微服务安全

微服务安全性可保护微服务架构中的每个小型自治单元。这种方法将大型软件程序划分为单独的较小服务，每个服务都运行在独立的进程中，服务之间通过轻量级的通信机制（如 HTTP API）进行通信。

正如视频所说，在朋友家的房子（整个架构），作为访问者，我们能够在一定时间内，可以访问客厅、厕所，但是不能访问朋友的主卧、孩子的房间。微服务安全就在其中发挥至关重要的作用。克里斯提安说，使用一个 Token，能够在酒店中自由出行指定房间、健身房，而无需重复验证，但又与员工的 Token 不同，其实在朋友房子也是一样的。

回到微服务安全。虽然微服务提高了软件的质量和灵活性，但也带来了新的风险。主要挑战包括潜在攻击点的增加以及跨不同服务管理各种安全协议的复杂性。有效的微服务安全性至关重要，因为任何单个服务中的漏洞都可能危及整个系统。

为了防止数据泄露、维护声誉和保护系统完整性，克里斯提安提过几个方法，这里结合网络资源，简单说说我的理解。

既然微服务在服务之间的通信中高度依赖 API，那么确保 API 的安全性对于防止未经授权访问、数据篡改或注入攻击至关重要。并且确保敏感数据在传输和存储时的安全性，比如不明文传输密码等。视频中也说过，使用不可修改的日志（Unmodified）实时监控服务活动，检测异常行为，并识别潜在的安全漏洞，以及 CIA Triad 的使用等等。

简而言之，新的技术应用，必然伴随新的问题出现。面对微服务带来的通信劫持等问题，本文进行了简单的说明。