The project student is expected to deliver a standalone device that can leverage existing detection techniques and new information that can be found in the claims of tokens in order to detect more complex attacks such as authorisation bypasses. Using machine learning techniques that incorporate this new information, the student should develop a system that can better learn normal behaviour to detect and alert on complex anomalies.

Nature of the work

A standalone device that can act as a WAF and detect more complex attacker techniques such as authorisation bypasses will be implemented.

New knowledge and skills that have to be mastered by the student

- Web Application Firewalls
- Heuristic based anomaly detection
- Token-based access control

Recommended reading

[1] Next Generation Firewall for Network Security: A Survey – Kishan Neupane et Al
[2] Critical analysis on web application firewall solutions – Abdul Razzaq et Al