"Adaptive security for microservices applications over the cloud-edge continuum"

Ph.D. thesis proposal in the Cloud and Large-Scale Systems group (CLSC) @ UCLouvain.

Advisor: **Pr. Etienne Rivière**, UCLouvain

This Ph.D. thesis proposal is offered in the context of the CyberExcellence project.

The CyberExcellence project started in January 2022. Its goal is to position Wallonia as a major actor in cybersecurity, covering many aspects from research to applications, and involving all stakeholders (industry, academia, institutions, etc.). The project aims at producing excellent science and train top-level experts in the topics of cybersecurity broadly construed. Among the different research objectives of the project is the security of novel and complex cloud infrastructure such as multi-vendor clouds, distributed clouds, and hierarchical clouds. This Ph.D. proposal will participate towards this goal by improving the security and ease of use and operation of complex, emerging cloud infrastructures, and will contribute to prototypes and proof-of-concept implementations in modern distributed cloud software.

Context

Emerging collaborative applications such as smart cyber-physical environments, augmented reality, or virtual spaces typically rely on cloud infrastructures to host applications backends, store shared state, and implement the logic of interactions between users. These applications also typically handle and store sensitive information, and are often critical to businesses operation. It is of primary importance to shield them from cybersecurity threats.

Traditional cloud infrastructures formed of centralized data centers have enabled ease-of-programming, scalability, and cost-efficiency. They also allow a unified, centrally controlled and managed application of security measures, within a unified trust model, as all the infrastructure is typically under the responsibility of a single provider.

Unfortunately, centralized data centers are a poor fit for latency-sensitive applications due to the significant network latency between users and data centers. They are also ill-suited to respect data sovereignty requirements, where data must remain in a specific administrative region. An emerging model is the *edge-cloud* model where large data centers are complemented by smaller ones distributed over the globe and operating close to the users. In contrast with the centralized cloud, smaller data centers may be under the responsibility of different actors. They also cannot leverage high-performance and secured network links but must resort to the ordinary Internet.

Problem

The complexity of edge-cloud infrastructures makes the task of writing efficient application backends a tedious task for programmers. It also makes the development and application of security policies and mechanisms complex for programmers and very error-prone.

We propose to revisit the way security enforcement is performed for applications deployed over the cloud-edge continuum, with the goal of achieving a tradeoff between security, performance, and flexibility. Security concerns in modern cloud applications are handled by a service mesh, which deploys sidecar proxies together with the containers hosting the (micro)services of the application implementing the business logic. These proxies implement,

for instance, the encryption of requests between microservices or can enable specific traffic routing and control policies.

Approach

This Ph.D. thesis will consider the following research problems to enable a seamless integration of security concerns in edge-cloud scenarios:

- It will allow transparent encryption of inter-microservices data in future edge-cloud service meshes, allowing to dynamically update the placement of services and data without impairing security properties;
- It will consider the automated addition of privacy-enhancing features to applications, such as the enforcement of pseudonymization or anonymization to the requests made between services, e.g., disallowing that a specific request be linkable with certainty to a particular user or group of users;
- It will devise networking mechanisms allowing better robustness against passive and active attacks performed on the interconnect between services over the general internet, and propose new countermeasures.

The research will target modern cloud software stack and application design principles. It will target solutions that do not impose a high level of complexity onto programmers.

One of the enabling technologies that the research may consider are trusted execution environments in the cloud (i.e., Intel SGX) but also on edge devices (ARM TrustZone). The integration of SGX-supported services and their enablement in a service mesh such as istio will benefit from previous work on pluginizable Envoy proxies performed in the Cloud and Large-Scale Computing group @ UCLouvain.

Profile and skills

This thesis is particularly suited for a candidate with interests in Cloud Computing, Operating Systems Security, and Network Security. The research will focus on a *systems* approach, meaning that the conceptual contributions must be validated by the development and evaluation of proof-of-concept prototypes.

Proficiency with a low-level systems language such as C or Rust is required. The researcher should have a good command of GNU/Linux systems. Experience with distributed systems or cluster computing is a plus. The candidate must have followed graduate-level security courses and be familiar with cryptography and systems security concepts.

In addition to the technical skills, the candidate is expected to be able to work in collaboration with other junior and senior researchers active in fields such as software engineering, database engineering, networking, and security. A team player attitude is necessary. Doing a Ph.D. in computer science and particularly in computer systems is a very rewarding but also a very challenging experience due to the need to build prototypes and to run evaluation campaigns on real hardware. The candidate should, therefore, be ready to invest significant conceptual and technical effort towards the realization of the Ph.D.

English will be the primary working language (i.e., speaking French is not a requirement). A candidate willing to learn French will have access to training by the university.

Environment

The Ph.D. position is fully funded for a total of 4 years (salary and research expenses). The Ph.D. candidate will be hosted in UCLouvain's ICTEAM (Institute for Information and Communication Technologies, Electronics and Applied Mathematics). She or he will interact with other members of the groups of the two promoters (Cloud and Large-Scale computing and Performance of Networked Systems). This Ph.D. topic synergizes with ongoing activities in these groups around the automated adaptation and deployment of microservices applications in cloud-edge continuum infrastructures, and software engineering for such applications. She or he will also participate to the training and dissemination activities of the CyberExcellence project.

ICTEAM is a top-level research institute with excellent facilities. The candidate will have access to several distributed clusters with high-end, recent servers and edge resources to test the contributions. UCLouvain is Belgium's largest French-speaking university and is ranked in the first 100 institutions for computer science and information systems by the QS World University Ranking. The position is in Louvain-la-Neuve, a modern city 30 kms south of Brussels with excellent quality of life and connectivity to Belgium, Europe, and the world.

Application

Interested students should send an application file (PDF only, in English) with the following information to both of the co-promoters:

- An up-to-date CV;
- Link to a copy of the publication(s), if any, and to Masters' thesis;
- If applicable, a link to a GitHub (or similar) profile with examples of personal software contributions;
- Masters' degree transcripts;
- The name and emails of up to three reference persons able to provide an assessment of the application. Reference letters sent by the applicant her/himself will be ignored;
- A short cover email detailing your motivation for pursuing a Ph.D. and your interest in this specific topic.

Application deadline: ASAP -- applications will be screened as they arrive. Feel free to send a declaration of intent or request for clarification before sending a formal application.

Suggested starting date: September 1st, 2022 (flexible)

Contact: etienne.riviere@uclouvain.be