EPFL SSCC's First Online Workshop ETH zürich


**Date:** Wednesday May 26th, from 13:00 until 15:00 (CET), followed by an open discussion until 16:00 max.

**Place:** Zoom (ID will be sent by e-mail after **registration**).

**Registration:** Free, open to the public. Register **here**.

**Program:**

- Short welcome message and introduction by the Swiss Support Center for Cybersecurity.
- Keynote by **André Duvillard**, delegate of the Swiss Security Network, on "*The role of policy and decision makers in providing better software supply chain security*".
- "T*oo Quiet in the Library: How Native Libraries Endanger Android Apps*" by **Mathias Payer**, professor at EPFL.
- "*Cascading Failures*" by **Dieter Sommer**, enterprise security architect at Raiffeisen Schweiz.
- "*Dependency Management in a large IT ecosystem*" by **Michael Bem**, head of supply chain cyber & infosec at UBS Schweiz.
- "*How to become cyber resilient when you suppliers are not?*" by **Roger Wirth**, head of cyber security at SwissGrid.
- "*Trustworthy Components by Example of a Security Protocol*" by **Jorge Luis Toro Pozo**, researcher in the information security group at ETHZ.
- "*Overview of Supply Chain Security Regulations within the EU*" by **Nele Achten**, researcher at the Center for Security Studies (CSS) at ETHZ.

Presentations, of ~15min each, are expected to last until 15:00. For those whose schedule permits, the online meeting room will stay open until 16:00 for a public discussion.

We look forward to seeing you at the workshop!

The workshop is organized by the Swiss Support Center for Cybersecurity (SSCC), in collaboration with the Center for Digital Trust (C4DT) at EPFL and the Zurich Information Security Center (ZISC) at ETHZ.

## About SSCC

As part of the Swiss National Cyber Strategy 2018-22, the Swiss federal institutes of technology (EPFL and ETHZ) have committed to the creation of the Swiss Support Center for Cybersecurity (SSCC). The mission of the SSCC is to support governmental and industrial bodies, as well as the Swiss society, in the process of facing today's increasing and complex challenges in cybersecurity.

By organising workshops on cybersecurity related topics, our intention is to bring stakeholders from various sectors together (currently, in the same virtual meeting room) and to shed light on these challenges from different angles.

## About the Workshop Topic

We believe that the variety of dependencies in modern IT systems provides several advantages, but also has a strong impact on the security and resilience of these systems. A number of recent incidents, such as the "SolarWinds attack" on US governmental agencies, underline the difficulty of securing systems that are composed of various apparently independent components. There are various types of attacks that exploit weaknesses in the software supply chain, often referred to as "supply chain attacks". Additionally, a number of proofs of concept have shown the simplicity and the impact of attacks against individual links of the dependency chain.

How aware are organisations of their IT dependencies? How do they manage them? How are dependencies taken into account in the decision process? in a startup? in a big company? in a critical military IT system? The goal of this workshop is to gather experiences, and to present approaches that tackle these dependency issues, from theoretical and practical points of view.

## Dependency Examples

There are manifold ways how dependencies manifest in modern IT systems. As mentioned in the introduction, modern IT systems consist of a variety of building blocks from many different sources.

A rather recent form of dependency is based on cloud services, where applications rely on backend services that are hosted by cloud providers. For example, Twitter apparently uses Google cloud services, as well as Amazon Web Services. Looking at the endless customer lists of cloud providers, such as Amazon, Google, and Microsoft, shows how many of the well-known applications depend on one or the other cloud provider.

The outage of cloud service providers and the resulting outage of customers reveal the criticality and the dependencies of the cloud providers. An example of such an outage includes the outage of Google's cloud services in June 2019. It made consumer services unavailable, such as Gmail, YouTube, Snapchat, as well as some Apple iCloud services and a variety of smart devices, such as thermostats, cameras, and baby phones. A similar outage affected some Amazon Web Service customers in November 2020 blocking vacuum cleaners, doorbells, and thousands of services that rely on AWS around the world.

## Potential Workshop Attendees

IT / security architects, CISOs, security engineers/researchers, and enterprise architects, etc. from industry, government, critical infrastructure, armed forces, and academia.