HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Bachelorarbeit 2018

XMPP-Grid Broker

Studenten: Fabian Hauser, Raphael Zimmermann

Betreuer: Prof. Dr. Andreas Steffen

Ausgabe: Montag, 19. Februar 2018

Abgabe: Freitag, 15. Juni 2018

Einführung

Die IETF Security Automation and Continuous Monitoring (SACM) Working Group verfolgt eine Publish-Subscribe Architektur [1] basierend auf dem XMPP Protokoll [2] mit dem potentiell Hunderte oder Tausende von Endpunkten (PCs oder IoT Geräte) in real-time Sicherheitsinformationen in einem XMPP-Grid publizieren können. Security Information und Event Management (SIEM) Systeme können sich dann als Subscriber gezielt auf gewisse Themen (realisiert als XMPP Nodes) abonnieren.

Ein Rapid-Prototype [3] eines XMPP-Grids basierend auf einem Openfire [4] XMPP Server und einem Python Broker Script wurde am IETF 100 Hackathon Singapur im November 2017 vordemonstriert.

Für die Administration des XMPP-Grids soll eine Broker Applikation mit einem grafischen Management Interface erstellt werden. Damit sollen Themen (XMPP-Nodes) erstellt und gelöscht, sowie Owner, Publisher oder Subscriber Rechte vergeben werden können. Es soll die Möglichkeit geschaffen werden, Themen hierarchisch zu Collections [8] zusammenzufassen. Ebenfalls sollen Management-Views über verfügbare Themen, persistierte Items, Subscriber und Publisher generiert werden können.

Aufgabenstellung

- Einarbeiten in den XMPP Grid Internet Draft [1], den XMPP Standard [2], sowie die XEP-0004 [5], XEP-0030 [6], XEP-0060 [7] und XEP-0248 [8] Extensions.
- Erfassen der Requirements für einen XMPP Grid Broker.
- Erarbeiten eines Architekturkonzepts für den XMPP Grid Broker, sowie Evaluation von geeigneten Technologien für die Implementation.
- Implementation, Test und Dokumentation

Links

[1] IETF I-D *draft-ietf-mile-xmpp-grid*
https://tools.ietf.org/html/draft-ietf-mile-xmpp-grid

[2] IETF RFC 6120 *Extensible Messaging and Presence Protocol (XMPP): Core*
https://tools.ietf.org/html/rfc6120

[3] IETF 100 Hackathon *XMPP-Grid Broker Prototype*
https://github.com/sacmwg/vulnerability-scenario/tree/master/ietf_hackathon/strongSwan

[4] Openfire Homepage
https://www.igniterealtime.org/projects/openfire/

[5] XEP-0004 *Data Forms*
https://xmpp.org/extensions/xep-0004.html

[6] XEP-0030 *Service Discovery*
https://xmpp.org/extensions/xep-0030.html

[7] XEP-0060 *Publish-Subscribe*
https://xmpp.org/extensions/xep-0060.html

[8] XEP-0248 *PubSub Collection Nodes*
https://xmpp.org/extensions/xep-0248.html

Rapperswil, 19. Februar 2018

Prof. Dr. Andreas Steffen