Équipe Réseaux
Sujet Secured M2M

Sujet de TER
2018–2019

Communication *Machine to Machine* sécurisée appliquée aux workflows

Lieu	Équipe Réseaux, ICube (UMR CNRS 7357)
Encadrant	Andreas Guillot (andreas.guillot@unistra.fr)

Contexte

Les techniques de cryptographie actuelles permettent à plusieurs machines de communiquer de manière sécurisée en encryptant le trafic sur un réseau. L'omniprésence d'architectures largement distribuées comme les clouds ou les réseaux de capteurs apportent de nouveaux enjeux aux communications, comme par exemple l'authentification d'un grand nombre d'utilisateurs, ou la gestion de l'ordonnancement des différentes communications entre elles.

Les workflows représentent l'organisation de plusieurs tâches entre elles. Un exemple de workflow est représenté sur la figure 1, où plusieurs tâches (les noeuds) vont communiquer entre elles (les arêtes). Dans cet exemple, la tâche A va être exécutée sur une machine qui enverra les résultats de cette tâche à B et E, qui peuvent se situer sur d'autres réseaux. Le workflow se terminera lorsque H aura reçu les informations de F et G et qu'il aura complété sa tâche.

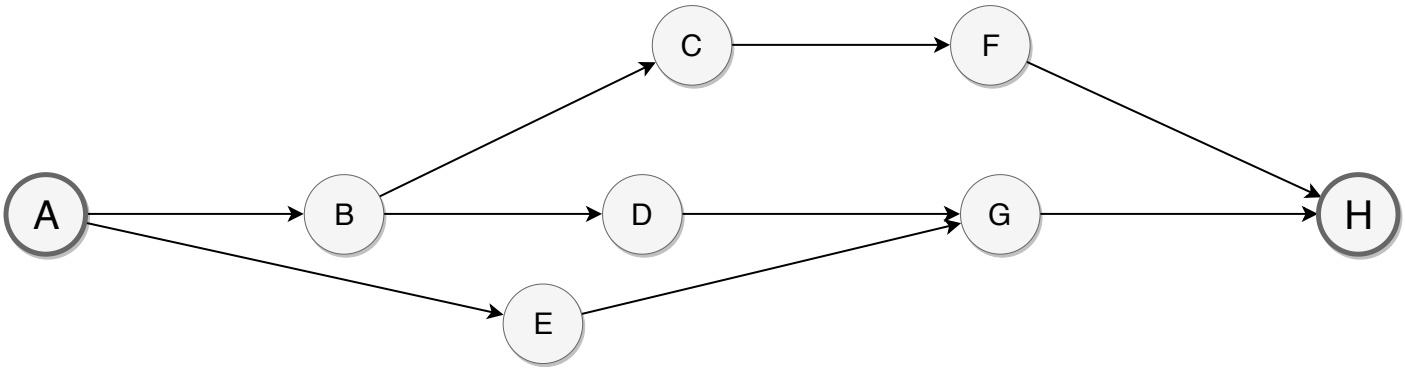

Figure 1 – Exemple de workflow contenant un ensemble de communications entre différents acteurs

Il est donc nécessaire de mettre en place une architecture qui va permettre à différents tâches d'un workflow d'échanger des informations entre elles de manière sécurisée tout en suivant les contraintes de communication qui seront décrites sur un schéma comme celui présenté sur la figure 1.

Sujet

Dans le cadre de ce TER, l'objectif principal sera de modéliser un système qui répondra aux besoins suivants : authentification sécurisée de plusieurs acteurs d'un même système, communication sécurisée entre plusieurs acteurs, et gestion de l'ordonnancement de plusieurs tâches entre elles.

La première partie du TER consistera à construire une bibliographie de textes scientifiques répondant aux besoins énoncés précédemment. Pour l'authentification, l'étudiant pourra analyser des solutions comme Kerberos [1] et se questionner sur la pertinence d'utilisation d'une telle architecture pour répondre à ces besoins. Quant à la communication de plusieurs acteurs, il ou elle pourra regarder quelles solutions existent pour la communication dans des environnements type cloud [2] [3] [4].

Références

[1] B Clifford Neuman and Theodore Ts'o. Kerberos : An authentication service for computer networks. IEEE Communications magazine, 32(9) :33–38, 1994.

[2] Shiping Chen, Surya Nepal, and Ren Liu. Secure connectivity for intra-cloud and inter-cloud communication. In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on, pages 154–159. IEEE, 2011.

[3] Dan Harkins and Dave Carrel. The internet key exchange (ike). Technical report, 1998.

[4] Hitesh Ballani, Keon Jang, Thomas Karagiannis, Changhoon Kim, Dinan Gunawardena, and Greg O'Shea. Chatty tenants and the cloud network sharing problem. In Nsdi, volume 13, pages 171–184, 2013.