UNIVERSITÄT BONN

MISPbump

Simple and Secure Synchronization of MISP-Instances

1. MISP – Malware Information Sharing Platform

MISP is an Open Source Thread Intelligence Platform for sharing, saving and correlating of information on Indicators of Compromise, vulnerabilities and other IT-Security related issues. Companies can use MISP independently or in cooperation with other companies to detect and fight attacks and threats on their IT-infrastructures, companies or staff. Nontechnical as well as technical information (MISP-Events) like digital artifacts can be connected to other relevant MISP-Events automatically. Furthermore, there are various OSINT-Feeds integrated by default which enable a simple and swift correlation with their internally created MISP-Events [1]. To comply with privacy policies of different enterprises MISP implements a filtering logic that enables sharing of information solely with selected peers or trust-groups [2]. According to the authors of MISP, over 6.000 companies worldwide already utilize MISP. Reputable organizations like CIRCL, CSSA, NATO, and FIRST maintain sharing communities [3].

2. Synchronisation of MISP-Instances

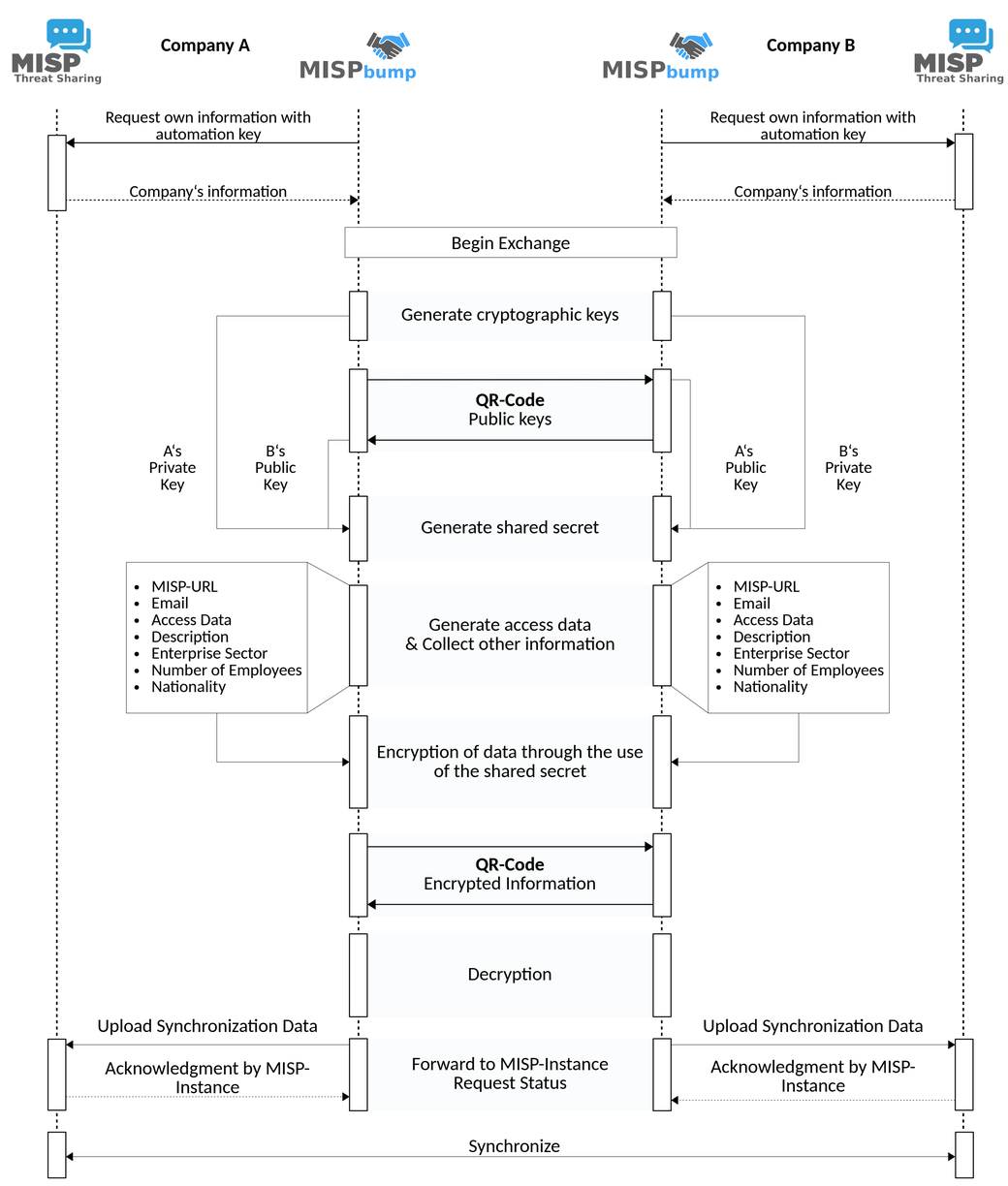
To enable sharing of MISP-Events between two companies these need to synchronize their respective MISP-Instances. The synchronization partners create a profile for the company they would like to share with on their own MISP-Instance. The required information need to be obtained and entered manually. These information range from shallow descriptions of the company to their enterprise sectors. The manual entry of these information might lead to incomplete or faulty profiles for their peers. Moreover, these potentially sensitive information might be in danger of being acquired by malicious third parties if an insecure medium is used for the information exchange. MISPbump has been developed to simplify and assist this process through a unified and secure method of synchronization.

3. What is MISPbump?

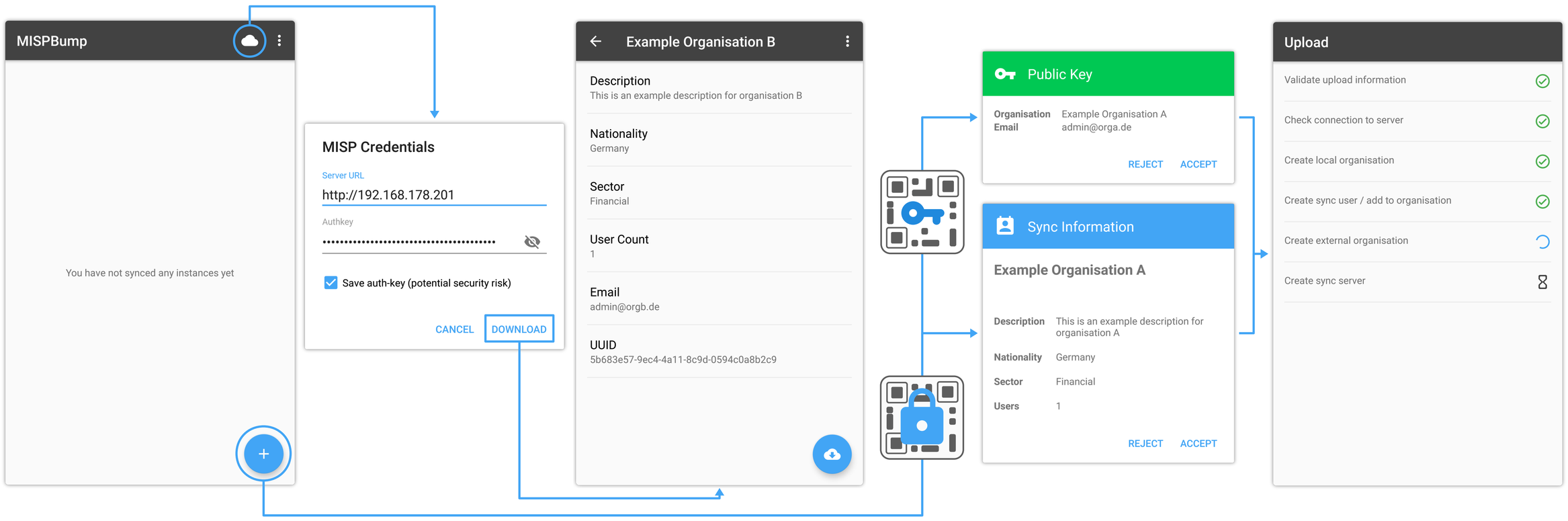
MISPbump is an Android App, that allows synchronization of MISP-Instances through the generation and exchange of encrypted QR-Codes. The necessary information for synchronization do not need to be entered or maintained manually but are loaded securely from the own MISP-Instance and are prepared for sharing with the respective peers. Only State-Of-The-Art technologies are used in MISPbump to ensure compliance with current security standards and those in the near future.

4. MISPbump Communication and Functionality

Below is a schematic depiction of the exchange protocol. Prior to the actual exchange, each MISPbump instance requests up-to-date information from the own MISP-Instance over a secure connection. The following protocol runs through three steps:
Key generation, exchanging public keys via QR-Codes that allow the exchange of encrypted synchronization data via a final QR-Code.



5. Screenshots



6. References

[1] MISP | Feeds (2019) https://misp-project.org/feeds
[2] MISP | Who (2019) https://misp-project.org/who
[3] MISP | Communities (2019) https://www.misp-project.org/communities/

Marc Ohm

itsec.cs.uni-bonn.de/overview/

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4

ohm@cs.uni-bonn.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung