ESTCube-2 - Security for Mission Control

Development proposal for a 4-person team.

ESTCube-2 is an in-development Estonian student satellite with educational and scientific missions. We operate on a microservices-based architecture across multiple servers in the University network. The current architecture is running on default settings and insecure. The development proposal is to secure the architecture and perform white hat penetration testing. This is a Dev-Ops oriented software project with a focus on eradicating anomalies and writing code where necessary to connect the applications. Example, implementing the login screen for the front-end.

What is the existing setup?

There are 4 servers (Development, Production, Continuous Integration, and Logging). Docker powers the applications and Jenkins for continuous integration. The applications lack authentication and authorisation. The SSL certificates are present on the machines but unused. There is a front-end built on React running on port 80/443 and other applications running on ports 8000-8500.

What needs to be done?.

- Write code and implement Google Single Sign-On for the front-end (React, Google Identity).
- Write code and implement RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) atop the OAuth2 framework (Google) for the front-end.
- Write code and transmit the audit logs to the existing log server.
- Write code and implement JWT to secure communication between the microservices.
- Implement Traefik as a HTTPS reverse proxy to secure all applications.
- Implement load balancing in Traefik/Docker swarm (up to you).
- Implement Docker secrets in the microservices to secure local credentials.
- Run application security test tools to analyse anomalies.
- Finally, perform white hat penetration testing.

Contact

Kristo Allaje  
kristo.allaje@estcube.eu

Umesh A Bhat  
umesh.bhat@estcube.eu