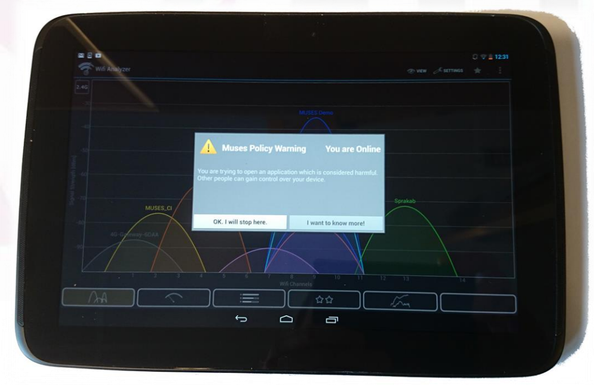
Multiplatform Usable Endpoint Security

Why

- Most Corporate security incidents are caused by organization insiders, either by their lack of knowledge or inadequate or malicious behavior.
- The Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) practice is becoming more common in all organizations.
- It poses new security threats and blurring the limits between corporate and personal use.

How

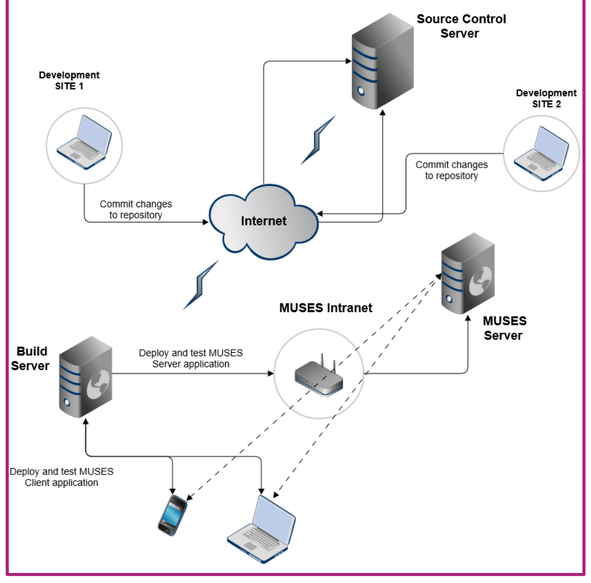
- MUSES will improve Corporate IP security by reducing the risks introduced by user behavior in BYOD/COPE scenarios.
- Raise the users' awareness of risky situations, assist them in dealing with those risks and actively enforcing security policies without introducing any hurdle in the human-computer interaction.
- MUSES will provide a device independent, user-centric and self-adaptive corporate security system



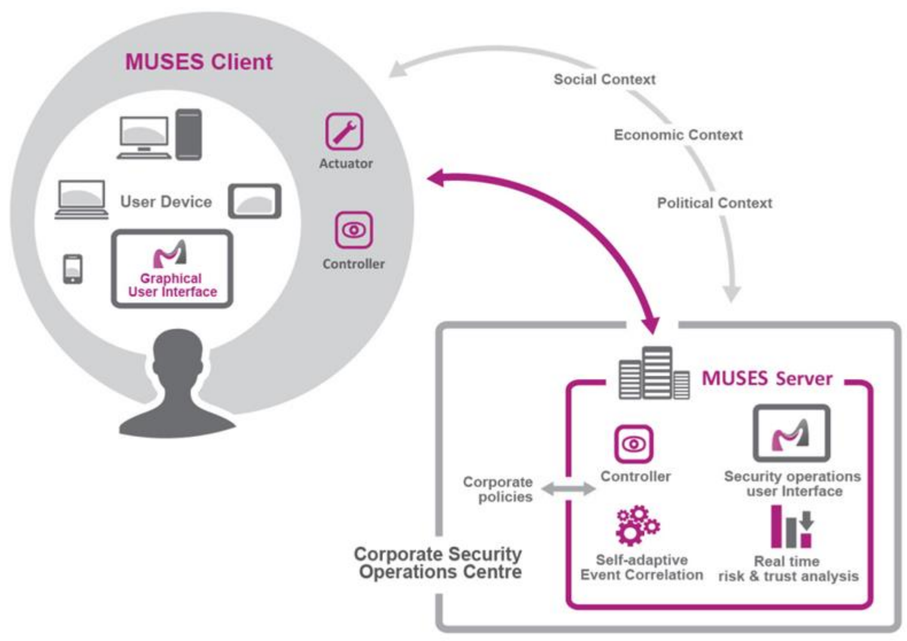
Continuous Integration

Daily system build, deploy and verification

- Code quality
- Unit tests
- System Test



MUSES Framework

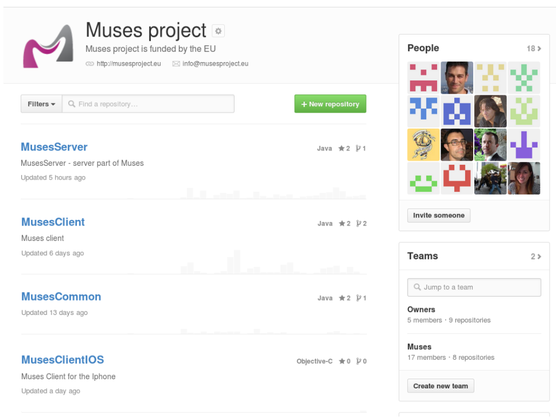


Open Source

Available on

https://github.com/MusesProject/

- Platform independent server
- Client for Android (Coming: iPhone and Windows)
- API for application integration

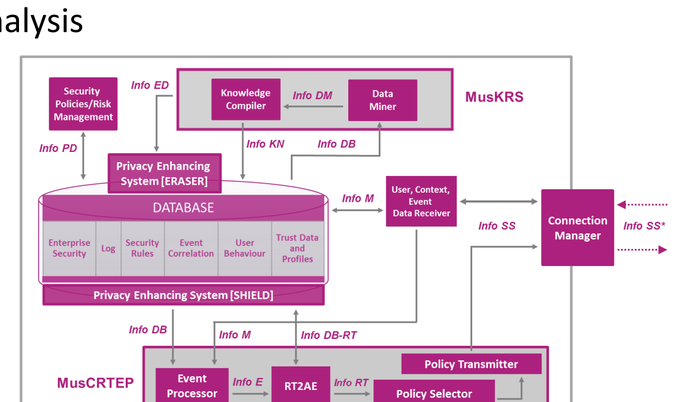


Design

Client-Server architecture with client-side proxies for situations where the device is working in offline mode. The client and server communicates using a secure transport layer with mutual authentication.

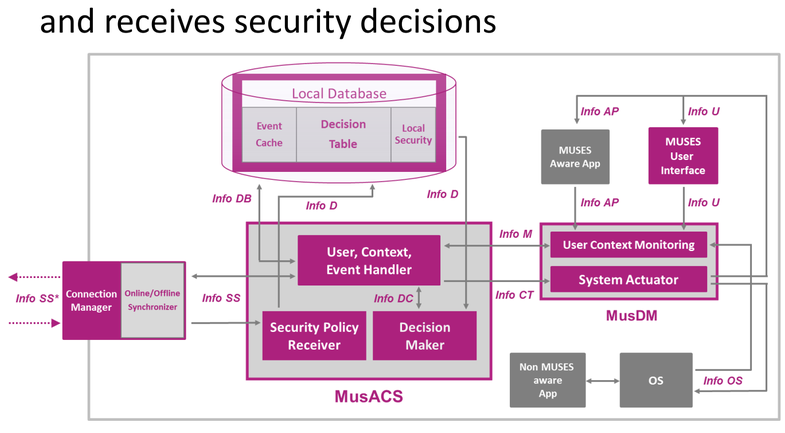
MUSES Server

- Corporate security policies
- Contains heavy-duty modules, like self-adaptive event correlation, context history, and real-time risk and trust analysis



MUSES Client

- Context sensors provide input for risks and trust analysis
- Actuators provides feedback and applies threat prevention
- Sends context information along with requests to the server and receives security decisions



SEVENTH FRAMEWORK PROGRAMME

www.musesproject.eu

Henrik Arfwedson, Markus Burvall, Yasir Ali
www.swedenconnectivity.com

- Project Number: 318508
- Project Acronym: MUSES
- Project title: Multiplatform Usable Endpoint Security
- Starting date: 01 October 2012
- Duration in months: 36
- FP7 Call: FP7-ICT-2011-8
- Funding scheme: Collaborative project-STREP